Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis

Christophe Ritzenthaler

UNIVERSITE PARIS 7 - DENIS DIDEROT
UFR de Mathématiques

Année : 2003 N° | | | | | | | | | | |

Thèse de Doctorat
Spécialité : Mathématiques
présentée et soutenue publiquement par
Christophe Ritzenthaler
le 25 juin 2003

Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis

---

Directeur
M. Jean-François Mestre

Rapporteurs
M. Henri Cohen
M. René Schoof

Jury
M. Henri Cohen
M. Jean-Marc Couveignes
M. Loïc Merel
M. Jean-François Mestre
M. François Morain
M. René Schoof

Remerciements

Cette partie, certainement la plus lue dans une thèse, est aussi la plus délicate à rédiger tant il est difficile de résumer en quelques mots les sentiments éprouvés pendant quatre ans ou plus. Qu'on m'en excuse par avance les oublis et maladresses. [1]

Tout d'abord, j'aimerais exprimer toute ma gratitude et mon admiration à mon directeur de thèse, Jean-François Mestre : la qualité de son enseignement, sa gentillesse et sa disponibilité ont été d'un apport inestimable dans l'élaboration de ce manuscrit ; l'originalité et la portée de ses travaux restent pour moi un modèle d'excellence.

Je souhaite remercier chaleureusement mes rapporteurs Henri Cohen et René Schoof pour l'attention qu'ils ont bien voulu porter à ma thèse ainsi que Jean-Marc Couveignes, Loïc Merel et François Morain qui me font l'honneur d'être membres de mon jury.

Plus généralement, c'est la communauté mathématique dans sa grande majorité que j'aimerais remercier pour m'avoir accepté (ainsi que mes idées et mes questions) sans préjugé et avec sympathie. En particulier, Robert Carls, Pierrick Gaudry, Marc Hindry, David Lehavi, Reynald Lercier, Joseph Oesterlé et Patrick Solé ont toute ma reconnaissance pour leur aide précieuse.

Il me faut aussi citer dans cette communauté l'ensemble des thésards de Chevaleret pour m'avoir fait partager leurs passions mathématiques ou autres. Un remerciement spécial à Esther dont les bonnes (et moins bonnes) humeurs ont égayé mes longs mois de rédaction.

En marge de cette communauté, mais indispensables, je voudrais remercier Mme Orion et Mme Wasse pour avoir balisé efficacement mon parcours administratif et Joël Marchand pour son aide informatique.

Il y a également tout ceux qui m'ont accompagné en dehors des mathématiques : ma famille bien sûr et en particulier mes parents. Cette thèse leur est dédiée avec toute mon affection. Mes amis également : je ne peux pas les citer tous mais j'ai une pensée particulière pour Anne, François, Eric et Jean parmi les «Lorrains» et pour Nico (pour m'avoir supporté pendant trois ans comme coloc, pour l'escalade, pour les questions d'info et le reste), Marie, Pôti, Alex, Croute, Manue et Pouss parmi les «Cachanais».

Et enfin, Laure, pour sa présence lumineuse à mes côtés.

[1] Voici une solution pour pallier partiellement à ce problème (ou pour personnaliser son exemplaire de thèse) : «je remercie également _____ de l'intérêt qu'il porte à mon travail».

Table des matières

Introduction

« Il faut beaucoup de connaissances pour faire de l'arithmétique... Si je vous dis 691*, vous pensez à quoi ? »*

Jean-Pierre Serre.

Le dénominateur commun des trois parties qui composent notre thèse est l'étude de courbes algébriques sur les corps finis. L'étude de leurs aspects géométriques et arithmétiques a été initiée par A. Weil au début du siècle dernier. Plus récemment d'autres points de vue sont venus enrichir le sujet : c'est le cas par exemple de l'analyse p-adique par l'intermédiaire des techniques de relèvements et de l'informatique (codes correcteurs d'erreurs et cryptographie) qui amène à prendre en compte les aspects effectifs.

Présentons maintenant les différentes parties.

Première partie

Ces travaux ont pour origine un article de A. Adler [Adl97]. Ce dernier y montre l'action d'un groupe sporadique, le groupe de Mathieu M_{11} d'ordre 7920, sur la courbe modulaire $X(11)$ en caractéristique 3. En caractéristique nulle, la modularité de $X(N)$, $N \geq 7$ premier, implique que son groupe d'automorphismes est exactement $L_2(N) := \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. Par réduction, $L_2(N) \subset \mathrm{Aut}(\overline{X(N)}_p)$ où on a noté $\overline{X(N)}_p$ la réduction modulo p du modèle de $X(N)$ sur $\mathbb{Z}[1/N]$ pour $p \neq N$. Dans le cas $N = 11$, la réduction modulo 3 fait donc surgir un groupe 60 fois plus grand. Un autre cas était déjà connu [Kur82], celui de $\overline{X(7)}_3$ qui correspond à la courbe de Klein $x^3y+y^3z+z^3x = 0$ (mais aussi à la courbe de Fermat $x^4+y^4+z^4 = 0$) et qui possède comme groupe d'automorphismes $\mathrm{PSU}(3, 3^2)$. Une question naturelle est alors de savoir si ces deux exemples s'inscrivent dans une famille plus vaste ou s'ils ne représentent que des coïncidences isolées. Dans un article — Manuscripta Math. **109** (2002) — nous avons montré les résultats suivants :

- Soit $p > 3$. Si la courbe $\overline{X(N)}_p$ est ordinaire alors son groupe d'automorphismes est $L_2(N)$.
- Si $p = 2$ (resp. $p = 3$) et si la courbe est ordinaire alors on montre que son groupe d'automorphismes est $L_2(N)$ sauf peut-être si $N-3$ (resp. $N-2$) est une puissance

de 4 (resp. 3) où il pourrait être un groupe simple dont on connaît l'ordre.
– Nous donnons également des critères restrictifs qui permettent de traiter des courbes au cas par cas. Nous montrons ainsi que en dehors de $p = 3$, le groupe des automorphismes de $\overline{X(11)}_p$ est toujours $L_2(11)$ et que $L_2(13)$ est le groupe des automorphismes de $\overline{X(13)}_p$ pour tout p.

Les arguments utilisés sont divers : des majorations de groupes d'automorphismes bien sûr mais aussi des propriétés plus arithmétiques liées aux formes modulaires afin de pouvoir calculer le p-rang des courbes $\overline{X(N)}_p$. Des lemmes relatifs aux équations diophantiennes et à la classification des groupes simples sont également démontrés.
Ainsi, il semble que les deux cas rencontrés soient des exceptions. Dans une communication privée, Robert Guralnick nous a par ailleurs affirmé qu'il a pu démontrer, par des méthodes semblables et dans un article en préparation, que seuls les deux cas évoqués voient leur groupe d'automorphismes augmenté.

Deuxième partie

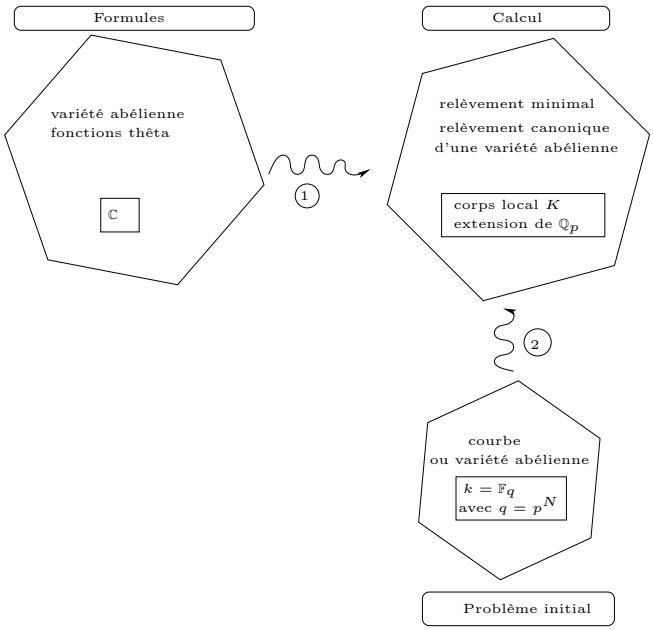
La motivation initiale de ce travail est la réponse à la question suivante : existe-t-il une courbe (lisse, projective) de genre 5 sur $\mathbb{F}_3$ avec 13 points rationnels ? Cette question s'inscrit dans la philosophie générale de recherche de courbes de genre fixé g sur un corps fini $\mathbb{F}_q$ possédant un nombre maximal de points rationnels, recherche utile aux codes correcteurs (du type Goppa). Dans le cas présent, i.e. $g = 5, q = 3$, on savait qu'il n'existe pas de telle courbe avec 14 points et on savait en construire avec 12 points. Nous présentons une courbe avec 13 points rationnels qui comble donc la lacune qui existait. Souvent ces courbes, courtisées pour leur propriétés arithmétiques, se trouvent de plus dotées d'une riche structure géométrique. Les imbrications entre ces deux aspects étant mal connues, l'explicitation de cas particuliers reste très importante. Dans cette optique, nous montrons que le groupe des automorphismes de notre courbe est constitué d'une unique involution, en utilisant des arguments de A. Beauville [Bea77] pour les intersections de quadriques. Nous montrons alors que la courbe est également revêtement non galoisien de trois courbes elliptiques. Un théorème de E.W. Howe et K. Lauter [HL02] permet de préciser le degré de ces revêtements. Nous donnons grâce à cela un algorithme permettant de trouver ces revêtements et nous l'appliquons à la détermination de deux d'entre eux.

Troisième partie

Après les groupes d'automorphismes, les courbes maximales, c'est ici un troisième aspect de la théorie des courbes sur un corps fini qui est abordé, nommément les méthodes de comptage de points rationnels sur de grandes extensions de $\mathbb{F}_p$. Le développement rapide de ce sujet est lié de très près à celui de la cryptographie qui utilise les jacobiennes des courbes de genre inférieur ou égal à 3 comme cryptosystèmes pour le logarithme discret. Avant 1985, on ne connaissait pas d'algorithme polynomial pour évaluer le cardinal de ces groupes. Le premier algorithme polynomial pour le cas elliptique a été proposé

par R. Schoof [Sch95] et consiste à regarder l'action du Frobenius sur des points de l-torsion pour diverses valeurs de l puis à recoller les informations par le théorème chinois. Mais ce n'est que récemment que le domaine a connu un nouvel essor sur les corps de petites caractéristiques, grâce à l'idée fondamentale de T. Satoh [Sat00] utilisant le relèvement canonique de la courbe sur un corps local. Cet algorithme donné initialement en caractéristique différente de 2 et 3 a ensuite été généralisé par M. Fouquet, P. Gaudry et R. Harley [FGH00] à ces deux derniers cas. L'idée de Satoh peut paraître paradoxale à priori : comment le passage d'un corps fini, où les calculs habituels (factorisation, etc.) sont réputés «faciles» à un corps infini permet-il de simplifier le problème ? L'énorme avantage de la caractéristique 0 est de permettre des arguments de nature plus analytique (convergence, action sur les différentielles, etc.). On aborde ainsi un paysage mathématique fait d'arithmétique, de géométrie et d'analyse que nous illustrons ainsi :

FIG. 1 – Le monde de l'A.G.M.



Sur cette base, et en utilisant la formidable «machine à produire des formules» qu'est la théorie des fonctions thêta, J.-F. Mestre [Mes00] a mis au point une variante particulièrement élégante et naturelle, appelée depuis par analogie avec le cas complexe, méthode A.G.M. (de l'acronyme Arithmetic Geometric Mean). Il en a ensuite proposé une généralisation aux cas hyperelliptiques de genre 2 et 3 (ordinaires). Ces améliorations ont permis, d'abord à P. Gaudry et R. Harley [GH00], puis à R. Lercier et D. Lubicz de calculer des polynômes caractéristiques sur F_{2^N}, les records actuels étant $N = 100002$ pour le genre 1 [LL02] et $N = 32770$ dans le cas du genre 2 [LL03] (rappelons que les tailles nécessaires à la cryptographie actuelle sont de l'ordre de $N = 100$).

Notre but est ici de donner une méthode basée sur des arguments similaires dans le cas du genre 3 ordinaire non hyperelliptique sur $\mathbb{F}_{2^N}$. A notre connaissance et bien que théoriquement des méthodes existent pour mener ce calcul efficacement (Lauder et Wan [Lau02]), aucune méthode n'a été implantée couvrant l'ensemble du cas de genre 3. La méthode générale que nous proposons ici a été implantée par l'auteur en MAGMA et a permis le calcul du polynôme caractéristique d'une courbe sur $\mathbb{F}_{2^{72}}$ en 25 heures. Des implantations utilisant des techniques de multiplication rapide sont en cours et devraient permettre de dépasser rapidement ce modeste record.

Comme nous allons le voir, ces travaux nous ont conduits à envisager divers aspects de l'algorithmique des courbes non hyperelliptiques que nous espérons bien entendu poursuivre, espérant développer des algorithmes aussi performants que dans le cas hyperelliptique.

Détaillons maintenant les différents chapitres qui constituent cette dernière partie.

Premier chapitre

Il contient essentiellement des rappels sur les variétés abéliennes sur $\mathbb{C}$ et la théorie des fonctions thêta ainsi que les liens avec les jacobiennes de courbes qui nous seront utiles dans les parties ultérieures. On y introduit également un certain nombre de formules (formule de duplication, de transformation, etc.) ; c'est la partie de gauche du dessin.

Deuxième chapitre

Ce chapitre constitue le «liant» théorique du dessin. Il nous a paru intéressant d'aborder en premier lieu le cas du genre 1 où les démonstrations sont «élémentaires» en montrant à la main comment les formules de géométrie complexe se transposent dans le mode 2-adique. De plus ce cas bien que maintenant classique, n'est en général que partiellement traité. Nous y avons de plus adjoint un autre point de vue (intersection de quadriques dans $\mathbb{P}^3$) qui éclaire plus naturellement les différents calculs et se généralise plus aisément en genre supérieur. Notons enfin que la pléthore d'informations disponibles dans ce cas permet d'espérer des améliorations notables en dimension supérieure ; nous y reviendrons en conclusion.
Nous abordons ensuite le cas général. On considère une variété abélienne ordinaire A sur $\mathbb{F}_{2^N}$ de dimension g. La théorie du relèvement canonique de Lubin, Serre et Tate [LST64] permet de lui associer une unique (à isomorphisme près) variété abélienne $\mathcal{A}_0 := A^{\uparrow}$ sur l'extension de degré N non ramifiée de $\mathbb{Q}_2$. La construction d'une tour de 2-isogénies relevant les actions du Frobenius par les formules de duplication, réalise alors un cycle de variétés abéliennes $(\mathcal{A}_i)$ telles que $\mathcal{A}_N$ est isomorphe à $\mathcal{A}_0$. L'action de cet isomorphisme sur les différentielles régulières s'exprime d'une part par le produit α des g racines du Frobenius unités 2-adiques et d'autre part (une fois la variété plongée dans $\mathbb{C}$) comme un rapport de carrés de thêta constantes au signe près. Un argument de convergence dû à

Robert Carls [Car02] montre alors que l'itération de ce processus sur un relèvement quelconque converge linéairement vers cette formule en 2-adique et permet d'entreprendre un processus itératif du calcul de α une fois connues les thêta constantes initiales.

Troisième chapitre

Le problème de la détermination de l'arithmétique de la variété abélienne (via un produit de racines de son polynôme caractéristique) passe donc par la détermination algébrique d'un rapport de thêta constantes. Sur notre dessin, il s'agit d'expliciter la flèche ①. Dans le cas hyperelliptique, le calcul de ce rapport est relié par la formule de Thomae à des invariants binaires (produit de différences d'abscisses de points de Weierstrass). Dans le cas du genre 3 non hyperelliptique, le calcul passe par la connaissance d'invariants ternaires : des produits de déterminants de bitangentes (Weber [Web76]). Les formules permettant de déterminer les 28 bitangentes à partir de 7 d'entre elles correctement choisies sont essentiellement dues à Riemann [Rie98]. Nous en donnons ici une formulation plus moderne, aussi bien du point de vue combinatoire que du point de vue géométrique par la considération de fibrés thêta caractéristiques. Nous la complétons en donnant une méthode simple pour déterminer les 7 bitangentes initiales lorsqu'une équation de la courbe est donnée sous la forme

$$C : \sqrt{x_1 u_1} + \sqrt{x_2 u_2} + \sqrt{x_3 u_3} = 0 \tag{1}$$

(que nous appelons modèle de Riemann), les u_i étant des formes linéaires en les x_i.
L'observation des bitangentes est également au coeur de la géométrie des quartiques sur $\overline{\mathbb{F}}_2$. Nous montrons que toute courbe ordinaire de genre 3 non hyperelliptique admet un modèle plan de la forme

$$\tilde{C} : Q^2 - xyz(x+y+z) = 0 \tag{2}$$

où Q est une conique vérifiant certaines conditions. Ce modèle est pour nous l'analogue de ceux bien connus dans les cas hyperelliptiques.

Quatrième chapitre

Maintenant que l'on possède une détermination algébrique des rapports de thêta constantes et une description des courbes qui nous intéressent sur $k = \mathbb{F}_{2^N}$, on s'attèle à la partie centrale du dessin afin de mettre au point un algorithme de calcul du polynôme caractéristique.
On montre tout d'abord comment relever le modèle plan (2) sur une extension de $\mathbb{Q}_2$ de telle manière que les calculs soient faciles à effectuer. Cela passe en particulier par la considération d'une version modifiée d'un revêtement du modèle de Riemann (1), en introduisant des termes *à la* Artin-Schreier. On montre alors que, sur ce modèle, les 28 bitangentes sont définies sur le corps de base et on identifie le noyau de la réduction. C'est la flèche ② dans notre dessin.
Ensuite, on montre comment récupérer, à partir de la seule connaissance du produit $\alpha = \pm\pi_1 \dots \pi_g$ des racines du Frobenius unités 2-adiques, le polynôme caractéristique au

signe près. En genres 1 et 2 ce nombre le détermine facilement. Pour $g = 3$ cela n'est plus le cas. J.-F. Mestre a alors proposé d'utiliser, en 2-adique, les méthodes de détermination du polynôme minimal d'un nombre algébrique à partir d'une approximation suffisante de celui-ci, basées sur l'algorithme LLL. Nous en proposons ici une version qui tient compte des spécificités du problème et permet une amélioration d'un facteur 2.
Enfin, pour lever l'ambiguïté sur le signe, nous proposons une méthode pour déterminer la réduction modulo 4 du polynôme caractéristique. Celle-ci s'appuie sur le calcul des points d'ordre 4 de la jacobienne au moyen de calculs dans le corps de fonctions.
Un résumé de l'algorithme ainsi qu'une illustration sur $\mathbb{F}_{2^{72}}$ complète le chapitre.

Cinquième chapitre

Ce dernier chapitre offre un point de vue totalement différent et constitue un travail mené parallèlement au précédent. Il s'appuie sur une construction géométrique de D. Lehavi [Leh02]. Ce dernier propose en effet une méthode permettant de construire à partir d'une courbe de genre 3 une autre courbe dont la jacobienne est $(2, 2, 2)$-isogène à celle de la première. Cela constitue donc une première étape vers une méthode géométrique A.G.M. Notre contribution est d'avoir permis l'identification de certains objets introduits à partir de constructions élémentaires (réseau de coniques, hessienne, cayleyenne, etc.) et d'avoir pu par ce biais réaliser une implémentation en MAGMA sur $\overline{\mathbb{Q}}$.

Première partie

Automorphismes

Chapitre 1

Automorphismes des courbes modulaires $X(N)$ en caractéristique p

1.1 Introduction

Il est bien connu que, si $q \geq 7$ est premier, les seuls automorphismes de la courbe modulaire $X(q)$ sont modulaires et forment un groupe isomorphe à $L(q) := \mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z})$ (cf. par exemple [Maz98]). D'après Igusa on sait également qu'une telle courbe admet un modèle sur $\mathrm{Spec}(\mathbb{Z}[1/q])$ qui a bonne réduction en tout p premier différent de q. Notons $\overline{X(q)}_p$ la courbe réduite modulo p pour p différent de q et $G_{q,p}$ le groupe des automorphismes de cette courbe ; $G_{q,p}$ contient bien sûr $L(q)$ et d'après Roquette , pour q donné, il n'existe qu'un nombre fini de p pour lesquels $G_{q,p}$ est distinct de $L(q)$. Par ailleurs Kuribayashi a prouvé que $G_{7,3}$ est isomorphe à $\mathrm{PSU}(3, 3^2)$ qui est d'ordre strictement plus grand que $L(7)$, et Adler et Rajan ont prouvé que $G_{11,3}$ est isomorphe au groupe de Mathieu M_{11}, lui aussi d'ordre strictement plus grand que $L(11)$.

Il est donc naturel de se demander si ce sont les seuls cas où $G_{q,p}$ est différent de $L(q)$. En particulier, se pourrait-il que $G_{q,3}$ soit toujours différent de $L(q)$, etc. ? Nous donnons dans cet article (cf. 1.4.3) le résultat partiel suivant :

Théorème 1.1
Soit p, q deux nombres premiers tels que $q \geq 7$ et $p \neq q$.

- *Soit $p > 3$. Si la courbe $\overline{X(q)}_p$ est ordinaire, $G_{q,p}$ est isomorphe à $L(q)$.*
- *Soit $p = 3$. Si la courbe $\overline{X(q)}_3$ est ordinaire, $G_{q,p}$ est isomorphe à $L(q)$ sauf peut-être si $q - 2$ est une puissance de 3 ($q - 2 = 3^\alpha$) où $G_{q,p}$ pourrait être un groupe simple tel que*
$$|G_{q,3}/L(q)| = \frac{(q-2)(q-3)}{6}.$$
- *Soit $p = 2$. Si la courbe $\overline{X(q)}_2$ est ordinaire, $G_{q,p}$ est isomorphe à $L(q)$ sauf peut-être si $q - 3$ est une puissance de 4 ($q - 3 = 4^\alpha$) avec $\alpha > 1$ où $G_{q,p}$ pourrait être*

un groupe simple tel que

$$|G_{q,2}/L(q)| = \frac{(q-3)(q-4)}{12}.$$

Rappelons qu'une courbe X sur un corps fini de caractéristique p est dite ordinaire si le p-rang de sa jacobienne, γ_X, est égal à sa dimension. Ce théorème résout en particulier la question dans les cas de $\overline{X(11)}_5$, $\overline{X(11)}_{23}$ et tous les $p < 50$ pour $\overline{X(13)}_p$ sauf $p = 7, 11$. Il permet également dans le cas $\overline{X(11)}_3$ de savoir que si un groupe d'ordre plus important agit, c'est forcément le groupe de Mathieu M_{11} (seul groupe simple d'ordre 7920).

La démonstration du théorème ci-dessus s'appuie sur les deux propositions suivantes (cf. 1.3.1 et 1.3.2) :

Proposition 1.2
Si $|G_{q,p}/L(q)| < q$ alors on a $G_{q,p} \simeq L(q)$. En particulier si $|G_{q,p}| \leq 84(g_X - 1)$ (avec g_X genre de $\overline{X(q)}_p$) alors $G_{q,p} \simeq L(q)$.

Proposition 1.3
Si $|G_{q,p}| > 84(g_X - 1)$ le revêtement $X = \overline{X(q)}_p \to Y = X/G_{q,p}$ est ramifié en exactement deux points de Y dont un seul est sauvagement ramifié.

Ces deux propositions, ainsi que des lemmes techniques sur les groupes de ramification supérieurs, nous permettent aussi de traiter plusieurs cas où $\overline{X(q)}_p$ n'est pas ordinaire et de montrer que $G_{11,p}$ est isomorphe à $L(11)$ pour $p \neq 3$ et que $G_{13,p}$ est toujours isomorphe à $L(13)$.

Remarque :
Le calcul du p-rang des courbes modulaires a ici un aspect effectif important. Nous montrons dans la section 1.4.2 comment déterminer celui-ci à à l'aide des polynômes de Hecke de T_p agissant sur les espaces de formes paraboliques de poids 2 des seules courbes $X_0(q), X_0(q^2)$ et $X_1(q)$. Grâce au logiciel MAGMA, nous avons pu calculer ainsi, par exemple, le 2-rang de la courbe $\overline{X(29)}_3$ (de genre 806) et constater qu'il s'agit bien d'une courbe ordinaire.

Voici le plan de l'article :
Dans la section 1.2 sont introduits des résultats concernant les courbes $X(q)$ et leur réduction ainsi que des rappels sur les groupes de ramification supérieurs et le théorème d'Hurwitz.
Dans la section 1.3 on démontre les propositions 1.2 et 1.3.
Dans la section 1.4 on introduit le p-rang, son calcul puis on démontre le théorème principal 1.1.
Enfin dans la section 1.5 on traite les cas particuliers $X(11)$ et $X(13)$.

1.2 Rappels sur les courbes modulaires et les revêtements

1.2.1 Les courbes modulaires $X(N)$

Soit N un entier supérieur ou égal à 3. Soit M_N le schéma modulaire pour les courbes elliptiques munies d'une structure de niveau N (i.e. pour une courbe elliptique E/S un isomorphisme de $(\mathbb{Z}/N\mathbb{Z} \times \mu_N)_S \to E[N]$ compatible avec les couplages) ; M_N existe et c'est une courbe affine au-dessus de $\mathrm{Spec}(\mathbb{Z}[1/N])$ (cf. Igusa [Igu59]). On peut compactifier ce schéma en un schéma M_N^* projectif lisse sur $\mathrm{Spec}(\mathbb{Z}[1/N])$ et $M_N^* \otimes \mathbb{C}$ est bien sûr isomorphe à la courbe modulaire de niveau N notée $X(N)$ sur $\mathbb{C}$. Soit p un nombre premier ne divisant pas N et $q_0 = p^f$ la plus petite puissance de p telle que $q_0 \simeq 1 \mod N$. Alors $M_N^* \otimes \mathbb{F}_p$ peut être considérée comme une courbe projective non-singulière sur $\mathbb{F}_{q_0}$. On note cette courbe $\overline{X(N)}_p$.

En fait Vélu ([Vel78], p.81) donne des équations à coefficients dans $\mathbb{Z}$ pour le schéma M_N^* sur $\mathrm{Spec}(\mathbb{Z}[1/N])$.

1.2.2 Rappels sur les revêtements galoisiens

Soit k un corps algébriquement clos de caractéristique $p > 0$. Une «courbe» sera toujours pour nous une courbe algébrique connexe, complète et non singulière sur k ; X étant une telle courbe, on note respectivement $\mathrm{g}_X, \mathrm{Aut}(X)$ son genre et son groupe d'automorphismes. Si G est un sous-groupe fini de $\mathrm{Aut}(X)$ (c'est toujours le cas si $g_X \geq 2$) et P un point de X on définit les groupes de ramification supérieure $G_i(P)$ $(i \geq 0)$ par

$$G_0(P) = \{\sigma \in G | \sigma \cdot P = P\}$$

et pour $i \geq 1$

$$G_i(P) = \{\sigma \in G_0(P) | ord_p(\sigma \cdot \pi_P - \pi_P) \geq i + 1\},$$

où π_P est une uniformisante en P et ord_p signifie «ordre au point P». Avant de rappeler quelques propriétés des $G_i(P)$ citons le théorème d'Hurwitz (voir par exemple [Sti73] pour une démonstration) :

Théorème 1.4
Soit $\pi_{X/Y} : X \to Y$ un revêtement de courbes, galoisien de degré n. Pour tout point $Q \in Y$ on définit e_Q (indice de ramification) et d_Q (exposant de la différente [Sti73]) de la manière suivante : si $G = Gal(X/Y)$ et $P \in X$ tel que $\pi_{X/Y}(P) = Q$ alors $e_Q = |G_0(P)|$ et $d_Q = \sum_0^\infty (|G_i(P)| - 1)$. Comme le revêtement est galoisien ceci est indépendant du choix de P. On a alors :

$$(2\mathrm{g}_X - 2)/n = 2\mathrm{g}_Y - 2 + \sum_{Q \in Y} \frac{d_Q}{e_Q}.$$

Les groupes $G_i(P)$ possèdent de plus les propriétés suivantes :

- $G_0(P) \supset G_1(P) \supset \ldots \supset G_m(P) \supsetneq G_{m+1}(P) = 1$, les $G_i(P)$ étant distingués dans $G_0(P)$.

– si $|G_0(P)| = Ep^\alpha$ avec $(E,p) = 1$ alors $|G_1(P)| = p^\alpha$, $G_0(P)/G_1(P)$ est un groupe cyclique d'ordre E.

Enfin en généralisant un résultat de Nakajima [Nak87, prop. 1], on a le lemme suivant :

Lemme 1.5
Si on pose $E = |G_0(P)/G_1(P)|$ et $q_i = |G_i(P)/G_{i+1}(P)|$ $(i \geq 1)$ alors $E \mid (E,i)(q_i - 1)$. En particulier $E \mid i(q_i - 1)$.

Démonstration :
D'après Serre [Ser68, prop. 9 p. 77] il existe des morphismes injectifs $\vartheta_0 : G_0(P)/G_1(P) \to k^*$ et $\vartheta_i : G_i(P)/G_{i+1}(P) \to k$ $(i \geq 1)$. Notons $\mu_E = Im(\vartheta_0)$ le groupe des racines E-ième de 1 et $\zeta = \vartheta_0(\overline{s_0})$ $(s_0 \in G_0(P))$ un générateur de ce groupe cyclique.
On sait qu'on a de plus la relation $\forall s \in G_0(P)$ et $\tau \in G_i(P)/G_{i+1}(P)$

$$\vartheta_i(s\tau s^{-1}) = \vartheta_0(\overline{s})^i \vartheta_i(\tau).$$

Soit $\mathbb{F}_{q_0}$ le corps engendré par $\mu = \zeta^i$ sur $\mathbb{F}_p$. Montrons que $Im(\vartheta_i)$ est un $\mathbb{F}_{q_0}$ espace vectoriel. Soit donc $\tau \in G_i(P)/G_{i+1}(P)$ et$\sum a_j\mu^j \in \mathbb{F}_{q_0}$ avec $a_j \in \mathbb{F}_p$ il suffit de montrer que $S = (\sum a_j\mu^j)\vartheta_i(\tau) \in Im(\vartheta_i)$. Or $S = \sum \mu^j \vartheta_i(\tau^{a_j}) = \sum (\zeta^j)^i \vartheta_i(\tau^{a_j}) = \sum \vartheta_i(s_0^j \tau^{a_j} s_o^{-1}) = \vartheta_i(\prod s_0^j \tau^{a_j} s_0^{-j}) \in Im(\vartheta_i)$. Donc $q_i = |Im(\vartheta_i)| = q_0^l$ où l est la dimension de $Im(\vartheta_i)$ sur $\mathbb{F}_{q_0}$. Or μ est une racine $\frac{E}{(i,E)}$-ième de l'unité donc $\frac{E}{(i,E)}$ divise $(q_0 - 1)$ et comme $q_i - 1 = q_0^l - 1$ c'est également un multiple de $\frac{E}{(i,E)}$. D'où le résultat.

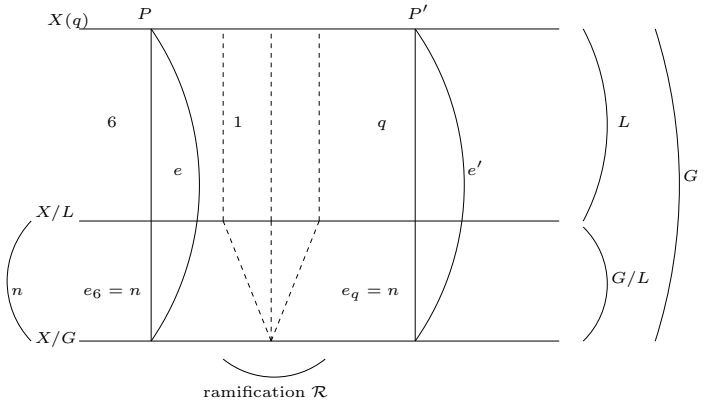
1.3 Démonstration des propositions 1.2 et 1.3

Soit $q \geq 7$ premier et p premier différent de q. On posera $L(q) = \mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z})$ ou $L = L(q)$ si aucune confusion n'est à craindre.
On posera de même pour la courbe modulaire $X = \overline{X(q)}_p$, $G_{q,p} = \mathrm{Aut}(\overline{X(q)}_p)$ ou $G = G_{q,p}$, $\mathrm{g}_X = \mathrm{g}_{\overline{X(q)}_p}$.
Notre but ici est double : tout d'abord donner un résultat analogue à celui de Serre sur $\mathbb{C}$ quand l'ordre de G est suffisamment petit (par ex. quand $|G| \leq 84(g-1)$). Puis dans le cas où le groupe des automorphismes ne respecte pas la majoration d'Hurwitz $84(g-1)$ de donner la structure du revêtement $X \to X/G$.

1.3.1 Démonstration de la proposition 1.2

(D'après une idée de Serre [Maz98].)
Évaluons le rapport $n = 84(\mathrm{g}_X - 1)/|\mathrm{PSL}_2(q)|$: Rappelons que pour $q \geq 7$ on a $\mathrm{g}_X = 1 + \frac{q-6}{12q}|L(q)|$. D'où $n < 7$ donc $n < q$. Ce qui démontrera le cas particulier. Posons maintenant $|G/L(q)| = n$.
Montrons alors que L est distingué dans G. L'action d'un élément d'ordre q sur G/L par multiplication à gauche est triviale car $q > n$. Il s'en suit que l'action de L sur G/L est triviale car L est engendré par ses éléments d'ordre q (les transvections). Donc L est normal dans G.

FIG. 1.1 – Cas $p = 3$



Soit $p > 3$. Si $e = 2, 3$ ou q on appelle X_e les trois points de $X/L(q) = \mathbb{P}^1$ dont les points de la fibre sont respectivement d'indice de ramification e. Ces trois points existent et sont distincts puisqu'ils représentent respectivement les classes d'isomorphismes des courbes elliptiques d'invariant $j = 0$ (de groupe d'automorphismes d'ordre 6), $j = 1728$ (de groupe d'automorphismes d'ordre 4) et $j = \infty$ (pour les pointes). Tout élément $t \in G$ normalise L donc induit un automorphisme t' de $\mathbb{P}^1$. Cet automorphisme fixe les 3 points X_e : c'est donc l'identité sur $\mathbb{P}^1$. Donc G agit trivialement sur $X/L(q)$ et $G = L$.

Considérons maintenant le cas où $p = 3$ (voir figure 1.1). On a toujours que L est distingué dans G donc le revêtement $X/L \simeq \mathbb{P}^1 \to X/G \simeq \mathbb{P}^1$ est galoisien d'ordre n. Le point d'indice 6 et le point d'indice q ou les points d'indice 1 dans le revêtement intermédiaire ne peuvent donc pas avoir la même image dans X/G : en effet on devrait par exemple avoir dans le revêtement inférieur $e_6 = e_q$ (car le revêtement est galoisien) et de plus $e = 6e_6 = qe_q$: impossible car $q \neq 6$. On a d'après la formule d'Hurwitz :

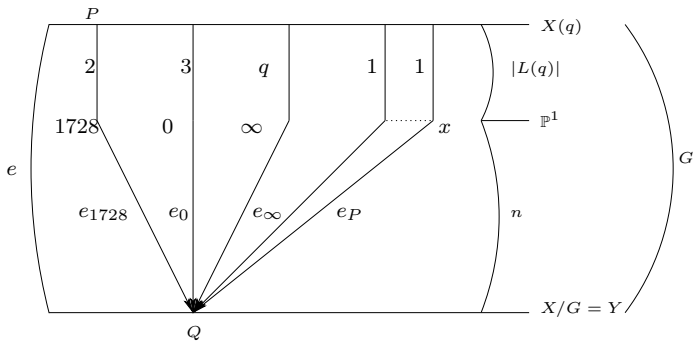
$$\frac{2\mathrm{g}_X - 2}{|G|} = \frac{q-6}{6qn} = \frac{\delta}{6n} + \frac{\delta'}{qn} + R,$$

où $\delta = \sum_{i=1}^{\infty}(G_i(P)-1)-1 > 0$ (car sauvagement ramifié) $\delta' = \sum_{i=1}^{\infty}(G_i(P')-1)-1 \geq -1$ et R est un nombre rationnel positif provenant de la ramification éventuelle de points dans le revêtement du bas. (on va montrer que $R = 0$.) On a donc $q - 6 = q\delta + 6\delta' + 6qnR$ Ce qui implique $\delta = 1, \delta' = -1$ et $R = 0$. Mais $\delta = 1$ implique que $|G_1(P)| = 3$ et $|G_2(P)| = 1$ donc d'après le lemme 1.5 on a $e = 6e_6 = 6n = 3E$ avec $E|(3-1) = 2$ donc $n = 1$ et $G \simeq L$.

Le cas $p = 2$ se traite de manière analogue.

Remarque :
La démonstration montre en outre que si G' est un sous-groupe de G qui contient L et si L est distingué dans G' alors $G' = L$.

FIG. 1.2 – Un unique point sauvagement ramifié



1.3.2 Démonstration de la proposition 1.3

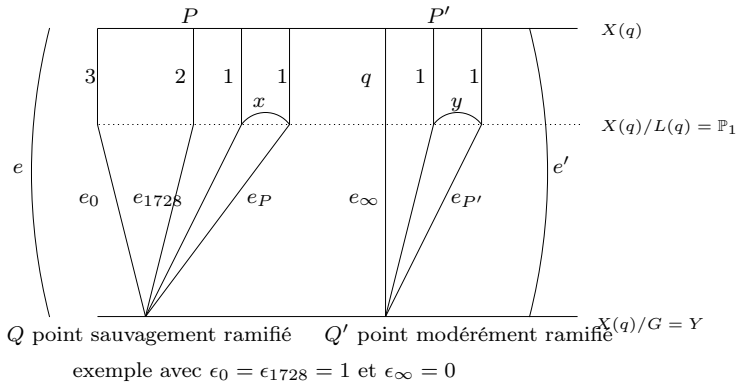
Montrons le résultat en détail dans le cas où $p > 3$. Dans ce cas on sait que le revêtement $X \to X/L(q)$ est ramifié au-dessus de 3 points d'indice $2, 3$ et q (donc modérément ramifié). Pour $p = 2, 3$ on indiquera les modifications à prendre en compte sachant que quand $p = 3$ le revêtement intermédiaire est ramifié au-dessus de deux points d'indice 6 et q et que pour $p = 2$ il est ramifié au-dessus de deux points d'indice 12 et q. D'après un résultat de Singh [Sin74, th. 3.1] il suffit de montrer que les configurations suivantes sont impossibles : un unique point de ramification, deux points sauvagement ramifiés, trois points de ramification dont les indices sont donnés dans le tableau ci-dessous ou quatre points d'indice 2.

e_1	3	4	6	5	4	3	e arbitraire
e_2	3	4	3	3	3	3	2
e_3	3	2	2	2	2	2	2

Les conditions sur le revêtement intermédiaire permettent d'éliminer sans calcul un grand nombre de cas. On montrera ici en détail comment on élimine le cas d'un unique point sauvagement ramifié. On pose $n = |G|/|L|$. On suppose que sur $Y = X/G$ un unique point Q est sauvagement ramifié et soit $P \in X$ tel que $\pi_{X/Y}(P) = Q$. (voir figure 1.2) On a d'après la formule d'Hurwitz : $\frac{q-6}{6qn} = -2 + \frac{d}{e}$ avec $d = e - 1 + \sum_1^\infty (|G_i(P)| - 1) = e + \delta$ avec $\delta > 0$ car le point est sauvagement ramifié. De plus puisqu'il n'y a qu'un point de ramification, les points de ramification d'indice 2,3 et q dans le revêtement intermédiaire se réduisent sur Q . Enfin notons x $(x \geq 0)$le nombre de points non ramifiés dans le revêtement intermédiaire pouvant se réduire également sur Q. En exploitant la figure grâce aux propriétés galoisiennes du revêtement, on a donc $2e_{1728} = 3e_0 = qe_\infty = e_P = e$. De la formule $n = e_0 + e_{1728} + e_\infty + xe_P$ on tire $n = Te$ avec $T = \frac{1}{2} + \frac{1}{3} + \frac{1}{q} + x$. En remplaçant dans la formule de Hurwitz on a $\frac{q-6}{6qn} = -1 + \frac{\delta T}{n}$ soit en simplifiant $q - 6 = 6qT(\delta - e)$. D'où $6qT|(q - 6)$ or $6qT > 5q$ donc $6qT > q - 6$. Impossible.

Dans les cas $p = 2$ et $p = 3$ on aurait respectivement $T = \frac{1}{12} + \frac{1}{q} + x$ et $T = \frac{1}{6} + \frac{1}{q} + x$ Donc $6qT = q/2 + 6 + 6qx$ et $6qT = q + 6 + 6qx$. Le cas $p = 3$ est donc clair. Pour $p = 2$

FIG. 1.3 – Deux points ramifiés dont un seul est sauvagement ramifié



on aurait $q+12|2q-12$ soit $q+12|36$: exclu.

Remarque :
Dans le cas de deux points de ramifications dont un seul est sauvagement ramifié on peut simplifier la formule d'Hurwitz. On introduit des constantes $\varepsilon_0, \varepsilon_{1728}, \varepsilon_\infty, \varepsilon'_0, \varepsilon'_{1728}, \varepsilon'_\infty$ valant 1 ou 0 et traduisant la présence des points d'indice de ramification 3,2,q dans le revêtement intermédiaire au dessus respectivement du point modérément ramifié ou du point sauvagement ramifié (voir l'exemple de la figure 1.3). On pose de plus $T = \frac{\epsilon_0}{3} + \frac{\epsilon_{1728}}{2} + \frac{\epsilon_\infty}{q} + x$ et $T' = \frac{\epsilon'_0}{3} + \frac{\epsilon'_{1728}}{2} + \frac{\epsilon'_\infty}{q} + y$. Après simplification on obtient $q-6 = 6qT\delta - 6qT'$. Enfin $n = TEp^\alpha = T'e'$ avec $\alpha > 0, (E,p) = 1$ et $(e',p) = 1$.

Dans le cas $p = 3$ le point d'indice de ramification intermédiaire 6 est bien évidemment sauvagement ramifié donc $T = 1/6 + \varepsilon_\infty/q + x$ et $T' = \varepsilon'_\infty/q + y$. De même dans le cas $p = 2$, $T = 1/12 + \epsilon_\infty/q + x$ et $T' = \epsilon'_\infty/q + y$.

1.4 Cas particulier : ordinarité

Pour préciser la nature de $G_{q,p}$ pour p et q quelconques nous allons faire une hypothèse sur la courbe $\overline{X(q)}_p$: nous allons supposer qu'elle est ordinaire c'est à dire que son p-rang est égal à son genre. Rappelons que le p-rang (encore appelé invariant de Hasse-Witt) d'une courbe X/k (k algébriquement clos de caractéristique p) est défini par

$$\gamma_X := \dim_{\mathbb{F}_p} H^1(X,\mathcal{O})^{F^*} = \dim_{\mathbb{F}_p} J[p]$$

où J désigne la jacobienne de X et $H^1(X,\mathcal{O})^{F^*}$ le sous-espace de $H^1(X,\mathcal{O})$ invariant par le Frobenius absolu. (cf. [BG97])

1.4.1 Utilisation du p-rang

La connaissance du p-rang permet l'utilisation de la formule de Deuring-Safarevic [Sub75, th. 4.2]. En utilisant cette formule et celle d'Hurwitz pour un revêtement de la forme $X \mapsto X/H$ avec H un p-groupe, on peut obtenir une majoration du nombre $m+1$ de groupes de ramification non triviaux (avec, par convention, $m = -1$ si le point n'est pas ramifié).

Proposition 1.6
$\sum_{i=2}^{\infty}(|G_i(P) - 1|) \leq 2(\mathrm{g}_X - \gamma_X)$. *En particulier on a l'inégalité* $m \leq \frac{2(\mathrm{g}_X - \gamma_X)}{p-1} + 1$.

Remarque :
On constate donc que lorsque la courbe est ordinaire $G_2(P) = \{1\}$ pour tout $P \in X$. Cela simplifie de manière notable l'étude de la ramification. Cette formule permet également d'établir le théorème suivant dû à Nakajima [Nak87] (voir plus précisément th. 1, corollary, th. 2, th. 3, la preuve du cas IV dans le th. 3, lemma 1 et lemma 2) et qui joue un rôle central dans la suite de notre étude puisqu'il permet en particulier de donner une bonne borne pour l'ordre des groupes d'automorphismes lorsque la courbe est ordinaire.
On dira que la majoration d'Hurwitz est respectée pour la courbe X si $|G| \leq 84(g_X - 1)$.

Théorème 1.7 (Nakajima) [Nak87]
Soit X une courbe de genre supérieur ou égal à deux et $G = \mathrm{Aut}(X)$. Soit H un p-sous-groupe de Sylow de G.

1. *Si $\gamma_X \geq 2$ alors*
$$|H| \leq c_p(\gamma_X - 1)$$
avec $c_p = p/(p-2)$ si $p \geq 3$ et $c_2 = 4$.
2. *Si $\gamma_X = 1$ et $p \geq 3$ alors la majoration d'Hurwitz est respectée .*
3. *Si $2 \leq \gamma_X \leq p-2$ ($p \geq 5$) alors la majoration d'Hurwitz est respectée.*
4. *Si $1 \leq \mathrm{g}_X - \gamma_X \leq (p-2)/2$ ($p \geq 5$) alors la majoration d'Hurwitz est respectée.*
5. *Si la courbe est ordinaire (i.e. $\mathrm{g}_X = \gamma_X$) alors $|G| \leq 84(\mathrm{g}_X - 1)\mathrm{g}_X$. Si on sait de plus que le revêtement $X \to X/G$ est ramifié au dessus de deux points exactement dont un seul est sauvagement ramifié d'indice $e := Ep^{\alpha}$ avec $(E,p) = 1$ et si $\mathrm{g}_{X/G} = 0$ alors si $E = 1$ $|G| \leq 24(\mathrm{g}_X - 1)$ et si $E \geq 2$ on a $|G| \leq 14e(\mathrm{g}_X - 1)$.*

1.4.2 Calcul du p-rang des courbes modulaires $\overline{X(q)}_p$

Pour une courbe quelconque le p-rang est un invariant difficile à calculer. Cependant en utilisant les résultats de [BG97] et d'Eichler-Shimura-Igusa (cf. [Igu59]) on a dans le cas de $\overline{X(q)}_p$

Théorème 1.8
Le p-rang de la courbe $\overline{X(q)}_p = M_q^* \otimes \mathbb{F}_p$ est égal au degré de la réduction modulo p de $\chi_p(u) := det(1 - T_p u | S_2(\Gamma(q)))$

Remarque :
Ce théorème est valable plus généralement pour les courbes modulaires $X(N), X_1(N), X_0(N)$ avec $N \geq 7$ un entier premier avec p. Il suffit donc de calculer le polynôme caractéristique de l'opérateur de Hecke T_p agissant sur $S_2(\Gamma(q))$. Malheureusement la dimension de cet espace est égal au genre de X et croît donc comme q^3. De plus les méthodes de calculs des espaces modulaires (via les symboles modulaires) ne sont souvent implantées que dans le cas de $S_2(\Gamma_0(N,\chi))$ où χ est un caractère. On peut cependant établir aisément le résultat suivant à l'aide d'un résultat de Kani et Rosen [KR89] et d'un résultat d'Imin Chen généralisé par De Smit et Edixhoven [Edx00, th. 1] :

Proposition 1.9
Soit $q \geq 7$ un nombre premier et p un nombre premier différent de q alors

$$\gamma_{\overline{X(q)}_p} = \gamma_{\overline{X_1(q)}_p} + \frac{q-1}{2}(\gamma_{\overline{X_0(q^2)}_p} - \gamma_{\overline{X_0(q)}_p}).$$

Comme de plus $\Gamma_1(q) = \oplus_{\chi \,\mathtt{cond.q}} \Gamma_0(q,\chi)$ on peut se ramener au calcul des polynômes de Hecke de T_p sur ces espaces qui est implanté dans MAGMA.

1.4.3 Démonstration du théorème 1.1

La démonstration s'organise en deux temps : on regarde d'abord ce que peut valoir le rapport $n = |G|/|L(q)|$. Puis dans les cas $p = 2, 3$ où n peut être strictement supérieur à 1, on montre la simplicité du groupe en question.

On suppose que la courbe ordinaire $X := \overline{X(q)}_p$ a un groupe d'automorphismes G d'ordre strictement supérieur à celui de $L(q)$. D'après la proposition 1.2 $|G|$ doit alors dépasser la borne d'Hurwitz $84(g_X - 1)$ et la proposition 1.3 nous dit que le revêtement $X \to X/G$ est ramifié au dessus de deux points exactement dont un seul est sauvagement ramifié. On peut se servir du théorème 1.7 (cas ordinaire avec les notations ci-dessus en accord avec celles du théorème) : on peut supposer que $E \geq 2$: sinon $|G| \leq 24(g_X - 1)$ donc inférieur à la borne d'Hurwitz (exclu) . Dans ce cas on a alors $|G| \leq 14e(g_X - 1)$. D'où :

$$n = \frac{|G|}{|L(q)|} \leq \frac{7(q-6)}{6q}e.$$

Enfin $n = Te$ donc $T \leq \frac{7(q-6)}{6q}$ ou $6qT \leq 7q - 42$. Avec les formules de la remarque 1.3.2 ceci montre en particulier que

- Quand $p > 3$ alors $x = 0$ ou $x = 1$ et dans ce dernier cas on a $\epsilon_0 = \epsilon_{1728} = 0$.
- Quand $p = 3$ alors $x = 0$.
- Quand $p = 2$ alors $x = 0$ ou $x = 1$. Ce cas similaire à $p = 3$ ne sera pas développé.

Comme $G_2(P) = \{1\}$ on a $\delta = p^\alpha - 2$. On peut pousser un peu plus loin l'écriture de la formule d'Hurwitz : on a $q - 6 = 6qT\delta - 6qT'$ soit $6qT' = 6qTp^\alpha - 2 \cdot 6qT - q + 6$.

On suppose maintenant $p > 3$.
Rappelons que $6qT = 2q\epsilon_0 + 3q\epsilon_{1728} + 6\epsilon_\infty + 6qx$ et que $x = 0$ ou 1.

Démontrons ici le cas $x = \epsilon_0 = \epsilon_{1728} = 0$ et $\epsilon_\infty = 1$, les autres cas sont sensiblement identiques.(voire plus simples)
On a $6qT = 6$ et $6qT' = 6p^\alpha - q - 6$ donc $6qT$ et $6qT'$ sont premiers entre eux vu les hypothèses sur q et p. Comme on a $6qTe = 6qT'e'$, $6qT'$ divise $e = Ep^\alpha$ et comme $(e', p) = 1$ on a p^α divise $6qT'$ donc $6qT'/p^\alpha$ divise E. Mais d'après le lemme 1.5 on sait que E divise $(q_1 - 1) = (p^\alpha - 1)$ car $G_2(P) = \{1\}$. D'où les deux contraintes :

$$\begin{cases} i) & p^\alpha | 6qT' \\ ii) & \frac{6qT'}{p^\alpha} | p^\alpha - 1 \end{cases}$$

La condition *i)* impose $q + 6 = p^\alpha d$ puis la condition *ii)* se traduit par $6qT'/p^\alpha = 6 - d$ divise $q + 6 - d$ d'où $q + 6 - d - (6 - d) = q$ doit être divisible par $6 - d \geq 1$. Donc puisque q est premier $d = 6 - q$ (exclu car $q \geq 7$) ou $6 - d = 1$ soit $d = 5$. On a donc $6qT' = 6p^\alpha - q - 6 = p^\alpha$ donc l'égalité $6qTe = 6qT'e'$ implique $e' = 6E$. Utilisons cela dans l'égalité d'Hurwitz

$$\frac{q-6}{6qn} = \frac{p^\alpha - 2}{e} - \frac{1}{e'} = \frac{5p^\alpha - 12}{6Ep^\alpha}.$$

Soit $n = \frac{(q-6)Ep^\alpha}{q(5p^\alpha - 12)}$. Comme on a d'autre part $5p^\alpha = q + 6$ on a $p^\alpha \leq (q+6)/5 < 2q/5$ et $E \leq p^\alpha - 1 < 2q/5$. Enfin $n < 2q/10 < q$. La proposition 1.2 montre que G est isomorphe à $L(q)$: exclu par hypothèse.

On suppose maintenant $p = 3$.
Premier cas : $6qT = q$ et $6qT' = 3^\alpha - 3q + 6$.

- Soit $\alpha = 1$ on a alors $6qT' = 6$. Comme $6qTe = 6qT'e'$ et E divise $3 - 1 = 2$ on a $e' = q$ et $E = 2$ mais alors d'après Hurwitz

$$\frac{q-6}{6qn} = \frac{3-2}{6} - \frac{1}{q} = \frac{q-6}{6q}$$

  donc $n = 1$: exclu.
- Si $\alpha \geq 2$ alors $d < q/3$. Or $q - d$ divise $3q - 6 - d$ ce qui implique $q - d$ divise $2q - 6$. Si on note $2q - 6 = D(q - d)$ on a l'encadrement $q - qD < 2q - 6 - D(q - d) < q(2 - 2D/3)$ donc $D = 2$. Mais alors $d = 3$. On doit donc avoir $q - 2 = 3^\alpha$. De plus $6qT' = 3^\alpha q - d = 3^\alpha(q - 3)$ d'où $q3^\alpha E = 3^\alpha(q - 3)e$ donc $q - 3$ divise E mais comme E divise $3^\alpha - 1 = q - 3$ on a $E = q - 3$ et $e = q$. La formule d'Hurwitz donne alors après simplification $n = (q - 2)(q - 3)/6$.

Le deuxième cas : $6qT = q + 6$ et $6qT' = (q + 6)3^\alpha - 3q - 6$ se traite par des arguments similaires.

On suppose toujours la courbe ordinaire et $p = 2$ ou 3. On montre maintenant que G, le groupe des automorphismes, est un groupe simple. Si $G = L(q)$, on a fini. On suppose qu'il contient strictement $L(q)$. On raisonne par l'absurde. Soit donc G' un sous-groupe distingué de G différent de G et de $\{1\}$. Considérons alors $H = G' \cap L(q)$. H est distingué dans $L(q)$. Comme $L(q)$ est simple on a $H = L(q)$ ou $H = \{1\}$.

– Si $H = L(q)$ on a alors $L(q) \subset G'$. Donc G' est un groupe d'automorphismes qui contient $L(q)$. Si $G' = L(q)$ alors $L(q)$ est distingué dans G ce qui est impossible d'après la remarque à la proposition 1.2. Donc G' contient strictement $L(q)$. Mais son ordre dépasse alors la borne d'Hurwitz et le revêtement $X \to X/G'$ est ramifié en deux points exactement dont un seul est sauvagement ramifié. On déroule alors la démonstration précédente et on conclut que $|G'/L(q)| = n = |G/L(q)|$ (n unique d'après le théorème !) donc $G' = G$: exclu.
– On a donc $G' \cap L(q) = \{1\}$. Comme G' est distingué dans G, $G'L(q)$ est un sous-groupe de G (en bijection avec $G' \times L(q)$.) G' n'étant par trivial $G'L(q)$ est différent de $L(q)$ et comme $L(q) \subset G'L(q)$ le même raisonnement que précédemment montre que $G'L(q) = G$. En particulier $|G'| = n$. De plus on a un morphisme de $\rho : L(q) \to \mathrm{Aut}(G')$. Or par simplicité de $L(q)$ on a $\mathrm{Ker}(\rho) = \{1\}$ ou $L(q)$. Si $\mathrm{Ker}(\rho) = L(q)$ alors ρ est trivial mais alors $G'L(q) \simeq G' \times L(q)$ et $L(q)$ est distingué dans G donc $L(q) = G$: exclu. Donc $\mathrm{Ker}(\rho) = \{1\}$ et $L(q)$ s'injecte dans $\mathrm{Aut}(G')$.

Pour poursuivre nous devons étudier la structure de G'. Soit $\{1\} \neq D \subset G'$ un groupe caractéristique de G'. Comme G' est distingué dans G on a D distingué dans G. Or $L(q) \cap D = \{1\}$ donc $L(q)$ est inclus strictement dans $L(q)D$ mais alors $L(q)D = G$ et $|D| = n = |G'|$ donc $D = G'$. G' n'admet donc pas d'autre groupe caractéristique que $\{1\}$ et lui-même, il est dit caractéristiquement simple. On sait [Rot95, p. 106] qu'un tel groupe est isomorphe à G_s^a où G_s est un groupe simple et a un entier. Nous allons montrer qu'ici $a = 1$ et que G' est donc un groupe simple.

Lemme 1.10
Il n'existe pas d'entier x pair tel que $x^a = 3^{\alpha-1}(3^\alpha - 1)/2$ avec $a \geq 2$ et $\alpha \geq 1$.
De même il n'existe pas d'entier x pair tel que $x^a = 4^{\alpha-1}(4^\alpha - 1)/3$ avec $a \geq 2$ et $\alpha \geq 1$.

Ceci est suffisant pour montrer que G' est simple puisque l'ordre d'un groupe simple est toujours pair.

Démonstration :
La démonstration de ce lemme s'appuie en partie sur des résultats d'arithmétique élémentaire et pour $a > 3$ sur l'étude d'une équation du type Fermat (cf. l'article de Merel [Mer99] pour les résultats et les notations). Montrons ici comment se traite la première équation dans ce cas. Posons $n = 3^{\alpha-1}(3^\alpha - 1)/2$, on cherche donc à résoudre $x^a = n$. On peut bien sûr se limiter au cas a premier. De plus $x = 3^b x'$ donc l'équation devient $2x'^a = 3^{ba+1} - 1$. Posons $3^b = y$ on a alors $3y^a - 2x'^a - 1 = 0$. On suppose l'existence d'une solution telle que x' est pair. On considère la courbe de Frey $E := E_{3y^a,-2x'^a,-z^a}$ et la représentation attachée $\rho_{E,[a]}$. Comme $a > 3$ la représentation $\rho_{E,[a]}$ est absolument irréductible [Mer99, th. 1.3] et modulaire [Mer99, th. 1.1]. Alors d'après [Mer99, th. 1.2] cette représentation est modulaire de niveau $N = \mathrm{Rad}_a(6(yx'z)^a)\epsilon_2(-2x'^a) = 6\epsilon_2(-2x'^a)$. Comme x' est pair et $a > 3$ on a $32|2x'^a$ donc $N = 6$. Mais $X_0(6)$ est de genre 0 il n'existe donc pas de représentation de niveau 6. D'où l'absence de solution.

Pour résumer nous avons un groupe G' simple de cardinal n tel que $L(q)$ s'injecte

dans le groupe des automorphismes de G'. Nous allons montrer que pour une raison de cardinalité ceci ne peut arriver. Dans le cas $p = 3$ $n = (q-2)(q-3)/6$ donc $n < q^2/4$ et $|L(q)| = q(q^2-1)/2$ donc $|G'|^{3/2} = n^{3/2} < |L(q)|$. De même dans le cas $p = 2$. Il reste donc à montrer

Lemme 1.11
Soit S un groupe simple. Alors $|\mathrm{Aut}(S)| < |S|^{3/2}$.

Démonstration :
Pour démontrer ce résultat que nous n'avons pu trouver dans la littérature, nous utilisons la classification des groupes simples (finis) ainsi que l'ordre du groupe des automorphismes extérieurs de ces groupes qui se trouvent dans l'ATLAS ([Atl85]). Rappelons que si S est un groupe simple on a $|\mathrm{Aut(S)}| = |\mathrm{S}||\mathrm{O(S)}|$ où O(S) représente les automorphismes extérieurs de S (i.e. ne provenant pas d'une action par conjugaison d'un élément du groupe). On peut donc également montrer que $|\mathrm{O(S)}| < \sqrt{|\mathrm{S}|}$.

- Si S est abélien, S est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour p premier. On sait qu'alors $\mathrm{Aut(S)} \simeq (\mathbb{Z}/\mathrm{p}\mathbb{Z})^*$ de cardinal $\phi(p) < p < p^{3/2}$.
- Si S est un groupe alterné A_n avec $n > 5$. On sait alors ([Pas68] th. 5.7) que si $n \neq 6$ $\mathrm{Aut(A_n)} \simeq \mathcal{S}_\mathrm{n}$ et que si $n = 6$ $|\mathrm{Aut(A_n)} : \mathcal{S}_\mathrm{n}| = 2$. Donc $|\mathrm{Aut(S)}| \leq 4|\mathrm{S}| < \mathrm{S}^{3/2}$.
- Si S est un des 26 groupes sporadiques on a $|\mathrm{O(S)}| \leq 2$ et $|S| > 4$.
- Si S est le groupe de Tits simple ${}^2F_4(2)'$. Alors $|\mathrm{O(S)}| = 6$ et $|S| > 36$.
- Si S est un groupe de Chevalley. Le tableau ci-dessous donne un minorant de l'ordre de chacun de ces groupes ainsi qu'un majorant de l'ordre des automorphismes extérieurs en fonction des paramètre.

S	minorant	majorant de O(S)	S	minorant	majorant de O(S)
$A_1(q)$	$q(q^2-1)/2$	q	$A_1(4)$	60	2
$A_n(q)$ $n \geq 2$	$q^{n(n+1)-1}$	q^2	${}^2A_n(q)$ $n \geq 3$	$q^{n(n+1)-1}$	q^3
${}^2A_2(q)$	$q^{10}/3$	$3q$	$B_2(q)$	$q^8/2$	$2q$
${}^2B_2(q)$	q^4	q	$B_n(q)$ $n \geq 3$ $n \geq 3$	$q^{n^2}/2$	q
$C_n(q)$ $n \geq 3$	$q^{n^2}/2$	q	$D_4(q)$	$q^{12}/4$	$12q$
${}^3D_4(q)$	q^{20}	$3q$	$D_n(q)$ $n \geq 5$	$q^{n(n-1)}/4$	$4q$
${}^2D_n(q)$ $n \geq 4$	$q^{n^2}/4$	$4q$	$G_2(q)$	q^6	q
${}^2G_2(q)$	q^6	q	$F_4(q)$	q^{24}	q
${}^2F_2(q)$	q^{18}	q	$E_6(q)$	$q^{36}/3$	$3q$
${}^2E_6(q)$	$q^{47}/3$	$3q$	$E_7(q)$	$q^{67}/2$	q
$E_8(q)$	q^{120}	q			

Remarque :
On peut remplacer l'hypothèse «ordinaire» dans le théorème par la condition plus faible $G_2(P) = \{1\}$ pour tout $P \in X$.
Pour juger de la «pertinence» du théorème il faudrait pouvoir évaluer la densité des p pour lesquels la courbe est ordinaire. On peut consulter à ce sujet les conjectures de [BG97] et les exemples ci-dessous.

1.5 Quelques cas particuliers

Cette partie a pour but d'illustrer l'utilisation des divers résultats démontrés plus haut. Il est à noter que grâce à un résultat de Roquette [Roq70] pour q fixé on étudie qu'un nombre fini de cas. En effet si $p > \mathrm{g}_X + 1$ alors $|G| \leq 84(\mathrm{g}_X - 1)$ et donc $G \simeq L(q)$ d'après 1.2. (le cas particulier $p = 2\mathrm{g}_X + 1$ est exclu pour des raisons de cardinalité sur G)
Ainsi pour $q = 7$ seuls 2 et 3 posent problème : $\overline{X(7)}_2$ est ordinaire donc le théorème permet de conclure que $G_{7,2} \simeq L(7)$ et $G_{7,3}$ est connu grâce à Kuribayashi [Kur82].

1.5.1 Cas $N = 11$

Théorème 1.12
Les fibres spéciales du schéma M_{11}^* en $p \neq 11$ ont pour groupe d'automorphismes :
- *si $p = 3$ le groupe de Mathieu M_{11} d'ordre 7920.*
- *si $p > 3$ et $p \neq 11$ ou $p = 2$ $\mathrm{PSL}_2(\mathbb{Z}/11\mathbb{Z})$ d'ordre 660.*

Démonstration :
Déterminons le p-rang γ de la courbe pour $p = 2 \ldots 23$ (dans ce cas on peut aussi utiliser la description explicite de la jacobienne de $X(11)$ comme produit de courbes elliptiques [Hec40]) :
- si $p = 2, 19$ E_1 et E_6 sont supersingulières donc $\gamma = 10$.
- si $p = 7, 13, 17$ alors E_6 est supersingulière et $\gamma = 21$.
- si $p = 3, 5, 23$ la courbe est ordinaire.

Considérons d'abord les cas simples :
- lorsque $\gamma = 10 \leq p - 2$: c'est le cas pour $p = 19$. Alors d'après le théorème 1.7 (cas 3) la majoration d'Hurwitz est respectée.
- lorsque $\gamma = 21 \geq g - (p-2)/2$: c'est le cas pour $p = 13, 17$. Alors d'après le théorème 1.7 (cas 4) la majoration d'Hurwitz est respectée.
- lorsque la courbe est ordinaire, le théorème montrent que pour $p = 5, 23$ G est isomorphe à $L(11)$.
- dans le cas $p = 3$ le résultat est connu grâce aux travaux d'Adler et de Rajan. (cf. [Adl97],[Raj98]) On remarque que $11 - 2 = 9$ donc dans ce cas le théorème est bien confirmé et on a justement $n = 12 = 7920/660$.

Nous démontrons en détail le cas $p = 7$. Le cas $p = 2$, plus long, se traite par des arguments similaires (on pourra également voir la démonstration du cas $p = 7, N = 13$). On raisonne par l'absurde en supposant que le groupe G est d'ordre strictement supérieur à $|L(q)|$. D'après la proposition préparatoire ce groupe a donc un ordre plus grand que la borne d'Hurwitz et donc d'après l'étude de la structure le revêtement $X \to X/G$ est ramifié au-dessus de deux points dont un seul est sauvagement ramifié. Soit $P \in \overline{X(11)}_7$ un point sauvagement ramifié. D'après la proposition 1.6 le nombre de groupes de ramification supérieure non triviaux est inférieur à $2\dot{(}26 - 21)/(7 - 1) + 1 < 3$ i.e. $G_3(P) = \{1\}$. De plus on sait que $|G_1(P)| \leq 7/5(21 - 1) \leq 28$ donc puisque le point est sauvagement ramifié et que c'est un p-groupe on a $G_1(P) \simeq \mathbb{Z}/7\mathbb{Z}$. On a alors deux

possibilités :

- soit $G_2(P) = \{1\}$: on peut dans ce cas appliquer le théorème.
- soit $G_2(P) \simeq \mathbb{Z}/7\mathbb{Z}$: dans ce cas en reprenant les notations du lemme 1.5 on a E divise 12. Revenons alors à la formule de base

$$\frac{q-6}{6qn} = \frac{5}{66n} = \frac{\delta}{e} + \frac{\delta'}{e'}$$

avec $\delta = -1 + (7-1) + (7-1) = 11$, $\delta' = -1$ et $e = 7E$. Soit après simplification

$$35Ee' = 66n(11e' - 7E).$$

On constate que comme 11 ne divise pas E il doit diviser e' et le point d'indice de ramification intermédiaire q est modérément ramifié. Comme dans le revêtement intermédiaire ce point a un indice de ramification égal à 11 on a $e' = 11d'$ et on a $n \geq d' = e'/11$. D'où $A = 66n(11e' - 7E) - 35Ee' \geq 11e'(6e' - 7E)$. Comme $e' \geq 11$ si on veut $A = 0$ cela implique $E \geq 9$ donc $E = 12$. On a alors $e \leq 14$ soit $e = 11$. Ce qui nous donne $35 \cdot 12 \cdot 11 = 66 \cdot 37n$: c'est impossible.

1.5.2 Cas $N = 13$

Théorème 1.13
Les fibres spéciales du schéma M_{13}^* en $p \neq 13$ ont pour groupe d'automorphismes $\mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ *d'ordre* 1092.

Démonstration :
Par le calcul des réductions modulo p des polynômes de Hecke associés aux opérateurs de Hecke T_p agissant sur $S_2(\Gamma(13))$ on détermine le p-rang de $\overline{X(13)}_p$ pour $p = 2 \ldots 47$, $p \neq 13$. On trouve

1. Pour $p = 7, 11$ le p-rang vaut 36.
2. Sinon le p-rang vaut 50. La courbe est donc ordinaire.

Le théorème permet de régler la question pour tous les $p \neq 7, 11$.

Le cas $p = 7$ La première étape est de déterminer les différentes suites de groupes de ramification pour le point sauvagement ramifié P.
Pour se faire on utilise 1.7 : on a déjà $7^\alpha \leq \frac{7}{5}(36-1) = 49$ donc $\alpha \leq 2$. Ensuite grâce à 1.6 on a $\sum_{i=2}^{\infty}(|G_i(P)| - 1) \leq 2(50 - 36) = 28$. Donc pour $i \geq 2$ on a $|G_i(P)| = 1$ ou 7 et pour $i > 5$ $|G_i(P)| = 1$. On a donc les cas suivants :

Cas	$\lvert G_1(P)\rvert$	$\lvert G_2(P)\rvert$	$\lvert G_3(P)\rvert$	$\lvert G_4(P)\rvert$	$\lvert G_5(P)\rvert$
1	49	7	7	7	7
2	49	7	7	7	1
3	49	7	7	1	1
4	49	7	1	1	1
5	49	1	1	1	1
6	7	7	7	7	7
7	7	7	7	7	1
8	7	7	7	1	1
9	7	7	1	1	1
10	7	1	1	1	1

Les cas $5, 10$ peuvent être exclus d'emblé car ils se rattachent au cas ordinaire ($|G_2(P)| = 1$). Notons $\delta = \sum_{i=1}^{\infty}(|G_i(P)| - 1) - 1$. De l'égalité d'Hurwitz

$$\frac{q-6}{6qn} = \frac{\delta}{e} - \frac{1}{e'}$$

on déduit

$$6qn(\delta e' - Ep^\alpha) = (q-6)Ep^\alpha e'$$

donc $e' \geq Ep^\alpha/\delta$. On sait de plus que $n \geq e'/q$ (car $n = T'e'$) donc

$$A = 6qn(\delta e' - Ep^\alpha) - (q-6)Ep^\alpha e' \geq e'(6\delta e' - qEp^\alpha).$$

Pour que A puisse être nul on a donc $e' \leq qEp^\alpha/(6\delta)$.
D'après le lemme 1.5 on a

Cas	1	2	3	4	6	7	8	9
E divise	6	6	6	6	30	24	18	12
δ	71	65	59	53	29	23	17	11

On constate que $q = 13$ ne divise pas E donc q divise e'. Si on note $e' = qd'$ on a alors l'encadrement

$$\frac{Ep^\alpha}{q\delta} \leq d' \leq \frac{Ep^\alpha}{6\delta}.$$

d' est un entier plus grand que 1 donc on a en particulier $Ep^\alpha \geq 6\delta$. On constate que ceci supprime les cas 1 à 4 et que pour les cas 6 à 9 on a $d' = 1$ donc $e' = 13$ et e égal respectivement $30 \cdot 7, 24 \cdot 7, 18 \cdot 7, 12 \cdot 7$. Mais d'après la formule d'Hurwitz $(\delta e' - e)$ divise $(q-6)ee'$. Or on constate que $(e, e') = 1$ donc $(\delta e' - e)$ doit diviser $q - 6 = 7$. Ce qui n'est pas le cas. Tous les cas ont donc été exclus d'où le résultat.

Cas $p = 11$ On utilise les mêmes arguments que précédemment :

1. $11^\alpha \leq \frac{11}{9}(36-1)$ donc $\alpha = 1$.
2. $\sum_{i=2}^{\infty}(|G_i(P)| - 1) \leq 28$ donc pour $i \geq 4$ $|G_i(P)| = 1$. On a donc les cas suivants :

Cas	$\lvert G_1(P)\rvert$	$\lvert G_2(P)\rvert$	$\lvert G_3(P)\rvert$
1	11	11	11
2	11	11	1
3	11	1	1

3. On peut de nouveau exclure le cas 3.
4. Dans le cas 1 on a E divise 30 donc q divise e'. Comme $\delta = 29$ on a $d' = 1$ soit $E = 30$, $e' = 13$ et $\delta e' - e = 47$. Comme 47 ne divise pas $(13-6)30 \cdot 11 \cdot 13$ ce cas est impossible.
5. Dans le cas 2 on a E divise 20 donc q e'. Comme $\delta = 19$ on a $d' = 1$ soit $E = 20$, $e' = 13$ et $\delta e' - e = 27$. Mais 27 ne divise pas $(13-6)20 \cdot 11 \cdot 13$: ce cas est donc impossible.

Bibliographie

[Adl97] A. Adler : The Mathieu group M_{11} and the modular curve $X(11)$. Proc. London Math. Soc. **74** (1997), 1-28.

[Atl85] J.H Conway, R.T Curtis, S.P Norton, R.A Parker : *Atlas of Finite Groups*, Clarenson Press, Oxford, (1985).

[Edx00] B. De Smit and B. Edixhoven : On a result of Imin Chen. Math. Research Letters **7** (2000), 147-153.

[BG97] P. Bayer and J. González : On the Hasse-Witt invariants of modular curves. Experimental Math. **6** (1997), 57-76.

[Hec40] E. Hecke : *Mathematische Werke*, Göttingen, 1959,36 (1937) 672-707 ; 41 (1940) 789-918.

[Igu59] J.Igusa : Kroneckerian models of fields of elliptic modular function. Amer. J. Math. **81**, (1959).

[KR89] E. Kani et M. Rosen : Idempotent relations and factors of Jacobians. Math, Ann. **284** (1989), 307-327.

[Kur82] I. Kuribayashi : On certain curves of genus three with many automorphisms. Tsukuba J. of Math. **6** (1982), 271-288.

[Maz98] B. Mazur : *Galois representations* in *Arithmetic Algebraic Geometry*, A. J. Scholl, London Mathematical Society, Lecture Note Series 254, p. 255, (*issu d'une lettre du 26 juin 96 de J.P. Serre*) (1998).

[Mer99] L. Merel : Arithmetic of elliptic curves and diophantine equations. Journal de Th. des Nombres de Bordeaux **11** (1999), 173-200.

[Nak87] S. Nakajima : p-ranks and automorphism groups of algebraic curves. Trans. amer. math. soc. **303** (1987), 595-607.

[Pas68] D.S. Passman, *Permutation Groups*, Mathematics Lecture Note Series, New-York, (1968).

[Raj98] C.S. Rajan : Automorphisms of $X(11)$ over characteristic 3 and the Mathieu group M_{11}. J Ramanujan Math. Soc. **13**, (1998), 63-72.

[Roq70] P. Roquette : Abschätzung der Automorphismenanzahl von Funktionenkörpern. Math. Z. **117**, (1970), 157-163.

[Rot95] J. J. Rotman : *An Introduction to the Theory of Groups*, fourth edition Springer-Verlag, (1995).

[Ser68] J.P. Serre : *Corps Locaux*, Hermann Paris , (1968).

[Sin74] B.Singh : On the group of automorphisms of a function field of genus at least two. J. Pure Appl. Alg. **4** (1974), 205-229.

[Sti73] H Stichtenoth : Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II. Arch. Math. **24** (1973), 527-544, 615-631.

[Sub75] D. Subrao : The p-rank of Artin-Schreier curves. Manuscripta Math. **16** (1975), 169-193.

[Vel78] J. Vélu : Courbes elliptiques munies d'un sous-groupe $\mathbb{Z}/n\mathbb{Z} \times \mu_n$. Bull. société math. de France **57**, (1978).

Deuxième partie

Courbe maximale

Chapitre 1

Existence d'une courbe de genre 5 sur $\mathbb{F}_3$ avec 13 points rationnels

1.1 Introduction

Soit $N_q(g)$ le nombre maximal de points rationnels sur $\mathbb{F}_q$ pour une courbe lisse de genre g sur $\mathbb{F}_q$. Grâce aux bornes de Weil on sait que $N_q(g)$ est inférieur ou égal à $q + 1 + 2g\sqrt{q}$. Ces bornes (même raffinées par la méthode d'Oesterlé) ne sont pas optimales et la détermination de $N_q(g)$ pour $g > 2$ reste incomplète.
Le cas qui nous préoccupe ici est celui des courbes de genre 5 sur $\mathbb{F}_3$. Les majorations explicites d'Oesterlé donne un nombre de points inférieur ou égal à 14, et Kristin Lauter a montré l'inégalité stricte (cf. [La99]). D'autre part on connaissait l'existence de courbes avec 12 points rationnels construites par des revêtements successifs (cf. [NX97]). Dans la présente note, nous nous proposons donc de combler la lacune existante en donnant explicitement une courbe de genre 5 avec 13 points rationnels comme l'intersection de 3 quadriques dans $\mathbb{P}^4$. Cette courbe est de plus exceptionnelle pour une autre raison : elle constitue, à ma connaissance, le premier exemple d'une courbe avec un nombre de points maximum qui est revêtement non galoisien d'une courbe elliptique. Nous donnons explicitement ce dernier.

1.2 Résultats

Proposition 1.1
La courbe C définie par

$$\begin{cases} q_1 = -x_1x_2 + x_3x_2 + x_3^2 - x_4^2 \\ q_2 = x_5x_1 - x_4x_2 \\ q_3 = x_1^2 + x_1x_2 - x_3^2 + x_5^2 \end{cases}$$

est une courbe de genre 5 qui possède 13 points sur $\mathbb{F}_3$.

Proposition 1.2

1. *$Aut_{\overline{\mathbb{F}_3}}(C) =< \omega >\simeq \mathbb{Z}/2\mathbb{Z}$ avec*

$$\omega : (x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_1 : x_2 : x_3 : -x_4 : -x_5).$$

2. *$D = C/ < \omega >$ a pour équation*

$$x_2^2(x_3x_2 + x_3^2 - x_1x_2) + (x_1^2 + x_1x_2 - x_3^2)x_1^2 = 0.$$

3. *C est revêtement non galoisien de degré 3 de la courbe elliptique $E : y^2 = x^3-x+1$. De plus si on prend comme modèle plan pour C*

$$x^4 + x^3y^3 - x^2 - xy^5 + y^5 + 2y = 0$$

le revêtement est donné par $(x : y : 1) \mapsto (x' : y' : 1)$ avec

$$\begin{cases} x' = \frac{-x^3-x^2y^3-x^2y^2+x^2+xy^5+xy^4-xy^3-xy^2+xy-y^6+y^5+y^4+y^3-y^2}{(y+1)(y-1)^2(y^3-y^2+y+1)} \\ y' = \frac{-x^3y-x^2y^5+x^2y^4-x^2y+xy^5+xy^4+xy^3-xy^2-xy+y^8+y^7+y^4-y^3-y^2-y+1}{(y+1)^2(y-1)^3(y^3-y^2+y+1)} \end{cases}$$

1.3 Démonstration

La courbe a été construite par une recherche exhaustive des sextiques planes de genre 5 passant par les 13 points rationnels du plan projectif (soit 3^{15} possibilités). Le plongement canonique permet alors d'obtenir un modèle lisse comme intersection de 3 quadriques dans $\mathbb{P}^4$.

D'autre part le polynôme caractéristique de C sur $\mathbb{F}_3$ se factorise en

$$(T^2 + 2T + 3)(T^2 + 3T + 3)(T^2 + 3)(T^4 + 4T^3 + 8T^2 + 12T + 9). \tag{1.1}$$

De plus sur $\mathbb{F}_{3^{24}}$, le polynôme caractéristique se scinde en

$$(T - 3^{12})^4(T^2 + 629918T + 3^{24})^3.$$

Sur $\mathbb{F}_{3^{24}}$ la jacobienne de la courbe C est donc isogène à $E^2 \times F^3$, avec E et F des courbes elliptiques qui sont absolument non-isogènes (par exemple parce que la première est supersingulière et pas l'autre). En particulier sur $\mathbb{F}_3$, C est revêtement de trois courbes elliptiques.

Pour montrer que C n'est revêtement galoisien d'aucune de ces courbes elliptiques, nous allons déterminer le groupe des automorphismes de C. On constate que

$$\omega : (x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_1 : x_2 : x_3 : -x_4 : -x_5)$$

est un automorphisme de la courbe. De plus $C/ < \omega >$ est une courbe de genre 2 (par la formule d'Hurwitz) qu'on peut obtenir par l'élimination des variables x_4 et x_5 sous la forme :

$$x_2^2(x_3x_2 + x_3^2 - x_1x_2) + (x_1^2 + x_1x_2 - x_3^2)x_1^2 = 0.$$

Montrons maintenant que cet automorphisme est le seul qui soit non trivial, on aura alors que C est revêtement non galoisien d'une courbe elliptique. C'est en fait une conséquence d'un théorème plus général dû à Beauville [Bea77, prop. 6.9] et qui donne exactement le groupe des automorphismes de C en fonction de ceux de la quintique définie ci-dessous. Mais nous avons besoin de quelque chose de moins précis et on obtient la démonstration élémentaire ci-dessous.
Puisque C est donnée sous forme canonique, tous les automorphismes de la courbe sont linéaires. Soit ψ un automorphisme de $\mathbb{P}^4$. C'est un automorphisme de C si et seulement si la matrice $M \in \mathrm{PGL}_5(\overline{\mathbb{F}}_3)$ qui le représente est telle que $q_i(Mv) = 0$ pour $i = 1, 2, 3$ et quelque soit ${}^t v = (x_1 : x_2 : x_3 : x_4 : x_5) \in C$.
Mais si M représente un automorphisme de C alors si on note Q_i les matrices des formes quadratiques q_i, ${}^t M Q_i M$ est une quadrique contenant C. Elle est donc combinaison linéaire des Q_i.
On considère alors l'ensemble S des $(x : y : z) \in \mathbb{P}^2$ tels que $\det(\mathrm{x\,Q_1 + y\,Q_2 + z\,Q_3}) = 0$. C'est une quintique lisse d'équation

$$-x^3 + y^2x - y^2 - x^4 + x + x^3y^2 - y^4x + y^4 = 0$$

qui ne possède qu'un seul automorphisme

$$\varphi : (x : y : z) \mapsto (x : -y : z).$$

On peut définir un morphisme de groupe μ de $\mathrm{Aut(C)} \subset \mathrm{PGL}_5(\overline{\mathbb{F}}_3)$ dans Aut(S) : si M est un automorphisme de la courbe C et si

$$\begin{cases} {}^t M Q_1 M = a_1 Q_1 + b_1 Q_2 + c_1 Q_3 \\ {}^t M Q_2 M = a_2 Q_1 + b_2 Q_2 + c_2 Q_3 \\ {}^t M Q_3 M = a_3 Q_1 + b_3 Q_2 + c_3 Q_3 \end{cases}$$

on a alors un automorphisme de S donnée par $(x : y : z) \mapsto (a_1x + a_2y + a_3z : b_1x + b_2y + b_3z : c_1x + c_2y + c_3z)$. De plus ce morphisme envoie ω sur φ.

Il suffit de montrer que μ est injectif. La quintique étant non singulière, la quadrique singulière $xQ_1 + yQ_2 + zQ_3$ associée à un point de la courbe (x, y, z) est de rang 4 et possède donc un unique point singulier. Soit $s : S \to \mathbb{P}^4$ qui associe à un point de la quintique le point singulier de la quadrique correspondante. Soit M un automorphisme de C qui se réduit sur l'identité de S. L'action de M en tant qu'automorphisme de $\mathbb{P}^4$ sur $s(S)$ est la même que celle induite par $s(\mu(M))$ qui est dans ce cas l'identité. Pour montrer qu'on a alors $M = \mathrm{Id}$ il suffit de prouver que les points de $s(S)$ ne sont pas contenus dans un hyperplan. C'est en fait une conséquence du lemme suivant :

Lemme 1.3
Soit F et G deux matrices de formes quadratiques non dégénérées d'un espace vectoriel E sur un corps k de caractéristique différente de 2 telles que $P(t) = \det(G - tF) = 0$ n'ait que des racines de multiplicité 1. Alors ces deux formes quadratiques sont simultanément diagonalisables.

Montrons tout d'abord comment ce lemme permet de conclure. Soit l une droite transverse à S et $p_0, \ldots, p_4$ les points d'intersection. On considère le pinceau de quadriques défini par l : il est engendré par deux quadriques non singulières d'équations $F = 0$ et $G = 0$ telles que $\det(F - tG) = 0$ n'a que des racines de multiplicités 1 (puisque l est transverse). On peut alors appliquer le lemme : dans une base qui diagonalise simultanément les deux quadriques on écrit $F = \sum X_i^2$ et $G = \sum \alpha_i X_i^2$ $\alpha_i \neq \alpha_j$. Avec ces coordonnées les images $s(p_i)$ sont alors tout simplement les points $(1:0:0:0:0), (0:1:0:0:0), \ldots, (0:0:0:0:1)$ qui ne sont évidemment pas dans un même hyperplan, d'où le résultat.

Démonstration :
Soit n la dimension de E. Soient λ_i, v_i ($\lambda_i \neq 0$ et $v_i \neq 0$) les n scalaires et vecteurs tels que $Fv_i = \lambda_i\, G_i v_i$. Nous allons montrer que les v_i sont une base orthogonale pour F et G. On a

$$\begin{aligned} {}^t v_j F v_i &= \lambda_i\, {}^t v_j G v_i && (1.2)\\ &= {}^t v_i F v_j \text{ par symétrie de } F && (1.3)\\ &= \lambda_j\, {}^t v_i G v_j && (1.4)\\ &= \lambda_j\, {}^t v_j G v_i \text{ par symétrie de } G && (1.5) \end{aligned}$$

Par hypothèse, les λ_i sont tous distincts on a donc par égalité de (1.4) et (1.5) que ${}^t v_j F v_i = {}^t v_j G v_i = 0$.

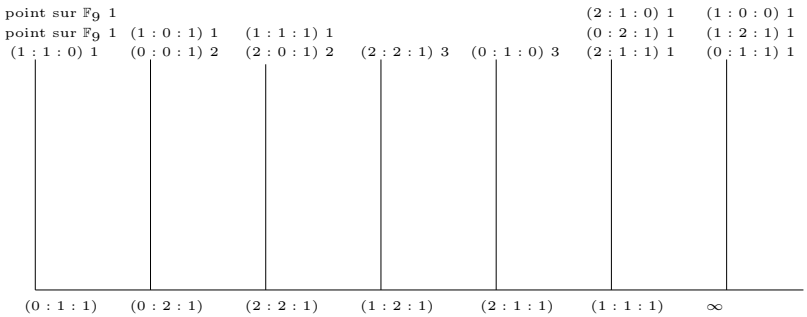
Nous allons donner explicitement un revêtement de C sur une courbe elliptique. On a le théorème suivant :

Théorème 1.4 [HL02]
Soit C une courbe sur $\mathbb{F}_q$ dont la jacobienne est isogène à un produit $\Lambda \times E$ avec E une courbe elliptique. Soit r le résultant des polynômes minimaux de la restriction de $F+V$ à E et Λ où F est l'endomorphisme de Frobenius de Jac(C) et V son dual. Alors il existe une courbe elliptique E' isogène à E et un morphisme de C sur E' dont le degré divise r.

On applique ce théorème au facteur T^2+3T+3 de (1.1). Il existe donc un revêtement de degré 3 de C vers une courbe E avec 7 points sur $\mathbb{F}_3$. A isomorphisme près cette courbe est unique d'équation $E : y^2 = x^3 - x + 1$.
Pour expliciter le revêtement, nous procédons comme suit :

- Au dessus d'au moins un point rationnel de E il existe trois points rationnels de C (éventuellement non distincts). Quitte à effectuer une translation on peut supposer que ce point est l'origine de la courbe elliptique.
- Pour chacune des $\binom{13}{1} + \binom{13}{2} + \binom{13}{3} = 377$ possibilités, on considère alors le diviseur D de degré 3 au dessus de l'origine constitué de ces trois points rationnels. Si $f : C \to E$ est le revêtement et si $g : E \to \mathbb{P}^1$ est l'application $(x:y:z) \mapsto (x:z)$

FIG. 1.1 – Ramification : cas du degré 3



alors $g \circ f \in \mathcal{L}(2D)$. Le théorème de Clifford montre que $l(2D) \leq 2$ et par Riemann-Roch on a que $l(2D) = 2$.

– Soit $\phi \in \mathcal{L}(2D)$ non constante. Pour $\psi_x = \phi, \phi + 1, \phi - 1$ on calcule $\psi^3 - \psi + 1$. Si cette fonction est le carré d'une autre fonction ψ_y alors on a le revêtement donné par $p \mapsto (\psi_x(p) : \psi_y(p) : 1)$.

Grâce à MAGMA, on réalise rapidement ces calculs. Deux modèles plans paraissent particulièrement intéressants pour C : le premier

$$x^4y^2 + x^2y^4 + y^6 + x^2 - y^2 + x^3 + xy^2 + 1 + x - x^4 = 0$$

est un modèle pour lequel l'involution est $y \mapsto -y$. Le second

$$x^4 + x^3y^3 - x^2 - xy^5 + y^5 + 2y = 0$$

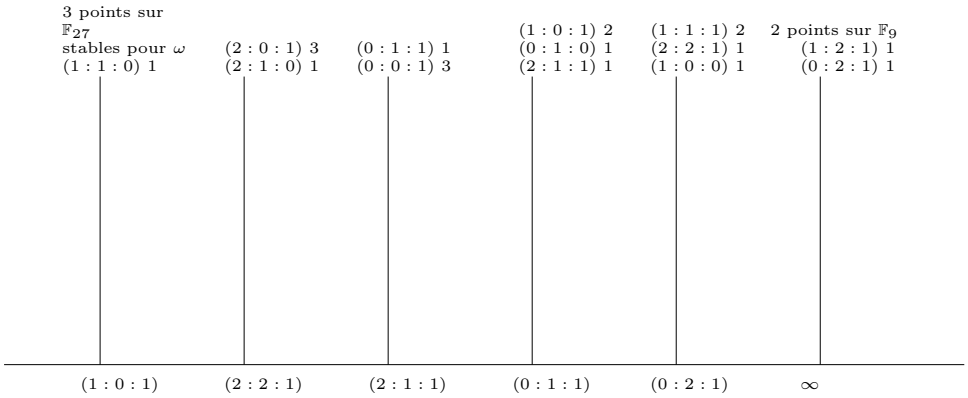
possède 13 points rationnels (tous les points de $\mathbb{P}^2(\mathbb{F}_3)$). Pour ce second modèle, un revêtement est donné par $(x : y : 1) \mapsto (x' : y' : 1)$ avec

$$\begin{cases} x' = \frac{-x^3-x^2y^3-x^2y^2+x^2+xy^5+xy^4-xy^3-xy^2+xy-y^6+y^5+y^4+y^3-y^2}{(y+1)(y-1)^2(y^3-y^2+y+1)} \\ y' = \frac{-x^3y-x^2y^5+x^2y^4-x^2y+xy^5+xy^4+xy^3-xy^2-xy+y^8+y^7+y^4-y^3-y^2-y+1}{(y+1)^2(y-1)^3(y^3-y^2+y+1)} \end{cases}$$

La figure 1.1 montre la ramification de f (le nombre derrière le point est l'indice de ramification. On constate en particulier que le revêtement est sauvagement ramifié).

Une méthode analogue permet de traiter le cas du facteur $T^2 + 2T + 3$ de (1.1). On trouve un revêtement de degré 4 dont la ramification est résumée ci-dessous :

FIG. 1.2 – Ramification : cas du degré 4



Remarque :
Dans les deux cas traités, une des fibres du revêtement est stable par l'action de l'involution (la fibre au-dessus de $(0 : 1 : 1)$ dans le premier cas et au-dessus de $(1 : 0 : 1)$ dans le second).

1.4 Conclusion

Il est tentant de chercher d'autres courbes de genre 5 revêtements d'une courbe de genre 2 afin d'évaluer leur nombre de points rationnels. On peut considérer à cet effet les courbes

$$\begin{cases} Q_1 = q_1 - x_4^2 \\ Q_2 = x_4 l_1 - x_5 l_2 \\ Q_3 = q_2 + x_5^2 \end{cases}$$

avec $q_1(x_1, x_2, x_3), q_2(x_1, x_2, x_3)$ deux formes quadratiques et $l_1(x_1, x_2, x_3), l_2(x_1, x_2, x_3)$ deux droites. Génériquement il s'agit d'une courbe de genre 5 revêtement double d'une courbe de genre 2 définie par $q_1 l_2^2 + q_2 l_1^2 = 0$. On présente ci-dessous sur $\mathbb{F}_q$ avec $q = 3, 9, 27$ les courbes obtenues sous cette forme ayant un grand nombre de points rationnels ainsi que les meilleures estimations connues en général [GV03].

3	$\begin{cases} Q_1 = -x_1x_2 + x_3x_1 + x_3^2 - x_4^2 \\ Q_2 = x_1x_4 - x_5x_2 \\ Q_3 = x_2^2 + x_1x_2 - x_3^2 + x_5^2 \end{cases}$	13	$12 - 14$
9	$\begin{cases} Q_1 = x_1^2 + x_1x_2 + x_1x_3 + wx_2x_3 - x_4^2 \\ Q_2 = x_1x_4 - x_2x_5 \\ Q_3 = x_1^2 - x_1x_2 - x_1x_3 + x_2^2 + w^6x_3^2 + x_5^2 \end{cases}$	30	$32 - 35$
27	$\begin{cases} Q_1 = -x_1x_3 + w^{17}x_2^2 + w^4x_2x_3 - x4^2 \\ Q_2 = x_1x_4 - x_2x_5 \\ Q_3 = x_1^2 + x_1x_2 + w^{16}x_2^2 + w^{11}x_2x_3 + x_3^2 + x_5^2 \end{cases}$	63	$72 - 75$

Bibliographie

[Bea77] A. Beauville : Variétés de Prym et Jacobiennes intermédiaires. Ann. Scient. Éc. Norm. Sup. 4^e série, **10**, (1977), 309-391.

[GV03] G. van der Geer et M. van der Vlugt, New table for the function $N_q(g)$, `http://www.wins.uva.nl/~geer` (2003).

[HL02] E.W. Howe & K. Lauter : Improved upper bounds for the number of points on curves over finite fields, `ArXiv:math.NT/0207101` v5, (2002).

[La99] K. Lauter : Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points, Proc. AMS **128**, (1999), 369-374.

[NX97] H. Niederreiter & C.P. Xing : Cyclotomic function fields, Hilbert class fields and global function fields with many rational places, Acta. Arithm. **79** (1997), 59-76.

Troisième partie

Méthode A.G.M.

Chapitre 1

Fonctions thêta et jacobiennes

Nous présentons ici quelques aspects classiques de la théorie des variétés abéliennes sur $\mathbb{C}$ essentiellement dans l'objectif d'obtenir des formules pour les fonctions thêta et les relations avec les jacobiennes de courbes. Ces résultats sont principalement issus de [Deb99], [Mum83], [RF74] et [Ros86] pour lesquels on a essayé d'harmoniser les notations.

1.1 Théorie élémentaire des fonctions thêta

1.1.1 Quelques rappels théoriques

Soit $A/\mathbb{C}$ une variété abélienne (i.e un groupe algébrique complet sur $\mathbb{C}$ et connexe) de dimension g. On sait qu'alors $A(\mathbb{C})$ est un tore complexe $\mathbb{C}^g/\Lambda$ où Λ est un réseau, que l'on peut définir intrinsèquement par $\mathrm{H}^0(A,\Omega^1)^*/\mathrm{H}_1(A,\mathbb{Z})$ où

$$\begin{array}{ccc} \mathrm{H}_1(A,\mathbb{Z}) & \hookrightarrow & \mathrm{H}^0(A,\Omega^1)^* \\ \gamma & \mapsto & \omega \mapsto \displaystyle\int_\gamma \omega \end{array}$$

Tous les tores complexes ne sont pas des variétés abéliennes. Celles-ci sont caractérisées par l'existence d'une forme hermitienne dite forme de Riemann qui est de plus définie positive.

Définition 1.1
On appelle forme de Riemann sur $A(\mathbb{C})$ une forme hermitienne H sur $\mathbb{C}^g$ telle que la forme réelle alternée $E = \mathrm{Im}(H)$ prenne des valeurs entières sur le réseau, i.e. $E(\lambda_1,\lambda_2) \in \mathbb{Z}$ $\forall \lambda_1,\lambda_2 \in \Lambda$.

De même que l'étude des courbes passe par l'étude des diviseurs ou de manière équivalente par l'étude des fibrés inversibles, on étudie les fibrés en droites sur A. Tout fibré en droites à isomorphisme près est caractérisé par un couple (H,α) appelé type du fibré où H est une forme de Riemann et α un semi-caractère pour H (cf. [Deb99, p. 39]). Ce type caractérise également les sections du fibré.

Définition 1.2
On appelle fonction thêta (normalisée) de type (H, α) une section du fibré correspondant, qu'on identifie à une fonction méromorphe de $\mathbb{C}^g$ vérifiant

$$\forall z \in \mathbb{C}^g,\ \forall \lambda \in \Lambda,\ \vartheta(z+\lambda) = \alpha(\lambda) \cdot q^{-i/2H(\lambda,\lambda)-iH(z,\lambda)} \cdot \vartheta(z)$$

où $q = \exp(i\pi)$ (avec la convention $q^z = \exp(i\pi z)$ pour tout $z \in \mathbb{C}$).

Remarquons qu'on obtient une autre normalisation en multipliant ces fonctions thêta par des fonctions thêta triviales (i.e. de la forme $q^{2(Q(z)+l(z)+c)}$ où Q est une forme quadratique, l une forme linéaire et c une constante).

On peut facilement calculer la dimension de l'espace des sections grâce au lemme suivant.

Lemme 1.3 [Ros86]
Soit Λ un $\mathbb{Z}$-module libre de rang $2g$ et E une forme alternée non dégénérée sur Λ. Il existe alors une base $\{\lambda_1, \ldots, \lambda_{2g}\}$de Λ, dite base symplectique, telle que la matrice de E dans cette base soit $\begin{pmatrix} 0 & E_1 \\ -E_1 & 0 \end{pmatrix}$ avec E_1 une matrice diagonale dont les termes diagonaux sont des entiers positifs e_i vérifiant $e_1 | \ldots | e_g$.
On appelle Pfaffien de E et on note $\mathrm{Pf}(E) = e_1 e_2 \ldots e_g$.

En fait, le Pfaffien peut être défini indépendant du choix d'une base. En particulier, si L est de type (H, α) avec $E = \mathrm{Im}(H)$ non dégénérée, on note $\mathrm{Pf}(L) = \mathrm{Pf}(E)$. On a le résultat suivant.

Théorème 1.4 [Ros86]
Soit L un fibré de type (H, α) tel que H soit définie positive. Alors $E = \mathrm{Im}(H)$ est non dégénérée et la dimension de l'espace des sections holomorphes de L est $\mathrm{Pf}(E)$.

Comme dans le cas des courbes, certains fibrés permettent alors de réaliser un plongement projectif de A. Plus précisément,

Théorème 1.5 (Lefschetz) [Deb99]
Soit A une variété abélienne et L un fibré en droite de type (H, α). Le fibré L est ample si et seulement si H est définie positive. Si tel est le cas, L^n est très ample (i.e. définit un plongement projectif de A) pour tout $n \geq 3$.

Remarque :
En fait E, et donc H, peut être définie plus intrinsèquement comme la première classe de Chern de L. Le théorème précédent est donc un cas particulier d'un théorème de Kodaira. (cf. [Deb99, VI.3.6]).
Dans le cas des courbes elliptiques, L est défini par un diviseur $D = \sum P_i$. La forme hermitienne H est alors un entier égal au degré de D.

L'ensemble des fibrés en droites sur A à isomorphisme près est muni d'une structure de groupe. On appelle groupe de Picard cet ensemble, noté $\mathrm{Pic}(A)$. Ce groupe est isomorphe au groupe des diviseurs de A, $\mathrm{Div}(A)$, quotienté par le groupe des diviseurs principaux, $\mathrm{Princ}(A)$ (cf. [Deb99, V.1.5]). On introduit également le sous-groupe $\mathrm{Div}_a(A)$ correspondant au sous-groupe des diviseurs dont le fibré associé possède une forme de Riemann nulle (il est dit algébriquement équivalent à 0) et on note $\mathrm{Pic}^0(A) = \mathrm{Div}_a(A)/\mathrm{Princ}(A)$. On peut alors montrer que $\mathrm{Pic}(A)$ et $\mathrm{Pic}^0(A)$ sont munies d'une structure de variété et on appelle $\mathrm{Pic}^0(A)$ la variété duale de A, notée $\hat{A}$. Du point de vue des tores, on a alors le résultat suivant :

Proposition 1.6 [Ros86]
Il existe un isomorphisme entre $Pic^0(A)$ et le dual de Pontryagin de Λ qui à un diviseur D dont le fibré a pour type $(0, \alpha)$ associe α.

Comme A est une variété abélienne, il existe sur A une forme de Riemann définie positive. Notons $E = \mathrm{Im}(H)$. Soit ϑ une fonction thêta associée à un fibré possédant cette forme de Riemann. La fonction thêta normalisée associée à $\vartheta(z+t)/\vartheta(z)$, pour $t \in \mathbb{C}^g$, a pour multiplieur $e^{-2i\pi E(t,\lambda)}$, pour $\lambda \in \Lambda$. Le diviseur associé à cette fonction est donc algébriquement équivalent à 0. D'autre part comme E est non dégénérée tout caractère de Λ est de cette forme. On a donc :

Corollaire 1.7 [Deb99, VI.4.2]
Si L est un fibré ample, l'application

$$\begin{array}{rcl} \phi_L : A & \to & \hat{A} \\ x & \mapsto & \tau_x^*(L) \otimes L^{-1} \end{array}$$

où τ_x est le morphisme de translation par x est une isogénie de degré $\det(E) = \mathrm{Pf}(L)^2$.

Cela nous permet d'introduire la notion de polarisation :

Définition 1.8
Une polarisation sur une variété abélienne $A/\mathbb{C}$ est une isogénie $\lambda : A \to \hat{A}$ telle que $\lambda = \phi_L$ pour un fibré ample L sur A.
On dit que λ est une polarisation principale si λ est un isomorphisme.

Une variété abélienne munie d'une polarisation (principale) est dite polarisée (principalement polarisée). Remarquons que cette définition est équivalente à se donner une variété abélienne avec une classe d'équivalence de plongements projectifs ou encore en termes de tores à se donner une forme de Riemann H définie positive à «translation près». En particulier, la polarisation est principale si et seulement si $E = \mathrm{Im}(H)$ est telle que $\mathrm{Pf}(E) = 1$ c'est-à-dire s'il existe une base symplectique de Λ telle que E ait pour matrice $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ dans cette base.

Proposition 1.9 [Deb99, VI.6.3]
Toute variété abélienne est isogène à une variété abélienne principalement polarisée. Plus précisément pour tout fibré en droites ample L sur A, il existe une variété abélienne B, un fibré en droites ample M définissant une polarisation principale sur B, et une isogénie $u : A \to B$ telle que $L \simeq u^*M$.

Remarque :
Le cas des variétés abéliennes principalement polarisées est particulièrement important. Par exemple si C est une courbe de genre g alors $\mathrm{Jac}(C) = \mathrm{Pic}^0(C)$ est une variété abélienne. De plus le choix d'un point $P_0 \in C$ définit un morphisme de $C \to \mathrm{Jac}(C)$ donné par $P \mapsto (P - P_0)$. L'image de C^{g-1} par ce morphisme définit un unique diviseur sur $\mathrm{Jac}(C)$ à translation près, noté Θ. Le fibré associé à ce diviseur défini une polarisation principale ([GH78, II.7]).

Nous allons maintenant montrer comment on se ramène à la situation classique que nous considérerons par la suite.
Soit $A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ une variété abélienne que l'on suppose principalement polarisée. Si on note H la forme de Riemann associée à cette polarisation et $E = \mathrm{Im}(H)$, alors il existe une base de Λ que l'on note $(\Gamma, \Delta) = (\gamma_1, \ldots, \gamma_g, \delta_1, \ldots, \delta_g)$ pour laquelle la matrice de E est $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. Quitte à faire un changement de base de $\mathbb{C}^g$, on peut alors prendre les vecteurs γ_i comme base de $\mathbb{C}^g$ et dans ce cas $A(\mathbb{C}) = \mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g\Omega$ où Ω est une matrice $g \times g$ qui, en raison des conditions sur H, est symétrique de partie imaginaire définie positive.

Définition 1.10
La matrice Ω est une matrice de Riemann de A.
L'ensemble des matrices complexes $g \times g$ symétriques de partie imaginaire définie positive est appelé demi-plan de Siegel, noté $\mathbb{H}_g$.

Remarque :
Par la suite, pour alléger les notations, nous noterons abusivement par des multiplications les produits scalaires et matriciels et nous omettrons les symboles «transpositions» lorsque le contexte est clair. Si e est un vecteur, ses composantes seront habituellement notées $(e_1, \ldots, e_g)$.

Considérons le fibré L de type (H, α) où $\alpha(\sum n_i\gamma_i + m_i\delta_i) = (-1)^{nm}$, pour $m, n \in \mathbb{Z}^g$. Il possède à un facteur multiplicatif près une seule section holomorphe ϑ telle que

$$\vartheta(z + \sum n_i\gamma_i + m_i\delta_i) = q^{-m\Omega m - 2mz}\vartheta(z)$$

(on n'obtient pas la formule de la définition 1.2 car la normalisation a été choisie différemment (cf. [Deb99, p.65,p.91])). On montre alors (cf. [Mum83, I,p.121]) qu'une telle

fonction s´écrit

$$\vartheta(z,\Omega) := \vartheta(z) = \sum_{n\in\mathbb{Z}^g} q^{n\Omega n+2nz}.$$

En particulier $\vartheta(-z,\Omega) = \vartheta(z,\Omega)$. Le fibré L est donc un fibré symétrique (i.e. $i^*(L) = L$ où $i : A \to A$, $x \mapsto -x$).

Cette formulation est le point de départ de l'étude menée par [Mum83] et [RF74] et dont nous allons rappeler certains aspects.

1.1.2 Premières propriétés

On reprend les notations de la fin de section précédente.

Définition 1.11
Soit $g \geq 1$. On appelle (thêta)-caractéristique une matrice $2 \times g$ de rationnels $\begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$ (qu'on note en abrégé $[\epsilon]$).
Lorsque ces éléments sont des entiers, on dit que $\begin{bmatrix} \varepsilon \\ \varepsilon \end{bmatrix}$ est paire (resp. impaire) si $\varepsilon\varepsilon' = 0$ (resp. 1) (mod 2). On appelle caractéristique réduite la matrice obtenue en réduisant modulo 2 les coefficients.

On considère alors des translatés de la fonction $\vartheta(z,\Omega)$ précédemment introduite.

Définition 1.12
On appelle fonction thêta caractéristique (de caractéristique $\begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$) la fonction

$$\vartheta[\epsilon](z,\Omega) = \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}(z,\Omega) = \sum_{n\in\mathbb{Z}^g} q^{(n+\varepsilon/2)\Omega(n+\varepsilon/2)+2(n+\varepsilon/2)(z+\varepsilon'/2)}.$$

On note aussi $\vartheta(z,\Omega) = \vartheta[0](z,\Omega) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(z,\Omega)$.

Remarque :
Attention aux facteurs 1/2 par rapport aux conventions de Mumford. C'est ici la convention plus géométrique du XIXème siècle qui est adoptée (comme dans [RF74]) en vue d'étudier spécifiquement les caractéristiques entières (voir chapitre 3).

Définition 1.13
Une période est un élément du réseau. On note $\begin{Bmatrix} \mu \\ \mu' \end{Bmatrix} = \sum \mu'_i\gamma_i + \sum \mu_i\delta_i$ avec $\mu, \mu' \in \mathbb{Z}^g$ (dans cet ordre).
Une demi-période est notée $\begin{pmatrix} \mu \\ \mu' \end{pmatrix} = \frac{1}{2}\begin{Bmatrix} \mu \\ \mu' \end{Bmatrix}$. C'est un élément de $A[2](\mathbb{C})$. Ces

éléments seront particulièrement importants par la suite. On note ainsi $e_i = \gamma_i/2$ *et* $f_i = \delta_i/2$.
A une caractéristique $[\epsilon] = \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$ *on associe le point de* $A(\mathbb{C})$, $\epsilon := \sum \varepsilon'_i e_i + \sum \varepsilon_i f_i$.
Inversement si ϵ *est un point de torsion de* $A(\mathbb{C})$ *on peut lui associer une caractéristique notée* $[\epsilon]$. *En particulier les caractéristiques réduites sont en bijection explicite avec les points de 2-torsion de A.*

On a alors les propriétés de quasi-périodicités suivantes :

Proposition 1.14

$$\vartheta \begin{bmatrix} \varepsilon + 2n \\ \varepsilon' + 2m \end{bmatrix} = q^{\varepsilon m} \cdot \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z, \Omega)$$

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z + \begin{Bmatrix} \mu \\ \mu' \end{Bmatrix}, \Omega) = q^{\varepsilon\mu' - \varepsilon'\mu - 2\mu z - \mu\Omega\mu} \cdot \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z, \Omega)$$

et

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z + \begin{pmatrix} \mu \\ \mu' \end{pmatrix}, \Omega) = q^{-\frac{1}{2}\mu(\varepsilon' + \mu') - \mu z - \frac{1}{4}\mu\Omega\mu} \cdot \vartheta \begin{bmatrix} \varepsilon + \mu \\ \varepsilon' + \mu' \end{bmatrix} (z, \Omega).$$

Lorsque la caractéristique est de plus entière, on a les propriétés suivantes :

Proposition 1.15

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (-z, \Omega) = (-1)^{\varepsilon\varepsilon'} \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z, \Omega).$$

En particulier $\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$ *est paire (resp. impaire) si et seulement si sa caractéristique l'est.*
Si $\varepsilon = \hat{\varepsilon} + 2\nu$ *et* $\varepsilon' = \hat{\varepsilon}' + 2\nu'$ *alors* $\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (z, \Omega) = (-1)^{\varepsilon\nu'} \vartheta \begin{bmatrix} \hat{\varepsilon} \\ \hat{\varepsilon}' \end{bmatrix} (z, \Omega)$.

Remarque :
On aura souvent à considérer des expressions impliquant des carrés de fonctions thêta de caractéristiques entières, on pourra donc utiliser la caractéristique réduite sans problème de signe.

Définition 1.16
Lorsque la caractéristique $[\epsilon]$ *est paire, on appelle thêta constante (de caractéristique* $[\epsilon]$*) la valeur* $\vartheta[\epsilon](0, \Omega)$. *S'il n'y a pas de risque de confusion on la note également* $\vartheta[\epsilon](\Omega)$.

L'introduction des fonctions thêta caractéristiques est justifiée par l'existence de certains espaces dont elles forment une base.

Définition 1.17
Soit f une fonction entière sur $\mathbb{C}^g$. Elle est dite quasi-périodique de poids l si

$$\forall m \in \mathbb{Z}^g,\ \begin{cases} f(z+m) = f(z) \\ f(z+m\Omega) = q^{-lm\Omega m - 2lmz} f(z) \end{cases}$$

On note R_l^Ω cet espace vectoriel.

Remarque :
Il est facile de constater que ces espaces ne sont rien d'autres que les espaces vectoriels des sections holomorphes des fibrés L^l.

Proposition 1.18
Une base de R_l^Ω est donnée par (attention aux coquilles dans [Mum83])

- *soit* $f_\varepsilon(z) = \vartheta \begin{bmatrix} 2\varepsilon/l \\ 0 \end{bmatrix} (lz, l\Omega)$ *avec* $\varepsilon \in \mathbb{Z}^g/l\mathbb{Z}^g$.
- *soit* $g_{\varepsilon'}(z) = \vartheta \begin{bmatrix} 0 \\ 2\varepsilon'/l \end{bmatrix} (z, \Omega/l)$ *avec* $\varepsilon' \in \mathbb{Z}^g/l\mathbb{Z}^g$.
- *soit si* $l = k^2$, $h_{\varepsilon,\varepsilon'}(z) = \vartheta \begin{bmatrix} 2\varepsilon/k \\ 2\varepsilon'/k \end{bmatrix} (kz, \Omega)$ *avec* $\varepsilon, \varepsilon' \in \mathbb{Z}^g/k\mathbb{Z}^g$.

On notera en exposant le poids l et on précisera également la matrice si besoin.
On a les expressions de changement de base suivantes :

$$g_{\varepsilon'} = \sum_{\varepsilon \in \mathbb{Z}^g/l\mathbb{Z}^g} q^{2\varepsilon\varepsilon'/l} f_\varepsilon \tag{1.1}$$

$$h_{\varepsilon,\varepsilon'} = \sum_{\mu \equiv \varepsilon \pmod{k}} q^{2\mu\varepsilon'/l} f_\varepsilon \tag{1.2}$$

$$f_\varepsilon = \frac{1}{k^g} \sum_{\mu \in \mathbb{Z}^g/k\mathbb{Z}^g} q^{-2\varepsilon\mu/l} h_{\varepsilon\mu} \tag{1.3}$$

$$g_{\varepsilon'} = \sum_{\mu \in \mathbb{Z}^g/k\mathbb{Z}^g} h_{\mu\varepsilon'} \tag{1.4}$$

Démonstration :
Montrons par exemple (1.3) et (1.4).

$$\begin{aligned} \sum_\mu q^{-2\varepsilon\mu/l} h_{\varepsilon\mu} &= \sum_\mu \sum_n q^{-2\varepsilon\mu/l} q^{(\varepsilon/k+n)\Omega(\varepsilon/k+n)+2(\varepsilon/k+n)(kz+\mu/k)} \\ &= \sum_n q^{(\varepsilon/l+n/k)l\Omega(\varepsilon/l+n/k)+2(\varepsilon/l+n/k)lz} \underbrace{\sum_\mu q^{2n\mu/k}}_{=k^g \text{ si } k|n, 0 \text{ sinon}} \\ &= k^g f_\varepsilon \end{aligned}$$

Ce qui donne bien le résultat attendu.
De même

$$\begin{aligned}\sum_{\mu} h_{\mu\varepsilon'} &= \sum_{\mu}\sum_{n} q^{(\mu/k+n)\Omega(\mu/k+n)+2(\mu/k+n)(kz+\varepsilon'/k)} \\ &= \sum_{n}\sum_{\mu} q^{(\mu+kn)\Omega/l(\mu+kn)+2(\mu+ln)(z+\varepsilon'/l)} \\ &= g_{\varepsilon'}\end{aligned}$$

car $\mu + kn$ décrit $\mathbb{Z}^g$.

Exemple :
Prenons $g = 1$ et $l = 4$. On a

$$\begin{cases} f_\varepsilon = \vartheta \begin{bmatrix} \varepsilon/2 \\ 0 \end{bmatrix} (4z, 4\Omega)\ , 0 \leq \varepsilon < 4 \\ g_{\varepsilon'} = \vartheta \begin{bmatrix} 0 \\ \varepsilon'/2 \end{bmatrix} (z, \Omega/4)\ , 0 \leq \varepsilon < 4 \\ h_{\varepsilon,\varepsilon'} = \vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} (2z, \Omega)\ , 0 \leq \varepsilon, \varepsilon' < 2 \end{cases}$$

d'où

$$\begin{array}{ll} f_0(z) = \frac{1}{2}(\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2z,\Omega) + \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2z,\Omega)) & g_0(z) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2z,\Omega) + \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (2z,\Omega) \\ f_1(z) = \frac{1}{2}(\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (2z,\Omega) - i\vartheta \begin{bmatrix} 1 \\ 1 \end{bmatrix} (2z,\Omega) & g_1(z) = \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2z,\Omega) + \vartheta \begin{bmatrix} 1 \\ 1 \end{bmatrix} (2z,\Omega) \\ f_2(z) = \frac{1}{2}(\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2z,\Omega) - \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2z,\Omega)) & g_2(z) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2z,\Omega) - \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2z,\Omega) \\ f_3(z) = \frac{1}{2}(\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (2z,\Omega) + i\vartheta \begin{bmatrix} 1 \\ 1 \end{bmatrix} (2z,\Omega)) & g_3(z) = \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2z,\Omega) - \vartheta \begin{bmatrix} 1 \\ 1 \end{bmatrix} (2z,\Omega) \end{array}$$

1.1.3 Equations définissant les variétés abéliennes

Nous avons vu que le théorème de Lefschetz 1.5 permet de définir un plongement de A dans un espace projectif grâce à L^n avec $n \geq 3$. Les bases précédemment introduites pour les espaces des sections holomorphes de ces fibrés permettent de préciser ce plongement. Par exemple pour $n = 4$ on a un plongement que l'on peut définir soit par

$$z \mapsto (\ldots : f_\varepsilon : \ldots)_{\varepsilon \in \mathbb{Z}^g/4\mathbb{Z}^g}$$

ou

$$z \mapsto (\ldots : g_{\varepsilon'} : \ldots)_{\varepsilon' \in \mathbb{Z}^g/4\mathbb{Z}^g}$$

ou encore par

$$z \mapsto (\ldots : h_{\varepsilon\varepsilon'} : \ldots)_{\varepsilon,\varepsilon' \in \mathbb{Z}^g/2\mathbb{Z}^g}$$

De plus Mumford montre dans [Mum83] comment obtenir des équations explicites pour des quadriques contenant l'image de A par le premier plongement. Ces formules reposent sur les deux formules, dites formules de duplication, suivantes :

Proposition 1.19 [RF74, Cor.IIA2.1],[Igu72, IV.th.2]

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}(z_1, 2\Omega) \cdot \vartheta \begin{bmatrix} \delta \\ \delta' \end{bmatrix}(z_2, 2\Omega) = \frac{1}{2^g} \sum_{\mu \in \mathbb{Z}^g/2\mathbb{Z}^g} q^{-\mu\varepsilon} \cdot \vartheta \begin{bmatrix} \varepsilon+\delta \\ \frac{\varepsilon'+\delta'}{2} + \mu \end{bmatrix}(\frac{z_1+z_2}{2}, \Omega) \cdot \vartheta \begin{bmatrix} \varepsilon-\delta \\ \frac{\varepsilon'-\delta'}{2} + \mu \end{bmatrix}(\frac{z_1-z_2}{2}, \Omega).$$

$$\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}(z_1, \Omega) \cdot \vartheta \begin{bmatrix} \delta \\ \delta' \end{bmatrix}(z_2, \Omega) = \sum_{\mu \in (\mathbb{Z}/2\mathbb{Z})^g} \vartheta \begin{bmatrix} \frac{\varepsilon+\delta}{2} + \mu \\ \varepsilon' + \delta' \end{bmatrix}(z_1+z_2, 2\Omega) \cdot \vartheta \begin{bmatrix} \frac{\varepsilon-\delta}{2} + \mu \\ \varepsilon' - \delta' \end{bmatrix}(z_1-z_2, 2\Omega).$$

Soit alors $X_\varepsilon = f_\varepsilon \in R_4^\Omega$. Des transformations élémentaires des formules ci-dessous permettent de donner les équations quadratiques suivantes

$$\lambda_{(c-d)\mu} \sum_{e \in \mathbb{Z}^g/2\mathbb{Z}^g} q^{e\mu} X_{a+2e} \cdot X_{b+2e} = \lambda_{(a-b)\mu} \sum_{e \in \mathbb{Z}^g/2\mathbb{Z}^g} q^{e\mu} X_{c+2e} X_{d+2e} \tag{1.5}$$

avec $a + b \equiv c + d \pmod{4\mathbb{Z}^g}$ et $\mu \in \mathbb{Z}^g/2\mathbb{Z}^g$. Les constantes sont définies par

$$\lambda_{x\mu} = \sum_{e \in \mathbb{Z}^g/2\mathbb{Z}^g} q^{e\mu} f^{(8)}_{x+4e}(0)$$

(si $\mu = 0$ on note simplement λ_x).
On a les mêmes expressions en remplaçant formellement X_ε par $Y_{\varepsilon'} = g_{\varepsilon'}$ et f par g (on note alors $\lambda'_{x\mu}$ les nouvelles constantes).

En fait on a une expression plus simple pour ces constantes :

Lemme 1.20
$\forall x \in \mathbb{Q}^g$ et $\mu \in \mathbb{Z}^g/2\mathbb{Z}^g$ on a

$$\lambda_{x\mu} = q^{-\mu x/2} h^{(4)}_{x/2\mu}(0, 2\Omega)$$

et

$$\lambda'_{x\mu} = 2^g h^{(4)}_{\mu x/2}(0, \Omega/2).$$

Démonstration :
Montrons par exemple la deuxième formule :

$$\begin{aligned}
\lambda'_{x\mu} &= \sum_e q^{e\mu} g^{(8)}_{x+4e}(0) \\
&= \sum_e q^{e\mu} \vartheta \begin{bmatrix} 0 \\ x/4+e \end{bmatrix} (0, \Omega/8) \\
&= \sum_e q^{e\mu} g^{(4)}_{x/2+2e}(0, \Omega/2) \\
&= \sum_e \sum_\varepsilon q^{e\mu} h_{\varepsilon(x/2+2e)}(0, \Omega/2) \\
&= \sum_\varepsilon h_{\varepsilon x/2}(0, \Omega/2) \underbrace{\sum_e q^{(\varepsilon+\mu)e}}_{=0 \text{ sauf si } \varepsilon=\mu} \\
&= 2^g h_{\mu x/2}(0, \Omega/2).
\end{aligned}$$

Une autre expression utile pour les constantes est simplement de remarquer qu'elles sont déterminées par la valeur $z = 0$:

Corollaire 1.21
Si $a+b \equiv c+d \pmod{4\mathbb{Z}^g}$ et $\mu \in \mathbb{Z}^g/2\mathbb{Z}^g$ les deux plongements précédents sont contenus respectivement dans l'intersection des quadriques

$$\begin{aligned}
&\left(\sum_e q^{e\mu} X_{c+2e}(0) \cdot X_{d+2e}(0)\right) \cdot \left(\sum_e q^{e\mu} X_{a+2e} \cdot X_{b+2e}\right) = \\
&\left(\sum_e q^{e\mu} X_{a+2e}(0) \cdot X_{b+2e}(0)\right) \cdot \left(\sum_e q^{e\mu} X_{c+2e} \cdot X_{d+2e}\right).
\end{aligned} \tag{1.6}$$

et

$$\begin{aligned}
&\left(\sum_e q^{e\mu} Y_{c+2e}(0) \cdot Y_{d+2e}(0)\right) \cdot \left(\sum_e q^{e\mu} Y_{a+2e} \cdot Y_{b+2e}\right) = \\
&\left(\sum_e q^{e\mu} Y_{a+2e}(0) \cdot Y_{b+2e}(0)\right) \cdot \left(\sum_e q^{e\mu} Y_{c+2e} \cdot Y_{d+2e}\right).
\end{aligned} \tag{1.7}$$

Enfin on peut donner le plongement en les $Z_{\varepsilon,\varepsilon'} = h_{\varepsilon,\varepsilon'}$. On a

$$\begin{aligned}
\sum_e q^{e\mu}\, Y_{a+2e} \cdot Y_{b+2e} &= \sum_e q^{e\mu} \sum_\varepsilon h_{\varepsilon(a+2e)} \sum_{\varepsilon'} h_{\varepsilon'(b+2e)} \\
&= \sum_{\varepsilon,\varepsilon'} h_{\varepsilon a}\, h_{\varepsilon' b} \sum_e q^{e(\mu+\varepsilon+\varepsilon')} \\
&= 2^g \sum_\delta Z_{\delta a} \cdot Z_{(\mu+\delta)b}
\end{aligned}$$

D'où :

Corollaire 1.22
Avec les mêmes conditions pour a, b, c, d et μ on a

$$\left(\sum_{\varepsilon} Z_{(\mu+\varepsilon)c}(0) \cdot Z_{\varepsilon d}(0)\right) \cdot \left(\sum_{\varepsilon} Z_{(\mu+\varepsilon)b} \cdot Z_{\varepsilon a}\right) = \left(\sum_{\varepsilon} Z_{(\mu+\varepsilon)a}(0) \cdot Z_{\varepsilon b}(0)\right) \cdot \left(\sum_{\varepsilon} Z_{(\mu+\varepsilon)c} \cdot Z_{\varepsilon d}\right). \tag{1.8}$$

Ces équations sont fondamentales : d'une part le plongement de A n'est pas seulement contenu dans l'intersection de ces quadriques, il est égal à celle-ci comme l'ont montré Kempf et Mumford (cf. [Mum66]). D'autre part comme l'a montré ce dernier, ces équations sont en un sens universel : elles sont valables pour toute variété abélienne sur un corps algébriquement clos de caractéristique différente de 2 dès lors que l'on donne une bonne généralisation de la notion de thêta constantes. Les formules (1.6), (1.7), (1.8) montrent que si l'origine est définie sur K alors les équations le sont aussi. Remarquons que pour les deux premières modèles cette condition implique que la moitié des points d'ordre 4 est définie sur K et pour le dernier la totalité des points d'ordre 2.

1.1.4 Formules de transformation

Lorsque A est une variété abélienne principalement polarisée, on a vu qu'on peut lui associer une matrice symplectique $\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. On introduit alors le groupe symplectique $\mathrm{Sp}(2g, \mathbb{R})$ qui est l'ensemble des matrices réelles $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ qui respecte la polarisation, i.e.

$${}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

On rappelle également la notation $\mathbb{H}_g$ pour l'ensemble des matrices Ω complexes symétriques de partie imaginaire définie positive. On montre alors :

Proposition 1.23 [Mum83]
$Sp(2g, \mathbb{R})$ agit sur $\mathbb{C}^g \times \mathbb{H}_g$ par

$$(z, \Omega) \mapsto ((C\Omega + D)^{-1}z, (A\Omega + B)(C\Omega + D)^{-1}).$$

De plus l'action est transitive sur $\mathbb{H}_g$.

Cette action peut être utilisée sur les fonctions thêta. On ne peut espérer de relation intéressante pour tout $\mathrm{Sp}(2g, \mathbb{R})$ (puisque l'action est transitive), mais pour les éléments de $\Gamma_g(1) = \mathrm{Sp}(2g, \mathbb{Z})$ on a le théorème fondamental suivant dit «formule de transformation» :

Proposition 1.24 [Igu72, V.§.2]

Soit $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z})$. *On a*

$$\begin{aligned} \vartheta \begin{bmatrix} 2(D\varepsilon - C\varepsilon') + (C^t D)_0 \\ 2(-B\varepsilon + A\varepsilon') + (A^t B)_0 \end{bmatrix} (0, (A\Omega + B)(C\Omega + D)^{-1}) = \\ \kappa(M) \cdot q^{\phi_{[\varepsilon]}(M)} \cdot \det(C\Omega + D)^{1/2} \cdot \vartheta \begin{bmatrix} 2\varepsilon \\ 2\varepsilon' \end{bmatrix} (0, \Omega) \end{aligned} \tag{1.9}$$

où A_0 *désigne la diagonale de* A, $\kappa(M)^2$ *une racine de l'unité ne dépendant que de* M *et*

$$\phi_{[\epsilon]}(M) = -\varepsilon^t DB\varepsilon + 2\varepsilon^t BC\varepsilon' - \varepsilon'^t CA\varepsilon' + (D\varepsilon' - C\varepsilon) \cdot (A^t B)_0.$$

Pour préciser la nature de $\kappa(M)^2$, nous allons introduire certains sous-groupes de $\Gamma_g(1)$.

Définition 1.25
Soit $N > 1$. *On appelle groupe modulaire de niveau* N *l'ensemble des matrices* $M \in \Gamma_g(1)$ *telles que* $M \equiv Id_{2g} \pmod N$. *Cette notion généralise celle de groupe modulaire pour les courbes modulaires* $X(N)$ *évoquée dans la partie I.*
On introduit également des groupes intermédiaires : $\Gamma_g(1,2)$ *l'ensemble des matrices* $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g(1)$ *telles que* $({}^tAC)_0$ *et* $({}^tBD)_0$ *soient paires et pour tout* $N > 0$ *pair,* $\Gamma_g(N, 2N)$, *l'ensemble des matrices* $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g(N)$ *telles que* $2N$ *divise* B_0 *et* C_0.

Remarque :
$\Gamma_g(4) \subset \Gamma_g(2,4) \subset \Gamma_g(2) \subset \Gamma_g(1,2) \subset \Gamma_g(1)$.
Pour $g = 1$, $\Gamma_1(4) = \Gamma_1(2,4)$.

On a alors :

Théorème 1.26 [Igu72, V.§.3]
$\kappa(M)^8 = 1$ *pour tout* $M \in \Gamma_g(1)$.
$M \mapsto \kappa(M)^2$ *est un caractère du groupe* $\Gamma_g(1,2)$.
Soit $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g(2)$ *on a*

$$\kappa(M)^2 = (-1)^{\mathrm{Tr}(D - Id)/2} = \pm 1.$$

En particulier $\kappa(M)^2 = 1$ *si* $M \in \Gamma_g(2,4)$.

On en déduit facilement :

Corollaire 1.27
Soit $[\epsilon]$ une caractéristique entière alors si $M \in \Gamma_g(2)$ on a

$$\vartheta \left[\begin{array}{c} \varepsilon \\ \varepsilon' \end{array} \right] (0, (A\Omega + B)(C\Omega + D)^{-1})^2 = \pm \det(C\Omega + D) \cdot \vartheta \left[\begin{array}{c} \varepsilon \\ \varepsilon' \end{array} \right] (0, \Omega)^2$$

avec le signe + si $M \in \Gamma_g(2, 4)$.

Les interprétations modulaires de ces sous-groupes sont bien connues. Rappelons-les dans les cas qui nous intéressent (cf. [Cha86]) :

- $\mathbb{H}_g/\Gamma_g(1)$ classifie les variétés abéliennes principalement polarisées à isomorphisme près.
- Plus généralement $\mathbb{H}_g/\Gamma_g(N)$ classifie les variétés abéliennes principalement polarisées (A, λ) munies d'un isomorphisme $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^g \times \mu_n^g$ respectant le couplage de Weil, à isomorphisme près.
- $\mathbb{H}_g/\Gamma_g(1, 2)$ classifie les variétés abéliennes principalement polarisées à isomorphisme près respectant le couplage de Weil sur $A[2] \times A[2]$.

1.2 Fonctions thêta et jacobienne

Comme nous l'avons vu dans le paragraphe précédent, si C est une courbe alors sa jacobienne $\mathrm{Jac}(C)$ est une variété abélienne principalement polarisée. Si C est une courbe algébrique (lisse) sur $k = \mathbb{C}$, c'est aussi une surface de Riemann et de nombreux résultats permettent d'étudier les diviseurs sur cette surface grâce aux fonctions thêta. Nous donnons ici pour références ultérieures et sans démonstration (cf. [RF74]) ces théorèmes fondamentaux.

1.2.1 Notations

On note

- $\mathrm{Div}(C)$ l'ensemble des diviseurs de C.
- $\mathrm{Div}^n(C)$ l'ensemble des diviseurs de degré n de C pour $n \in \mathbb{Z}$.
- $\mathrm{D}^n(C)$ l'ensemble des diviseurs effectifs de degré n pour $n > 0$.
- $\mathrm{Princ}(C)$ l'ensemble des diviseurs principaux de C.
- $k(C)$ le corps des fonctions rationnelles sur une courbe C.
- On note pour deux diviseurs $\sim$ la relation d'équivalence linéaire (i.e. $D \sim D'$ si et seulement si il existe $f \in k(C)$ tel que $(f) = D - D'$).
- $\mathrm{Pic}(C)$ l'ensemble des fibrés inversibles sur C à isomorphisme près.
- $\mathrm{ind}(D)$ l'indice d'un diviseur (i.e $\dim \mathcal{L}(K - D)$ où K est le diviseur canonique).

Soit C une surface de Riemann de genre $g > 0$. On note (Γ, Δ) une base symplectique de l'homologie, $\zeta = (\zeta_1, \ldots, \zeta_g)$ des différentielles régulières normales par rapport à cette base (i.e. si $\gamma_1, \ldots, \gamma_g$ est la base Γ, $\int_{\gamma_j} \zeta_i = \delta_{ij}$) et Ω la matrice de Riemann. Soit $P_0 \in C$

et $D = \sum_{i=1}^{n} P_i$ un diviseur effectif on note

$$u_{P_0}(D) = \sum_{i=1}^{n} \int_{P_0}^{P_i} \zeta$$

vu comme un élément de $\mathrm{Jac}(C) = \mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g\Omega$ (où cette somme est bien définie puisqu'elle est définie à une période près.) On peut prolonger par linéarité cette définition à tous les diviseurs. On définit $u : \mathrm{Div}^0(C) \to \mathrm{Jac}(C)$ l'application u_{P_0} qui ne dépend pas du choix de P_0 dans ce cas.
Si $z = (z_1, \ldots, z_g), z' = (z'_1, \ldots, z'_g) \in \mathbb{C}^g$ on note $z \equiv z'$ pour indiquer que z est égal à z' en tant qu'élément de $\mathrm{Jac}(C)$.

1.2.2 Théorèmes

Théorème 1.28 (Abel) [RF74, IV.th.17]
Soit D et D' deux diviseurs alors

$$D \sim D' \iff \forall P_0 \in C,\ u_{P_0}(D) \equiv u_{P_0}(D').$$

Cela traduit simplement le fait que u_{P_0} induit un isomorphisme entre $\mathrm{Div}^n(C)/\mathrm{Princ}(C)$ et $\mathrm{Jac}(C)$ pour tout n.

Théorème 1.29 (théorème d'inversion de Jacobi)
Soient $e \in \mathbb{C}^g$ et $P_0 \in C$. Il existe $D \in \mathrm{D}^g(C)$ tel que $e \equiv u_{P_0}(D)$.

Pour une variété abélienne principalement polarisée nous avons introduit au paragraphe 1.1.2 les fonctions thêta caractéristiques. Les fonctions $s(z) = \vartheta[\epsilon](z - e, \Omega)$, avec $e \in \mathbb{C}^g$ et $[\epsilon]$ une caractéristique quelconque, peuvent être considérées comme des translatés de ces premières. En composant avec $u_{P_0} : C \to \mathrm{Jac}(C)$ on obtient donc des sections holomorphes de fibrés sur C caractérisées par leur diviseur des zéros si elles sont non nulles. Plus précisément on a le théorème suivant :

Théorème 1.30 [RF74, V.th.1]
Soient $P_0 \in C$, $[\epsilon]$ une caractéristique et $e \in \mathbb{C}^g$, alors la section $s(P) = \vartheta[\epsilon](u_{P_0}(P) - e)$ (où, pour simplifier les notations, on oublie la dépendance en Ω) est soit identiquement nulle, soit son diviseur des zéros D de degré g est caractérisé (en tant que diviseur et pas seulement à équivalence linéaire près) par la relation

$$u_{P_0}(D) + K_{P_0} \equiv e + \epsilon$$

où K_{P_0} est un élément de $\mathrm{Jac}(C)$ ne dépendant que de C, de la base d'homologie et de P_0, appelée constante de Riemann.

Remarque :
En fait le théorème [RF74, V.th.1] est moins précis puisqu'il donne uniquement la caractérisation du diviseur D à équivalence linéaire près et pas son unicité en tant que

diviseur. Mais ceci résulte en particulier du fait que $\mathrm{ind}(D) = 0$.

On a la condition nécessaire et suffisante de nullité ci-dessous :

Théorème 1.31 [RF74, V.th.2]
Avec les notations du théorème précédent, une condition nécessaire et suffisante pour que s soit identiquement nulle est que $e + \epsilon \equiv u_{P_0}(D) + K_{P_0}$ avec $D \in \mathrm{D}^g(C)$ tel que $\mathrm{ind}(D) > 0$.

Les points d'annulation de $\vartheta[\epsilon]$ (quand celle-ci n'est pas nulle) sont également caractérisés par :

Théorème 1.32 [RF74, V.th.3]
Une condition nécessaire et suffisante pour que $\vartheta[\epsilon](e) = 0$ est que pour tout $P_0 \in C$ il existe $D \in \mathrm{D}^{g-1}(C)$ tel que $e \equiv u_{P_0}(D) + K_{P_0} + \epsilon$.

Théorème 1.33 (théorème d'annulation de Riemann) [RF74, V.th.5]
Une condition nécessaire et suffisante pour que $\vartheta[\epsilon](z, \Omega)$ soit nulle ainsi que toutes ses dérivés partielles jusqu'à l'ordre $s-1$ mais qu'une au moins des dérivées partielles d'ordre s soit non nulle en e ou $-e$ est que

$$e \equiv u_{P_0}(D) + K_{P_0} + \epsilon$$

pour un $P_0 \in C$ et $D \in \mathrm{D}^{g-1}(C)$ tel que $\mathrm{ind}(D) = s$.

Remarque :
Pour une formulation plus moderne et plus géométrique on pourra consulter par exemple [GH78].

Chapitre 2

Le cadre théorique

Nous détaillons dans ce chapitre la méthode A.G.M. dans le cas des courbes elliptiques sur $\mathbb{C}$ puis sur $\mathbb{Q}_2$ en montrant comment, dans le premier cas, celle-ci détermine les périodes de la courbe elliptique et comment, dans le second cas, elle permet de calculer le polynôme caractéristique selon l'idée introduite par Mestre (cf. [Mes00],[Mes02]). Après quoi, nous montrons comment on peut étendre cette méthode en genre supérieur dans le cas 2-adique.

2.1 Le cas du genre 1

Le point de vue complexe est essentiellement les articles [BM89] et [Cox84]. Le point de vue 2-adique n'a jamais fait à ma connaissance l'objet d'une étude complète et apporte donc quelques précisions. Le traitement par les équations de Mumford est quant à lui original.

2.1.1 Sur $\mathbb{C}$

C'est historiquement le premier cas traité : Lagrange ([Lag67, t.II,p.253-312]) et Gauss ([Gau70, t.III,p.352-353,261-403]) ont introduit la moyenne arithmético-géométrique (A.G.M. en anglais) dans le but de calculer les intégrales elliptiques. Ils ont en particulier montré :

Théorème 2.1
Soit a, b deux réels tels que $0 < b < a$. On a

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2\mathrm{M}(a,b)}.$$

où on note $\mathrm{M}(a,b)$ (moyenne arithmético-géométrique de a et b) la limite commune des suites définies par

$$\begin{cases} a_0 = a & a_{n+1} = \frac{a_n + b_n}{2} \\ b_0 = b & b_{n+1} = \sqrt{a_n b_n} \end{cases}$$

Puisque

$$|a_{n+1} - b_{n+1}| = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n} + \sqrt{b_n})^2} \leq \frac{(a_n - b_n)^2}{8b_1}$$

ces deux suites adjacentes convergent quadratiquement. Ce procédé est donc en particulier nettement préférable aux méthodes traditionnelles d'intégration numérique.
La démonstration repose sur un astucieux changement de variables qui transforme les paramètres a, b de l'intégrale en a_1, b_1. Par itération et passage à la limite, on obtient alors le théorème.
Pour mieux comprendre ce résultat, nous allons «l'algébriser» par le changement de variables $x = e_3 + (e_2 - e_3)\sin^2 t$ avec

$$\begin{cases} a_0^2 & = e_1 - e_3 \\ b_0^2 & = e_1 - e_2 \\ 0 & = e_1 + e_2 + e_3 \end{cases}$$

Le théorème devient alors :

Théorème 2.2

$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{P(x)}} = \frac{\pi}{2\mathrm{M}(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$

avec $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, $e_3 < e_2 < e_1$.

On reconnaît l'intégrale d'une forme différentielle régulière sur la courbe $E : y^2 = P(x)$. Plus précisément si on note $\mathbb{C}/\Lambda$ avec $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (ω_1 réel et ω_2 imaginaire pur) le tore complexe $E(\mathbb{C})$, on a l'isomorphisme

$$\begin{array}{rccll} u : & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0 : 1 : 0) & z \in \Lambda \end{array}$$

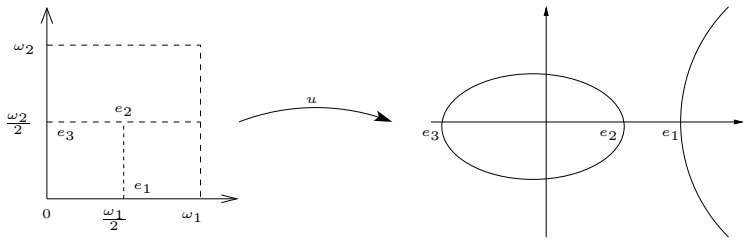
et (voir figure 2.1)

$$\omega_1 = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} \frac{d\mathcal{P}(z)}{\mathcal{P}'(z)} = 2\int_{e_3}^{e_2} \frac{dx}{y} = 2\int_{e_3}^{e_2} \frac{dt}{\sqrt{P(t)}}$$

On est donc ramené au problème plus géométrique du calcul d'une période d'une forme différentielle de première espèce sur une surface de Riemann.

Posons $\tau = \omega_2/\omega_1$. Les relations entre fonctions thêta et la fonction $\mathcal{P}$ (ou le théorème de Thomae [Mum83, II]) permettent d'exprimer un lien entre ω_1, les thêta constantes et

FIG. 2.1 – L'application u



les coefficients de la courbe : on a en effet

$$\begin{cases} \omega_1\sqrt{e_1-e_3} = & \pi\cdot\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^2 \\ \omega_1\sqrt{e_1-e_2} = & \pi\cdot\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^2 \end{cases}$$

Or la duplication des thêta constantes en genre 1 (cf. proposition 1.19) est exactement l'algorithme A.G.M.

$$\begin{cases} a_0=\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^2 & a_n=\vartheta\begin{bmatrix}0\\0\end{bmatrix}(2^n\tau)^2 \\ b_0=\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^2 & b_n=\vartheta\begin{bmatrix}0\\1\end{bmatrix}(2^n\tau)^2 \end{cases}$$

Comme

$$\lim_{\mathrm{Im}\,\tau\to+\infty}\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)=\lim_{\mathrm{Im}\,\tau\to+\infty}\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)=1$$

on a :

$$\mathrm{M}\left(\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^2,\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^2\right)=1.$$

En combinant ces résultats et par linéarité on retrouve le résultat du théorème 2.2

$$\omega_1\cdot\mathrm{M}(\sqrt{e_1-e_3},\sqrt{e_1-e_2})=\pi.$$

Reformulons cela plus géométriquement. Si on pose

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0-(e_1-e_3))(x_0-(e_1-e_2)) && (2.1)\\ &= x_0\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^4\right)\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^4\right) && (2.2)\\ &= x_0(x_0-a_0^2)(x_0-b_0^2), && (2.3) \end{aligned}$$

qui est isomorphe à E, on peut construire le diagramme suivant

$$\begin{array}{ccc} \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau & \xrightarrow[u]{\simeq} & E_\tau(\mathbb{C}) \\ {\scriptstyle F}\uparrow & & \uparrow{\scriptstyle f} \\ \mathbb{C}/\mathbb{Z}+\mathbb{Z}2\tau & \xrightarrow[u]{\simeq} & E_{2\tau}(\mathbb{C}) \end{array}$$

où $F : z \mapsto z$ et f est l'isogénie de degré 2 qui rend le diagramme commutatif. Les formules de duplication et les formules (2.2) et (2.3) montrent que $E_{2\tau}$ a pour équation $y_1^2 = x_1(x_1 - a_1^2)(x_1 - b_1^2)$. On peut alors expliciter l'application f et sa duale $\hat{f}$ (voir par exemple [BM89]) :

$$f : (x_1, y_1) \quad \mapsto \quad (x_1(1 + \frac{a_1^2 - b_1^2}{x_1 - a_1^2}), \frac{y_1(x_1^2 - 2x_1a_1^2 + a_1^2b_1^2)}{(x_1 - a_1^2)^2}) \tag{2.4}$$

$$\hat{f} : (x_0, y_0) \quad \mapsto \quad (\frac{y_0^2}{4x_0^2} + (\frac{a+b}{2})^2, -\frac{y_0(a^2b^2 - x_0^2)}{8x_0^2}) \tag{2.5}$$

(en particulier $< (0,0) >$ est le noyau de $\hat{f}$).

Puisque $F^*dz = dz$, on a

$$f^*\left(\frac{dx_0}{y_0}\right) = (u \circ F \circ u^{-1})^*\left(\frac{dx_0}{y_0}\right) = (F \circ u^{-1})^* dz = (u^{-1})^* dz = \frac{dx_1}{y_1}$$

donc en particulier

$$\omega_1 = 2\int_{e_1}^{\infty} \frac{dx}{y} = 2\int_0^{-\infty} \frac{-i}{2}\frac{dx_0}{y_0} = \int_0^{-\infty} -i\frac{dx_1}{y_1}.$$

On réitère le procédé :

$$E_{2^n\tau} \to E_{2^{n-1}\tau} \to \ldots \to E_{2\tau} \to E_\tau.$$

A la limite, on obtient $E_\infty : y^2 = x(x - \mathrm{M}(a_0, b_0)^2)^2$. Cette courbe est de genre 0, elle est donc paramétrisable et on a encore

$$\omega_1 = \int_0^{-\infty} -i\frac{dx}{\sqrt{x(x - M(a_0,b_0)^2)^2}} = \left[-2\frac{\mathrm{Arctan}(\frac{\sqrt{\mathrm{x}}}{\mathrm{M(a_0,b_0)}})}{\mathrm{M(a_0,b_0)}}\right]_0^{-\infty} = \frac{\pi}{\mathrm{M}(a_0,b_0)}.$$

L'histoire ne s'arrête pas là comme le rappelle Cox dans [Cox84] reprenant des travaux de Gauss. Si $a, b \in \mathbb{C}$ et non plus seulement à $\mathbb{R}^+$, tels que $b/a \notin \{0, 1, -1\}$ avec par exemple $|a| \geq |b|$, on aimerait pouvoir appliquer l'algorithme précédent. Le problème essentiel étant la définition d'une «bonne racine carrée».

Définition 2.3
$b_1 = \pm\sqrt{ab}$ est appelé bonne racine si $|a_1 - b_1| \leq |a_1 + b_1|$ et si $|a_1 - b_1| = |a_1 + b_1|$ on a de plus $\mathrm{Im}(b_1/a_1) > 0$.
Une paire de suite (a_n, b_n) déduite de l'A.G.M. est dite acceptable si b_{n+1} est le bon choix pour $\sqrt{a_nb_n}$ pour tout n sauf un nombre fini.

On a facilement en maniant quelques inégalités :

Proposition 2.4
(a_n) et (b_n) convergent vers une limite commune non nulle si et seulement si (a_n, b_n) est acceptable.

On définit alors :

Définition 2.5
Une valeur μ est une moyenne arithmético-géométrique de (a, b) s'il existe une paire acceptable convergeant vers μ. On note $\{\mathrm{M}(a, b)\}$ l'ensemble de ces valeurs.
La valeur obtenue lorsqu'à chaque étape est effectuée un bon choix est appelée valeur simple notée $\mathrm{M}(a, b)$.

On a le résultat fondamental :

Théorème 2.6 (Gauss)
Soit $\mu = M(a, b)$ et $\lambda = \mathrm{M}(a + b, a - b)$ alors toute valeur $\mu' \in \{\mathrm{M}(a, b)\}$ est donnée par

$$\frac{1}{\mu'} = \frac{d}{\mu} + \frac{ic}{\lambda}$$

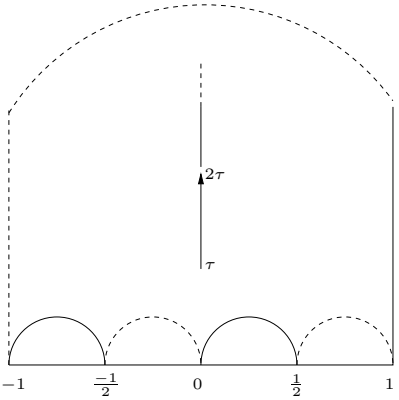
avec c, d premiers entre eux tels que $d \equiv 1 \pmod 4$ et $c \equiv 0 \pmod 4$.

La démonstration de ce théorème introduit de manière naturelle l'espace des modules $\mathbb{H}/\Gamma^2(4)$ où on note

$$\Gamma^2(4) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a \equiv d \equiv 1 \pmod 4, c \equiv 0 \pmod 4, b \equiv 0 \pmod 2\}$$

(attention à ne pas le confondre avec $\Gamma_2(4)$ introduit au paragraphe 1.1.4).
Cet espace de module paramétrise les courbes elliptiques avec un point d'ordre 2 et un point d'ordre 4 à isomorphisme près, ce qui justifie à posteriori l'écriture $y^2 = x(x - 1)(x - (b/a)^2)$. La méthode A.G.M. peut alors être interprétée comme un cheminement vers le bord de cet espace constitué des courbes dégénérées.

FIG. 2.2 – Domaine fondamental pour $\Gamma^2(4)$



Remarque :
On peut montrer que π/μ et $i\pi/\lambda$ sont deux périodes de la courbe $E : y^2 = x(x-a^2)(x-b^2)$ telles que $\tau = i\mu/\lambda$ appartient au domaine fondamental de la figure 2.2. L'ensemble des valeurs $1/\mu'$ est donc au facteur π près un sous-ensemble du réseau des périodes de E.
Si on écrit $\{\mathrm{M}(a,b)\} = \left\{\frac{c\tau+d}{\mathrm{M}(a,b)}\right\}$ avec $d \equiv 1 \pmod 4$ et $c \equiv 0 \pmod 4$ on constate que π/μ est de norme minimale pour ce sous-ensemble.

2.1.2 Sur $\mathbb{Q}_2$: première approche

On note k un corps fini de cardinal $q = 2^N$ et K l'unique extension non ramifiée de $\mathbb{Q}_2$ de degré N de valuation v (normalisée telle que la valuation de l'uniformisante π égale à 1) et d'anneau des entiers $\mathcal{O}$. L'extension étant non ramifiée, on notera en fait $\pi = 2$. Si on note $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_2)$ la substitution de Frobenius, celle-ci induit par définition un automorphisme de $k \simeq \mathcal{O}/2\mathcal{O}$ (encore noté σ) tel que $\sigma(x) = x^2$ pour $x \in k$.

Le cas 2-adique partage avec le cas réel l'avantage de la définition d'une bonne racine carrée. En effet soit $a \in 1 + 8\mathcal{O}$. On note alors $b = \sqrt{a}$ l'unique élément de $1 + 4\mathcal{O}$ tel que $b^2 = a$.
Si $a, b \in K$ tels que $b/a \in 1 + 8\mathcal{O}$ on définit

$$\mathrm{M}(a,b) = (\frac{a+b}{2}, a\sqrt{\frac{b}{a}}).$$

On peut remarquer que si $(a_1, b_1) = \mathrm{M}(a,b)$ alors $a_1, b_1 \in \mathcal{O}$ et $b_1/a_1 \in 1 + 8\mathcal{O}$. On peut ainsi définir une double suite (a_i, b_i) au moyen de M. Contrairement au cas réel, cette suite ne converge pas (sauf si $b/a \in 1 + 16\mathcal{O}$, cf. [HM89] où est étudié le cas de mauvaise réduction grâce à la courbe de Tate). C'est pour cela qu'on note maintenant $\mathrm{M}(a,b)$ une itération et non plus la limite de la suite.

Notre objectif est de montrer comment l'utilisation de l'opération M permet le calcul du nombre de points d'une courbe elliptique ordinaire E sur $k = \mathbb{F}_{2^N}$.
Par la suite on note Fr le «petit» Frobenius, $E^{(i)}$ ses images itérées i fois et Ve son isogénie duale. On note $\phi : E \to E$ l'endomorphisme de Frobenius de E et V son isogénie duale.

E admet un unique (à isomorphisme près) relèvement sur K, dit canonique, $E^{\uparrow}$ caractérisé par l'une ou l'autre des deux propriétés suivantes :
- $\mathrm{End}_K(E^{\uparrow}) = \mathrm{End}_k(E)$.
- Il existe une isogénie $\mathrm{Fr}^{\uparrow} : E^{\uparrow} \to {}^{\sigma}(E^{\uparrow})$ relevant $\mathrm{Fr} : E \to E^{(1)}$.

Soit ϕ l'endomorphisme de Frobenius de E. On a

$$|E| = q + 1 - \mathrm{Tr}(\phi)$$

la trace de ϕ étant la trace de son action sur $V_l = T_l \otimes \mathbb{Q}$ pour $l \neq 2$. La représentation de $\mathrm{End}_k^0(E) = \mathrm{End}_k(E) \otimes \mathbb{Q}$ sur le module de Tate l-adique étant fidèle, c'est aussi la trace en tant qu'élément du corps $\mathrm{End}_k^0(E)$. Si $\phi^{\uparrow} \in \mathrm{End}_K(E^{\uparrow})$ relève ϕ par égalité de $\mathrm{End}_K(E^{\uparrow})$ et de $\mathrm{End}_k(E)$ c'est donc également la trace de $\phi^{\uparrow}$. En caractéristique nulle, la trace d'une isogénie f de degré d est donnée par son action sur les formes différentielles régulières. Si on note ω une telle forme non nulle pour $E^{\uparrow}$ et si $f^*(\omega) = \lambda\,\omega$ alors

$$\mathrm{Tr}(f) = \lambda + \frac{d}{\lambda}.$$

En résumé, si $(\phi^{\uparrow})^*\omega = \lambda\,\omega$ on a

$$\mathrm{Tr}(\phi) = \lambda + \frac{2^N}{\lambda}.$$

On est donc ramené au calcul de λ.

Soit une courbe elliptique ordinaire $\tilde{E}$ et E un modèle minimal de $\tilde{E}$ sur $\mathcal{O}$. D'après [Sil92, chap.VII, 2.1] on a une suite exacte

$$0 \to \{P \in E(K)/\tilde{P} = \tilde{O}\} \to E(K) \to \tilde{E}(k) \to 0$$

La courbe $\tilde{E}$ étant ordinaire, $\tilde{E}[2](k) \simeq \mathbb{Z}/2\mathbb{Z}$. Il existe donc un unique point $Q \in E[2](K)$ qui se réduit sur $\tilde{O}$. Par un changement de variables on se ramène à $Q = (0 : 0 : 1)$. On peut alors écrire $E : y^2 = x(x - a_0^2)(x - b_0^2)$.
Pratiquement, on réalise cela comme suit : soit $y^2 + xy = x^3 + a_2x^2 + a_4x$ une courbe ordinaire sur k (on peut toujours supposer $a_6 = 0$ en posant $Y = y + \sqrt{a_6}$) que l'on remonte sur K en $Y^2 = (y + x/2)^2 = x(x^2 + (4a_2 + 1)/4x + 1)$. le membre de gauche se factorise sur K en $x(x-\alpha)(x-\beta)$ avec $v(\alpha) = -2$ et $v(\beta) = 2$. On effectue le changement de variables $X = x - \alpha$ et on obtient le polynôme $X(X + \alpha)(X + \alpha - \beta)$. De plus

$$v(\frac{\alpha - \beta}{\alpha} - 1) = v(\frac{\alpha}{\beta}) = 4. \tag{2.6}$$

On pose alors $a_0^2 = -\alpha$ et $b_0^2 = \beta - \alpha$. La congruence ci-dessus montre que nous pouvons utiliser M et définir $(a_1, b_1) = \mathrm{M}(a_0, b_0)$ puis la courbe $E_1 : y_1^2 = x_1(x_1 - a_1^2)(x_1 - b_1^2)$.

Remarque :
Nous voyons ici que a_1, b_1 n'interviennent que par leurs carrés qui sont bien définis sur K et que l'on peut calculer en restant dans K en remarquant que

$$\begin{cases} a_1^2 = (a_0^2 + b_0^2 + 2a_0b_0)/4 \\ b_1^2 = a_0b_0 \end{cases}$$

et que $a_0b_0 = \sqrt{(a_0b_0)^2} = a_0^2\sqrt{(b_0/a_0)^2}$.
Notons que si $a_6 \neq 0$ et que l'on relève l'équation à l'identique, les points de Weierstrass auraient pu être dans une extension ramifiée (c'est par exemple le cas avec $y^2 + xy = x^3 + 1$). En pratique, cela doit être évité. Nous reviendrons plus généralement sur ces problèmes au chapitre 4.

Supposons maintenant que $E = \mathcal{E}_0$ est le relèvement canonique de $\tilde{E}$. On note dans ce cas α_i et β_i les éléments de la suite (a_i, b_i) et $\mathcal{E}_i = E_i$ les courbes elliptiques 2-isogènes qui s'en déduisent pas l'A.G.M.

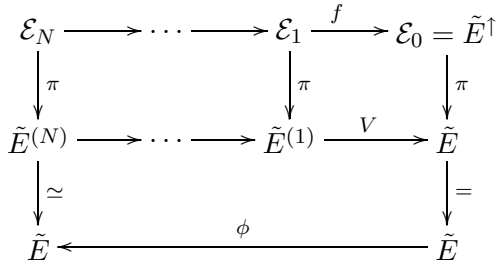
Proposition 2.7
Dans le diagramme suivant

$$\begin{array}{ccccc} \mathcal{E}_1 & \underset{\hat{f}}{\overset{f}{\rightleftarrows}} & \mathcal{E}_0 & \longleftarrow & < Q > \\ \downarrow \pi & & \downarrow \pi & & \downarrow \pi \\ \tilde{E}^{(1)} & \underset{\mathrm{Fr}}{\overset{\mathrm{Ve}}{\rightleftarrows}} & \tilde{E} & \longleftarrow & < \tilde{O} > \end{array}$$

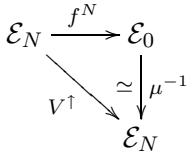
$\mathcal{E}_1 \simeq {}^{\sigma}\mathcal{E}_0$ est le relèvement canonique de $\tilde{E}^{(1)}$ et f, donnée par l'A.G.M. (formule (2.4)), est le relèvement du «petit» Verschiebung Ve *(isogénie duale de* Fr*).*

Démonstration :
Soit $\mathrm{Fr}^{\uparrow}$ le relèvement de Fr. L'isogénie Fr est caractérisée par son noyau qui est l'unique point de 2-torsion non nul Q qui se réduit sur $\tilde{O}$. Par notre changement de variables, il s'agit du point $(0, 0)$. Or d'après la formule (2.5), $\hat{f}$ est une isogénie de degré 2 de même noyau. Donc $\mathrm{Fr}^{\uparrow} = \hat{f}$ et $\mathcal{E}_1$ est isomorphe à ${}^{\sigma}\mathcal{E}_0 = (\tilde{E}^{(1)})^{\uparrow}$, par la deuxième propriété du relèvement canonique.

En itérant on obtient la tour d'isogénies



Par unicité du relèvement canonique à isomorphisme près, on a $\mathcal{E}_N \simeq \tilde{E}^{\uparrow}$. On a donc le diagramme suivant :



Notons $(\mu^{-1})^*(\omega_N) = u \cdot \omega_0$ alors

$$(V^{\uparrow})^*(\omega_N) = (\mu^{-1} \circ f^N)^*(\omega_N) = (f^N)^*(\mu^{-1})^*(\omega_N) = (f^N)^*(u \cdot \omega) = u \cdot \omega_N$$

car l'action de f sur les différentielles est l'identité (comme nous l'avons remarqué dans le cas complexe). Comme $V^{\uparrow}$ et $\phi^{\uparrow}$ sont duales ($V^{\uparrow} \circ \phi^{\uparrow} = [2^N]$), $\lambda = 2^N/u$. Or on a :

Lemme 2.8
Soit $E/K : y^2 = x(x-a^2)(x-b^2)$ et $E'/K : y'^2 = x'(x'-a'^2)(x'-b'^2)$ avec $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 (mod\ 2)$. Si E et E' sont isomorphes alors $x = u^2x'$ et $y = u^3y'$ avec $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$.

Démonstration :
Les courbes étant isomorphes, il existe d'après [Sil92, chap.III] $(u, r) \in (\mathcal{O}^* \times K)$ tel que $x = u^2x' + r$ et $y = u^3y'$. Il nous suffit donc de montrer que $r = 0$. Avec les notations habituelles, [Sil92, chap.III,1.2], on a facilement que

$$\begin{aligned} -4u^2(a'^2 + b'^2) = b'_2 &= b_2 + 12r = -4(a^2 + b^2) + 12r \\ 0 = u^6 b'_6 &= 4r(r - a^2)(r - b^2) \end{aligned}$$

La première égalité nous montre que $r \equiv 0 (\mathrm{mod}\ 2)$ et la seconde nous montre que $r = 0$ car ni a^2 ni b^2 ne sont congrus à 0. La première égalité nous donne alors la valeur de u^2.

Ceci permet bien sûr de trouver u, et donc $\mathrm{Tr}(\phi)$, au signe près mais c'est sous la forme suivante que le résultat est plus connu :

Théorème 2.9 [Mes00]

$$\mathrm{Tr}(\phi) = \pm \left(\frac{\alpha_1}{\alpha_{N+1}} + 2^N \frac{\alpha_{N+1}}{\alpha_1} \right). \tag{2.7}$$

Démonstration :
Considérons les courbes $\mathcal{E}_1$ et $\mathcal{E}_{N+1}$. Comme $\tilde{E}$ est isogène à $\tilde{E}^{(1)}$ sur k, leurs polynômes caractéristiques du Frobenius sont les mêmes donc en particulier leurs traces. On est donc ramené à regarder le rapport u_1^2 pour ces deux nouvelles courbes.
L'invariant d'une courbe $E : y^2 = x(x-a)(x-b)$ est donnée par

$$j(E) = 2^8 \frac{((b/a)^2 - (b/a) + 1)^3}{(b/a)^2((b/a) - 1)^2}.$$

$\mathcal{E}_0$ et $\mathcal{E}_N$ étant isomorphes, on a donc $j(\mathcal{E}_0) = j(\mathcal{E}_N)$. Si on note $\lambda = (\beta_0/\alpha_0)^2$ on a d'après [Sil92, chap.III] que $(\beta_N/\alpha_N)^2 \in \{\lambda, 1/\lambda, \lambda - 1, 1/(\lambda - 1), \lambda/(1-\lambda), (1-\lambda)/\lambda\}$. Par la congruence (2.6) et les propriétés de M, on constate que $v(\beta_N/\alpha_N - 1) = 3$. Ainsi $(\beta_N/\alpha_N)^2 = \lambda$ ou $1/\lambda$. En fait, les conventions prises dans l'extraction de la racine nous montrent plus précisément que $(\beta_N/\alpha_N) = (\alpha_0/\beta_0)$ ou (β_0/α_0). On a alors

$$u_1^2 = \frac{\alpha_1^2 + \beta_1^2}{\alpha_{N+1}^2 + \beta_{N+1}^2} = \frac{\alpha_1^2}{\beta_1^2} \frac{1 + (\beta_1/\alpha_1)^2}{1 + (\beta_{N+1}/\alpha_{N+1})^2}.$$

Or $\beta_1^2 = \alpha_0\beta_0$ et $\alpha_1^2 = (\alpha_0^2 + \beta_0^2 + 2\alpha_0\beta_0)/4$, on étudie donc le rapport

$$\frac{\alpha_0\beta_0}{\alpha_0^2 + \beta_0^2 + 2\alpha_0\beta_0} \Big/ \frac{\alpha_N\beta_N}{\alpha_N^2 + \beta_N^2 + 2\alpha_N\beta_N}.$$

Comme

$$\frac{\alpha_N\beta_N}{\alpha_N^2 + \beta_N^2 + 2\alpha_N\beta_N} = \frac{\beta_N/\alpha_N}{1 + 2\beta_N/\alpha_N + (\beta_N/\alpha_N)^2}$$

que α_N/β_N soit égal à α_0/β_0 ou son inverse, le rapport vaut 1 et on a donc le résultat.

Remarque :
On peut facilement régler la question du signe de la trace. En effet $1 - |\tilde{E}| \equiv \mathrm{Tr}(\phi) \equiv \pm(\alpha/\alpha_N) \pmod 4$. Le signe est donc déterminer par $|\tilde{E}| \pmod 4$. Comme on a toujours un point de 2 torsion sur k (le noyau du Verschiebung) ce nombre est congru à 0 ou 2 modulo 4. Il est congru à 0 si et seulement si il y a un point d'ordre 4 sur k. Donc $\mathrm{Tr}(\phi) \equiv 1 \pmod 4$ si et seulement si il y a un point d'ordre 4 défini sur k.
Notons que, par symétrie de l'A.G.M., la formule (2.7) est également valable en remplaçant les α_i par β_i.

Nous allons montrer pour finir que l'A.G.M. ne nécessite pas le calcul préalable du relèvement canonique : elle fournit un procédé de convergence vers ce modèle qui permet «d'approximer» à volonté la formule (2.7).

Soit donc $E = E_0 : y_0^2 = x_0(x_0 - a_0^2)(x_0 - b_0^2)$ un relèvement minimal de $\tilde{E}$ sur $\mathcal{O}$ et $E_i : y_i^2 = x_i(x_i - a_i^2)(x_i - b_i^2)$ la suite de courbes 2-isogènes qui s'en déduit par itération de l'A.G.M. On utilise le théorème suivant :

Théorème 2.10 [VPV01, §. 2]
Soit $x \in \mathcal{O}$ tel que $x \equiv j(\tilde{E}^{\uparrow}) \pmod{2^i}$ avec $i \in \mathbb{N}$. Alors il existe un unique $y \in \mathcal{O}$ tel que $y \equiv x^2 \pmod 2$ et $\Phi_2(x, y) = 0$. De plus $y \equiv j((\tilde{E}^{(1)})^{\uparrow}) \pmod{2^{i+1}}$.

Rappelons que Φ_p désigne le polynôme modulaire d'ordre p. Il possède en particulier la propriété suivante : si E et E' sont deux courbes elliptiques reliées par une isogénie de degré p alors $\Phi_p(j(E), j(E')) = 0$.
On a bien sûr $\Phi_2(E_i, E_{i+1}) = 0$. Un calcul simple permet de montrer de plus la congruence ci-dessous :

Lemme 2.11
$j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.

L'itération de l'A.G.M. conduit ainsi à la congruence

$$j(E_n) \equiv j((\tilde{E}^{(n)})^{\uparrow}) \pmod{2^{n+1}}.$$

Considérons la suite (E_{Nn}). D'après le théorème 2.10, on a convergence de cette famille de courbes vers le relèvement canonique de E. De plus $f^N : \mathcal{E}_N \to \mathcal{E}_0$ est congru modulo 2^{Nn+1} au morphisme de $E_{N(n+1)} \to E_{Nn}$ (plus précisément, il s'agit de l'extension de f^N aux modèles de Néron de $\mathcal{E}_N$ et de $\mathcal{E}_0$ qui vérifie cette propriété). De même l'isomorphisme $\mu : \mathcal{E}_N \to \mathcal{E}_0$ est congru à l'isomorphisme de $E_{N(n+1)} \to E_{Nn}$. On a donc

$$\frac{a_{Nn}}{a_{N(n+1)}} \equiv \frac{\alpha}{\alpha_N} \pmod{2^{Nn+1}}.$$

Plus généralement, les courbes E_i étant toutes isogènes entre elles sur K, on a

$$\mathrm{Tr}(\phi) \equiv \frac{a_i}{a_{i+N}} + \frac{2^N a_{i+N}}{a_i} \pmod{2^{i+1}}.$$

Comme $|\mathrm{Tr}(\phi)| \leq 2\sqrt{2^N}$, il suffit de prendre $i = N/2$ et d'itérer l'A.G.M. $\lfloor 3N/2 \rfloor + 1$ fois.

2.1.3 Sur $\mathbb{Q}_2$: deuxième approche

Nous proposons de montrer ici comment l'écriture avec les équations de Mumford (paragraphe 1.1.3) permet de cerner plus naturellement les calculs de l'A.G.M. Quand $g = 1$, ces équations se réduisent en effet à l'intersection de deux quadriques dans $\mathbb{P}^3$:

$$\begin{array}{rcl} \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau & \hookrightarrow & \mathbb{P}^3 \\ z & \mapsto & (X_0 : X_1 : X_2 : X_3) \end{array}$$

avec $E_\tau = \begin{cases} \lambda_2(X_0^2 + X_2^2) = 2\lambda_0 X_1 X_3 \\ \lambda_2(X_1^2 + X_3^2) = 2\lambda_0 X_0 X_2 \end{cases}$ où $X_i = \vartheta \begin{bmatrix} i/2 \\ 0 \end{bmatrix} (4z, 4\tau)$ et $\lambda_i = 2\vartheta \begin{bmatrix} i/2 \\ 0 \end{bmatrix} (0, 8\tau)$.

On considère maintenant l'isogénie donnée par le diagramme

$$\begin{array}{ccc} \mathbb{C}/\mathbb{Z}+\mathbb{Z}2\tau & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau \\ \downarrow & & \downarrow \\ E_{2\tau} & \xrightarrow{\quad f \quad} & E_\tau \end{array}$$

En notant avec un $'$ les variables et constantes du plongement correspondant à 2τ, les formules de duplication (proposition 1.19) amènent

$$f((X_0' : X_1' : X_2' : X_3')) = (X_0'^2 + X_2'^2 : \mu(X_1'X_0' + X_2'X_3') : X_1'^2 + X_3'^2 : \mu(X_2'X_1' + X_0'X_3'))$$

avec

$$\mu = \frac{X_0(0)}{X_1(0)} = \frac{\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0,4\tau)}{\vartheta \begin{bmatrix} 1/2 \\ 0 \end{bmatrix}(0,4\tau)} = \frac{\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0,\tau) + \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix}(0,\tau)}{\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}(0,\tau)}.$$

Ces mêmes formules montrent que $\begin{cases} \lambda_0^2 = \lambda_0'^2 + \lambda_2'^2 \\ \lambda_2^2 = 2\lambda_0' \lambda_2' \end{cases}$ qui correspond à une itération de l'A.G.M. «descendant».

Les formules qui relient le modèle plan à ce modèle dans $\mathbb{P}^3$ permettent d'obtenir une différentielle régulière :

$$\omega = \frac{X_0\, dX_2 - X_2\, dX_0}{X_3^2 - X_1^2}.$$

On trouve alors

$$f^*(\omega) = \frac{2\lambda_0'}{\lambda_2'\mu^2}\, \omega'.$$

Le facteur multiplicatif s'écrit également

$$u = \frac{2\lambda_0'}{\lambda_2'\mu^2} = 2\frac{\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}(0,\tau)^2}{\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0,\tau)^2 - \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix}(0,\tau)^2} = \frac{\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}(0,\tau)^2}{\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}(0,2\tau)^2}. \tag{2.8}$$

On retrouve ainsi naturellement le facteur de la formule (2.7) de l'action sur les différentielles.

Remarque :
Le facteur multiplicatif n'intervient pas ici dans l'isomorphisme final mais dans l'action de chacun des relèvements du Frobenius.
Les modèles de Mumford ont également de jolies propriétés par rapport à leurs points d'ordre 4. Pour celui donné ici, les images des points d'ordre 4 avec $z \in \frac{1}{4} < \delta_i >$ sont simplement des permutations circulaires des coordonnées de l'image de l'origine.

2.2 Cas général

2.2.1 Polynôme caractéristique

Soient A, B deux variétés abéliennes de dimension g sur un corps K. Pour toute isogénie $f : A \to B$ on peut définir le degré de f comme le cardinal de $\ker f$ en tant que schéma en groupes fini. Supposons $A = B$. Comme $\deg(nf) = \deg(n)\deg(f) = n^{2g}\deg(f)$, on peut étendre cette définition à $\mathrm{End}^0(A) = \mathrm{End}(A)\otimes\mathbb{Q}$ en posant $\deg(f) = n^{-2g}\deg(nf)$ avec $nf \in \mathrm{End}(A)$.

Définition 2.12
On appelle polynôme caractéristique de $f \in \mathrm{End}^0(A)$, l'unique polynôme unitaire de degré $2g$ à coefficients rationnels tel que $P(n) = \deg(f - n)$, $\forall n \in \mathbb{Z}$. On le note χ_f.
Si $f \in \mathrm{End}(A)$ alors $\chi_f \in \mathbb{Z}[X]$.

C'est un résultat fondamental pour l'arithmétique que ce polynôme peut être calculé à partir de la restriction de f au module de Tate.

Théorème 2.13 [Mil86, prop.12.9]
Soit p la caractéristique de K. Pour tout premier $l \neq p$, si on note $V_l(A) = T_l(A)\otimes\mathbb{Q}$ on a quelque soit $f \in \mathrm{End}(A)$, $\chi_f(X) = \det(f - XI_{2g}|_{V_l(A)})$.

Si A est définie sur un corps fini $k = \mathbb{F}_q$ avec $q = p^N$, A possède un endomorphisme privilégié, le Frobenius noté ϕ.

Définition 2.14
On appelle polynôme caractéristique de A le polynôme caractéristique de ϕ. On le note χ_A. Si C/k est une courbe (lisse projective) sur k, on définit le polynôme caractéristique de C comme le polynôme caractéristique de sa jacobienne. On le note χ_C.

La connaissance du polynôme caractéristique est déterminante pour la compréhension de l'arithmétique de A et de sa géométrie (structure de l'anneau des endomorphismes, etc.). Citons simplement :

Théorème 2.15 [Mil86, prop. 19.1]
Soit $\chi_A = \prod(X - a_i)$ alors

$$\forall n \in \mathbb{N},\ |A(\mathbb{F}_{q^n})| = \prod(1 - a_i^n).$$

$|a_i| = \sqrt{q}$ (Hypothèse de Riemann).
Si C est une courbe définie sur k,

$$\forall n \in \mathbb{N},\ |C(\mathbb{F}_{q^n})| = q^n + 1 - \sum a_i^n.$$

Etudions maintenant certaines propriétés des polynômes caractéristiques.
Soit K un corps local complet pour une valuation discrète v de corps résiduel $k = \mathbb{F}_q$ et

d'anneau des entiers $\mathcal{O}$. Soit A une variété abélienne sur K ayant bonne réduction. On note $\tilde{A}/k$ sa réduction. Si $f : A \to B$ une isogénie alors B a également bonne réduction et on peut définir une isogénie $\tilde{f} : \tilde{A} \to \tilde{B}$ qui rend le diagramme suivant commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ \tilde{A} & \xrightarrow{\tilde{f}} & \tilde{B} \end{array}$$

Proposition 2.16
Supposons $A = B$ alors $\chi_f = \chi_{\tilde{f}}$. En particulier $\deg(f) = \deg(\tilde{f})$ *et* $\mathrm{End}(A) \to \mathrm{End}(\tilde{A})$ *est injective.*

Démonstration :
Considérons le modèle de Néron $\mathcal{A}/\mathcal{O}$ de A. Par propreté, toute endomorphisme g de A se prolonge en une isogénie $\mathcal{G} : \mathcal{A} \to \mathcal{A}$. Comme $\mathrm{Spec}(\mathcal{O})$ est connexe, $\deg \mathcal{G}_{|K} = \deg \mathcal{G}_{|k}$ donc $\deg g = \deg \tilde{g}$. Par définition du polynôme caractéristique, on peut alors conclure.

Si K est maintenant un corps de nombre et A/K une variété abélienne, $A(\mathbb{C})$ est un tore complexe $\mathbb{C}^g/\Lambda$ avec $\Lambda \simeq \mathrm{H}_1(A, \mathbb{Z})$. En plus de la représentation l-adique, $\mathrm{End}^0(A)$ admet deux autres représentations fidèles :

- $\rho_{\mathbb{C}} : \mathrm{End}^0(A) \to \mathrm{End}(\mathbb{C}^g)$ appelée représentation complexe. Elle est équivalente à la représentation sur les différentielles invariantes.
- $\rho_{\mathbb{Z}} : \mathrm{End}^0(A) \to \mathrm{End}(\Lambda \otimes \mathbb{Q})$ appelée représentation rationnelle.

La représentation l-adique et la représentation rationnelle sont équivalentes (après tensorisation par $\mathbb{Q}_l$). La représentation rationnelle est la somme de la représentation complexe et de sa conjuguée. On conclut ainsi :

Proposition 2.17
Soit $f \in \mathrm{End}^0(A)$, avec A une variété abélienne complexe. Alors

$$\chi_f(X) = \det(\rho_{\mathbb{Z}}(f) - XI_{2g}) = \det(\rho_{\mathbb{C}}(f) - XI_g)\det(\overline{\rho_{\mathbb{C}}(f)} - XI_g).$$

Remarque :
Lorsque de plus $A = \mathrm{Jac}(C)$, on peut considérer un plongement canonique $\psi : C \to \mathrm{Jac}(C)$ qui permet d'identifier $\mathrm{H}^0(A, \Omega^1)$ et $\mathrm{H}^0(C, \Omega^1)$ en associant à une différentielle invariante ω sur A, la différentielle régulière $\omega \circ \psi$. Via cette identification, la représentation complexe est équivalente à une représentation sur les différentielles régulières de C.

2.2.2 Ordinarité

Soit A une variété abélienne de dimension g sur $k = \mathbb{F}_q$ avec $q = p^N$. On note

- $\phi : A \to A$ l'endomorphisme de Frobenius de A (de degré q^g).

– $V : A \to A$ son isogénie contragradiante (i.e. telle que $\phi V = V\phi = q$) appelée Verschiebung .
– Fr : $A \to A^{(1)}$ le petit Frobenius d'images itérées $A^{(i)}$ (au lieu de la notation habituelle $A^{(p^i)}$) de degré p^g.
– Ve : $A^{(1)} \to A$ son isogénie contragradiante.

Remarque :
Nous réservons le terme isogénie duale d'une isogénie $f : A \to B$ à l'isogénie $\hat{f} : \hat{B} \to \hat{A}$. Notons que si A est une variété polarisée, on peut définir l'involution de Rosati † : $\mathrm{End}^0(A) \to \mathrm{End}^0(A)$. Pour k un corps fini, $V = \phi^\dagger$ si et seulement si la polarisation est rationnelle sur k (cf. [Ser01]). C'était bien le cas dans le paragraphe précédent, ce qui justifie à posteriori l'appelation isogénie duale pour le Verschiebung des courbes elliptiques.

Le p-rang est un invariant important qui stratifie l'espace des modules des variétés abéliennes sur $\overline{k}$. Nous allons nous intéresser au cas générique que constituent les variétés abéliennes ordinaires :

Définition 2.18 [Del69]
Une variété abélienne A sur k de dimension g est dite ordinaire si elle vérifie l'une des conditions équivalentes suivantes

1. *$A[p](\overline{k})$ est de cardinal maximal égal à p^g. On dit encore que son p-rang est égal à g (voir partie I).*
2. *La composante neutre du schéma en groupe $A[p]$ est de type multiplicatif (donc géométriquement isomorphe à une puissance de μ_p).*
3. *V, Ve sont séparables.*
4. *La moitié exactement des racines de χ_A dans $\overline{\mathbb{Q}}_p$ sont des unités p-adiques. En d'autres termes, X^{g+1} ne divise pas $\chi_A(X) \pmod p$.*

Le dernier critère fournit en pratique un bon moyen de tester l'ordinarité (voir également la partie I : la réduction modulo p du polynôme caractéristique donne le p-rang de la variété abélienne).

Si de plus A est k-simple, on a les conséquences suivantes pour son anneau des endomorphismes :

Proposition 2.19 [Gon98]
Si A est ordinaire, alors $\mathrm{End}_k^0(A) = \mathbb{Q}(\phi)$ (équivalent à $[\mathrm{End}_k^0(A) : \mathbb{Q}] = 2g$ ou encore χ_A n'a que des racines simples).
Réciproquement, si $\mathrm{End}_k^0(A)$ est commutatif (équivalent à $\mathrm{End}_k^0(A) = \mathbb{Q}(\phi)$) et p totalement décomposé dans $\mathbb{Q}(\phi)$ alors A est ordinaire.

2.2.3 Relèvement canonique

On reprend les notations du paragraphe précédent que l'on complète ainsi : K est l'unique extension non ramifiée de $\mathbb{Q}_p$ de valuation discrète v, d'anneau des entiers $\mathcal{O}$, d'idéal maximal $\mathcal{M}$ et de corps résiduel k.

Les variétés abéliennes ordinaires ont des propriétés agréables vis-à-vis de la théorie du relèvement :

Théorème 2.20 [Mes72, V, th.3.3, Cor. 3.4]
Il existe un unique (à isomorphisme près) schéma abélien $A^\uparrow$ sur Spec($\mathcal{O}$) caractérisé par le fait que sa fibre spéciale est isomorphe à A et que

$$\mathrm{End}_K(A^\uparrow) \simeq \mathrm{End}_k(A).$$

On appelle $A^\uparrow$ le relèvement canonique de A. Si $f \in \mathrm{End}_k(A)$, on note $f^\uparrow \in \mathrm{End}_K(A^\uparrow)$ son relèvement canonique.

Remarque :
Ce théorème a été démontré dans le cas des courbes elliptiques par Deuring ([Deu41], [Lan70], voir aussi [Sil92] pour l'interprétation en tant que groupe formel) puis généralisé par Lubin, Serre et Tate [LST64].

Il suit de la démonstration du théorème 2.20 que :

Corollaire 2.21
Soit $\hat{A}$ la variété duale de A. Alors $(\hat{A})^\uparrow \simeq \hat{A^\uparrow}$.
De plus, toute polarisation de A définie sur k (resp. polarisation principale) de A se relève en une polarisation de $A^\uparrow$ définie sur K (resp. polarisation principale).

Sur k, le petit Frobenius coïncide avec l'action galoisienne du Frobenius de k. Si on appelle σ la substitution de Frobenius de $K/\mathbb{Q}_p$, qui relève l'action galoisienne sur k, σ n'est pas le relèvement du petit Frobenius. On a toutefois :

Corollaire 2.22 [Mes72, Appendix, Cor 1.2]
$A^\uparrow$ est le relèvement canonique de A si et seulement si il existe $\mathrm{Fr}^\uparrow : A^\uparrow \to {}^\sigma(A^\uparrow)$ *relevant* Fr.

Remarque :
Il découle des travaux de Shimura-Taniyama sur les variétés abéliennes de type CM ([Shi98], voir également [Oor97]) qu'on peut en fait définir le modèle canonique sur $\overline{\mathbb{Q}}$. On utilisera cette propriété au paragraphe suivant afin de permettre l'emploi des outils de la géométrie complexe introduits au chapitre 1. Si $\mathcal{A}$ est le relèvement canonique sur K, on notera $\mathcal{A}_{\mathbb{C}}$ le relèvement canonique vu sur $\overline{\mathbb{Q}}$. Un point de vue complémentaire est celui de Deligne [Del69] : si on introduit un plongement $\psi : \overline{\mathbb{Q}}_p^{nr} \hookrightarrow \mathbb{C}$, alors $\mathcal{A}_{\mathbb{C}} = \mathcal{A} \otimes_\psi \mathbb{C}$. En

particulier, cette extension des scalaires induit fonctoriellement un isomorphisme entre $\mathrm{H}_1(\mathcal{A}_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{Z}_l$ et $T_l(\mathcal{A})$. Par la suite, si X est une variété définie sur K, on notera $X_{\mathbb{C}} = X \otimes_{\psi} \mathbb{C}$.

2.2.4 Application à l'A.G.M.

On se restreint désormais au cas $p = 2$. La variété abélienne A/k est supposée ordinaire, principalement polarisée sur k et simple. On suppose de plus que les 2^g points de 2-torsion de A sont définis sur k.

Soit $A^{\uparrow}$ son relèvement canonique et $F = \mathrm{Fr}^{\uparrow}$. On note $\mathcal{A} = A^{\uparrow}(K)$.

Lemme 2.23
Tous les points de 2-torsion de $\mathcal{A}$ sont définis sur K.

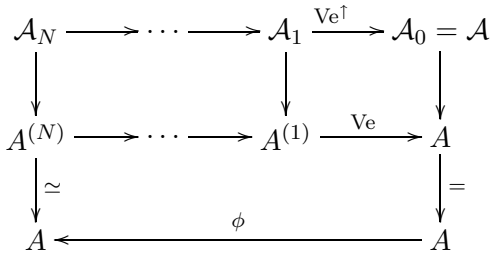
Démonstration :
A étant ordinaire, la partie locale de $A[2]$ n'a pas de point sur k. Tous les points de $A[2]^{et}$ sont donc rationnels. Le corps K étant complet ceci implique que $A^{\uparrow}[2]^{et} = (\mathbb{Z}/2\mathbb{Z})^g$. Or $A^{\uparrow}[2] = A^{\uparrow}[2]^{loc} \times A^{\uparrow}[2]^{et} = (\mu_2)^g \times (\mathbb{Z}/2\mathbb{Z})^g$ car $A^{\uparrow}$ est le relèvement canonique (cf. [Del69]) et $A^{\uparrow}[2]^{loc}$ est le dual de Cartier de $A^{\uparrow}[2]^{et}$. On a ainsi $\mathcal{A}[2] = (\mathbb{Z}/2\mathbb{Z})^{2g}$.

En particulier, le noyau de F est défini sur K. On peut préciser :

Lemme 2.24
$N = (\ker F)(K)$ est un $\mathbb{F}_2$-espace vectoriel isotrope maximal pour le couplage de Weil (induit par le relèvement de la polarisation principale).

Démonstration :
Comme A est ordinaire, le schéma en groupes fini et plat $\ker F$ est de type multiplicatif. Son dual de Cartier est donc étale. La polarisation principale de A se relève en une polarisation principale sur $A^{\uparrow}$ qui permet de définir le couplage de Weil de $A^{\uparrow}[2] \times A^{\uparrow}[2] \to \mu_2$. Ce couplage étant non dégénérée, on a $(\ker F)^{\perp} = \ker(A^{\uparrow}[2] \to \mathrm{Hom}(\ker F, \mu_2))$ et donc $A^{\uparrow}[2]/(\ker F)^{\perp}$ s'identifie au dual de Cartier de $\ker F$. Ce dernier est en particulier étale. Comme tout morphisme d'un schéma en groupes de type multiplicatif dans un schéma en groupes étale est nul, $\ker F$ est un sous-schéma de $(\ker F)^{\perp}$. En particulier $N = (\ker F)(K)$ est un sous-groupe isotrope maximal de $\mathcal{A}[2](K)$.

On considère la tour de 2-isogénies suivante similaire au cas elliptique



où $\mathcal{A}_{i+1} = {}^{\sigma}\mathcal{A}_i$ d'après le corollaire 2.22. Puisque les sous-groupes définissant les isogénies sont isotropes, cette tour d'isogénie est naturellement polarisée. Par unicité du relèvement canonique à isomorphisme près, $\mathcal{A}_N$ et $\mathcal{A}$ sont isomorphes. Notons $\mu : \mathcal{A}_N \to \mathcal{A}$ un isomorphisme. La polarisation de A étant définie sur k, par commutativité du diagramme précédent, μ est en fait un isomorphisme de variétés abéliennes principalement polarisées.

Nous allons avoir besoin du lemme suivant :

Lemme 2.25 [Mil86]
Soit $(A/\mathbb{C}, \lambda)$ une variété abélienne polarisée. Soit E la forme alternée sur $\Lambda = \mathrm{H}_1(A, \mathbb{Z})$ qui lui est associée. Alors le diagramme suivant

$$\begin{array}{rccccc} \tilde{E}: & \mathrm{H}_1(\mathrm{A},\mathbb{Z}) & \times & \mathrm{H}_1(\mathrm{A},\mathbb{Z}) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & \downarrow & & \downarrow & & \downarrow \\ e_2^{\lambda}: & A[2] & \times & A[2] & \longrightarrow & \{\pm 1\} \end{array}$$

commute, i.e. $e_2^{\lambda}(a/2, a'/2) = (-1)^{\tilde{E}(a,a')}$ pour a, a' deux périodes quelconques.

En d'autres termes, pour une variété principalement polarisée, toute base symplectique pour le couplage d'intersection est une base symplectique pour le couplage de Weil. Comme $N = \ker(F)(K)$ est isotrope pour le couplage de Weil, $\ker(\mathrm{Ve}^{\uparrow})(K) = \mathcal{A}[2]/N = N^{\perp}$ l'est également. On peut donc choisir une base symplectique (Γ, Δ) de $\mathrm{H}_1(\mathcal{A}_{\mathbb{C}}, \mathbb{Z})$ de telle sorte que $\frac{1}{2} < \gamma_1, \ldots, \gamma_g >= N_{\mathbb{C}}$. Si $\mathcal{A}_{\mathbb{C}} = \mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g\Omega$, alors le choix de la base ci-dessus montre que

$$(\mathcal{A}_N)_{\mathbb{C}} = \mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g 2^N \Omega.$$

Notons $\mu_{\mathbb{C}} : (\mathcal{A}_N)_{\mathbb{C}} \to \mathcal{A}_{\mathbb{C}}$ l'isomorphisme qui se déduit de μ. Les 2^g points de 2-torsion de A étant rationnels, l'action du Frobenius est triviale sur ces points. Par commutativité du diagramme précédent, il en est de même de $\mu_{\mathbb{C}}$ sur les relèvements de ces points. Par dualité, on a le même résultat sur les 2^g points de N et donc sur tous les points de 2-torsion. On en déduit :

Proposition 2.26
$\mathcal{A}_{\mathbb{C}}$ et $(\mathcal{A}_N)_{\mathbb{C}}$ sont deux représentants d'une classe de $\mathbb{H}_g/\Gamma_g(2)$.

Exemple :
Considérons le cas $g = 1$ et $N = 1$. La seule courbe elliptique ordinaire sur $\mathbb{F}_2$ est $y^2 + xy = x^3 + x$ d'invariant 1 et d'anneau des endomorphismes l'anneau des entiers de

$\mathbb{Q}(\sqrt{-7})$. D'après [Sil94, prop. 2.3.1], son relèvement canonique sur $\mathbb{Q}$ est donc la courbe d'invariant $j = -3375$. Celle-ci est isomorphe à $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ avec $\tau = (5+\sqrt{-7})/4$. Or on a

$$\frac{\tau}{2} = \frac{\tau+2}{-2\tau+3}$$

dont la matrice associée est $\begin{pmatrix} 1 & 2 \\ -2 & 3 \end{pmatrix} \in \Gamma_1(2)$. On a de plus $\mathbb{Z} + \mathbb{Z}\tau = u(\mathbb{Z} + \mathbb{Z}\tau/2)$ avec $u = -2\tau + 3 = (-1-\sqrt{-7})/2$ de norme 2.

Soit $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g(2)$ la matrice représentant $\mu_{\mathbb{C}}$. D'après le corollaire 1.27, pour toute caractéristique entière $[\epsilon]$

$$\vartheta[\epsilon](0, 2^N\Omega)^2 = \pm \det(C\Omega + D) \cdot \vartheta[\epsilon](0,\Omega)^2.$$

D'autre part, d'après la proposition 1.23, l'action de $\mu_{\mathbb{C}}$ sur $\mathbb{C}^g$ est donnée par $z \mapsto (C\Omega + D)^{-1}z$. On a ainsi

$$\mu_{\mathbb{C}}^*(dz_1 \wedge \ldots \wedge dz_g) = \det(C\Omega + D)^{-1} \cdot (dz_1^{(N)} \wedge \ldots \wedge dz_g^{(N)}).$$

Avec le choix des bases effectuées ci-dessus, les isogénies $\mathrm{Ve}_{\mathbb{C}}$ agissent trivialement sur les différentielles. On en conclut :

Théorème 2.27
Pour toute caractéristique $[\epsilon]$ entière, on a

$$\vartheta[\epsilon](0,\Omega)^2 = \pm \det(\rho_{\mathbb{C}}(V_{\mathbb{C}}^{\uparrow})) \cdot \vartheta[\epsilon](0, 2^N\Omega)^2.$$

La variété abélienne A étant ordinaire et simple, la proposition 2.19 montre que $\mathrm{End}^0(A) = \mathbb{Q}(\phi)$. Par définition du relèvement canonique, $\mathrm{End}(\mathcal{A}_{\mathbb{C}}) = \mathrm{End}(\mathcal{A}) = \mathbb{Q}(\phi)$ et $\mathcal{A}_{\mathbb{C}}$ est à multiplication complexe. En particulier si $\phi_1, \ldots, \phi_{2g}$ désigne $2g$ plongements complexes de $\mathbb{Q}(\phi)$ telles que $\phi_{g+i} = \overline{\phi_i}$ pour $1 \leq i \leq g$, alors la représentation complexe $\rho_{\mathbb{C}}$ est équivalente à la somme des ϕ_i, $i = 1, \ldots, g$. Il existe donc une base de différentielles invariantes ω_i telles que $\forall f \in \mathbb{Q}(\phi)$, $f^*(\omega_i) = \phi_i(f)\,\omega_i$. Appliquons cela au cas $f = V_{\mathbb{C}}^{\uparrow}$. Comme A est ordinaire, la définition 2.18 montre d'une part que V est séparable et d'autre part que le polynôme caractéristique de A possède exactement g racines, $\pi_1, \ldots, \pi_g$ qui sont des unités 2-adiques. La séparabilité entraine que pour toute différentielle invariante ω, $V^*(\omega) \neq 0$ donc, à permutation près, $\forall i \in \{1, \ldots, g\}$, $\phi_i(V_{\mathbb{C}}^{\uparrow}) = \pi_i$. En particulier, $\det(\rho_{\mathbb{C}}(V_{\mathbb{C}}^{\uparrow})) = \pi_1 \ldots \pi_g$.

Théorème 2.28
Soit $\pi_1, \ldots, \pi_g$ les racines de χ_A qui sont des unités 2-adiques. Avec les notations ci-dessus, supposons qu'il existe $[\epsilon]$ tel que $\vartheta[\epsilon](0,\Omega) \neq 0$. Alors $\vartheta[\epsilon](0, 2^N\Omega)$ est non nulle et

$$\frac{\vartheta[\epsilon](0,\Omega)^2}{\vartheta[\epsilon](0, 2^N\Omega)^2} = \pm(\pi_1 \ldots \pi_g).$$

Nous sommes ainsi parvenu à une généralisation de la formule du cas elliptique. Dans une prépublication, R. Carls [Car02] montre comment généraliser la partie itérative de la méthode précédente. Nous rappelons son théorème principal.

Théorème 2.29 [Car02, Th.3]
Soit A une variété abélienne ordinaire sur k, $\mathcal{A}/\mathcal{O}$ un schéma abélien de fibre spéciale A. On définit alors une suite

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

où les noyaux des isogénies sont les composantes $\mathcal{A}_i[2]^{loc}$. On a alors

$$\lim_{n\to\infty} \mathcal{A}_{nN} = A^{\uparrow}$$

i.e. pour tout n, $(\mathcal{A}_{Nn})/\mathcal{O}^{(Nn+1)} = (A^{\uparrow}_{Nn})/\mathcal{O}^{(Nn+1)}$ où l'on note $\mathcal{O}^{(i)} = \mathcal{O}/\mathcal{M}^i$.

En particulier, la convergence est linéaire. Pratiquement cela signifie qu'après n itérations (qui sont réalisées par les formules de duplication (proposition 1.19) pour les fonctions thêta caractéristiques) on obtient une variété $\mathcal{A}_n$ à partir de laquelle toute la théorie précédente est valable à la précision 2-adique n. D'où le résultat final en combinant les deux théorèmes précédents :

Théorème 2.30
Soit $\pi_1, \dots, \pi_g$ les racines de χ_A qui sont des unités 2-adiques. Considérons alors un relèvement quelconque $\mathcal{A}$ de A sur K. On effectue n itérations de la suite d'isogénies du théorème 2.29 dont on reprend les notations. Si $\vartheta[\epsilon](0,\Omega)$ est une thêta constante non nulle associée à $(\mathcal{A}_n)/\mathbb{C}$ alors $\vartheta[\epsilon](0,2^N\Omega)$ est non nulle et le rapport

$$\frac{\vartheta[\epsilon](0,\Omega)^2}{\vartheta[\epsilon](0,2^N\Omega)^2}$$

est égal à $\pm(\pi_1 \dots \pi_g)$ avec une précision 2-adique $n+1$.

Nous souhaitons appliquer cette théorie à la détermination du polynôme caractéristique d'une variété abélienne ordinaire sur $\mathbb{F}_{2^N}$. Le calcul des rapports initiaux $\vartheta[\epsilon](0,\Omega)^2/\vartheta[0](0,\Omega)^2$ constitue la première étape de ce travail. Dans les cas hyperelliptiques, cela peut être effectué par la formule de Thomae [Mum83, II]. Dans le cas du genre 3 non hyperelliptique, c'est l'objet du chapitre suivant.

Chapitre 3

La détermination des thêta constantes dans le cas de genre 3 non hyperelliptique

Nous donnons dans ce chapitre les formules permettant la détermination algébrique du rapport des thêta constantes pour une courbe de genre 3 non hyperelliptique sur $\mathbb{C}$. Ces formules (découvertes par Weber) s'appuient sur la connaissance des 28 bitangentes à une quartique plane lisse, sujet cher à la géométrie du XIXème siècle. Une partie préliminaire introduit la notion de système principal qui permet de comprendre de manière naturelle la combinatoire sous-jacente au problème.

3.1 Système principal

Ce paragraphe a pour but de généraliser la définition des caractéristiques entières définies au paragraphe 1.1.2 afin d'en donner une formulation indépendante du choix d'une base pour l'homologie et d'introduire la notion de système principal. C'est la formulation moderne utilisée dans [GH01] dont nous reprenons ici les principales définitions et propriétés. Nous démontrons également quelques lemmes techniques que nous utiliserons dans les paragraphes ultérieurs.

3.1.1 Forme quadratique et caractéristique

Soit V un $\mathbb{F}_2$-espace vectoriel de dimension $2g$ et $\langle , \rangle$ une forme bilinéaire non dégénérée alternée (i.e. $\langle v, v\rangle = 0$, $\forall v \in V$ et l'application $v \mapsto f_v : u \mapsto \langle u, v\rangle$ est un isomorphisme de V sur son dual).
On note $\mathrm{Sp}(V)$ le groupe des automorphismes de V qui préservent $\langle , \rangle$.

Définition 3.1
Un sous-espace $X \subset V$ est dit isotrope si $\langle x, x'\rangle = 0$, $\forall x, x' \in X$.

Un sous-espace X isotrope maximal (pour l'inclusion) est de dimension g et on peut lui associer une décomposition $V = X \oplus Y$ où Y est isotrope maximal et en dualité pour $\langle , \rangle$ avec X.

Notation 3.1.1
Dans la suite si $(e_1, \dots e_g)$ est une base isotrope maximale de X on note $(f_1, \dots, f_g)$ la base duale de Y. On dit que $(e_1, \dots, e_g, f_1, \dots, f_g)$ est une base symplectique de V.

Définition 3.2
Une fonction $q : V \to \mathbb{F}_2$ est appelée forme quadratique sur V (relativement à $\langle , \rangle$) si

$$q(v + u) = q(v) + q(u) + \langle v, u \rangle.$$

On note QV l'ensemble des formes quadratiques sur V. L'ensemble QV est un espace principalement homogène sur V :

- si $q \in$ QV et $v \in V$ on définit $q + v$ par $(q + v)(u) = q(u) + \langle v, u \rangle$, $\forall u \in V$.
- si $q, q' \in$ QV on définit $v = q + q'$ par l'unique v tel que $\langle v, u \rangle = q(u) + q'(u)$, $\forall u \in V$.

Cela confère à $W = V \cup$ QV une structure de $\mathbb{F}_2$-espace vectoriel de dimension $2g + 1$. Le groupe $\mathrm{Sp}(V)$ agit sur QV par $q \mapsto Tq$ définie par : $Tq(v) = q(T^{-1}v)$. On peut étendre linéairement cette action sur W.

Définition 3.3
Soit $(e_1, \dots, e_g, f_1, \dots, f_g)$ une base symplectique et $q \in QV$. On définit l'invariant d'Arf de q par $|q| = \sum q(e_i)q(f_i)$.

En fait ceci est indépendant du choix d'une base :

Proposition 3.4 [GH01, prop.1.11]
$|q|$ est indépendant du choix d'une base symplectique. On a les formules :

- $|Tq| = |q|$, $\forall T \in Sp(V)$.
- $|q + v| = |q| + q(v)$, $\forall v \in V$.

De plus le groupe $Sp(V)$ a deux orbites sur QV, la première constituée des $2^{g-1}(2^g + 1)$ formes d'invariant 0 dites paires, et la deuxième des $2^{g-1}(2^g - 1)$ formes d'invariant 1 dites impaires.

Remarque :
Soit $(e_1, \dots, e_g, f_1, \dots, f_g)$ une base symplectique. La forme $q \in$ QV est entièrement déterminée par les $q(e_i), q(f_i)$ qui valent 0 ou 1. On peut donc noter $q = \begin{bmatrix} q(e_i) \\ q(f_i) \end{bmatrix}$. De même si $v = \sum \alpha_i e_i + \sum \beta_i f_i$ on note $v = \begin{pmatrix} \beta_i \\ \alpha_i \end{pmatrix}$ (dans cet ordre).

Avec ces notations, on a par exemple si $q = \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$, $q' = \begin{bmatrix} \delta \\ \delta' \end{bmatrix}$ et $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

$$q + v = \begin{bmatrix} \varepsilon + \alpha \\ \varepsilon' + \beta \end{bmatrix} \text{ et } q + q' = \begin{pmatrix} \varepsilon + \delta \\ \varepsilon' + \delta' \end{pmatrix}$$

et $|q| = \sum \varepsilon_i \varepsilon'_i$.
Ces notations sont alors cohérentes avec celles de Rauch et Farkas [RF74] introduites au paragraphe 1.1.2 et de Weber [Web76] pour les caractéristiques entières réduites et les demi-périodes. Dans ce chapitre, on ne considère que des caractéristiques entières réduites :

Définition 3.5
Soit $(e_1, \ldots, e_g, f_1, \ldots, f_g)$ une base symplectique fixée. Avec les notations ci-dessus, on appelle caractéristique la matrice $2 \times g$ d'une forme quadratique. La parité d'une caractéristique est celle de sa forme quadratique associée.

Lorsqu'une base est fixée, on utilisera la désignation de caractéristique de préférence à celle de forme.

3.1.2 Ensemble principal

Soit $S = \{q_1, \ldots, q_{2g+1}\}$ un ensemble de $2g+1$ vecteurs indépendants engendrant W et appartenant à QV. Si $w = \sum \alpha_i q_i$ avec $\alpha_i = 0, 1 \in \mathbb{N}$ on définit $\#w = \sum \alpha_i$.

Définition 3.6
On dit que S est principal si l'invariant d'Arf de $q = \sum \alpha_i q_i$ dans QV ne dépend que de la classe de l'entier impair $\#q \pmod 4$.

On remarque tout de suite qu'un tel ensemble est tel que $|q_1| = \ldots = |q_{2g+1}|$. On note également $q_S = \sum q_i$ qui est tel que $|q_S| \equiv |q_i| + g \pmod 2$.

Proposition 3.7 [GH01, prop 2.1]
Pour tout g il existe un ensemble principal avec $|q_i| = \begin{cases} 0 & g \equiv 0, 1 \pmod 4 \\ 1 & g \equiv 2, 3 \pmod 4 \end{cases}$
De plus $Sp(V)$ agit transitivement sur l'ensemble des ensembles principaux.

La notion d'ensemble principal est également développée dans [RF74] mais d'un autre point de vue :

Théorème 3.8
Un ensemble $S = \{q_1, \ldots, q_{2g+1}\}$ de $2g+1$ formes est un ensemble principal si et seulement si toutes les formes ont même parité et si pour tout $q_i \in S$ on a $\langle q_i + q_j, q_i + q_k \rangle = 1$ pour i, j, k distincts (on dit que l'ensemble S est azygétique).

Démonstration :
Soit $S = \{q_1, \ldots, q_{2g+1}\}$ un ensemble principal il suffit de montrer qu'il est azygétique. En calculant avec une base symplectique on peut facilement montrer la formule suivante :

$$|q_i + q_j + q_k| = |q_i| + |q_j| + |q_k| + \langle q_i + q_j, q_i + q_k \rangle$$

Puisque l'ensemble S est principal, les $|q_i|$ sont tous égaux et $|q_i + q_j + q_k|$ est de parité opposée donc dans tous les cas $\langle q_i + q_j, q_i + q_k \rangle = 1$.
La réciproque découle de [RF74, II.th. 8].

Pour faire le lien avec la notion de «vollständigen Systeme» de Weber, nous allons particulariser ces résultats au cas $g = 3$. Par définition, un ensemble principal est alors un ensemble $S = \{q_1, \ldots, q_7\}$ de 7 formes quadratiques impaires formant une base de W et telles que

- $q_i + q_j + q_k$ est paire pour i, j, k distincts.
- $q_i + q_j + q_k + q_l + q_m$ est impaire pour i, j, k, l, m distincts.
- $q_S = \sum q_i$ est paire.

On voit pour des raisons de cardinalité que toute forme impaire s'écrit soit q_i soit $q_S + q_i + q_j$ $(i \neq j)$ et que toute forme paire distincte de q_S s'écrit $q_i + q_j + q_k$ avec i, j, k distincts.

On a le critère suivant :

Proposition 3.9 [GH01, prop.2.4]
Soit $S = \{q_1, \ldots, q_7\}$ sept formes impaires telles que $q_i + q_j + q_k$ est paire pour i, j, k distincts. Alors S est un ensemble principal.

On peut maintenant montrer l'équivalence avec la définition de Weber.

Théorème 3.10
Soit q une forme paire quelconque. Il existe un ensemble $S = \{q_1, \ldots, q_7\}$ (principal) de 7 formes impaires telles que $q + q_i + q_j$ pour tout $i \neq j$ soit impaire. Inversement tout ensemble de 7 formes impaires vérifiant cette propriété est un ensemble principal.

Démonstration :
Par transitivité de l'action de $\mathrm{Sp}(V)$ sur les formes paires, il existe un système principal $S = \{q_1, \ldots, q_7\}$ tel que $q = \sum q_i$. On sait qu'alors $q+q_i+q_j$ est impaire. Réciproquement, on se donne 7 formes impaires q_i vérifiant la propriété. Calculons $|q_i+q_j+q_k|$ pour i, j, k distincts. On a vu que

$$|q_i + q_j + q_k| = |q_i| + |q_j| + |q_k| + \langle q_i + q_j, q_i + q_k \rangle = 1 + \langle q_i + q_j, q_i + q_k \rangle.$$

Il suffit donc de montrer que $\langle q_i + q_j, q_i + q_k \rangle = 1$. Or on a

$$\langle q_i + q_j, q_i + q_k \rangle = \langle q + q_j, q + q_k \rangle + \langle q + q_i, q + q_j \rangle + \langle q + q_i, q + q_k \rangle$$

et par exemple

$$\underbrace{|q+q_j+q_k|}_{=1} = \underbrace{|q|}_{=0} + \underbrace{|q_i|}_{=1} + \underbrace{|q_j|}_{=1} + \langle q+q_j, q+q_k\rangle.$$

Donc $\langle q+q_j, q+q_k\rangle = 1$ et de même pour les deux autres. D'où le résultat.

Comment détermine-t-on effectivement un tel ensemble ? Pour cela, nous allons introduire la notion de groupe caractéristique.

Définition 3.11
Soit $v \in V \setminus \{0\}$. On appelle groupe (caractéristique) de v l'ensemble des paires de formes (q_i, q_j) tels que q_i et q_j soit impaires et $v = q_i + q_j$.

Remarque :
Weber parle également du groupe d'une caractéristique. En effet il a fait au préalable le choix d'une base symplectique. Une fois ce choix fait, il existe une forme privilégiée qui a $\sum \alpha_i e_i + \sum \beta_i f_i$ associe $\sum \alpha_i\beta_i$ et qui correspond à $[0] = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. L'application $v \mapsto [0]+v$ définit alors une bijection entre V et QV qui permet de confondre les deux notions (et de parler ainsi par exemple de la parité de v où du groupe de q). Nous effectuerons également cette identification pour éviter de surcharger les notations dans le calcul des thêta constantes.
Remarquons enfin que par transitivité de l'action de $\mathrm{Sp}(V)$ sur les formes paires, pour tout q_0 paire, il existe une base symplectique dans laquelle $q_0 = [0]$.

Lemme 3.12
Soit $v \in V \setminus \{0\}$. Alors le groupe de v est de cardinal 6.

Démonstration :
Soit $S = \{q_1 \dots, q_7\}$ un ensemble principal. On distingue alors plusieurs cas

- $v = q_S + q_1 = (q_S + q_1 + q_2) + (q_2) = (q_S + q_1 + q_3) + (q_3) = (q_S + q_1 + q_4) + (q_4) = (q_S + q_1 + q_5) + (q_5) = (q_S + q_1 + q_6) + (q_6) = (q_S + q_1 + q_7) + (q_7)$
- $v = q_1 + q_2 = (q_1) + (q_2) = (q_S + q_1 + q_3) + (q_S + q_2 + q_3) = (q_S + q_1 + q_4) + (q_S + q_2 + q_4) = (q_S + q_1 + q_5) + (q_S + q_2 + q_5) = (q_S + q_1 + q_6) + (q_S + q_2 + q_6) = (q_S + q_1 + q_7) + (q_S + q_2 + q_7)$
- $v = q_S + q_1 + q_2 + q_3 = (q_1) + (q_S + q_2 + q_3) = (q_2) + (q_S + q_1 + q_3) = (q_3) + (q_S + q_1 + q_2) = (q_S + q_4 + q_5) + (q_S + q_6 + q_7) = (q_S + q_4 + q_6) + (q_S + q_5 + q_7) = (q_S + q_4 + q_7) + (q_S + q_5 + q_6)$

qui à la numérotation près couvrent tous les cas. D'où le résultat.

Proposition 3.13 [Web76, VII p.25]
Soit q_S une forme paire et q_1 une forme impaire quelconque. On forme le groupe de

$q_S + q_1$

$$q_S + q_1 = q_2 + q_2' = q_3 + q_3' = q_4 + q_4' = q_5 + q_5' = q_6 + q_6' = q_7 + q_7'.$$

Pour une seule des deux caractéristiques q_2 ou q_2' (supposons q_2) le groupe de $q_S + q_2$ s'écrit alors

$$q_S + q_2 = q_1 + q_2' = q_3 + q_3'' = q_4 + q_4'' = q_5 + q_5'' = q_6 + q_6'' = q_7 + q_7''.$$

L'ensemble $\{q_1, \ldots, q_7\}$ est principal.

Exemple :

On suppose une base fixée et soit $q_S = [0]$. Choisissons $q_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ on a alors

$$\begin{aligned} q_S + q_1 &= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

Choisissons $q_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ on a

$$\begin{aligned} q_S + q_2 &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \end{aligned}$$

On a donc le système principal :

$$q_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad q_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad q_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad q_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$q_5 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad q_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad q_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Remarque :
On peut montrer (cf. [GH01]) que pour q_S fixé il existe 8 ensembles principaux de somme q_S. Les formes impaires étant au nombre de 28, chacune d'elles apparaît donc 2 fois dans chaque ensemble principal.

Nous allons maintenant donner pour références ultérieures les démonstrations de certaines propriétés (parmi les nombreuses sur le sujet) relatives aux caractéristiques :

Lemme 3.14
Soit $q_1+q_2 = q_3+q_4$ deux décompositions appartenant à un même groupe. Alors quelque soit q paire, soit $q+q_1+q_3$ est impaire soit $q+q_1+q_4$ est impaire.

Démonstration :
On choisit un ensemble principal de somme $q_S = q$ et on analyse les différents cas de la démonstration du lemme 3.12.

Lemme 3.15
Soit $\{x_i\}$ un ensemble principal de somme q_S et u_1, u_2, u_3 impaires telles que $q_S+x_1+u_1 = q_S+x_2+u_2 = q_S+x_3+u_3$ et telles que ces sommes soient paires. Alors

$$\begin{cases} u_1 = q_S + x_2 + x_3 \\ u_2 = q_S + x_1 + x_3 \\ u_3 = q_S + x_1 + x_2 \end{cases}$$

Démonstration :
On constate que $u_k = q_S + x_i^{(k)} + x_j^{(k)}$, pour $k = 1, 2, 3$, soit $x_1+x_2 = x_i^{(1)}+x_j^{(1)}+x_i^{(2)}+x_j^{(2)}$ et par unicité de l'écriture on a par exemple $x_j^{(1)} = x_j^{(2)}$ et donc $x_1+x_2 = x_i^{(1)}+x_i^{(2)}$. Si $x_i^{(1)} = x_1$ alors $q_S+x_1+u_1 = x_j^{(1)}$ est impaire : exclu. Donc $x_i^{(1)} = x_2$ et $x_i^{(2)} = x_1$. On a alors $u_1+u_3 = x_1+x_3 = x_2+x_j^{(1)}+x_i^{(3)}+x_j^{(3)}$ soit par exemple $x_i^{(3)} = x_2$ et alors $x_j^{(3)} = x_1$ puisque $q_S+x_3+u_3$ est paire. On a facilement $x_j^{(1)} = x_j^{(2)} = x_3$.

Lemme 3.16
Toute forme paire q peut s'écrire comme la somme de 3 formes impaires présentes deux à deux dans un même groupe mais non appariées.

Démonstration :
On choisit un ensemble principal $S = \{q_1, \ldots, q_7\}$ tel que $q_S \neq q$ et on peut alors supposer $q = q_1+q_2+q_3$. On a alors

$$q_S + q_4 = (q_1) + (q_S+q_1+q_4) = (q_2) + (q_S+q_2+q_4) = (q_3) + (q_S+q_3+q_4).$$

Lemme 3.17
Soit χ, χ' deux formes paires distinctes et p_1, p_2 deux formes impaires telles que $\chi+\chi' = p_1+p_2$. Alors les groupes $\chi+\chi'$ et $p_1+\chi'$ ont exactement 4 formes impaires en commun.

Démonstration :
On considère alors un ensemble principal $S = \{q_1, \ldots, q_7\}$ tel que $q_S = \chi'$ et $q_1 = p_1$. La forme χ étant différente de χ' on peut supposer $\chi = q_1+q_2+q_3$ et on alors

$$\begin{aligned} \chi'+\chi &= (q_1) + (q_S+q_2+q_3) = (q_2) + (q_S+q_1+q_3) = (q_3) + (q_S+q_1+q_2) \\ &= (q_S+q_4+q_5) + (q_S+q_6+q_7) = (q_S+q_4+q_6) + (q_S+q_5+q_7) \\ &= (q_S+q_4+q_7) + (q_S+q_5+q_6) \end{aligned}$$

et

$$\begin{aligned}\chi' + p_1 &= (q_S + q_1 + q_2) + (q_2) = (q_S + q_1 + q_3) + (q_3) = (q_S + q_1 + q_4) + (q_4) \\ &= (q_S + q_1 + q_5) + (q_5) = (q_S + q_1 + q_6) + (q_6) = (q_S + q_1 + q_7) + (q_7)\end{aligned}$$

qui possèdent $q_2, q_3, q_S + q_1 + q_3, q_S + q_1 + q_2$ en commun.

3.2 Plongement canonique d'une courbe de genre 3

Une courbe désignera par la suite une variété algébrique absolument irréductible, projective, lisse, de dimension 1 sur un corps k.

3.2.1 Rappels

Soit C une courbe sur k que l'on suppose algébriquement clos. Soit D un diviseur sur C on peut lui associer plusieurs constructions :

- (une classe d'isomorphismes) de fibrés inversibles que l'on note $L(D)$. On note également $\mathcal{O}(D)$ le faisceau des sections (régulières) de ce fibré.
- Un ensemble de fonctions rationnelles $\mathcal{L}(D) = \{f \in k(C)^* \ / \ (f) + D \geq 0\} \cup \{0\}$. Cet espace vectoriel est isomorphe à $H^0(C, \mathcal{O}(D))$ par l'application $f \mapsto f \otimes s_0$ où s_0 est une section de $L(D)$. On sait que cet espace est de dimension finie et on note $l(D) = \dim(\mathcal{L}(D))$.
- un système linéaire $|D|$ égal à l'ensemble des diviseurs effectifs linéairement équivalents à D. Cet ensemble est en bijection avec $\mathbb{P}(\mathcal{L}(D))$ et peut donc être muni d'une structure d'espace projectif. Si on suppose le système linéaire $|D|$ sans point base (i.e. l'intersection des supports des éléments de $|D|$ est vide) on peut définir une application $i_D : C \to \mathbb{P}(\mathcal{L}(D))^*$ en associant à P l'hyperplan des éléments $s \in \mathcal{L}(D)$ qui ne s'annulent pas en P. De manière plus explicite, si $s_0, \ldots, s_N$ est une base de $\mathcal{L}(D)$, on note $i_D(P) = (s_0(P) : \ldots : s_N(P))$.

Inversement, l'isomorphisme entre $\mathrm{Pic}(C)$ et $\mathrm{Div}(C)/\mathrm{Princ}(C)$ permet d'associer à chaque classe d'isomorphismes de fibrés inversibles L un diviseur D à équivalence linéaire près tel que $L = L(D)$. On note $H^0(L)$ l'espace vectoriel des sections régulières de L et $\mathrm{h}^0(L) = l(D)$ sa dimension.

Nous allons particulariser cela au cas du diviseur canonique K pour une courbe C de genre $g_C \geq 2$. On note $\mathcal{K} = L(K)$ le fibré associé au diviseur canonique. On rappelle que les sections de ce fibré sont canoniquement en bijection avec les différentielles régulières de la courbe. On a en particulier $l(K) = g_C$.

Avec ces notations, on a le théorème fondamental :

Théorème 3.18 (Th. Riemann-Roch) [Har75, Th. IV.1.3]
Pour tout diviseur D sur C,

$$l(D) - l(K - D) = \deg D + 1 - g_C.$$

Proposition 3.19
i_K est un plongement, appelé plongement canonique, si et seulement si C est non hyperelliptique.

Démonstration :
Il suffit de montrer que le fibré $\mathcal{K}$ est très ample et d'après les critères [Har75, IV.3.1] ceci est équivalent à montrer que $\forall P, Q \in C$ on a $\dim |K - P - Q| = g_C - 3$. Or d'après le théorème 3.18,

$$\dim |P + Q| - \dim |K - P - Q| = 2 + 1 - g_C.$$

On s'est ramené à étudier $\dim |P + Q|$.
Si la courbe est hyperelliptique il existe $f : C \to \mathbb{P}^1$ de degré 2. Le diviseur $D = f^*(\infty)$ est un diviseur effectif de degré 2. La fonction $f \in \mathcal{L}(D)$ donc $\dim |D| = 1$ et $\dim |K - P_1 - P_2| = g_C - 2$.
Inversement si $\dim |P + Q| > 0$, il existe une fonction non constante $f \in \mathcal{L}(P + Q)$ et donc un morphisme de degré 2 de C vers $\mathbb{P}^1$. La courbe est alors hyperelliptique.

Corollaire 3.20
C est non hyperelliptique si et seulement si quelque soit $P, Q \in C$ on a $l(P + Q) = 1$.

3.2.2 Cas des courbes de genre 3

Proposition 3.21
Soit C une courbe de genre 3 non hyperelliptique. Son plongement canonique est une quartique plane non singulière. Inversement toute quartique plane non singulière est le plongement canonique d'une courbe de genre 3 non hyperelliptique.

Démonstration :
Soit C une courbe de genre $g_C = 3$ non hyperelliptique. D'après la proposition 3.19, i_K est alors un plongement dans $\mathbb{P}^{g_C - 1}$ de degré $2g_C - 2 = 4$. La courbe $i_K(C)$ est une quartique plane non singulière.
Inversement si C est une quartique plane non singulière, c'est une courbe lisse de genre $g_C = \frac{(\deg C - 2)(\deg C - 1)}{2} = 3$. De plus la formule d'adjonction nous donne

$$\mathcal{K} = (\mathcal{K}_{\mathbb{P}^2} + C)|_C = (-3H + 4H)|_C = H|_C$$

où $\mathcal{K}_{\mathbb{P}^2}$ est le fibré canonique de $\mathbb{P}^2$ et H est le fibré hyperplan sur $\mathbb{P}^2$ associé à une section de $\mathcal{O}(1)(\mathbb{P}^2)$. Donc C est plongée canoniquement dans $\mathbb{P}^2$. En particulier C n'est pas hyperelliptique.

Remarque :
En fait toute courbe de $\mathbb{P}^{g_C - 1}$ non dégénérée de genre g et de degré $2g - 2$ provient d'un plongement canonique (cf. [GH78]).

Si $k = \mathbb{C}$, on peut donner une autre caractérisation de l'hyperellipticité. On rappelle qu'une thêta constante est la valeur $\vartheta[\epsilon](0)$ pour un ϵ pair (cf. paragraphe 1.1.2).

Proposition 3.22
Une courbe C de genre 3 est non hyperelliptique si et seulement si ses thêta constantes sont toutes non nulles.

Démonstration :
Soit C de genre 3 et $[\epsilon]$ une caractéristique paire. Alors d'après le théorème 1.33, $\vartheta[\epsilon](z,\Omega)$ est nulle en 0 si et seulement s'il existe un diviseur D de degré 2 tel que $u_{P_0}(D)+K_{P_0} \equiv \epsilon$ et $\mathrm{ind}(D) \geq 2$. Or $\mathrm{ind}(D) = l(D)$ donc on peut supposer $D = P_1 + P_2$ effectif et d'après le corollaire 3.20, $l(P_1+P_2) \geq 2$ est équivalent à C hyperelliptique.

3.3 Bitangentes des courbes de genre 3

On considère maintenant, et jusqu'à la fin du chapitre, une courbe C de genre 3 non hyperelliptique plongée canoniquement dans $\mathbb{P}^2$ (dont on notera les coordonnées (x_1,x_2,x_3)) sur un corps algébriquement clos k .
Le fibré canonique de C est la restriction du fibré linéaire sur $\mathbb{P}^2$. On a donc une correspondance biunivoque entre les droites de $\mathbb{P}^2$ et $|K|$ qui à une droite l associe le diviseur d'une différentielle régulière ω telle que $(\omega) = (l \cdot C)$.

Génériquement, une droite de $\mathbb{P}^2$ coupe la quartique C en quatre points distincts. Analysons les autres possibilités d'intersection

- $(l \cdot C) = 2P + Q + R$, P, Q, R distincts : la droite l est alors tangente à la courbe C en P.
- $(l \cdot C) = 3P + Q$, P, Q distincts : on dit que le point P est un point d'inflexion pour C.
- $(l \cdot C) = 2P + 2Q$, P, Q distincts : la droite l est tangente à C en P et Q. On dit que l est une bitangente de C.
- $(l \cdot C) = 4P$. On dit encore que la droite l est une bitangente. P est un point d'hyperinflexion. Mais ce cas n'est pas générique. En effet on considère l'ensemble $V \subset \mathbb{P}^{14} \times \mathbb{P}^2 \times (\mathbb{P}^2)^*$ des triplets (q,x,l) (q quartique, x point, l droite) avec les conditions $x \in q, x \in l$ et $\mathrm{J}^i_x q(l) = 0$ pour $i = 1,2,3$. On a en tout 5 conditions donc V est un espace de dimension $18-5 = 13$ donc de codimension 1 dans l'espace des quartiques.

Le fibré canonique étant ici la restriction du fibré hyperplan de $\mathbb{P}^2$, on a la proposition suivante.

Proposition 3.23
Les bitangentes sont en bijection canonique avec les différentielles régulières (à un coefficient multiplicatif près) qui ont deux zéros doubles.

Nous allons étudier les bitangentes de C géométriquement et analytiquement.

Définition 3.24
Soit L un fibré sur C. On dit que c'est un fibré thêta caractéristique si $L \in Pic^2(C)$ et

$L^2 = \mathcal{K}$. On note Σ l'ensemble de ces fibrés.
On définit $I(L) \equiv \dim H^0(C, \mathcal{O}(L)) \pmod 2$. On dit que L est pair (resp. impair) si $I(L) \equiv 0$ (resp. 1). On note Σ_0 (resp. Σ_1) l'ensemble des fibrés thêta caractéristique pairs (resp. impairs).

Lemme 3.25
On a une bijection canonique entre l'ensemble des bitangentes à C et Σ_1.

Démonstration :
Soit l une bitangente à C. On a $(l \cdot C) = 2P + 2Q \sim K$ et on définit $L = L(P + Q)$. On a bien sûr que $L \in \mathrm{Pic}^2(C)$ et $L^2 = L(2P + 2Q) = \mathcal{K}$. De plus $l(P + Q) = 1$ d'après le corollaire 3.20. Donc $L(D) \in \Sigma_1$.
Inversement soit $L \in \Sigma_1$. Comme $I(L) \equiv 1$ on a $h^0(L) \geq 1$ donc il existe une section (régulière) s de L. Si on note $D = (s)$ puisque $L = L(D) \in \mathrm{Pic}^2(C)$ on a $D \sim P + Q$ et $2D \sim K$. Donc $2P + 2Q$ est le diviseur d'intersection d'une bitangente.
Enfin, ces deux constructions sont réciproques l'une de l'autre.

Corollaire 3.26
Soit $L \in \Sigma$. Alors $L \in \Sigma_1$ si et seulement si il existe un diviseur effectif (unique) D de degré 2 tel que $L = L(D)$.

Démonstration :
En effet si $L = L(D) \in \Sigma_0$ avec D effectif on aurait $l(D) \geq 2$. Exclu.

Lemme 3.27
On a une bijection non canonique entre Σ et $Jac(C)[2]$.

Démonstration :
Soit $L = L(D_0) \in \Sigma$. A $\epsilon \in \mathrm{Jac}(C)[2]$ on associe $L = L(D_0 + \epsilon) \in \Sigma$. Cette application est bijective.

3.3.1 Cas où k est de caractéristique différente de 2

Dans ce cas $V = \mathrm{Jac}(C)[2](k)$ est un espace vectoriel de dimension 6 et il est de plus muni comme nous l'avons vu d'une forme bilinéaire symplectique non dégénérée provenant du couplage de Weil. L'ensemble Σ est alors un espace principalement homogène sur V qui peut être identifié avec l'ensemble des formes quadratiques sur V par : si $L = L(D) \in \Sigma$ et $v \in V$

$$L \circ v = l(D + v) + l(D) \pmod 2$$

en particulier $I(L) = l(D)$ correspond à l'invariant d'Arf sur cet espace (la notation $L \circ v$ est préférable à la notation $L(v)$ que l'on pourrait confondre avec celle du fibré $L(D+v)$.).

La connaissance du cardinal des formes impaires (proposition 3.4) et le lemme 3.25 montrent :

Corollaire 3.28
Une quartique plane non singulière possède 28 bitangentes distinctes.

Remarque :
Historiquement, on a d'abord utilisé une méthode géométrique pour évaluer le nombre de bitangentes. Supposons que k soit de caractéristique différente de 2 et 3 et soit $\phi : P \mapsto \mathrm{T}_P(C) \in (\mathbb{P}^2)^*$ ($T_P(C)$ tangente à C en P) le morphisme dont l'image notée C^* est appelée courbe duale de C . On montre facilement que le degré de C^*, encore appelé classe de C , est égal à $\deg C^* = 4 \cdot 3 = 12$ [Har75, IV.ex.2.3] et que les points d'inflexion (resp. les bitangentes) de C correspondent aux pointes (resp. aux nœuds ordinaires) de C^*.
De plus C et C^* sont birationnellement équivalentes donc si on suppose que C^* n'a pour singularités que des pointes et des nœuds ordinaires (c'est génériquement vrai) alors d'après la formule de Plücker

$$g_{C^*} = g_C = 3 = \frac{(12-1)(11-1)}{2} - |\{\text{nœuds}\}| - |\{\text{pointes}\}|.$$

Si C est générique, les points d'inflexion de C sont les points d'intersection de C avec sa courbe hessienne, ici de degré 6, soit 24 points. La formule ci-dessus nous donne alors $55 - 24 - 3 = 28$ nœuds sur C^* soit 28 bitangentes à C.

Les isomorphismes précédents permettent d'associer à une bitangente une forme impaire. On peut donc définir :

Définition 3.29
On appelle système d'Aronhold la donnée de 7 bitangentes dont les formes associées forment un ensemble principal.

Si β est une bitangente, on note $[\sqrt{\beta}]$ la forme qui lui est associée (voir lemme 3.43 pour une justification de la notation). Si (β_i), $i = 1 \dots 7$, est un système d'Aronhold de somme q_S on note β_{ij} les bitangentes dont la forme associée est $q_S + [\sqrt{\beta_i}] + [\sqrt{\beta_j}]$.

3.3.2 Cas particulier $k = \mathbb{C}$

On peut dans ce cas considérer C comme une surface de Riemann de genre 3 et on note comme au paragraphe 1.2 (Γ, Δ) une base symplectique de l'homologie, $\zeta = (\zeta_1, \zeta_2, \zeta_3)$ des différentielles régulières normales par rapport à cette base et Ω la matrice des périodes. On a alors des isomorphismes explicites entre

$$\mathrm{Jac}(C) = \mathrm{Pic}^0(C) \simeq \mathrm{Div}^0(C)/\mathrm{Princ}(C) \simeq \mathbb{C}^3/\mathbb{Z}^3 + \mathbb{Z}^3\Omega.$$

Le dernier isomorphisme est donné classiquement par l'application $u : D = \sum P_i - Q_i \mapsto \sum \int_{Q_i}^{P_i} \zeta$. Soit $P_0 \in C$ et $n \in \mathbb{N}^*$. Rappelons qu'on peut aussi définir une application $u_{P_0} : \mathrm{Div}^n(C) \to \mathrm{Jac}(C)$ par $u_{P_0}(D) = u(D - nP_0)$.
Le choix d'une base pour l'homologie détermine une forme symplectique non dégénérée

sur $\mathrm{Jac}(C)[2] \simeq \frac{1}{2}\mathrm{H}_1(C,\mathbb{Z})/\mathrm{H}_1(C,\mathbb{Z})$ et nous avons vu qu'elle coïncide avec le couplage de Weil (cf. lemme 2.25).
Ce choix permet en outre de préciser la bijection du lemme 3.27. En effet, il existe alors un fibré particulier $L_0 = L(D_0)$ qui correspond à la caractéristique [0] et dont on peut caractériser le diviseur de manière précise : le choix d'une base de l'homologie et d'un point base détermine une constante de Riemann K_{P_0} tel que $u_{P_0}(K) \equiv -2K_{P_0}$. On a alors pour $L(D) \in \Sigma$, $u_{P_0}(2D) \equiv u_{P_0}(K) \equiv -2K_{P_0}$ soit $u_{P_0}(D) + K_{P_0} \equiv \epsilon$ avec $\epsilon \in \mathrm{Jac}(C)[2]$. On définit D_0 par $u_{P_0}(D_0) + K_{P_0} \equiv 0$.

Proposition 3.30
On a une bijection entre Σ et $Jac(C)[2]$ donnée par : si $L = L(D) \in \Sigma$, on a $\forall P_0 \in C$ $u_{P_0}(D) + K_{P_0} \equiv \epsilon$ avec $\epsilon \in Jac(C)[2]$.

Remarque :
Remarquons que ϵ est en fait indépendant du choix d'une origine puisque $\forall P_0' \in C$ on a $K_{P_0'} \equiv K_{P_0} + 2u_{P_0}(P_0')$.

Définition 3.31
Si $\epsilon \in Jac(C)[2]$, on note $L = L_\epsilon$ le fibré thêta caractéristique associé. On notera également $[\epsilon]$ la caractéristique associée à ϵ (c'est un cas particulier de la définition 1.13).

3.3.3 Cas où $k = \overline{\mathbb{F}}_2$

Ce cas est fondamentalement différent du cas complexe. Nous reprenons ici l'étude qu'en font Stöhr et Voloch dans [SV87].
Soit $f \in k(C)$ telle que $df \neq 0$. D'après [Mum71] en développant f en série entière au voisinage d'un point, on constate que df n'a que des zéros et des pôles de multiplicités multiples de 2. On peut alors définir $(df) = 2D_0$. Le diviseur D_0 ne dépend pas du choix de f : en effet si $f_1, f_2 \in k(C) \setminus k(C)^2$, il existe $a, b \in k(C)$ tel que $f_1 = a^2 f_2 + b^2$ et $df_1 = a^2 df_2$ et donc si on note $(df_i) = 2D_i$ on a $D_1 = (a) + D_2$.

Définition 3.32
On appelle D_0 le diviseur thêta caractéristique canonique de C et $L(D_0)$ le fibré thêta caractéristique canonique.

Proposition 3.33 [SV87, prop.3.1]
Il existe une ($\frac{1}{2}$-linéaire) bijection entre l'espace des différentielles régulières exactes et $\mathcal{L}(D_0)$.

Proposition 3.34 [SV87, prop. 3.3]
Il y a une bijection canonique entre l'ensemble des différentielles régulières logarithmiques non nulles et l'ensemble des fibrés thêta caractéristiques non canoniques qui envoie w sur $L((w)/2)$.

On rappelle qu'une différentielle ω est dite exacte (resp. logarithmique) s'il existe $f \in k(C)$ (resp. $f \in k(C)^*$) telle que $\omega = df$ (resp. $\omega = df/f$). Remarquons que contrairement aux différentielles exactes, les différentielles logarithmiques ne forment pas un k-espace vectoriel mais uniquement un $\mathbb{F}_2$-espace vectoriel.

L'étude de ces différentielles peut être menée grâce à l'opérateur de Cartier C qui est un opérateur (1/2)-linéaire et qui vérifie en particulier :

Proposition 3.35 [Ser58]
- *ω est une différentielle exacte* $\iff$ $\mathrm{C}(\omega) = 0$.
- *ω est une différentielle logarithmique* $\iff$ $\mathrm{C}(\omega) = \omega$.

L'opérateur C n'est pas un opérateur linéaire mais il existe une décomposition de l'espace des différentielles régulières en somme directe de deux sous-espaces $V_s \oplus V_n$ telle que la restriction de C à V_n soit nilpotente et la restriction de C à V_s soit bijective. De plus les différentielles logarithmiques régulières forment une base de V_s.
On montre alors (cf. [Ser58, prop.10]) que la dimension de V_s est égale à l'invariant d'Hasse-Witt de la courbe, c'est-à-dire son p-rang (ici $p = 2$, voir paragraphe 1.4 partie I pour une définition). On a en particulier :

Corollaire 3.36
Le groupe des différentielles régulières logarithmiques est un groupe fini d'ordre 2^{γ_C} où γ_C est le 2-rang de la courbe.

Lorsque la courbe est ordinaire, $V_s = \mathrm{H}^0(C, \Omega)$ donc $\mathrm{C}(\omega) = 0$ si et seulement si $\omega = 0$. La dimension de l'espace des différentielles régulières exactes est donc 0 qui est aussi la dimension de $L(D_0)$ d'après la proposition 3.33. En particulier le corollaire 3.26 montre que $L(D_0) \notin \Sigma_1$. Par contre à chaque différentielle régulière logarithmique est associé un fibré de Σ_1 d'après la proposition 3.34. On a donc la conclusion suivante en utilisant le lemme 3.25.

Théorème 3.37
C est ordinaire si et seulement si elle a exactement 7 bitangentes.

Démonstration :
Il nous reste à voir que si C n'est pas ordinaire alors elle a moins de 7 bitangentes. En effet, si $\gamma_C = 0, 1$ ou 2 alors on a d'après ce qui précède que le nombre de bitangentes est $4, 2$ ou 1. D'où le résultat.

Grâce à ce résultat, on peut trouver une forme canonique pour C.

Proposition 3.38
C est isomorphe sur k à une courbe d'équation

$$(ax^2 + by^2 + cz^2 + dxy + exz + fyz)^2 - xyz(x + y + z) = 0$$

avec la condition suivante

$$abc(a+b+d)(a+c+e)(b+c+f)(a+b+c+d+e+f+1) \neq 0.$$

Inversement toutes les courbes qui vérifient ces conditions sont des courbes de genre 3 *ordinaires et non hyperelliptiques.*

Démonstration :
Remarquons qu'une droite est une bitangente en caractéristique 2 lorsque le polynôme qu'elle définit en exprimant l'appartenance à la droite et à la courbe n'a que des puissances paires en les variables. Considérons alors deux bitangentes qu'on peut prendre égales à x et y. Les coefficients en x^3z, z^3x, y^3z, z^3y doivent donc être nuls. Supposons que deux autres bitangentes soient concourantes en 0, soit par exemple $x - y = 0$ et $x - \alpha y = 0$. On aurait alors une équation de la forme $(\text{conique})^2 + xy(\text{droite})^2 = 0$. Mais alors toutes les droites passant par l'origine seraient des bitangentes : exclu. Au plus 3 bitangentes sont donc concourantes. Comme nous avons 7 bitangentes, on peut donc par une transformation linéaire prendre 4 des bitangentes pour $x, y, z, x+y+z$ d'où la forme annoncée.
Les conditions sur les coefficients s'obtiennent tout simplement en calculant les dérivées partielles et en exprimant la condition de lissité.
Inversement toute courbe définie par cette équation et qui vérifie les conditions sur les coefficients est une courbe de genre 3 non hyperelliptique d'après la proposition 3.21. De plus, on constate facilement que $x = 0, y = 0, z = 0, x + y + z = 0$ et $x = y, x = z, y = z$ sont des bitangentes à la courbe. La courbe est donc ordinaire par le théorème 3.37.

Remarque :
On pourra aussi consulter [Wal95] pour les cas de supersingularité.

Proposition 3.39
Si on suppose C ordinaire définie par une quartique à coefficients dans $k_0 = \mathbb{F}_{2^N}$, alors C est isomorphe à une quartique de la forme ci-dessus sur une extension de degré au plus 7 *de k_0.*

Démonstration :
Si les bitangentes sont définies sur k_0 on a le résultat. Les bitangentes sont déterminées par les diviseurs des différentielles logarithmiques, il suffit donc d'étudier le corps de définition k_0' de ces différentielles. Notons $G = \mathrm{Gal}(k_0'/k_0)$. G agit sur les différentielles logarithmiques régulières qui forment un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. De plus cette action est fidèle car si $\sigma \in G$ agit trivialement, les différentielles sont définies sur l'extension qui correspond à $G/ < \sigma >$. Le groupe G est donc un sous-groupe cyclique de $\mathrm{GL}_3(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_7)$: son ordre est $1, 2, 3, 4$ ou 7 (c'est, par exemple, un cas particulier du théorème de Dickson [Hup67]).

L'extension est parfois de degré 7 comme le montre l'exemple :

Exemple :

$$C : x^4 + x^3z + x^2y^2 + xy^3 + xy^2z + xz^3 + y^3z + y^2z^2 + yz^3 + z^4 = 0$$

a pour bitangentes les droites d'équation

$$x = \alpha y + \alpha^3 + \alpha + 1$$

où les α sont les 7 racines du polynôme irréductible sur $\mathbb{F}_2$, $a^7 + a^3 + 1$.

3.4 Fonctions racines

On suppose à nouveau dans toute cette partie que $k = \mathbb{C}$. On suppose également fixée une base pour l'homologie de C ce qui nous permettra de confondre les notations propres à $\mathrm{Jac}(C)[2]$ et à Σ et de parler de la caractéristique d'un point de 2-torsion.

3.4.1 Définition et premières propriétés

On a la généralisation de la notion de fibré thêta caractéristique suivante.

Lemme 3.40
Pour tout $n \in \mathbb{N}^*$, on a une bijection entre les fibrés de degré $2n$ tels que $L^2 = \mathcal{K}^n$ et $\mathrm{Jac}(C)[2]$ donnée par : si $L = L(D)$, $\forall P_0 \in C$

$$u_{P_0}(D) + nK_{P_0} \equiv \epsilon$$

avec $\epsilon \in \mathrm{Jac}(C)[2]$. On note $L_\epsilon^{(n)}$ ce fibré. Si $[\epsilon] = \sum_{i=1}^n [\epsilon_i]$ alors $L_\epsilon^{(n)} = L_{\epsilon_1} \otimes \ldots \otimes L_{\epsilon_n}$.

Remarque :
On ne peut pas définir cette notion indépendamment du choix d'une base ou — ce qui revient essentiellement au même — du choix d'un fibré thêta caractéristique du moins pour les n pairs. En effet si $n = 2m + 1$ on se ramène canoniquement au cas $n = 1$ en considérant les fibrés $L \otimes \mathcal{K}^{-m}$. Pour n pairs, on est dans la situation analogue à celle de l'identification de $\mathrm{Jac}(C)[2]$ avec Σ.

Définition 3.41
On appelle fonction abélienne de caractéristique $[\epsilon]$ une section du fibré thêta caractéristique impaire L_ϵ.
On appelle fonction racine (d'ordre 2) de degré n et de caractéristique $[\epsilon]$ une section du fibré $L_\epsilon^{(n)}$. Si $\psi \in L_\epsilon^{(n)}$ on posera également $[\psi] := [\epsilon]$ et (ψ) le point d'ordre 2 correspondant dans la jacobienne (le contexte permettra de distinguer cette notation de celle du diviseur de la section ψ).
Si $\psi \in L_\epsilon^{(n)}$ et $\psi' \in L_{\epsilon'}^{(m)}$ alors $\psi\psi' \in L_{\epsilon+\epsilon'}^{(n+m)}$ ce qui justifie la notation $[\psi\psi'] = [\epsilon] + [\epsilon']$.

Nous allons nous intéresser aux dimensions des espaces des sections de ces fibrés.

Proposition 3.42

$$On\ a\ h^0(L_\epsilon^{(n)}) = \begin{cases} 0 & si\ n = 1\ et\ [\epsilon]\ paire \\ 1 & si\ n = 1\ et\ [\epsilon]\ impaire \\ 3 & si\ [\epsilon] = [0]\ et\ n = 2 \\ 2n-2 & sinon \end{cases}$$

Démonstration :
Les deux premiers cas résultent du corollaire 3.26.
Le troisième cas est trivial.
Pour $n = 2$ et $[\epsilon] \neq [0]$ on peut écrire $L = L_{\epsilon_1} \otimes L_{\epsilon_2}$ avec $[\epsilon_1] \neq [\epsilon_2]$ impaires (en considérant le groupe $[\epsilon]$). On a alors $h^0(\mathcal{K} \otimes L_{\epsilon_1}^{-1} \otimes L_{\epsilon_2}^{-1}) = 0$ car si $L_{\epsilon_1} = L(P_1 + Q_1)$ et $L_{\epsilon_2} = L(P_2 + Q_2)$ alors $K - P_1 - Q_1 - P_2 - Q_2 \sim 2(P_1 + Q_1) - P_1 - Q_1 - P_2 - Q_2 \sim P_1 + Q_1 - P_2 + Q_2$. Or puisque la courbe est non hyperelliptique $\mathcal{L}(P_1 + Q_1)$ contient uniquement des fonctions constantes donc $l(P_1 + Q_1 - P_2 - Q_2) = 0$. Par Riemann-Roch $h^0(L) = 2 + 1 - 3 + 0 = 2$.
Si $n > 2$ alors on a trivialement le résultat puisque $\deg(\mathcal{K} \otimes L^{-1}) < 0$.

Dans les cas $n = 1, 2, 3$ on peut décrire une base de l'espace des sections de la manière suivante :

Lemme 3.43

1. *Soit $L \in \Sigma_1$. Puisque $L^2 = \mathcal{K} = H_{|C}$, si $s \in H^0(L)$ alors s^2 peut être considérer comme une section hyperplane dont une équation est celle de la bitangente à la courbe donnée par la bijection du lemme 3.25. Si $l = 0$ est une équation de la bitangente, on note $\sqrt{l}$ la section qui engendre $H^0(L)$ (qui est de dimension 1 d'après la proposition 3.42).*
2. *Soit maintenant $[\epsilon]$ une caractéristique quelconque non nulle et*
$$[\epsilon] = [\sqrt{u_1}] + [\sqrt{v_1}] = [\sqrt{u_2}] + [\sqrt{v_2}]$$
deux décompositions distinctes appartenant au groupe de $[\epsilon]$ alors
$$H^0(L_\epsilon^{(2)}) =< \sqrt{u_1 v_1}, \sqrt{u_2 v_2} > .$$
3. *Si $[\epsilon] = 0$ alors si u_1, u_2, u_3 sont trois bitangentes telles que $[\sqrt{u_1}] + [\sqrt{u_2}] + [\sqrt{u_3}]$ soit paire alors*
$$H^0(L_0^{(2)}) = H^0(\mathcal{K}) =< u_1, u_2, u_3 > .$$
4. *Soit enfin $[\epsilon]$ paire et trois décompositions d'un même groupe*
$$[\sqrt{u_1}] + [\sqrt{v_1}] = [\sqrt{u_2}] + [\sqrt{v_2}] = [\sqrt{u_3}] + [\sqrt{v_3}] \neq [0]$$
telles que
$$[\sqrt{u_1}] + [\sqrt{u_2}] + [\sqrt{u_3}] = [\epsilon]$$
alors
$$H^0(L_\epsilon^{(3)}) =< \sqrt{u_1 u_2 u_3}, \sqrt{u_1 v_2 v_3}, \sqrt{v_1 u_2 v_3}, \sqrt{v_1 v_2 u_3} > .$$

Démonstration :
Montrons le cas 2. Pour cela il suffit de montrer que $\sqrt{u_1v_1}$ n'est pas proportionnel à $\sqrt{u_2v_2}$. Sinon $\sqrt{\frac{u_1v_1}{u_2v_2}}$ est une constante. Notons alors $(\sqrt{u_1}) = P_1 + P_2$ et $(\sqrt{v_1}) = P_3 + P_4$. Comme u_1, u_2, v_1, v_2 sont des bitangentes distinctes on a donc par exemple $(\sqrt{u_2}) = P_1 + P_3$ mais alors $\left(\sqrt{\frac{u_1}{u_2}}\right) = P_2 - P_3$ soit $\left(\frac{u_1}{u_2}\right) = 2P_2 - 2P_3$. Mais dans ce cas $f = u_1/u_2$ induit un revêtement de degré 2 de C sur $\mathbb{P}^1$: exclu puisque la courbe n'est pas hyperelliptique.
Montrons le cas 3 : soit $[\epsilon] = [\sqrt{u_1u_2u_3}] \neq [0]$. On sait alors qu'il existe trois bitangentes distinctes v_1, v_2, v_3 et distinctes deux à deux de $u_1 = 0, u_2 = 0, u_3 = 0$ (car toutes de caractéristiques distinctes) telles que $[\epsilon] = [\sqrt{u_1v_1}] = [\sqrt{u_2v_2}] = [\sqrt{u_3v_3}]$. D'après ce qui précède on a alors une relation linéaire $\sqrt{u_1v_1}+\sqrt{u_2v_2}+\sqrt{u_3v_3} = 0$ (on a ajusté v_1, v_2, v_3 pour que les coefficients valent 1) qui élevée au carré donne une relation algébrique

$$(u_3v_3 - u_1v_1 - u_2v_2)^2 - 4u_1v_1u_2v_2 = 0.$$

La quartique C étant irréductible, ceci est une équation de la quartique. Si on suppose maintenant que u_1, u_2, u_3 sont liés alors ces trois bitangentes sont concourantes en un point $P \in C$. On voit facilement que ce point devrait de plus être singulier ; exclu.
Montrons enfin le dernier cas. On suppose à nouveau une relation du type

$$\lambda_1\sqrt{u_1u_2u_3} + \lambda_2\sqrt{u_1v_2v_3} + \lambda_3\sqrt{v_1u_2v_3} + \lambda_4\sqrt{v_1v_2u_3} = 0 \tag{3.1}$$

où on a normalisé v_1, v_2, v_3 tels que

$$\sqrt{u_1v_1} + \sqrt{u_2v_2} + \sqrt{u_3v_3} = 0. \tag{3.2}$$

On peut supposer λ_3 et λ_4 non tous nuls car sinon on est ramené à $\lambda_1\sqrt{u_2u_3}+\lambda_2\sqrt{v_2v_3} = 0$ qu'on a traité en 2.
En multipliant la relation (3.1) par $\sqrt{u_1u_2u_3}$ et en utilisant (3.2) on trouve alors

$$u_1(\lambda_1u_2u_3 + \lambda_2(u_1v_1 - u_2v_2 - u_3v_3) - \lambda_3u_2v_1 - \lambda_4u_3v_1) = (\lambda_3u_2 - \lambda_4u_3)(u_2v_2 - u_3v_3).$$

Comme C est une quartique irréductible, cette équation de degré 3 doit en fait être identiquement nulle en particulier u_1 doit diviser le second membre (en effet par les arguments précédents puisque λ_3 et λ_4 sont non nuls, le second membre n'est pas nul). Or on a vu que u_1, u_2, u_3 étaient linéairement indépendantes donc u_1 divise $(u_2v_2-u_3v_3)$. Mais alors puisque $(u_2v_2 - u_3v_3 - u_1v_1)^2 = 4u_1v_1u_3v_3$ est une équation de la quartique C, celle-ci ne serait pas irréductible. Exclu ; donc les quatre sections sont linéairement indépendantes.

Corollaire 3.44 (Riemann)
Soit u_i, v_i des bitangentes toutes distinctes à une courbe C telles que

$$[\sqrt{u_1}] + [\sqrt{v_1}] = [\sqrt{u_2}] + [\sqrt{v_2}] = [\sqrt{u_3}] + [\sqrt{v_3}]$$

Quitte à multiplier les v_i par des constantes il existe un modèle de C (que nous appelerons modèle de Riemann), sous la forme

$$C : \sqrt{x_1u_1} + \sqrt{x_2u_2} + \sqrt{x_3u_3} = 0.$$

3.4.2 Fonction racine et fonction thêta

Nous allons maintenant relier les sections des fibrés thêta caractéristiques de degré n aux fonctions thêta caractéristiques.

Soit $\vartheta[\epsilon](z-e)$ une fonction thêta. Celle-ci peut-être vu comme une section d'un fibré L sur $\mathrm{Jac}(C)$ (cf. chapitre 1). Soit alors un point $P_0 \in C$ et $u_{P_0} : C \to \mathrm{Jac}(C)$ l'application d'Abel. Alors $u_{P_0}^*(L)$ est un fibré sur C et si $s(P) = \vartheta[\epsilon](u_{P_0}(P) - e)$ n'est pas identiquement nulle on a $u_{P_0}^*(L) = L((s))$.

Commençons par montrer la non nullité de certaines sections.

Lemme 3.45
Soit $[\epsilon]$ une caractéristique quelconque et $P_0 \in C$ alors la fonction $f(P) = \vartheta[\epsilon](u_{P_0}(P))$ n'est pas identiquement nulle.

Démonstration :
Lorsque $[\epsilon]$ est paire, c'est une conséquence de la proposition 3.22.
Si $[\epsilon]$ est impaire, évaluons df au voisinage de P_0. On a

$$df = \sum_{i=1}^{3} \frac{\partial \vartheta[\epsilon](z)}{\partial z_i}(0)\ \zeta_i.$$

Cette expression est nulle si et seulement si chaque terme est nulle. Or d'après le théorème 1.33, cela implique l'existence de $D \in \mathrm{D}^2(C)$ tel que $\mathrm{ind}(D) \geq 2$. Exclu.

Proposition 3.46
Soit $f(P) = \vartheta[\epsilon](u_{P_0}(P))$ de zéros P_1^0, P_2^0, P_3^0. Alors quelques soient $P_1, P_2, P_3 \in C$ tels que $\mathrm{ind}(P_1 + P_2 + P_3) = 0$, si on note $e = u(P_1 + P_2 + P_3 - P_1^0 - P_2^0 - P_3^0)$, alors la section

$$g(P) = \vartheta[\epsilon](u_{P_0}(P) - e)$$

a pour diviseur $P_1 + P_2 + P_3$.

Démonstration :
En effet, $\forall P_0 \in C$ on a $u_{P_0}(P_1^0+P_2^0+P_3^0)+K_{P_0} \equiv \epsilon$ donc $e \equiv u_{P_0}(P_1+P_2+P_3)+K_{P_0}+\epsilon$. Comme $\mathrm{ind}(P_1+P_2+P_3) = 0$, g est non identiquement nulle d'après le théorème 1.31 et son diviseur, D, est caractérisé d'après le théorème 1.30 (a priori à équivalence linéaire près mais comme on l'a dit en tant que diviseur) par $u_{P_0}(D) + K_{P_0} \equiv e + \epsilon$. Mais cette relation est bien vérifiée par $P_1 + P_2 + P_3$ donc $D = P_1 + P_2 + P_3$.

Proposition 3.47
Soit $[\omega] \neq 0$ et ψ l'unique (à un coefficient multiplicatif près) fonction racine de degré 2 et de caractéristique $[\omega]$ qui s'annule en un zéro P_1 d'une fonction abélienne $\varphi \in L_\epsilon$ de diviseur $P_1 + P_2$. Si on note Q_1, Q_2, Q_3 les trois autres zéros de ψ, ce sont également les zéros de $f(P) = \vartheta[\omega + \epsilon](u_{P_2}(P))$.

Démonstration :
On a les relations $u_{P_2}(P_1+P_2)+K_{P_2}\equiv\epsilon$ et $u_{P_2}(P_1+Q_1+Q_2+Q_3)+2K_{P_2}\equiv\omega$ d'où

$$u_{P_2}(Q_1+Q_2+Q_3)+K_{P_2}\equiv\epsilon+\omega.$$

Comme on sait de plus que f n'est pas identiquement nulle d'après le lemme 3.45, son diviseur des zéros est caractérisé par la relation ci-dessus. Le diviseur $Q_1+Q_2+Q_3$ est donc le diviseur de f.

3.4.3 Application à la détermination des thêta constantes

Soit φ une fonction abélienne de zéros P_1, P_2. Soit ψ une fonction racine de degré 2 qui s'annule en P_2 et Q_1, Q_2, Q_3. D'après la proposition 3.47, le diviseur des zéros de $\vartheta[\psi\varphi](u_{P_1}(P))$ est égal à $Q_1+Q_2+Q_3$.
Soit maintenant $R_1, R_2, R_3 \in C$ et posons

$$w_0 \equiv u(R_1+R_2+R_3-Q_1-Q_2-Q_3).$$

On note également $[\omega]$ une caractéristique quelconque et on suppose que

- $\vartheta[\psi\varphi](u_{P_1}(P)-w_0)$ est non identiquement nulle c'est-à-dire d'après le théorème 1.31 et la proposition 3.47, qu'on a choisi R_1, R_2, R_3 tels que $\mathrm{ind}(R_1+R_2+R_3)=0$.
- $\vartheta[\omega](u_{P_1}(P)-w_0)$ est non identiquement nulle. On note alors R_1', R_2', R_3' ses zéros. On a aussi (cf. théorème 1.31) que $\mathrm{ind}(R_1'+R_2'+R_3')=0$.

Il est clair que génériquement R_1, R_2, R_3 vérifient ces hypothèses. En effet $\{z$ t.q. $\vartheta[\psi\varphi](z-u_{P_1}(Q_1+Q_2+Q_3))=0\}\cup\{z$ t.q. $\vartheta[\omega](z-u_{P_1}(Q_1+Q_2+Q_3))=0\}$ est la réunion de deux hypersurfaces de $\mathrm{Jac}(C)$. Comme $u_{P_1}: D^3(C)\to\mathrm{Jac}(C)$ est surjective (théorème d'inversion de Jacobi), génériquement $R_1+R_2+R_3$ est tel que $\vartheta[\psi\varphi](w_0)\neq 0$ et $\vartheta[\omega](w_0)\neq 0$ et donc les deux sections sont non identiquement nulles.

Soit maintenant χ et χ' deux fonctions racines de degré 3 telles que

- $[\chi], [\chi']$ sont paires,
- $[\chi]+[\chi']=[\psi\varphi]+[\omega]$
- $(\chi)=R_1+R_2+R_3+S_1+S_2+S_3$
- χ' s'annule en S_1, S_2, S_3 et trois autres points S_1', S_2', S_3'.

On considère alors les deux sections :

$$\begin{cases} g(P)=\frac{\chi(P)}{\chi'(P)} \\ f(P)=\frac{\vartheta[\psi\varphi](u_{P_1}(P)-w_0)}{\vartheta[\omega](u_{P_1}(P)-w_0)}. \end{cases}$$

Lemme 3.48
$f(P)=A_1\,g(P)$ où A_1 ne dépend pas de P.

Démonstration :
D'après la proposition 3.46, $\vartheta[\psi\varphi](u_{P_1}(P)-w_0)$ s'annule en R_1,R_2,R_3. On a donc

$$u_{P_1}(R_1+R_2+R_3)+K_{P_1}\equiv w_0+(\psi\varphi) \tag{3.3}$$
$$u_{P_1}(R'_1+R'_2+R'_3)+K_{P_1}\equiv w_0+\omega \tag{3.4}$$
$$u_{P_1}(R_1+R_2+R_3+S_1+S_2+S_3)+3K_{P_1}\equiv(\chi) \tag{3.5}$$
$$u_{P_1}(S_1+S_2+S_3+S'_1+S'_2+S'_3)+3K_{P_1}\equiv(\chi') \tag{3.6}$$

soit en effectuant $(3.3)-(3.4)-(3.5)+(3.6)$:

$$u_{P_1}(S'_1+S'_2+S'_3-R'_1-R'_2-R'_3)\equiv 0.$$

Mais comme $\mathrm{ind}(R'_1+R'_2+R'_3)=0$, on a $R'_1+R'_2+R'_3=S'_1+S'_2+S'_3$ soit $\mathrm{div}(f/g)=0$ et $f(P)=A_1g(P)$.

Remarque :
Puisque $\mathrm{ind}(R_1+R_2+R_3)=0$ et $\mathrm{ind}(S'_1+S'_2+S'_3)=0$, χ et χ' sont complètement déterminées à une constante multiplicative près.

Lemme 3.49
A_1^2 ne dépend pas du choix de Q_1,Q_2,Q_3, R_1,R_2,R_3, S_1,S_2,S_3 et du choix d'une fonction abélienne φ.

Démonstration :
Pour montrer cela nous allons transformer l'expression de $f(P)$.
On a

$$u(R_1-Q_1+R_2-Q_2+R_3-Q_3+S_1-P_2+S_2-P_1+S_3-P_2)\equiv[\chi]+[\psi\varphi].$$

Posons $v(P)\equiv u(P+S_1+S_2+S_3-2P_1-2P_2)$ on a

$$\begin{aligned}(\chi)+(\psi\varphi)+v(P)&\equiv \underbrace{u(R_1+R_2+R_3-Q_1-Q_2-Q_3)}_{w_0}+\\ &u_{P_1}(P)+2u(S_1+S_2+S_3-2P_2-P_1)\\ &\equiv u_{P_1}(P)-w_0+2\underbrace{u(R_1+R_2+R_3+S_1+S_2+S_3-Q_1-Q_2-Q_3-2P_2-P_1)}_{\equiv(\chi\psi\varphi)}\\ &\equiv u_{P_1}(P)-w_0.\end{aligned}$$

On obtient

$$f(P)^2=\left(\frac{\vartheta[\psi\varphi]((\chi)+(\psi\varphi)+v(P))}{\vartheta[\omega](v(P)+(\chi)+(\psi\varphi))}\right)^2=\pm\left(\frac{\vartheta[\chi](v(P))}{\vartheta[\chi'](v(P))}\right)^2 \tag{3.7}$$

Soit $f(P)^2=\pm\left(\frac{\vartheta[\chi](v(P)}{\vartheta[\chi'](v(P))}\right)^2$ et $g(P)^2=A^2f(P)^2$ où A^2 se déduit de A_1^2 par multiplication par ±1 (ne dépendant que des caractéristique $[\chi],[\chi'],[\psi\varphi]$).

Sous cette forme il n'y a plus de dépendance en ψ (donc en Q_1, Q_2, Q_3) ni en R_1, R_2, R_3. Comme de plus A_1, donc A^2, ne dépend pas de P l'écriture de $v(P)$ nous montre que A^2 ne dépend pas non plus de S_1, S_2, S_3.
Enfin, si on choisit une autre fonction abélienne φ' de zéros P'_1, P'_2, alors $2u(P_1 + P_2 - P'_1 + P'_2) \equiv 0$ donc le rapport ne change pas.

On notera jusqu'à la fin du paragraphe $\equiv$ entre deux fonctions à valeurs complexes pour signifier que l'une se déduit de l'autre par multiplication par une constante non nulle.

Soit maintenant $[\chi] + [\chi'] = [\sqrt{u_1}] + [\sqrt{u_2}]$ avec $(\sqrt{u_1}) = T_1 + T'_1$ et $(\sqrt{u_2}) = T_2 + T'_2$. Notons γ_1 et γ_2 les deux demi-périodes telles que $[\gamma_1] = [\sqrt{u_1}] + [\varphi]$ et $[\gamma_2] = [\sqrt{u_2}] + [\varphi]$. Remarquons qu'on a

$$\begin{cases} \gamma_1 \equiv u(T_1 + T'_1 - P_1 - P_2) \\ \gamma_2 \equiv u(T_2 + T'_2 - P_1 - P_2) \end{cases}$$

On considère les deux cas particuliers suivants :

$$S_1 = T'_1, S_2 = T_1, S_3 = T'_1 \tag{3.8}$$
$$S_1 = T'_1, S_2 = T_2, S_3 = T'_2 \tag{3.9}$$

et on note $v_1(P)$ (resp. $v_2(P)$) les expressions $v(P)$ qui en résultent.

Pour $P = T_1$ on a

$$\begin{cases} \vartheta[\chi](v_1(T_1)) \equiv \vartheta[\chi](2\gamma_1) \equiv \vartheta[\chi](0) \neq 0 \\ \vartheta[\chi'](v_2(T_1)) \equiv \vartheta[\chi'](2\gamma_1) \equiv \vartheta[\chi'](0) \neq 0 \\ \vartheta[\chi](v_2(T_1)) \equiv \vartheta[\chi](\gamma_1 + \gamma_2) \equiv \vartheta[\chi'](0) \neq 0 \\ \vartheta[\chi'](v_2(T_1)) \equiv \vartheta[\chi'](\gamma_1 + \gamma_2) \equiv \vartheta[\chi](0) \neq 0 \end{cases}$$

(la non nullité des expressions provenant de la proposition 3.22 puisqu'on a supposé $[\chi]$ et $[\chi']$ paires).
Les zéros de $\vartheta[\chi](v_1(P))$ (resp. de $\vartheta[\chi](v_2(P))$) vérifient alors exactement les hypothèses du début du paragraphe.

Appelons χ_1, χ'_1 (resp. χ_2, χ'_2) les fonctions racines χ, χ' qui sont définies par ces zéros à une constante multiplicative près.

L'invariance de A fournit les expressions

$$\begin{cases} \left(\frac{\vartheta[\chi](v_1(P))}{\vartheta[\chi'](v_1(P))}\right)^2 = A^2 \left(\frac{\chi_1(P)}{\chi'_1(P)}\right)^2 \\ \left(\frac{\vartheta[\chi](v_2(P))}{\vartheta[\chi'](v_2(P))}\right)^2 = A^2 \left(\frac{\chi_2(P)}{\chi'_2(P)}\right)^2 \end{cases}$$

En évaluant en $P = T_1$ dans ces deux expressions, on obtient

$$\begin{cases} \left(\frac{\vartheta[\chi](\gamma_1+\gamma_1)}{\vartheta[\chi'](\gamma_1+\gamma_1)}\right)^2 = \left(\frac{\vartheta[\chi](0)}{\vartheta[\chi'](0)}\right)^2 = A^2\left(\frac{\chi_1(T_1)}{\chi_1'(T_1)}\right)^2 \\ \left(\frac{\vartheta[\chi](\gamma_1+\gamma_2)}{\vartheta[\chi'](\gamma_1+\gamma_2)}\right)^2 = (-1)^{|[\chi]+[\chi']|}\left(\frac{\vartheta[\chi'](0)}{\vartheta[\chi](0)}\right)^2 = A^2\left(\frac{\chi_2(T_2)}{\chi_2'(T_2)}\right)^2 \end{cases}$$

Proposition 3.50

$$\left(\frac{\vartheta[\chi](0)}{\vartheta[\chi'](0)}\right)^4 = (-1)^{|[\chi]+[\chi']|}\left(\frac{\chi_1(T_1)\chi_2'(T_1)}{\chi_1'(T_1)\chi_2(T_1)}\right)^2.$$

Nous allons chercher une expression simple de ce dernier produit. D'après le lemme 3.17, les deux groupes $[\chi]+[\chi']$ et $[\chi']+[\sqrt{u_1}]$ ont quatre caractéristiques impaires en commun. On note

$$\begin{cases} [\chi]+[\chi'] = [\sqrt{u_1}]+[\sqrt{u_2}] = [\sqrt{y_1}]+[\sqrt{y_2}] = [\sqrt{z_1}]+[\sqrt{z_2}] \\ [\chi']+[\sqrt{u_1}] = [\sqrt{y_1}]+[\sqrt{z_1}] = [\sqrt{y_2}]+[\sqrt{z_2}]. \end{cases}$$

Marquons par un exposant $(1),(2),(3)$ la valeur de chacune de ces sections aux points S_1, S_2, S_3. D'après 3.43 on peut écrire à une constante multiplicative près (que l'on choisit ici égale à 1) en supposant S_1, S_2, S_3 distincts :

$$\chi(P) = \begin{vmatrix} \sqrt{u_1y_1z_1} & \sqrt{u_1y_2z_2} & \sqrt{u_2y_1z_2} & \sqrt{u_2y_2z_1} \\ \sqrt{u_1^{(1)}y_1^{(1)}z_1^{(1)}} & \sqrt{u_1^{(1)}y_2^{(1)}z_2^{(1)}} & \sqrt{u_2^{(1)}y_1^{(1)}z_2^{(1)}} & \sqrt{u_2^{(1)}y_2^{(1)}z_1^{(1)}} \\ \sqrt{u_1^{(2)}y_1^{(}2)z_1^{(2)}} & \sqrt{u_1^{(2)}y_2^{(2)}z_2^{(2)}} & \sqrt{u_2^{(2)}y_1^{(2)}z_2^{(2)}} & \sqrt{u_2^{(2)}y_2^{(2)}z_1^{(2)}} \\ \sqrt{u_1^{(3)}y_1^{(}3)z_1^{(3)}} & \sqrt{u_1^{(3)}y_2^{(3)}z_2^{(3)}} & \sqrt{u_2^{(3)}y_1^{(3)}z_2^{(3)}} & \sqrt{u_2^{(3)}y_2^{(3)}z_1^{(3)}} \end{vmatrix}$$

et

$$\chi'(P) = \begin{vmatrix} \sqrt{u_2y_2z_2} & \sqrt{u_2y_1z_1} & \sqrt{u_1y_2z_1} & \sqrt{u_1y_1z_2} \\ \sqrt{u_2^{(1)}y_2^{(1)}z_2^{(1)}} & \sqrt{u_2^{(1)}y_1^{(1)}z_1^{(1)}} & \sqrt{u_1^{(1)}y_2^{(1)}z_1^{(1)}} & \sqrt{u_1^{(1)}y_1^{(1)}z_2^{(1)}} \\ \sqrt{u_2^{(2)}y_2^{(}2)z_2^{(2)}} & \sqrt{u_2^{(2)}y_1^{(2)}z_1^{(2)}} & \sqrt{u_1^{(2)}y_2^{(2)}z_1^{(2)}} & \sqrt{u_1^{(2)}y_1^{(2)}z_2^{(2)}} \\ \sqrt{u_2^{(3)}y_2^{(}3)z_2^{(3)}} & \sqrt{u_2^{(3)}y_1^{(3)}z_1^{(3)}} & \sqrt{u_1^{(3)}y_2^{(3)}z_1^{(3)}} & \sqrt{u_1^{(3)}y_1^{(3)}z_2^{(3)}} \end{vmatrix}$$

Remarque :
Ces formules ne sont bien sûr plus valables lorsque le point S_1 est par exemple égal à S_2 mais on se convaincra aisément qu'elles restent valables pour le rapport $\chi(P)/\chi'(P)$ (par un analogue de la règle de l'Hôpital) en fixant S_2 et S_3 puis en faisant tendre S_1 vers S_2.

En tenant compte de la remarque ci-dessus et en particularisant à (3.8) (resp. à (3.9)) pour lesquelles $x_1^{(2)} = 0, x_1^{(3)} = 0$ (resp. $x_2^{(2)} = 0, x_2^{(3)} = 0$) on obtient les expressions

suivantes :

$$\frac{\chi_1(T_1)}{\chi_1'(T_1)} = \frac{\sqrt{y_1^{(0)}z_1^{(0)}y_2^{(1)}z_2^{(1)}} - \sqrt{y_2^{(0)}z_2^{(0)}y_1^{(1)}z_1^{(1)}}}{\sqrt{y_2^{(0)}z_1^{(0)}y_1^{(1)}z_2^{(1)}} - \sqrt{y_1^{(0)}z_2^{(0)}y_2^{(1)}z_1^{(1)}}} \cdot \frac{\sqrt{y_1^{(2)}z_2^{(2)}y_2^{(3)}z_1^{(3)}} - \sqrt{y_1^{(3)}z_2^{(3)}y_2^{(2)}z_1^{(2)}}}{\sqrt{y_1^{(2)}z_1^{(2)}y_2^{(3)}z_2^{(3)}} - \sqrt{y_1^{(3)}z_1^{(3)}y_2^{(2)}z_2^{(2)}}}$$

$$\frac{\chi_2(T_1)}{\chi_2'(T_1)} = \frac{\sqrt{y_2^{(0)}z_1^{(0)}y_1^{(1)}z_2^{(1)}} - \sqrt{y_1^{(0)}z_2^{(0)}y_2^{(1)}z_1^{(1)}}}{\sqrt{y_1^{(0)}z_1^{(0)}y_2^{(1)}z_2^{(1)}} - \sqrt{y_2^{(0)}z_2^{(0)}y_1^{(1)}z_1^{(1)}}} \cdot \frac{\sqrt{y_1^{(2)}z_1^{(2)}y_2^{(3)}z_2^{(3)}} - \sqrt{y_1^{(3)}z_1^{(3)}y_2^{(2)}z_2^{(2)}}}{\sqrt{y_1^{(2)}z_2^{(2)}y_2^{(3)}z_1^{(3)}} - \sqrt{y_1^{(3)}z_2^{(3)}y_2^{(2)}z_1^{(2)}}}$$

où on a noté avec l'exposant (0) l'évaluation en T_1.
Dans la première expression l'exposant (0) représente le même point que l'exposant (2) et l'exposant (1) que l'exposant (3), on constate donc que

$$\frac{\chi_1(T_1)}{\chi_1'(T_1)} = 1.$$

Il nous reste à étudier la deuxième fraction. Pour cela on sait qu'il existe une relation linéaire entre trois fonctions racines de degré 2 :

$$h_1\sqrt{u_1u_2} + h_2\sqrt{y_1y_2} + h_3\sqrt{z_1z_2} = 0$$

qui, puisqu'on a $x_1^{(0)} = x_1^{(1)} = 0$ et $x_2^{(2)} = x_2^{(3)} = 0$ donne les quatre relations

$$h_2^2\ y_1^{(i)}y_2^{(i)} = h_3^2\ z_1^{(i)}z_2^{(i)}\ i = 0, 1, 2, 3.$$

Grâce à elles, on peut écrire

$$\frac{\sqrt{y_2^{(0)}z_1^{(0)}y_1^{(1)}z_2^{(1)}} - \sqrt{y_1^{(0)}z_2^{(0)}y_2^{(1)}z_1^{(1)}}}{\sqrt{y_1^{(0)}z_1^{(0)}y_2^{(1)}z_2^{(1)}} - \sqrt{y_2^{(0)}z_2^{(0)}y_1^{(1)}z_1^{(1)}}} = \frac{\sqrt{y_1^{(1)}y_1^{(0)}}}{\sqrt{y_2^{(1)}y_2^{(0)}}} \frac{z_2^{(1)}y_2^{(0)} - z_2^{(0)}y_2^{(1)}}{z_2^{(1)}y_1^{(0)} - z_2^{(0)}y_1^{(1)}} \tag{3.10}$$

$$\frac{\sqrt{y_1^{(2)}z_1^{(2)}y_2^{(3)}z_2^{(3)}} - \sqrt{y_1^{(3)}z_1^{(3)}y_2^{(2)}z_2^{(2)}}}{\sqrt{y_1^{(2)}z_2^{(2)}y_2^{(3)}z_1^{(3)}} - \sqrt{y_1^{(3)}z_2^{(3)}y_2^{(2)}z_1^{(2)}}} = \frac{\sqrt{y_2^{(2)}y_2^{(3)}}}{\sqrt{y_1^{(2)}y_1^{(3)}}} \frac{z_2^{(3)}y_1^{(2)} - z_2^{(2)}y_1^{(3)}}{y_2^{(3)}z_2^{(2)} - y_2^{(2)}z_2^{(3)}} \tag{3.11}$$

Puisque de plus u_i, y_j, z_k sont linéairement indépendants pour tout triplet $(i, j, k) \in \{1, 2\}^3$, on peut poser les relations «projectives» (i.e. avec des coefficients dans $\mathbb{P}^1$)

$$\begin{cases} z_1 = a_1y_1 + b_1y_2 + c_1u_1 = a_1'y_1 + b_1'y_2 + c_1'u_2 \\ z_2 = a_2y_1 + b_2y_2 + c_2u_1 = a_2'y_1 + b_2'y_2 + c_2'u_2. \end{cases}$$

On a alors par un calcul immédiat :

$$\frac{z_2^{(1)}y_2^{(0)} - z_2^{(0)}y_2^{(1)}}{z_2^{(1)}y_1^{(0)} - z_2^{(0)}y_1^{(1)}} = \frac{a_2}{b_2} \text{ et } \frac{z_2^{(3)}y_1^{(2)} - z_2^{(2)}y_1^{(3)}}{y_2^{(3)}z_2^{(2)} - y_2^{(2)}z_2^{(3)}} = \frac{b_2'}{a_2'}.$$

D'autre part puisque

$$\begin{cases} h_2^2\ y_1^{(i)}y_2^{(i)} - h_3^2\ (a_1y_1^{(i)} + b_1y_2^{(i)}) \cdot (a_2y_1^{(i)} + b_2y_2^{(i)}) = 0 & \text{pour } i = 0, 1 \\ h_2^2\ y_1^{(i)}y_2^{(i)} - h_3^2\ (a_1'y_1^{(i)} + b_1'y_2^{(i)}) \cdot (a_2'y_1^{(i)} + b_2'y_2^{(i)}) = 0 & \text{pour } i = 2, 3 \end{cases}$$

On a

$$\frac{\sqrt{y_1^{(1)}y_1^{(0)}}}{\sqrt{y_2^{(1)}y_2^{(0)}}} = \sqrt{\frac{b_1b_2}{a_1a_2}} \text{ et } \frac{\sqrt{y_2^{(2)}y_2^{(3)}}}{\sqrt{y_1^{(2)}y_1^{(3)}}} = \frac{a_1'b_2'}{a_2'b_1'}.$$

D'où en résumé le théorème :

Théorème 3.51 [Web76, §.24]
Soit $[\chi]$ et $[\chi']$ deux caractéristiques paires. Si on écrit $[\chi]+[\chi'] = [\sqrt{u_1}]+[\sqrt{u_2}]$ avec $[\sqrt{u_1}]$ et $[\sqrt{u_2}]$ deux caractéristiques impaires, les groupes de $[\chi]+[\chi']$ et de $[\chi']+[\sqrt{u_1}]$ ont quatre caractéristiques impaires en commun. Notons

$$\begin{cases} [\chi]+[\chi'] = [\sqrt{u_1}]+[\sqrt{u_2}] = [\sqrt{y_1}]+[\sqrt{y_2}] = [\sqrt{z_1}]+[\sqrt{z_2}] \\ [\chi']+[\sqrt{u_1}] = [\sqrt{y_1}]+[\sqrt{z_1}] = [\sqrt{y_2}]+[\sqrt{z_2}] \end{cases}$$

On écrit

$$\begin{cases} z_1 = a_1y_1+b_1y_2+c_1u_1 = a_1'y_1+b_1'y_2+c_1'u_2 \\ z_2 = a_2y_1+b_2y_2+c_2u_1 = a_2'y_1+b_2'y_2+c_2'u_2 \end{cases}$$

On a alors

$$\left(\frac{\vartheta[\chi](0)}{\vartheta[\chi'](0)}\right)^4 = (-1)^{|[\chi]+[\chi']|} \ \frac{a_2\,b_1\,a_1'\,b_2'}{a_1\,b_2\,a_2'\,b_1'}.$$

En particulier, si on suppose $[\chi'] = [0]$ et qu'on s'est donné un système d'Aronhold $(\beta_i)_{i=1\ldots7}$ on peut écrire $[\chi] = [\sqrt{\beta_i}]+[\sqrt{\beta_j}]+[\sqrt{\beta_k}]$, i,j,k distincts. On a alors par exemple : $u_1 = \beta_{ij}$, $u_2 = \beta_k$, $y_1 = \beta_i$, $y_2 = \beta_{jl}$, $z_1 = \beta_j$ et $z_2 = \beta_{ik}$.
Soit en notant : $[\beta_{l_1},\beta_{l_2},\beta_{l_3}] = \det(\beta_{l_1},\beta_{l_2},\beta_{l_3})$:

Corollaire 3.52

$$\left(\frac{\vartheta[\chi](0)}{\vartheta(0)}\right)^4 = \frac{[\beta_i,\beta_j,\beta_{ij}][\beta_{ik},\beta_{jk},\beta_{ij}][\beta_j,\beta_{jk},\beta_k][\beta_i,\beta_{ik},\beta_k]}{[\beta_j,\beta_{jk},\beta_{ij}][\beta_i,\beta_{ik},\beta_{ij}][\beta_i,\beta_j,\beta_k][\beta_{ik},\beta_{jk},\beta_k]}.$$

3.5 Détermination d'un système d'Aronhold

Comme nous venons de le voir, la détermination des thêta constantes nécessite la connaissance préalable des 28 bitangentes. Les équations de ces droites sont bien connues depuis Riemann et Weber mais ces deux derniers supposent données les équations d'un système d'Aronhold. Nous allons donc tout d'abord montrer comment on détermine ce dernier.

Soit C : $\sqrt{u_1v_1}+\sqrt{u_2v_2}+\sqrt{u_3v_3} = 0$ un modèle de Riemann de la courbe (cf. corollaire 3.44). Soit q_0 une forme paire pour laquelle q_0+v avec $v = [\sqrt{u_1}]+[\sqrt{v_1}] \neq 0$ est une forme paire (on a $|q_0+v| = |q_0|+q_0(v) = q_0(v)$ il suffit donc que $q_0(v) = 0$). On considère alors une base de l'homologie pour laquelle $q_0 = [0]$.

D'après le lemme 3.14, on peut supposer $[\sqrt{u_1}]+[\sqrt{u_2}]$ et $[\sqrt{u_1}]+[\sqrt{u_3}]$ impaires et ainsi $[\sqrt{v_1}]+[\sqrt{v_2}]$ et $[\sqrt{v_1}]+[\sqrt{v_3}]$ le sont également. Mais alors on peut former

$$\begin{aligned}
[\sqrt{u_1}] &= [\sqrt{u_2}]+[\sqrt{v_1}]+[\sqrt{v_2}] = [\sqrt{u_3}]+[\sqrt{v_1}]+[\sqrt{v_3}] = [\sqrt{u_4}]+[\sqrt{v_4}] \\
&= [\sqrt{u_5}]+[\sqrt{v_5}] = [\sqrt{u_6}]+[\sqrt{v_6}] = [\sqrt{u_7}]+[\sqrt{v_7}] \\
[\sqrt{u_2}] &= [\sqrt{u_1}]+[\sqrt{v_1}]+[\sqrt{v_2}] = [\sqrt{u_3}]+[\sqrt{v_2}]+[\sqrt{v_3}] = [\sqrt{u_4}]+[\sqrt{v'_4}] \\
&= [\sqrt{u_5}]+[\sqrt{v'_5}] = [\sqrt{u_6}]+[\sqrt{v'_6}] = [\sqrt{u_7}]+[\sqrt{v'_7}]
\end{aligned}$$

d'après la proposition 3.13, et donc (u_i), $i = 1 \dots 7$ forment un système d'Aronhold tel que $q_S = [0]$. On utilise maintenant le lemme 3.15 et donc $[\sqrt{v_i}] = [\sqrt{u_j}]+[\sqrt{u_k}]$, $i, j, k \in \{1, 2, 3\}$ distincts. On suppose les caractéristiques ainsi fixées par la suite.

Il nous reste à déterminer u_4, u_5, u_6, u_7 en fonction de l'équation de la courbe. Considérons $s \in L^{(2)}_{(\sqrt{x_1})}$. D'après le lemme 3.43, on peut écrire $s = \lambda\sqrt{u_2v_3} + \sqrt{u_3v_2}$ soit

$$s^2 = \lambda^2(u_2v_3) + \lambda(u_1v_1 - u_2v_2 - u_3v_3) + (u_3v_2).$$

Les sections s^2 sont donc paramétrées par une famille de coniques qui dégénèrent pour 6 valeurs de λ pour lesquelles s est scindée en produit de deux facteurs linéaires. Or on peut écrire le groupe de

$$\begin{aligned}
[\sqrt{u_1}] &= [\sqrt{u_2}]+[\sqrt{v_3}] = [\sqrt{u_3}]+[\sqrt{v_2}] = [\sqrt{u_4}]+[\sqrt{v_4}] \\
&= [\sqrt{u_5}]+[\sqrt{v_5}] = [\sqrt{u_6}]+[\sqrt{v_6}] = [\sqrt{u_7}]+[\sqrt{v_7}]
\end{aligned}$$

et donc en particulier le produit de chacun des couples de bitangentes est un élément de $L^{(2)}_{(\sqrt{u_1})}$ dont le carré se scinde en produit de deux facteurs linéaires. Les valeurs de dégénérescence de la famille de coniques fournissent ainsi les douze bitangentes du groupe. On procède de même avec $s \in L^{(2)}_{(\sqrt{u_2})}$ pour laquelle on a

$$s^2 = \lambda^2(u_1v_2) + \lambda(u_3v_3 - u_2v_2 - u_1v_1) + (u_3v_1)$$

et le groupe de

$$\begin{aligned}
[\sqrt{u_2}] &= [\sqrt{u_1}]+[\sqrt{v_3}] = [\sqrt{u_3}]+[\sqrt{v_1}] = [\sqrt{u_4}]+[\sqrt{v'_4}] \\
&= [\sqrt{u_5}]+[\sqrt{v'_5}] = [\sqrt{u_6}]+[\sqrt{v'_6}] = [\sqrt{u_7}]+[\sqrt{v'_7}]
\end{aligned}$$

Les bitangentes communes au deux groupes sont $u_3, v_3, u_4, u_5, u_6, u_7$. On détermine donc ces quatre dernières par l'algorithme suivant :

1. On calcule $D_1(\lambda)$, déterminant de la hessienne de la famille $Q_1(\lambda) = \lambda^2(u_2v_3) + \lambda(u_1v_1 - u_2v_2 - u_3v_3) + (u_3v_2)$.
2. On calcule $R_1(u_1, u_2, u_3)$ le résultant par rapport à λ de D_1 et Q_1.

3. On calcule de même $R_2(\lambda)$ par rapport à la famille $Q_2(\lambda) = \lambda^2(u_1v_3) + \lambda(u_2v_2 - u_1v_1 - u_3v_3) + (u_3v_1)$.
4. On calcule le p.g.c.d. R de R_1 et R_2. Les bitangentes $u_3 = 0$ et $v_3 = 0$ sont facteurs de ce polynôme qu'on divise donc par ces deux expressions. On note encore R le résultat qui est alors un polynôme homogène de degré 4. Les facteurs linéaires de ce polynôme sont les 4 bitangentes que l'on cherche.

Remarque :
Géométriquement on peut interpréter la condition d'être un système d'Aronhold de la manière suivante : soient trois bitangentes $\beta_1, \beta_2, \beta_3$ de diviseurs $(\beta_1), (\beta_2), (\beta_3)$. Les 6 points de tangence avec C sont sur une conique si et seulement si il existe un diviseur D de degré 2 tel que $(\beta_1) + (\beta_2) + (\beta_3) + D = 2K$. Le diviseur D est le diviseur d'une bitangente β_4 et on a donc $L((\beta_1) + (\beta_2) + (\beta_3) - K) = L((\beta_4))$. Un système d'Aronhold est donc caractérisé par le fait que les points de tangences de trois quelconques de ses bitangentes ne sont jamais sur une conique.

3.6 Détermination des bitangentes

Etant donnée une courbe C sous une forme de Riemann $\sqrt{u_1v_1}+\sqrt{u_2v_2}+\sqrt{u_3v_3} = 0$, nous avons montré comment on détermine un système d'Aronhold $\{u_i\}$, $i = 1 \dots 7$. D'après le lemme 3.43, puisque $[\sqrt{u_i}] + [\sqrt{u_j}] + [\sqrt{u_k}]$ est paire pour $i, j, k \in \{1, \dots, 4\}$, u_i, u_j, u_k ne sont pas concourantes. On peut donc considérer une transformation projective de $\mathbb{P}^2$ (de coordonnées x_1, x_2, x_3) envoyant u_1, u_2, u_3 et u_4 sur $x_1, x_2, x_3, x_1+x_2+x_3$. Le système d'Aronhold s'écrit maintenant :

$$\begin{cases} \beta_1 : x_1 = 0 & \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0 \\ \beta_2 : x_2 = 0 & \beta_6 : a'_1x_1 + a'_2x_2 + a'_3x_3 = 0 \\ \beta_3 : x_3 = 0 & \beta_7 : a''_1x_1 + a''_2x_2 + a''_3x_3 = 0 \\ \beta_4 : x_1 + x_2 + x_3 = 0 & \end{cases}$$

Inversement étant donnée 7 droites quelconques, elles déterminent 14 conditions algébriques sur l'espace des quartiques de dimension 14. Il existe donc toujours une quartique (possiblement singulière) admettant ces droites comme bitangentes. Ce n'est que récemment que L. Caporaso, E. Sernesi dans [CS00] et D. Lehavi dans [Leh02] ont pu montrer qu'un système d'Aronhold détermine en fait une unique courbe à isomorphisme près. La courbe C est donc déterminée par ces 7 droites que nous prenons maintenant comme point de départ. Riemann montre alors comment construire une quartique sous la forme

$$\sqrt{x_1v_1} + \sqrt{x_2v_2} + \sqrt{x_3v_3} = 0 \tag{3.12}$$

pour laquelle elles forment un système d'Aronhold (et cette quartique est donc isomorphe à C). Il montre en même temps comment on peut obtenir les équations des 21 bitangentes restantes en fonctions des a_i, a'_i, a''_i. Nous récapitulons ici pour référence ces équations.

On introduit des coefficients normalisants k, k', k'' déterminés par

$$\begin{pmatrix} \frac{1}{a_1} & \frac{1}{a'_1} & \frac{1}{a''_1} \\ \frac{1}{a_2} & \frac{1}{a'_2} & \frac{1}{a''_2} \\ \frac{1}{a_3} & \frac{1}{a'_3} & \frac{1}{a''_3} \end{pmatrix} \begin{pmatrix} \lambda \\ \lambda' \\ \lambda'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix},$$

$$\begin{pmatrix} \lambda a_1 & \lambda' a'_1 & \lambda'' a''_1 \\ \lambda a_2 & \lambda' a'_2 & \lambda'' a''_2 \\ \lambda a_3 & \lambda' a'_3 & \lambda'' a''_3 \end{pmatrix} \begin{pmatrix} k \\ k' \\ k'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}.$$

Lemme 3.53
Dans l'équation de la quartique (3.12), v_1, v_2, v_3 sont solutions du système

$$\begin{cases} v_1 + v_2 + v_3 + x_1 + x_2 + x_3 = 0 \\ \frac{v_1}{a_1} + \frac{v_2}{a_2} + \frac{v_3}{a_3} + ka_1x_1 + ka_2x_2 + ka_3x_3 = 0 \\ \frac{v_1}{a'_1} + \frac{v_2}{a'_2} + \frac{v_3}{a'_3} + k'a'_1x_1 + k'a'_2x_2 + k'a'_3x_3 = 0 \\ \frac{v_1}{a''_1} + \frac{v_2}{a''_2} + \frac{v_3}{a''_3} + k''a''_1x_1 + k''a''_2x_2 + k''a''_3x_3 = 0 \end{cases}$$

Remarque :
Bien sûr, on a seulement besoin de trois quelconques de ces équations. En fait, si on normalise les a_i, a'_i, a''_i sous la forme $\alpha_i = \sqrt{k}a_i, \alpha'_i = \sqrt{k'}a'_i$ et $\alpha''_i = \sqrt{k''}a''_i$, la connaissance des α_i, α'_i détermine les α''_i et donc la courbe C d'où $6 = 3g_C - 3$ coefficients pour l'espace des modules. Nous n'effectuons pas cette normalisation car elle conduit dans les calculs à considérer sur $\mathbb{Q}_2$ des extensions ramifiées.

On peut alors déterminer les 21 autres bitangentes qu'on note β_{ij} avec $1 \leq i < j \leq 7$.

Théorème 3.54 (Riemann) [Rie98]

$$\beta_1 : x_1 = 0 \quad \beta_2 : x_2 = 0 \quad \beta_3 : x_3 = 0$$
$$\beta_{23} : v_1 = 0 \quad \beta_{13} : v_2 = 0 \quad \beta_{12} : v_3 = 0$$

$$\beta_4 : x_1 + x_2 + x_3 = 0 \qquad \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0$$
$$\beta_6 : a'_1x_1 + a'_2x_2 + a'_3x_3 = 0 \quad \beta_7 : a''_1x_1 + a''_2x_2 + a''_3x_3 = 0$$

$$\beta_{14} : v_1 + x_2 + x_3 = 0 \qquad \beta_{15} : \frac{u_1}{a_1} + ka_2x_2 + ka_3x_3 = 0$$
$$\beta_{16} : \frac{v_1}{a'_1} + k'a'_2x_2 + k'a'_3x_3 = 0 \quad \beta_{17} : \frac{v_1}{a''_1} + k''a''_2x_2 + k''a''_3x_3 = 0$$

$$\beta_{24} : x_1 + v_2 + x_3 = 0 \qquad \beta_{25} : ka_1x_1 + \frac{v_2}{a_2} + ka_3x_3 = 0$$
$$\beta_{26} : k'a'_1x_1 + \frac{v_2}{a'_2} + k'a'_3x_3 = 0 \quad \beta_{27} : k''a''_1x_1 + \frac{v_2}{a''_2} + k''a''_3x_3 = 0$$

$$\beta_{34} : x_1 + x_2 + v_3 = 0 \qquad \beta_{35} : ka_1x_1 + ka_2x_2 + \frac{v_3}{a_3} = 0$$
$$\beta_{36} : k'a'_1x_1 + k'a'_2x_2 + \frac{v_3}{a'_3} = 0 \quad \beta_{37} : k''a''_1x_1 + k''a''_2x_2 + \frac{v_3}{a''_3} = 0$$

$$\beta_{67} : \frac{v_1}{1-ka_2a_3} + \frac{v_2}{1-ka_3a_1} + \frac{v_3}{1-ka_1a_2} = 0$$
$$\beta_{57} : \frac{v_1}{1-k'a_2'a_3'} + \frac{v_2}{1-k'a_3'a_1'} + \frac{v_3}{1-k'a_1'a_2'} = 0$$
$$\beta_{56} : \frac{v_1}{1-k''a_2''a_3''} + \frac{v_2}{1-k''a_3''a_1''} + \frac{v_3}{1-k''a_1''a_2''} = 0$$

$$\beta_{45} : \frac{v_1}{a_1(1-ka_2a_3)} + \frac{v_2}{a_2(1-ka_3a_1)} + \frac{v_3}{a_3(1-ka_1a_2)} = 0$$
$$\beta_{46} : \frac{v_1}{a_1'(1-k'a_2'a_3')} + \frac{v_2}{a_2'(1-k'a_3'a_1')} + \frac{v_3}{a_3'(1-k'a_1'a_2')} = 0$$
$$\beta_{47} : \frac{v_1}{a_1''(1-ka_2''a_3'')} + \frac{v_2}{a_2''(1-k''a_3''a_1'')} + \frac{v_3}{a_3''(1-k''a_1''a_2'')} = 0$$

Chapitre 4

Application au calcul du polynôme caractéristique

Nous allons appliquer les résultats des deux chapitres précédents au calcul du polynôme caractéristique d'une courbe $\tilde{C}$ de genre 3 ordinaire non hyperelliptique sur $k = \mathbb{F}_{2^N}$ ayant ses 2^g points de 2-torsion sur k. Dans ce cas, le théorème 2.30 permet d'affirmer qu'un certain rapport de thêta constantes (toujours non nulles en genre 3 non hyperelliptique) permet d'obtenir le produit, au signe près, des racines du Frobenius unités 2-adiques. Nous montrerons que, pour $g \leq 3$, la connaissance de ce nombre permet de retrouver généralement le polynôme caractéristique tout entier. Avant cela, il nous faut introduire un bon relèvement de $\tilde{C}$: nous souhaitons en particulier que toutes les bitangentes (et donc les rapports de thêta constantes) soient faciles à calculer, c'est-à-dire

1. que le modèle puisse se ramener sans difficulté à un modèle de Riemann (cf. corollaire 3.44).
2. que toutes les bitangentes soient définies sur le corps de relèvement.

Comme c'est déjà le cas en genre 1, si le modèle n'est pas convenablement choisi, il peut arriver que les calculs s'effectuent dans des extensions ramifiées. Nous proposons dans le paragraphe suivant un bon modèle. Enfin, nous identifions le noyau du Frobenius ce qui permet de mettre en place le processus itératif de la fin du chapitre 2.

Par la suite on note K l'extension non ramifiée de $\mathbb{Q}_2$ de degré N et $\mathcal{O}$ son anneau des entiers de corps résiduel k, π une uniformisante et v la valuation. Lorsque le contexte est clair, l'extension étant non ramifiée on notera aussi $\pi = 2$.

4.1 Bon modèle de calcul

4.1.1 Rappels des cas hyperelliptiques

Nous avons vu au paragraphe 2.1.2 qu'une courbe elliptique ordinaire sur k est toujours isomorphe sur k à $\tilde{E} : y^2 + xy = x^3 + a_2x^2 + a_4x$ et qu'à partir de cette courbe on trouve facilement un modèle sur K pour lequel tous les calculs s'effectuent dans le corps

de définition.
Dans le cas hyperelliptique, Mestre [Mes02] propose la méthode suivante : On considère une courbe hyperelliptique de genre g ordinaire sur k

$$\tilde{C} : y^2 + yh(x) = u(x)$$

où u, h sont des polynômes de degré $g+1$ tels que h soit scindé de racines simples. En particulier, les 2^g points d'ordre 2 de la jacobienne sont définis sur k. Si $v(x)$ est un polynôme de degré $g+1$, on effectue le changement de variables $y = Y + v$ et on obtient :

$$\tilde{C} : Y^2 + Yh = u + v^2 + hv.$$

Le membre de gauche est divisible par h si et seulement si $u + v^2$ l'est. On regarde ce polynôme dans l'anneau $k[x]/h$. Puisque h n'a que des racines simples, cet anneau est isomorphe à k^{g+1}. Il suffit donc que l'image de u soit un carré dans chacun de ces corps ce qui est toujours possible. Il existe alors v tel que le membre de gauche est divisible par h.
On est ainsi ramené à la situation :

$$\tilde{C} : y^2 + yh(x) = h(x)u(x).$$

On remonte cette équation à l'identique sur K. En multipliant par 4, on a alors

$$C : Y^2 = (2y + h(x))^2 = h(x)(h(x) + 4u(x)).$$

La réduction de $h(x)$ est séparable, le lemme d'Hensel [Cas86, Chap. IV] montre que ce polynôme est scindé sur K, de même pour $h(x) + 4u(x)$. Tous les points de Weierstrass sont alors définis sur K et peuvent être groupés deux par deux. On a

$$C : Y^2 = \prod_{i=1}^{g+1} (x - r_i)(x - (r_i + 4s_i))$$

$r_i, s_i \in K$. Il est ainsi facile d'identifier sur ce modèle le groupe N des points d'ordre 2 de la jacobienne qui se réduisent sur O. Une fois cela fait, il existe (lemme 2.24) une base symplectique (e_i, f_i) telle que $N =< e_i >$. Si on note $A = \mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g\Omega$ le modèle complexe associé à la jacobienne de C, le quotient A/N s'identifie à $\mathbb{C}^g/\mathbb{Z}^g + \mathbb{Z}^g 2\Omega$. On retrouve donc la situation de la fin du chapitre 2. Les rapports

$$\left(\vartheta \begin{bmatrix} 0 \\ \varepsilon' \end{bmatrix} (0, 2^n\Omega) / \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (0, \Omega) \right)^2$$

sont faciles à calculer en fonction de

$$\left(\vartheta \begin{bmatrix} 0 \\ \varepsilon' \end{bmatrix} (0, 2^{n-1}\Omega) / \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (0, \Omega) \right)^2$$

grâce aux formules de duplication (proposition 1.19). Les rapports initiaux

$$\left(\vartheta\left[\begin{array}{c}0\\ \varepsilon'\end{array}\right](0,\Omega)/\vartheta\left[\begin{array}{c}0\\ 0\end{array}\right](0,\Omega)\right)^2$$

s'obtenant quant à eux grâce à la formule de Thomae ([Mum83] ou [Fay73, p.46]).

Remarque :
De faciles congruences (à partir de la formule de Thomae) permettent de montrer que les 2^g rapports de thêta constantes de la forme $\left(\vartheta\left[\begin{array}{c}0\\ \varepsilon'\end{array}\right](0,\Omega)/\vartheta\left[\begin{array}{c}0\\ 0\end{array}\right](0,\Omega)\right)^2$ (avec le choix de base ci-dessus) sont congrus à 1 modulo 8. Ceci permet d'identifier N avec n'importe quelle choix de base symplectique (la propriété restant valable par les formules de transformation).

4.1.2 Cas du genre 3

Soit $\tilde{C}$ une courbe de genre 3 sur k ordinaire et non hyperelliptique que l'on suppose donnée sous la forme

$$\tilde{C} : (ax^2 + by^2 + cz^2 + dxy + exz + fyz)^2 - xyz(x + y + z) = 0 \tag{4.1}$$

avec a, b, c, d, e, f vérifiant les conditions de la proposition 3.38. Les 7 bitangentes étant rationnelles, les $2^3 = 8$ points de 2-torsion sont sur k.

On cherche donc un bon modèle C relevant $\tilde{C}$.
Tout comme l'équation $y^2 = x^3 + ax + b$ doit être transformée en caractéristique 2 en $y^2 + xy = x^3 + ax + b$, nous allons transformer notre modèle de Riemann sur $\mathbb{C}$ en rajoutant des termes *à la* Artin-Schreier. Plus précisément, nous allons transformer une courbe qui est un revêtement de $\tilde{C}$ de degré 2. Remarquons pour cela que le modèle de Riemann $C : \sqrt{x_1u_1} + \sqrt{x_2u_2} + \sqrt{x_3u_3} = 0$ amène à considérer la courbe $\hat{C}$

$$\begin{cases} Y_1^2 = x_1u_1 \\ Y_2^2 = x_2u_2 \\ Y_3^2 = x_3u_3 \\ Y_1 + Y_2 + Y_3 = 0 \end{cases}$$

La courbe $\hat{C}$ est une courbe de genre 5 revêtement double non ramifiée de C. Le revêtement est donné par $\pi : (Y_1 : Y_2 : Y_3 : x_1 : x_2 : x_3) \mapsto (x_1 : x_2 : x_3)$ (c'est le modèle lisse dont le corps de fonctions est $k(C)(\sqrt{(x_1/u_1)})$, cf. [Mum74]).

Considérerons la courbe $\hat{C}$ sur $k = \mathbb{F}_{2^N}$:

$$\begin{cases} Y_1^2 + l_1 Y_1 = l_1 v_1 \\ Y_2^2 + l_2 Y_2 = l_2 v_2 \\ Y_3^2 + l_3 Y_3 = l_3 v_3 \\ l_1 + l_2 + l_3 = 0 \\ Y_1 + Y_2 + Y_3 = l \end{cases}$$

où $l_1, l_1, l_2, v_1, v_2, v_3$ et l sont linéaires. Un peu de calcul formel permet de montrer alors :

Proposition 4.1
$\tilde{C}$ donnée par le modèle (4.1) est isomorphe sur k à la courbe quotient du modèle ci-dessus par le morphisme $(Y_1 : Y_2 : Y_3 : x' : y' : z') \mapsto (x' : y' : z')$ avec

$$\begin{cases} l_1 = x', l_2 = y', l_3 = x' + y' \\ l = z' \\ v_1 = bcy' + (c + f)z' \\ v_2 = acx' + dcy' + (c + e)z' \\ v_3 = acx' + (d + b)cy' + (1 + c + e + f)z' \end{cases}$$

L'isomorphisme étant donné par $x' = x/\sqrt{c}, y' = y/\sqrt{c}$ et $z' = \sqrt{c}z$.

Pour simplifier les notations, on supprime par la suite les $'$.

On relève à l'identique les expressions obtenues sur K sauf pour l_3 qu'on relève sur K en $l_3 = -2z - x - y$. Le modèle sur K est alors

$$\begin{cases} (2Y_1 + l_1)^2 = x \cdot (x + 4(bcy + (c + f)z)) \\ (2Y_2 + l_2)^2 = y \cdot (y + 4(acx + dcy + (c + e)z)) \\ (2Y_3 + l_3)^2 = (-2z - x - y) \cdot ((-2z - x - y) + 4(acx + (d + b)cy + (1 + c + e + f)z)) \\ (2Y_1 + l_1) + (2Y_2 + l_2) + (2Y_3 + l_3) = 0 \end{cases}$$

La courbe quotient est un modèle de $\tilde{C}$ sur K. Finalement, si on effectue le changement de coordonnées $x = x_1, y = x_2, z = -(x_1 + x_2 + x_3)/2$, on obtient un modèle de Riemann

$$C : \sqrt{x_1 \underbrace{(4v_1 + l_1)}_{=u_1}} + \sqrt{x_2 \underbrace{(4v_2 + l_2)}_{=u_2}} + \sqrt{x_3 \underbrace{(4v_3 + l_3)}_{=u_3}} = 0 \tag{4.2}$$

Nous allons montrer le résultat suivant :

Théorème 4.2
Le modèle (4.2) a toutes ses bitangentes définies sur K.

Démonstration :
Remarquons qu'il suffit de montrer que le système d'Aronhold est défini sur K. Nous allons montrer cela pour le modèle précédant le changement de coordonnées (ce qui revient bien entendu au même puisque celui-ci est rationnel). On a ainsi

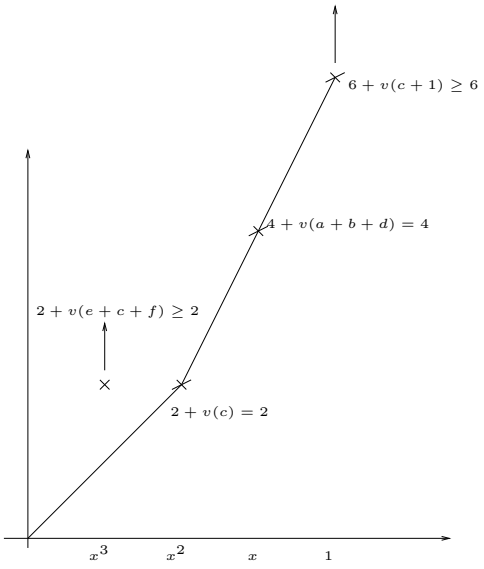
$$C : \sqrt{l_1\underbrace{(4v_1 + l_1)}_{=u_1}} + \sqrt{l_2\underbrace{(4v_2 + l_2)}_{=u_2}} + \sqrt{l_3\underbrace{(4v_3 + l_3)}_{=u_3}} = 0$$

Appelons β_i les bitangentes qui composent le système d'Aronhold. On peut supposer $\beta_1 = l_1, \beta_2 = l_2$ et $\beta_3 = l_3$. Il nous reste donc à montrer que les bitangentes β_i, $i = 4, 5, 6, 7$ sont rationnelles.
Reprenons l'algorithme permettant de les déterminer (paragraphe 3.5). On considère la famille de coniques

$$Q_3(\lambda) = l_1u_2\lambda^2 + (l_3u_3 - u_2l_2 - u_1l_1)\lambda + l_2u_1.$$

Deux paires de bitangentes sont évidentes et correspondent à $\lambda = 0$ et $\lambda = \infty$. Le déterminant $D_3(\lambda)$ de la hessienne de la famille Q_3 est donc de degré 5 et divisible par λ. La valeur $\lambda = 0$ ne donnant pas de bitangente β_i pour $i \geq 4$, on considère le polynôme $P(\lambda) = D_3(\lambda)/(8\lambda)$. On veut étudier les valuations des racines λ_i de ce polynôme. Pour cela on effectue le changement de variable $\mu = \lambda + 1$. On obtient $P(\mu) \equiv \mu^4 \pmod{\pi}$. Plus précisément son polygone de Newton est le suivant

FIG. 4.1 – Polygone de Newton de P



Les flèches indiquent que la valuation peut être supérieure en ces points. Les valeurs fixes des valuations de c et $a + b + d$ sont imposées par les conditions de la proposition

3.38.
On constate que toutes les racines sont congrues à 0 modulo π donc $\lambda_i \equiv 1 \pmod{\pi}$. On pose alors $\lambda = -1 + \pi\mu$. En réinjectant dans P on obtient alors $P(\lambda)/16 = \mu^2(\mu + c)^2 \pmod{\pi}$. Deux racines sont donc de la forme $-1 - \pi c \pmod{\pi^2}$ et deux autres de la forme $-1 \pmod{\pi^2}$. Ces deux expressions montrent alors que

$$Q_3(\lambda_i)/4 = \begin{cases} (cy+z)(cx+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 - \pi c \quad \pmod{\pi^2} \\ z(cx+cy+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 \quad \pmod{\pi^2} \end{cases}$$

On effectue le même calcul avec la famille $Q_1(\lambda) = u_3 l_2 \lambda^2 + (u_1 l_1 - u_2 l_2 - u_3 l_3)\lambda + l_3 u_2$. On obtient alors

$$Q_1(\lambda_i)/4 = \begin{cases} (cx+cy+z)(cy+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 - \pi c \quad \pmod{\pi^2} \\ z(cx+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 \quad \pmod{\pi^2} \end{cases}$$

Et enfin avec la famille $Q_2(\lambda) = u_3 l_2 \lambda^2 + (u_1 l_1 - u_2 l_2 - u_3 l_3)\lambda + l_3 u_2$:

$$Q_2(\lambda_i)/4 = \begin{cases} (cx+cy+z)(cx+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 - \pi c \quad \pmod{\pi^2} \\ z(cy+z) & \pmod{\pi} \quad \text{lorsque } \lambda_i = -1 \quad \pmod{\pi^2} \end{cases}$$

Les bitangentes $\beta_4, \beta_5, \beta_6, \beta_7$ doivent apparaître non appariées dans les 3 familles ci-dessus. Supposons que β_4 se réduise sur $cx + cy + z$. Est-il possible que β_5 se réduise également sur $cx + cy + z$? Les groupes de Q_3 montrent alors que ni β_6 ni β_7 ne se réduisent sur z. Les groupes de Q_2 permettent d'en déduire que $cy + z$ est la réduction de β_6 ou de β_7. Mais dans ce cas les groupes de Q_1 montrent que β_4 et (β_6 ou β_7) ou β_5 et (β_6 ou β_7) sont appariées : exclu.
Ainsi, les bitangentes β_i, $i = 4, \ldots, 7$ se réduisent sur quatre droites distinctes. Or l'algorithme permet de construire un polynôme homogène de degré 4 en x, y, z dont les facteurs linéaires sont exactement les β_i, $i = 4, 5, 6, 7$. On sait de plus maintenant que ces bitangentes se réduisent modulo π sur des facteurs distincts. Un analogue du lemme de Hensel à plusieurs variables (ou tout simplement en coupant par 3 droites les 4 bitangentes et en se ramenant ainsi à une seule variable) permet alors de conclure que les β_i sont définies sur le corps de base.

Remarque :
Si l'on effectue le changement de variables $x = X/c$ et $y = Y/c$, le système d'Aronhold du relèvement ainsi obtenu relève exactement les 7 bitangentes de $\tilde{C}$. Néanmoins ce modèle est moins pratique pour les calculs.

A la constante c près (voir la remarque ci-dessus) et après avoir choisi $\beta_4, \beta_5, \beta_6, \beta_7$ on peut donc écrire la table de réduction des bitangentes :

β_1	β_2	β_3
x	y	$x+y$
β_{23}	β_{13}	β_{12}
x	y	$x+y$

i	β_i	β_{1i}	β_{2i}	β_{3i}
4	$x+y+z$	$y+z$	$x+z$	z
5	$x+z$	z	$x+y+z$	$y+z$
6	z	$x+z$	$y+z$	$x+y+z$
7	$y+z$	$x+y+z$	z	$x+z$

On identifie alors facilement le noyau du Frobenius : il est constitué des (moitiés) des diviseurs d'intersection des bitangentes qui se réduisent sur la même droite. Choisissons pour système principal les caractéristiques de l'exemple 3.1.2. On a alors pour noyau le sous-espace engendré par

$$\begin{cases} [1] + ([2] + [3]) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ ([1] + [5]) + [6] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ ([3] + [5]) + [7] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{cases}$$

Nous savions (lemme 2.24) que ce sous-espace est isotrope, nous avons simplement choisi l'ordre des bitangentes $\beta_4, \ldots, \beta_7$ afin qu'il corresponde avec le sous-espace engendré par e_1, e_2, e_3 (definition 1.13).
On peut maintenant terminer l'identification des bitangentes qu'il nous manque encore. Pour cela, on considère la famille de conique $Q(\lambda) = l_1u_1\lambda^2 + (l_3u_3 - l_1u_1 - l_2u_2)\lambda + l_2u_2$. Les arguments de la démonstration précédente s'appliquent encore : les bitangentes (β_{ij}, β_{kl}), $i, j, k, l \in \{4, 5, 6, 7\}$ distincts, se réduisent sur (x, x), (y, y) et $(x + y, x + y)$. Pour les identifier on utilise le noyau. En effet x doit être la réduction d'une bitangente β_{kl} tel que $[1] + [k] + [l]$ est la caractéristique d'un élément du noyau. C'est donc β_{47} ou β_{56}. Ceci complète notre classification :

β_{45}	β_{67}	β_{46}	β_{57}	β_{47}	β_{56}
y	y	$x + y$	$x + y$	x	x

Remarque :
On peut regretter le manque de symétrie des modèles que nous considérons. Pourquoi en effet privilégier la variable z ? Si on essaie de construire un modèle plus symétrique, par exemple $x' = y + z, y' = x + z, z' = x + y$ et $l = x' + y' + z'$, nous n'avons pu déterminer v_1, v_2, v_3 permettant de retrouver tous les modèles plans (4.1). Plus précisément on obtient une sous-variété de codimension 1 donnée par la condition supplémentaire $a + b + c + d + e + f = 0$.
Comme dans le cas hyperelliptique, il apparaît que les rapports

$$\left(\vartheta \begin{bmatrix} 0 \\ \varepsilon' \end{bmatrix}(0)/\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0)\right)^2$$

associés aux choix des bases ci-dessus sont ceux congrus à 1 modulo 8.

4.2 Méthode A.G.M. 2-adique

4.2.1 L'algorithme

Résumons ici les différentes étapes qui forment ce que l'on peut appeler les méthodes A.G.M. 2-adiques. Etant donnée une courbe $\tilde{C}$ de genre g, ordinaire, sur $k = \mathbb{F}_{2^N}$, la

mise en œuvre d'une méthode A.G.M. pour la détermination du polynôme caractéristique procède de la manière suivante :

1. on relève la courbe sur une extension K non ramifiée de $\mathbb{Q}_2$. Ce relèvement ne doit pas être quelconque si l'on veut pouvoir effectuer les calculs dans une extension non ramifiée. Nous avons rappelé les modèles elliptiques et hyperelliptiques aux paragraphes 2.1.2 et 4.1.1. Dans le cas du genre 3 non hyperelliptique c'est le paragraphe 4.1.2.
2. Une fois en caractéristique nulle, par analogie avec le cas complexe, on calcule, en fonction des coefficients de ce modèle, 2^g rapports de «thêta constantes» de la forme suivante
$$\left(\frac{\vartheta \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}(0)}{\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0)} \right)^2_{\varepsilon,\varepsilon' \in \mathbb{Z}^g/2\mathbb{Z}^g}$$
Dans le cas hyperelliptique, ce calcul s'effectue au moyen d'invariants binaires par la formule de Thomae [Mum83, livreII].
Dans le cas du genre 3 non hyperelliptique, les 8 rapports qui nous intéressent parmi les $2^{g-1}(2^g+1) = 36$ non nulles sont, avec le choix de l'ordre pour les bitangentes β_i, $i = 4, 5, 6, 7$, indiqué au paragraphe précédent, ceux de la forme $\varepsilon = 0$. Ces rapports sont congrus à 1 modulo 8. On les note $(A_e^{(0)})_{e \in (\mathbb{Z}/2\mathbb{Z})^g}$.
Nous avons vu au chapitre 3 que le calcul de ces rapports en fonction des coefficients de la courbe est basé sur des invariants ternaires. On pourra également consulter [Rit03] où les formules sont regroupées sans démonstration.
3. On duplique ces constantes par les formules de la proposition 1.19, ce qui s'écrit formellement
$$A_e^{(i+1)} = \frac{1}{2^g} \sum_{f \in (\mathbb{Z}/2\mathbb{Z})^g} A_e^{(i)} \sqrt{\frac{A_{e+f}^{(i)}}{A_e^{(i)}}}$$
la racine carrée de $x \in 1 + 8\mathcal{O}$ étant choisie congrue à 1 modulo 4.
4. Le théorème 2.30 montre alors que $\left(A_e^{(N(n+1))} / A_e^{(N)} \right)$ converge linéairement vers $\alpha = \pm \pi_1 \dots \pi_g$ où les π_i sont les g racines du Frobenius inversibles modulo 2.

Il nous reste à montrer comment (pour $g \leq 3$) la connaissance d'une approximation convenable de cette limite est essentiellement suffisante pour recouvrir le polynôme caractéristique de la courbe. C'est l'objet des paragraphes suivants.

4.2.2 Polynôme symétrique

Soit C une courbe de genre g sur $k = \mathbb{F}_q$ ($q = 2^N$, $N > 3$). On note
$$\chi(X) = \chi_C(X) = \prod_{i=1}^{g} (X - \pi_i)(X - \overline{\pi_i})$$
son polynôme caractéristique décomposé sur $\mathbb{C}$.

Définition 4.3
On appelle polynôme symétrique de C/k le polynôme unitaire de degré 2^{g-1} dont les racines sont les $X + q^g/X$ avec X décrivant les produits de g termes appartenant successivement à $\{\pi_1, \overline{\pi_1}\}, \ldots, \{\pi_g, \overline{\pi_g}\}$ (attention : chaque $X + q^g/X$ est décrit deux fois et on n'en conserve qu'un). On note ce polynôme P_{sym}.

Lemme 4.4
P_{sym} est à coefficients dans $\mathbb{Z}$.

Démonstration :
Soit $\mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ alors il existe une permutation $\sigma \in \mathcal{S}_g$ telle que $\mu(\pi_i) = \pi_{\sigma(i)}$ ou $\overline{\pi_{\sigma(i)}}$ (et on a alors $\mu(\overline{\pi_i}) = \overline{\pi_{\sigma(i)}}$ ou $\pi_{\sigma(i)}$). Donc μ permute les racines de P_{sym}. D'où le résultat.

On suppose maintenant la courbe ordinaire. Une des caractérisations de l'ordinarité (cf. définition 2.18) montre que parmi les $2g$ racines 2-adiques de χ exactement g sont des unités, on les note $\pi_1, \ldots, \pi_g$ (les g autres sont encore notées par abus de notations $\overline{\pi_i} = q/\pi_i$).

Lemme 4.5
Soit $g > 1$. Le polynôme symétrique détermine l'ensemble $\{\pi_i^2\}$. Si de plus χ est irréductible, le polynôme symétrique détermine $\chi(\pm X)$.

Démonstration :
Montrons-le pour π_1^2. Le nombre $\omega = \pi_1\overline{\pi_2 \ldots \pi_g} + \overline{\pi_1}\pi_2 \ldots \pi_g$ est une racine du polynôme symétrique et $\pi_1\overline{\pi_2 \ldots \pi_g}$ est la racine de valuation $N(g-1)$ de

$$X^2 - \omega X + q^g.$$

Parmi les racines de P_{sym}, $\pi_1 \ldots \pi_g + \overline{\pi_1 \ldots \pi_g}$ est la seule de valuation nulle. Grâce à elle, on détermine de même $\pi_1 \ldots \pi_g$. On a alors

$$(\pi_1 \ldots \pi_g)(\pi_1\overline{\pi_2 \ldots \pi_g}) = \pi_1^2 q^{g-1}.$$

Si χ est irréductible alors π_1 détermine χ. Or si π_1 est racine de $\chi(X)$, $-\pi_1$ est racine de $\chi(-X)$. D'où le résultat.

Les relations entre l'irréductibilité de P_{sym} et de χ sont subtiles comme le montre le lemme ci-dessous :

Lemme 4.6
Si la racine unité de P_{sym} appartient à $\mathbb{Z}$ alors la jacobienne de C est isogène à la puissance g-ième d'une courbe elliptique sur une extension de degré au plus n de k avec $\phi(n) \leq g(g-1)$ où ϕ est la fonction d'Euler.

Démonstration :
Reprenons la démonstration de [Mes02] que nous allons préciser.

Notons pour tout $1 \leq i, j \leq g$ $z_{ij} = \pi_i/\pi_j$. Comme $\beta \in \mathbb{Z}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ laisse stable la partition $\{\pi_1, \ldots, \pi_g\} \cup \{\overline{\pi_1}, \ldots \overline{\pi_g}\}$ (par des considérations de valuations par exemple) et l'ensemble $\{z_{ij}\}$ est un ensemble stable de nombres algébriques entiers en dehors de 2 puisque $\beta \in \mathbb{Z}$ et entiers au-dessus de 2 donc entiers algébriques et de module 1. Ce sont des racines de l'unité et donc $\mathrm{Jac}(C)$ est isogène sur une extension k' de k à E^g.
Pour préciser le degré maximal de cette extension, remarquons que $|\{z_{ij}\}| \leq 2\binom{g}{2} + 1$ et que si z est une racine n-ième primitive de l'unité, le cardinal de son orbite sous l'action du groupe de Galois absolu est égal à $\phi(n)$ donc $\phi(n) \leq \binom{g}{2}$.

Remarque :
Pour $g = 2$, les degrés des extensions possibles sont $1, 2, 3, 4$ et 6 et 6 est bien le plus grand entier tel que $\phi(6) \leq 2$. Pour $g = 3$ on vérifie que les degrés des extensions possibles sont, outre les cinq précédents, 5 et 7. Or on a par exemple $\phi(18) = 6$. La borne n'est donc pas optimale. Il est amusant de se demander quelle pourrait être cette borne. La question ne semble pas être évidente : en effet on a le résultat de Singer suivant (voir [Sin38] et aussi [Alb66]) : soit g tel que $g - 1$ soit une puissance d'un nombre premier alors il existe g entiers $a_1 = 0, \ldots, a_g$ tels que $a_i - a_j$, $1 \leq i, j \leq g$ représentent tous les résidus modulo $g^2 - g + 1$. Soit donc g tel que $g - 1$ soit une puissance d'un nombre premier et tel que $g^2 - g + 1$ soit premier (c'est le cas par exemple pour $g = 102$) alors si ζ est une racine primitive $(g^2 - g + 1)$-ème de l'unité on peut poser $z_i/z_1 = \zeta^{a_i}$. Alors l'ensemble des $\{z_{ij}\}$ contient toutes les racines $(g^2 - g + 1)$-ième de l'unité en particulier il est stable par Galois. La borne est donc atteinte pour ces valeurs.

Nous allons maintenant analyser les cas $g \leq 3$ successivement. Pour chacun d'entre eux nous montrerons

1. comment la connaissance de P_{sym} détermine essentiellement $\chi(\pm X)$ (sans calculer toutes ses racines).
2. comment la connaissance d'une approximation suffisante du produit $\alpha = \pm\pi_1 \ldots \pi_g$ permet généralement de déterminer $P_{\mathrm{sym}}(\pm X)$. On notera par la suite $\beta = \alpha + \overline{\alpha}$. C'est une racine de $P_{\mathrm{sym}}(\pm X)$.
3. comment on peut lever les ambiguïtés sur les signes.

Remarque :
Pour le genre 4 et plus, la connaissance de β ne permet pas toujours de déterminer $\{\pi_i^2\}$ (cf. [Mes02]). C'est un des obstacles à une généralisation de l'A.G.M. sous sa forme actuelle (c'est-à-dire avec la seule connaissance de β).

4.2.3 Cas $g = 1$

Si on note

$$\chi = X^2 - aX + q = (X - \pi)(X - \overline{\pi})$$

on a

$$P_{\mathrm{sym}} = X - (\pi + \overline{\pi}) = X - a.$$

La connaissance du polynôme symétrique est donc équivalente à la connaissance du polynôme caractéristique.
Comme nous l'avons vu il suffit de de déterminer u modulo $2^{\lceil d/2+1 \rceil}$ pour connaître a au signe près et $|C| \pmod 4$ pour lever l'indétermination sur le signe.

Pour les applications il suffit de prendre des courbes dont on sait par avance qu'elles ont un point d'ordre 4 rationnel. C'est le cas par exemple des courbes qui se relèvent sur K en $y^2 = x(x-a^2)(x-b^2)$ avec a et b définis sur K. En effet ces dernières sont isogènes à $y^2 = x(x-a_1^2)(x-b_1^2)$ avec $a_1 = (a+b)/2$ et $b_1^2 = ab$. Le point $P = (a\,a_1 : a\,a_1\,(a-b)/2 : 1)$ est un point d'ordre 4 tel que $2P = (a_1^2 : 0 : 1)$. Ce point ne se réduit donc pas sur O.

Remarque :
En utilisant des implantations très efficaces de l'A.G.M. (en particulier pour le calcul des racines carrées), Gaudry et Harley [GH01] ont pu calculer le polynôme caractéristique d'une courbe elliptique sur $\mathbb{F}_{2^{11003}}$. Plus récemment, Lercier et Lubicz [LL02] ont mené ce calcul sur $\mathbb{F}_{2^{100002}}$ en 82 heures !

4.2.4 Cas $g = 2$

Si on note

$$\chi = X^4 - aX^3 + bX^2 - aqX + q^2$$

alors

$$P_{\text{sym}} = X^2 + (2q - b)X + q(a^2 - 2b).$$

La connaissance de P_{sym} détermine donc de manière élémentaire (par une racine carrée) $\chi(\pm X)$.

Intéressons nous à la détermination de P_{sym} :
Si $\beta \in \mathbb{Z}$ alors le lemme 4.6 implique que $\text{Jac}(C)$ est isogène à E^2 sur une extension de degré au plus 6 et on détermine facilement le polynôme caractéristique de E en fonction de β.
Si $\beta \notin \mathbb{Z}$ alors β détermine $P_{\text{sym}}(\pm X)$. On a plus précisément :

Lemme 4.7
Supposons $\alpha = \pi_1\pi_2$. *La connaissance de* $\alpha \pmod{8q^2}$ *et de* $|\text{Jac}(C)| \pmod 4$ *détermine* $P_{\text{sym}}(X)$.

Démonstration :
Notons $P_{\text{sym}} = X^2 - sX + qp$. On a $|s| = |\pi_1\pi_2 + \overline{\pi_1\pi_2} + \pi_1\overline{\pi_2} + \overline{\pi_1}\pi_2| \leq 4q$ et de même $|p| = |\pi_1^2 + \pi_2^2 + \overline{\pi_1}^2 + \overline{\pi_2}^2| \leq 4q$. De plus $s \equiv \alpha \pmod q$ et donc, si on pose $s_1 = (s-\alpha)/q$, il suffit de connaître $s_1 \pmod{16}$ pour obtenir s. D'autre part $s_1 = (\frac{\pi_1}{\pi_2} + \frac{\pi_2}{\pi_1}) + \frac{q}{\alpha}$ soit $\alpha s_1 = \pi_1^2 + \pi_2^2 + q$. Donc $p \equiv \alpha s_1 \pmod q$ et si on pose $p_1 = (p - \alpha s_1)/q$ il suffit de déterminer $p_1 \pmod{16}$ pour obtenir p. Nous allons voir que $p_1 \equiv -1 \pmod q$. En effet

puisque β est une racine de P_{sym} on a $2\beta = s \pm \sqrt{\Delta}$ avec $\Delta = (s_1 q + \alpha)^2 - 4q(qp_1 + \alpha s_1)$ soit

$$(\alpha + \frac{2q^2}{\alpha} - s_1 q)^2 = (\alpha - s_1)^2 - 4q^2 p_1.$$

En simplifiant on obtient $p_1 \equiv -1 \pmod{q}$. Ecrivons alors $p_2 = (p_1 + 1)/q$ on a

$$\begin{cases} p = \alpha s_1 - q + q^2 p_2 \\ s = \alpha + q s_1 \end{cases}.$$

Exprimons maintenant $|\text{Jac}(C)| \equiv 1 - a + b \pmod{q}$. Puisque $b \equiv \alpha \pmod{q}$ on a $a^2 \equiv p + 2b \equiv \alpha s_1 + 2\alpha \pmod{q}$. On a besoin de connaître $s_1 \pmod{16}$. Il suffit de connaître $a \pmod{8}$. On connaît alors s exactement donc on peut déterminer $s_1 = (s - \alpha)/q \pmod{16q}$ si on connaît $\alpha \pmod{16q^2}$. Mais alors $p \equiv -q + \alpha s_1 \pmod{16q}$ et donc s et p sont déterminés.
Remarquons qu'en fait on n'a besoin de déterminer $|\text{Jac}(C)|$ que modulo 8 car comme $s \equiv \alpha \pmod{q}$, s est impair donc $|s| < 4q$. Il suffit d'obtenir $s_1 \pmod{8}$ et $a \pmod{4}$.

Remarque :
Avec le modèle introduit au paragraphe 4.1.1, on a directement $|\text{Jac}(C)| \equiv 0 \pmod{4}$ (les points de 2-torsion sont sur k).

Il reste deux problèmes de signe à résoudre : celui de α et celui de χ. L'addition dans la jacobienne d'une courbe de genre 2 pouvant être effectuée de manière efficace, la solution la plus simple consiste à multiplier un point par l'ordre escompté du groupe des points rationnels de la jacobienne. Remarquons que quitte à utiliser cette méthode, il suffit aussi de déterminer α modulo q ($2N$ itérations) et de tester les 4 valeurs possibles pour s_1 apparaissant dans la démonstration.

Remarque :
En utilisant cet algorithme et des techniques similaires au genre 1, Lercier et Lubicz [LL03] ont effectué le calcul du polynôme caractéristique d'une courbe de genre 2 sur $F_{2^{32770}}$ en 8 jours.

4.2.5 Cas $g = 3$

Si on note $\chi = X^6 - aX^5 + bX^4 - cX^3 + bqX^2 - aq^2X + q^3$ alors

$$\begin{aligned} P_{\text{sym}} =& X^4 - c_1 X^3 + q(b_1^2 - 2a_1 c_1 - 2q(a_1^2 - 2b_1))X^2 \\ & - q^2 c_1 (a_1^2 - 2b_1 - 8q)X + q^3(c_1^2 + qa_1(a_1^3 - 4a_1 b_1 + 8c_1)) \end{aligned}$$

avec $a_1 = a, b_1 = b - 3q, c_1 = c - 2qa$.

Analysons tout d'abord les liens entre P_{sym} et χ :

– Si χ est irréductible alors, d'après le lemme 4.5, P_{sym} détermine χ au signe près. Mais puisque $c = c_1 + 2qa$ est non nul (la courbe étant ordinaire), P_{sym} détermine en fait exactement χ.
– En toute généralité la connaissance de P_{sym} détermine c. Le coefficient en X donne b_1 en fonction de a_1^2 donc en exprimant b_1 par cette relation dans le coefficient constant de P_{sym}, a_1 vérifie une équation de degré 4. Si χ n'est pas irréductible, il est toutefois possible que cette équation admette deux solutions entières. C'est par exemple le cas pour

$$P_{\text{sym}} = X^4 - 105X^3 - 4621qX^2 + 9765q^2X + 117425q^3$$

avec $q = 2^5$ pour lequel on a $\alpha_1 = -5$ et $\alpha_2 = 19$ qui conduisent respectivement à $\chi(X) = P_1(X)P_2(X)$ et $\chi'(X) = P_1(X)P_2(-X)$ avec

$$P_1(X) = X^2 - 7X + q \text{ et } P_2(X) = X^4 + 12X^3 + 79X^2 + 12qX + q^2.$$

Par la suite, on suppose pour simplifier que $\mathrm{Jac}(C)$ est absolument simple. En particulier χ est irréductible. Considérons différents cas selon le degré de β :

– Si $\beta \in \mathbb{Z}$ alors, d'après le lemme 4.6, $\mathrm{Jac}(C)$ est isogène sur une extension de degré au plus 7 à E^3 avec E une courbe elliptique. Ce cas est donc exclu.
– Si β est de degré 2 nous allons montrer que $\mathrm{Jac}(C)$ est isogène à un produit $E^2 \times F$ où E, F sont des courbes elliptiques sur une extension de degré au plus 12 de k. En effet remarquons qu'alors $P_{\text{sym}}(X) = P_1P_2$ avec P_1, P_2 de degré deux à coefficients dans $\mathbb{Z}$. On peut supposer

$$P_1(X) = (X - (\pi_1\pi_2\pi_3 + \overline{\pi_1\pi_2\pi_3}))(X - (\overline{\pi_1}\pi_2\pi_3 + \pi_1\overline{\pi_2\pi_3})).$$

L'expression des coefficients en fonction des racines montre que $(\pi_1+\overline{\pi_1})^2+(\pi_2\pi_3+\overline{\pi_2\pi_3})^2 \in \mathbb{Z}$ et $(\pi_1 + \overline{\pi_1})(\pi_2\pi_3 + \overline{\pi_2\pi_3}) \in \mathbb{Z}$. On en déduit $\pi_1^2 + \overline{\pi_1}^2 \in \mathbb{Z}$ et $\pi_2^2\pi_3^2 + \overline{\pi_2^2\pi_3^2} \in \mathbb{Z}$ donc en utilisant le lemme 4.6 on a le résultat. Ce cas est donc également exclu.
– Si β de degré 3 il peut arriver (cf. [Mes02]) que la jacobienne de C soit absolument simple. Mais β détermine tout de même les π_i^2 puisque si on a tous les produits de trois valeurs propres du Frobenius sauf disons $\pi_1\pi_2\overline{\pi_3}$ et son conjugué on a par exemple $q^2\pi_1^2 = (\pi_1\pi_2\pi_3)(\pi_1\overline{\pi_2\pi_3})$, $q^2\pi_2^2 = (\pi_1\pi_2\pi_3)(\overline{\pi_1}\pi_2\overline{\pi_3})$ et $q^2\pi_3^2 = (\overline{\pi_1}\pi_2\pi_3)(\pi_1\overline{\pi_2}\pi_3)$.
– Si β est de degré 4 alors β détermine $P_{\text{sym}}(\pm X)$. Remarquons que puisque χ est supposé irréductible, $P_{\text{sym}}(-X)$ détermine $\chi(-X)$. On peut donc supposer $\alpha = \pi_1\pi_2\pi_3$. Le coefficient $|c_1|$ est inférieur à $q^{3/2}$ mais on ne connaît c_1 que modulo q ($c_1 \equiv \alpha \pmod q$). Contrairement au cas du genre 2, le nombre de chiffres supplémentaires à déterminer dans le développement 2-adique de c_1 croît avec N et on ne peut espérer obtenir ainsi un petit nombre de P_{sym} que l'on pourrait ensuite discriminer. Toutefois nous montrerons dans le paragraphe suivant comment on peut obtenir χ, mais au prix de la connaissance de α avec une grande précision ($\approxeq 12N$).

Il reste le problème du signe de χ. Comme c est impair celui-ci peut être déterminé par la connaissance de $\chi \pmod 4$, c'est-à-dire de l'action du Frobenius sur les points d'ordre 4 de la jacobienne. La courbe C, définie par (4.1), a toutes ses bitangentes rationnelles et donc tous les points d'ordre 2 de sa jacobienne le sont également. Posons $D_\infty = (z \cdot C)$. Pour exhiber les points d'ordre 4, il suffit de trouver les diviseurs $D - D_\infty$ avec D effectif de degré 4 tel que $2(D - D_\infty) = \epsilon$ où ϵ est un point d'ordre 2 (défini comme la moitié de la différence des diviseurs d'intersection de 2 bitangentes). $2D$ est le diviseur des zéros d'une fonction de $L(2D_\infty + \epsilon)$ (qui est de dimension 6), chaque zéro étant double. En caractéristique 2, il est très facile d'exprimer formellement cette condition, de trouver ainsi les diviseurs et de vérifier leur rationnalité. Une variante de cette méthode est illustrée dans l'exemple 4.3.

4.2.6 Détermination de P_{sym} dans le cas $g = 3$

Nous proposons ici d'adapter au cas 2-adique des méthodes de détermination de polynômes minimaux de nombres algébriques.
Rappelons leur principe dans le cas réel (cf. [Coh93]) : soit β un réel algébrique dont le polynôme minimal est de degré m. On cherche à déterminer ce polynôme lorsqu'on connaît β avec une précision suffisante. On se ramène tout d'abord à un problème linéaire en posant $\beta_i = \beta^i$ pour $i = 0, \ldots, m$ et on cherche des entiers r_i tels que $\sum r_i \beta_i \approxeq 0$.
On introduit la forme quadratique définie positive suivante :

$$Q((s_0, \ldots, s_m)) = s_1^2 + \ldots + s_m^2 + C(s_0\beta_0 + \ldots + s_m\beta_m)^2.$$

Si C est grand, un vecteur dans le réseau $(\mathbb{Z}^{m+1}, Q)$ est un petit vecteur pour la norme Q si $\sum s_i\beta_i \approxeq 0$. Une procédure standard (LLL ou ShortestVector de MAGMA) permet de trouver de tels vecteurs dans le réseau à condition que C soit bien choisi. Lorsque la précision est suffisante, le polynôme obtenue est alors le polynôme minimal de β.
Nous allons adapter cet algorithme au cas 2-adique lorsque le polynôme minimal de β est de degré 4. Comme nous l'avons vu dans le paragraphe précédente, ce polynôme est de la forme $X^4 + r_3X^3 + qr_2X^2 + q^2r_1X + q^3r_0$. Supposons que β soit déterminé avec une précision 2^δ. Nous allons chercher une relation linéaire entre $(\beta_{-1}, \beta_4, \beta_3, \beta_2, \beta_1, \beta_0) = (2^\delta, \beta^4 \pmod{2^\delta}, \beta^3 \pmod{2^\delta}, q\beta^2 \pmod{2^\delta}, q^2\beta \pmod{2^\delta}, q^3 \pmod{2^\delta})$. Nous savons également que le coefficient dominant de P_{sym} est 1. Nous allons donc pondérer le coefficient correspondant dans la forme quadratique que nous définissons par :

$$\begin{aligned} Q((s_{-1}, s_4, s_3, s_2, s_1, s_0)) = {} & 2^{\lfloor \delta/2+N \rfloor} s_4^2 + 2^{3N} s_3^2 + 2^{2N} s_2^2 + 2^N s_1^2 + s_0^2 \\ & + C(s_{-1}\beta_{-1} + s_4\beta_4 + s_3\beta_3 + s_2\beta_2 + s_1\beta_1 + s_0\beta_0)^2. \end{aligned}$$

Oublions un instant les coefficients devant les s_i^2 $(i \leq 3)$ qui n'ont qu'un rôle secondaire. Si on divise $(\beta_{-1}, \beta_4, \beta_3, \beta_2, \beta_1, \beta_0)$ par 2^δ on se ramène à chercher une relation entre des réels proches de 1 connus avec une précision $1/2^\delta$. D'après Cohen [Coh93], C doit alors être compris entre 2^δ et $2^{2\delta}$; on prendra $C = 2^\delta$. De plus il faut que la précision soit au moins de $1/2^{dr}$ où r est la «taille» des coefficients r_i et d la dimension du réseau. Ces coefficients sont plus petits (par les inégalités de Hasse-Weil) que 2^{3N}. Si on prend

$r = 2^{2N}$ on peut espérer un résultat satisfaisant avec $\delta = 12N$.
Regardons maintenant les termes devant les s_i^2. Si on examine plus précisément les bornes pour les coefficients de P_{sym} on obtient les résultats suivants : $1, q^{3/2}, q \cdot q^2, q^2 \cdot q^{5/2}, q^3 \cdot q^3$. Heuristiquement les r_i, $i = 4 \dots 1$ forment une suite croissante. On met donc un pondérateur inversement proportionnel dans la forme quadratique devant les s_i^2.

Remarque :
GP version 2.1.3 possède une fonction algdep qui permet de déterminer des relations algébriques en p-adique en ajoutant un $O(p^\delta)$ à la valeur entière de l'approximation de la racine. Mais cette fonction ne tient pas compte de toutes les spécificités de notre polynôme, nous l'avons donc reprogrammée dans MAGMA en utilisant deux algorithmes différents de recherche de vecteurs minimaux :

- LLL qui est la méthode utilisée également par GP.
- la fonction ShortestVector qui détermine exactement les vecteurs minimaux. Lorsque la dimension du réseau est faible (≤ 6) cette fonction est presque aussi rapide que LLL. Cependant elle ne semble pas apporter d'amélioration sensible.

On a vu que la précision nécessaire est directement subordonnée à la taille des coefficients et à la dimension du réseau. Puisqu'on connaît c_1 à q près on peut écrire $c_1 = c_1' + qc_1''$ et ainsi diminuer la taille des coefficients. Néanmoins ce procédé augmente la dimension du réseau et donc la précision nécessaire sur β.
Une autre possibilité serait l'utilisation de l'algorithme PSLQ qui est spécifique à la détermination de relations linéaires. En particulier cet algorithme ne demande pas la détermination délicate de la constante C. Pourtant cette méthode ne donne pas d'aussi bon résultats que notre version de LLL : l'explication la plus simple est que PSLQ ne tient pas compte du fait que le polynôme recherché est unitaire.

4.3 Exemple

On considère la courbe suivante :

$$\tilde{C} : (x^2 + \omega^2 y^2 + \omega^4 z^2 + \omega xy + (\omega^2 + 1)xz + (\omega^3 + 1)yz)^2 - xyz(x + y + z) = 0$$

définie sur $k = F_{2^N}$, $N = 72$ où ω engendre le groupe multiplicatif k^*.
Les calculs sont réalisés grâce au logiciel MAGMA version 2.9 sur un Pentium III à 1.13 Ghz avec 2 GigaOctets de mémoire centrale.
On calcule les v_1, v_2, v_3 du modèle de la proposition 4.1

$$\begin{aligned} v_1 &= \omega^6 y + (\omega^4 + \omega^3 + 1)z \\ v_2 &= \omega^4 x + \omega^5 y + (\omega^4 + \omega^2 + 1)z \\ v_3 &= \omega^4 x + (\omega^6 + \omega^5)y + (\omega^4 + \omega^3 + \omega^2 + 1)z \end{aligned}$$

On note K l'extension de degré N non ramifiée de $\mathbb{Q}_2$, $\mathcal{O}$ son anneau d'entiers et $w \in \mathcal{O}$ qui se réduit sur ω. Le modèle (4.2) de C est défini par

$$\begin{aligned}
u_1 &= (-2w^4-2w^3-1)x_1+(4w^6-2w^4-2w^3-2)x_2+(-2w^4-2w^3-2)x_3\\
u_2 &= (2w^4-2w^2-2)x_1+(4w^5-2w^4-2w^2-1)x_2+(-2w^4-2w^2-2)x_3\\
u_3 &= (2w^4-2w^3-2w^2-2)x_1+(4w^6+4w^5-2w^4-2w^3-2w^2-2)x_2+\\
&\quad (-2w^4-2w^3-2w^2-1)x_3
\end{aligned}$$

On effectue le calcul des 4 bitangentes qui nous manquent grâce à l'algorithme du paragraphe 3.5 (temps : 1/2 heure) puis de l'ensemble des bitangentes et des 8 rapports

$$\left(\frac{\vartheta\left[\begin{array}{c}0\\ \varepsilon'\end{array}\right](0)}{\vartheta\left[\begin{array}{c}0\\ 0\end{array}\right](0)}\right)^4_{\varepsilon'\in\mathbb{Z}^3/2\mathbb{Z}^3}$$

relatifs au noyau du Frobenius (et congrus à 1 modulo 16) grâce aux théorèmes 3.52 et 3.54 (temps : 15 mn).
On calcule leur racine carrée dans K

$$\begin{cases}
1+O(2^4)\\
1+(w^{16}+w^{14}+w^{12}+w^{11}+w^9+w^5+w^4)\cdot 2^3+O(2^4)\\
1+(w^{16}+w^{14}+w^{12}+w^{11}+w^{10}+w^8+w^4+w^3)\cdot 2^3+O(2^4)\\
1+(w^{10}+w^9+w^8+w^5+w^3)\cdot 2^3+O(2^4)\\
1+(w^6+w^4+w^3)\cdot 2^3+O(2^4)\\
1+(w^{16}+w^{14}+w^{12}+w^{11}+w^9+w^6+w^5+w^3)\cdot 2^3+O(2^4)\\
1+(w^{16}+w^{14}+w^{12}+w^{11}+w^{10}+w^8+w^6)\cdot 2^3+O(2^4)\\
1+(w^{10}+w^9+w^8+w^6+w^5+w^4)\cdot 2^3+O(2^4)
\end{cases}$$

On effectue l'itération de la formule de duplication $12N$ fois (temps : 24 heures) qui nous donne, au signe près, la valeur du produit des racines du Frobenius inversibles modulo 2

$$\beta = 1+2^8+2^9+2^{11}+2^{13}+2^{15}+2^{16}+2^{17}+2^{18}+2^{21}+2^{23}+2^{24}+\ldots+2^{787}+2^{790}+2^{791}+O(2^{793})$$

On trouve, grâce à LLL (temps : 1 seconde), le polynôme minimal de β :

$$\begin{aligned}
P_{\mathrm{sym}}(X) &= X^4-52767044410803560460262696266497\ X^3-\\
&\quad 781212772777107947195275720338911086462869 09\cdot 2^{72}\ X^2+\\
&\quad 610161746623391968394415142270976679056928051874538813\cdot 2^{2\cdot 72}\ X+\\
&\quad 469183305653261508552887758516448848907202890239058995098519034 89\cdot 2^{3\cdot 72}
\end{aligned}$$

D'où le polynôme caractéristique au signe près

$$\begin{aligned} P(X) &= X^6 - 9925657555\ X^5 + 1108548370771462406931\ X^4 \\ &\quad -1465122295271513046512452800130 57\ X^3 + 1108548370771462406931 \cdot 2^{72} X^2 \\ &\quad -9925657555 \cdot 2^{2 \cdot 72}\ X + 2^{3 \cdot 72}. \end{aligned}$$

Pour déterminer le signe, on étudie les points d'ordre 4 de la jacobienne. Plus précisément dans notre cas, 2^6 divise $P(1)$ mais 2^4 ne divise pas $P(-1)$. Il suffit donc que la jacobienne de $\tilde{C}$ possède un point d'ordre 4 rationnel pour conclure que $P(X)$ est le «bon» polynôme. Considérons par exemple le point d'ordre 2 $(P_1 + Q_1 - (P_2 + Q_2)) = \frac{1}{2}((x \cdot \tilde{C}) - (y \cdot \tilde{C}))$. On cherche un point de la jacobienne sous la forme $D = P+Q+R-3P_2$ tel que $2D = P_1 + Q_1 - (P_2 + Q_2)$ ou encore $2(P + Q + R) - (P_1 + Q_1 + 5P_2 - Q_2) = 0$. En utilisant le logiciel MAGMA, on montre que l'espace $L(P_1 + Q_1 + 5P_2 - Q_2)$ qui est de dimension 4, contient une fonction définie sur $\mathbb{F}_{2^{72}}$ ayant trois zéros rationnels de multiplicité 2, d'où l'existence d'un point d'ordre 4 rationnel sur $\mathbb{F}_{2^{72}}$ (temps : 10 secondes).

Remarque :
A posteriori on constate que la précision nécessaire est seulement de $10 \cdot 72$, le calcul est alors réalisé en 21 heures. Il serait donc très utile d'avoir une meilleure borne pour LLL. L'utilisation de méthodes de multiplication rapides dans la boucle de duplication permettrait d'améliorer sensiblement les performances de l'algorithme (en extrapolant les temps pour le genre 1, on obtient 10 mn pour le calcul ci-dessus). Une implémentation efficace est en cours.

Chapitre 5

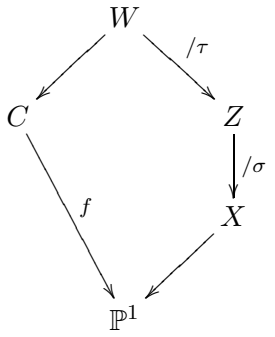
Une construction géométrique

Nous présentons ici une construction de nature purement géométrique décrite par David Lehavi dans sa thèse [Leh02] et que nous avons rendu implémentable. L'itération de cette construction pourrait être la description d'une méthode A.G.M. géométrique mais nous verrons qu'un certain nombre de problèmes s'opposent encore à sa réalisation effective et efficace. Malgré cela, la diversité des objets introduits, l'éclairage qu'ils apportent sur les notions précédemment étudiées seront peut-être utiles pour d'autres questions relatives aux courbes de genre 3 (points de Weierstrass, calculs sur la jacobienne, etc.).

5.1 Construction géométrique

Nous rappelons ici les principales étapes de la construction de Lehavi qui à une courbe C de genre 3 associe une courbe C' de genre 3 dont les jacobiennes sont $(2,2,2)$-isogènes. Les constructions sont valables sur un corps algébriquement clos de caractéristique différente de 2 et 3.

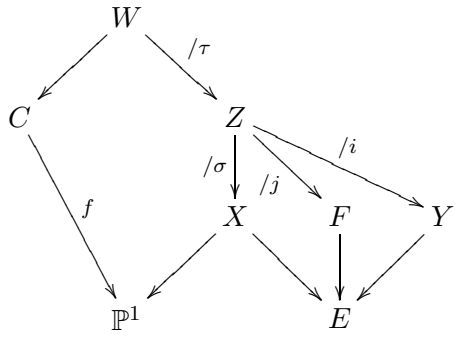
Soient donc C une courbe de genre 3 non hyperelliptique et $\alpha \in \mathrm{Jac}(C)[2] \setminus \{0\}$. On choisit f un morphisme de $C \to \mathbb{P}^1$ tel que le diviseur des zéros de f, $(f)_0$, satisfasse $(f)_0 \sim K_C + \alpha$ où K_C est le diviseur canonique de C. Comme $\mathrm{h}^0(K_C + \alpha) = 2$, f est unique aux automorphismes de $\mathbb{P}^1$ près. On effectue alors la transformation trigonale définie dans [Don92] :



avec $W = \overline{C \times_{\mathbb{P}^1} C \setminus \text{diag}} = \{(p,q)/p+q < K_C + \alpha\}$. W admet une involution $\tau : (p,q) \mapsto (q,p)$. On définit $Z = W/\tau$. Z a également une involution naturelle σ définie par : si $\{p,q\} \subset f^{-1}(r)$ pour $r \in \mathbb{P}^1$ on lui associe l'élément de $f^{-1}(r) \setminus \{p,q\}$. On note $X = Z/\sigma$.

Lemme 5.1 [Leh02, lem.3.7]
Soit Θ le diviseur thêta sur Jac(C). *L'application $Z \to \Theta \cap (\Theta + \alpha)$ $\{p,q\} \mapsto p+q$ est un isomorphisme.*

A l'aide de cette identification, on définit alors les involutions de Z, $i : d \mapsto d - \alpha$ et $j : d \mapsto K_C - d$ (on a $\sigma = i \circ j$). On pose $Y = Z/i$, $F = Z/j$ et $E = Z/ < i,j >$. Ceci complète notre diagramme de la manière suivante :



On note Σ l'ensemble des points fixes dans Z par l'involution j.

Lemme 5.2 [Leh02, lem.3.11]
Les diviseurs associés aux fibrés thêta caractéristiques de C dans Z sont les points de Σ. Ils sont au nombre de 12, *leurs caractéristiques sont toutes impaires et appariées par i.*

On note $\{p_i, \overline{p_i}\}$ les 6 paires de bitangentes représentant les éléments de Σ appariés par i. On note $q_1, \ldots, q_6$ les points de Σ/i vus comme points de ramification de Y/E.

Théorème 5.3 [Leh02, th.3.15]
Il y a une correspondance biunivoque entre les partitions de $\{q_1, \ldots, q_6\}$ *en trois paires avec une paire distinguée et les drapeaux isotropes* $\mathcal{L}_1 \subsetneq \mathcal{L}_2 \subsetneq \mathcal{L} \subset \mathrm{Jac}(C)[2]$ *tels que* $\mathcal{L}_1 =< \alpha >$.

Proposition 5.4 [Leh02, prop.4.12]
La courbe Z *est génériquement lisse.*

Remarque :
D. Lehavi nous a confirmé une petite imprécision à cet endroit de sa thèse puisque Z n'est pas toujours lisse dans le cas non hyperelliptique. En effet les points singuliers de Z sont les éléments $\{p, q\}$ tels que $2(p+q) = K_C + \alpha$ [Leh02, lem.4.3]. On peut donner un exemple pour lequel de tels points apparaissent : $C : V^2 - UW = 0$ avec $V = y^2 - 1, U = x^2 - 1, W = 3 \cdot (5/6x - 5/6y + 1)^2 - (y^2 - 1)$. La courbe C est de genre 3 non hyperelliptique. Posons

$$\begin{aligned} \alpha &= \frac{1}{2}((x=1)\cdot C) - ((x=-1)\cdot C) \\ &= (1:1:1) + (1:-1:1) - (-1:1:1) - (-1:-1:1) \in \mathrm{Jac}(C)[2] \end{aligned}$$

(car $x = 1$ et $x = -1$ sont des bitangentes). On vérifie alors facilement que

$$\begin{aligned} 2K_C = ((U+V=0)\cdot C) &= \underbrace{(1:1:1) + (1:-1:1) + (-1:1:1) + (-1:-1:1)}_{=K_C+\alpha} \\ &\quad +2(-7/5:-1/5:1) + 2(1/5:7/5:1). \end{aligned}$$

De tels exemples peuvent être facilement construits par la théorie que nous allons introduire ultérieurement en regardant C comme l'enveloppe de la famille de coniques $\lambda^2 U + 2\lambda^2 V + W = 0$ dont les points de tangence à C sont définis par les points d'intersection de $\lambda U + V = 0$ et de $\lambda V + W = 0$. Pour avoir ce cas pathologique, il suffit donc que pour $\lambda = 1$, par exemple, les coniques $U + V = 0$ et $V + W = 0$ soient tangentes en 2 points.

On supposera désormais qu'on est dans le cas générique.

Corollaire 5.5 [Leh02, cor.4.4]
Les courbes X, Y, E, F *sont lisses de genres respectifs* $4, 4, 1, 1$.

La construction trigonale permet d'interpréter la jacobienne de C comme une variété de Prym (cf. [Mum74]). Plus précisément on a :

Théorème 5.6 [Leh02, th.4.13]
$\mathrm{Jac}(C) \simeq \mathrm{Prym}(Z/X)$ *et sous cette identification le noyau de l'application norme de* $\mathrm{Jac}(C) \simeq \mathrm{Prym}(Z/X) \to \mathrm{Prym}(Y/E)$ *est* $\alpha^{\perp}$.

Soit $k : C \hookrightarrow |K_C|^* = \mathbb{P}^2$ le plongement canonique. On définit $\psi : \mathrm{Sym}^2(C) \to \mathbb{P}^{2*}$ par $\{p, q\} \mapsto (k(p)k(q))$ (la droite passant pas $k(p)$ et $k(q)$). L'application $i_F : F \mapsto \mathbb{P}^{2*}$ induite par ψ est un plongement de degré 3.

Proposition 5.7 [Leh02, cor.6.5]

- *F est l'unique courbe de degré 3 passant par les $p_i^*, \overline{p_i}^*$ (si p est une droite de $\mathbb{P}^2$, p^* est le point associé dans $\mathbb{P}^{2*}$).*
- *Il existe $\pi \in \mathrm{Jac}(F)[2]$ tel que $p_i^* - \overline{p_i}^* = \pi^*$. On a alors $E = F/\pi^*$ réalisée comme le lieu des intersections dans $\mathbb{P}^2$ des droites $l, i(l)$ pour $l^* \in F$. En particulier les points q_i sont les intersections de p_i et $\overline{p_i}$ et sont sur E.*
- *Les points q_i sont de plus sur une conique Q.*

Avec ces notations, on définit également $\pi \in \mathrm{Jac}(E)[2]$ par $F \simeq E/\pi$.

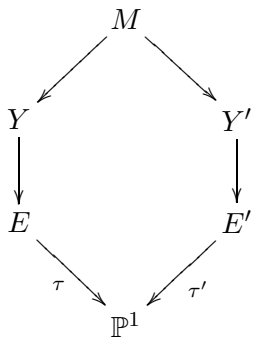
Toutes ces constructions sont justifiées par le résultat suivant :

Théorème 5.8 [Leh02, th.1.4]
On a génériquement une équivalence entre les données suivantes :

- *La donnée d'une courbe C de genre 3 non hyperelliptique et d'un point de 2-torsion à isomorphisme près.*
- *Un revêtement Y/E, Y de genre 4 et E de genre 1 avec le choix d'un élément $\pi \in \mathrm{Jac}(E)[2] \setminus \{0\}$ à isomorphisme près.*
- *Une configuration plane $E, Q \hookrightarrow \mathbb{P}^2$ de degrés 3 et 2 respectivement, E, Q lisses dont l'intersection est transverse, à transformation projective près avec le choix de $\pi \in \mathrm{Jac}(E)[2] \setminus \{0\}$.*

Un de nos objectifs dans le prochain paragraphe sera de rendre cette équivalence explicite.

Cette première construction a permis de «casser» la courbe de genre 3 en deux objets plus simples : une conique et une cubique. On va effectuer une nouvelle construction à partir de cette configuration afin d'obtenir une nouvelle conique et une nouvelle cubique qui seront associées par l'équivalence ci-dessus à une courbe C' de genre 3 dont la jacobienne est $(2, 2, 2)$-isogène à celle de C.
Soit $\mathcal{L}$ un sous-espace isotrope maximal de $\mathrm{Jac}(C)[2]$ avec $< \alpha >= \mathcal{L}_1 \subsetneq \mathcal{L}_2 \subsetneq \mathcal{L}$. La donnée de $\mathcal{L}_2$ est équivalente, d'après le théorème 5.3, à la donnée de deux points $q_1, q_2 \in \Sigma/i$. On considère alors l'unique revêtement double $\tau : E \to \mathbb{P}^1$ tel que $\tau(q_1) = \tau(q_2)$. On effectue la transformation bigonale (cf. [Don92])



Théorème 5.9 [Leh02, th.10.2]
Génériquement, il existe une courbe C' de genre 3 et $\alpha' \in \mathrm{Jac}(C')[2] \setminus \{0\}$ tels que
- $\mathrm{Jac}(C') = \mathrm{Jac}(C)/\mathcal{L}$.
- *$Y' \to E'$ est associé à C', α' par la construction trigonale avec $\alpha' = \mathcal{L}_2^{\perp}/\mathcal{L}$.*

De plus on peut caractériser Y', E' par une configuration plane E', Q' qui est construite comme suit. Soit t le point d'intersection résiduel de $(q_1 q_2)$ avec E. E' est alors l'unique cubique passant par t, les quatre points de ramification de τ et les quatre points de $\{q_3, q_4, q_5, q_6\} = Q \cap E \setminus \{q_1, q_2\}$. De plus les droites (tq_i) sont tangentes à E' en q_i pour $i = 3, 4, 5, 6$. Enfin Q' est l'unique conique passant par les quatre points de ramification de τ et par les deux autres points (en dehors de t) d'intersection de $(q_1 q_2)$ avec E'.

5.2 Eléments de géométrie des courbes de degré ≤ 4

Les propriétés de polarité pour les coniques ont été étudiées de longue date. Pour les courbes de degré supérieur, ces notions ont fait l'objet d'investigations au cours du XIXème et du XXème siècle. Nous aurons besoin d'étudier en détails le cas des cubiques et ses liens avec les réseaux de coniques comme il est fait dans [Sal79]. Pour la commodité du lecteur, nous donnons ici les résultats dont nous avons besoin avec leur démonstration. Certaines sont originales.

Soit $\mathbb{P}^2$ le plan projectif de coordonnées $(x : y : z)$. Si U est un polynôme homogène en x, y, z on note $U_{x^i y^j z^k} = \frac{\partial}{\partial x^i \partial y^j \partial z^k} U$.
On appelle matrice hessienne de U la matrice des dérivées partielles secondes de U. On la note $\mathcal{H}(U)$. On appelle hessienne de U le déterminant de cette matrice et on le note $\mathrm{H}(U)$.
Si p est un point et M une matrice 3×3 à coefficients polynomiaux, on note M_p la matrice obtenue en évaluant les coefficients de M en p. On fera attention à ne pas confondre cette notation avec Mp qui représente l'opération de multiplication matricielle.
On appelle (droite) polaire par rapport à U en $p = (x_0 : y_0 : z_0)$ la droite $xU_x(p) + yU_y(p) + zU_z(p) = 0$. Si U est de degré 2 c'est aussi la droite $x_0 U_x + y_0 U_y + z_0 U_z = 0$.

Si E est une cubique, on appelle conique polaire par rapport à E en p la conique $x_0E_x + y_0E_y + z_0E_z = 0$. C'est aussi la conique dont la matrice hessienne est $\mathcal{H}(S)_p$.

5.2.1 Réseaux de coniques

Soient U, V, W trois coniques telles que $U \cap V \cap W = \emptyset$. On note $\mathcal{S}$ le réseau

$$< U, V, W >= \{\lambda U + \mu V + \nu W,\ (\lambda : \mu : \nu) \in \mathbb{P}^2\}.$$

On note E le lieu des points de $\mathbb{P}^2$ tel que les polaires par rapport à toutes les coniques de $\mathcal{S}$ en ces points soient concourantes.

Théorème 5.10
E est la courbe définie par le déterminant de la matrice jacobienne de U, V, W (la matrice est notée $\mathcal{J}(\mathcal{S})$) et est appelée jacobienne de $\mathcal{S}$, notée $\mathrm{J}(\mathcal{S})$.

Démonstration :
Par linéarité on voit qu'il suffit que les polaires par rapport à U, V et W soient concourantes. Soit $p \in \mathbb{P}^2$. La polaire par rapport à U en p est la droite $xU_x(p) + yU_y(p) + zU_z(p) = 0$, de même pour V et W. La condition de concourance s'énonce alors

$$\begin{vmatrix} U_x(p) & V_x(p) & W_x(p) \\ U_y(p) & V_y(p) & W_y(p) \\ U_z(p) & V_z(p) & W_z(p) \end{vmatrix} = 0$$

et le membre de gauche est par définition le déterminant de la matrice jacobienne de U, V, W.

Remarque :
Considérons deux coniques du réseau, S_1 et S_2. Toute conique passant par $S_1 \cap S_2$ (avec des conditions de tangence en cas de points multiples) est une conique du réseau $\mathcal{S}$ (en effet une conique passant par $S_1 \cap S_2$ s'écrit $\lambda S_1 + \mu S_2$, $(\lambda, \mu) \in \mathbb{P}^1$). Considérons alors deux droites d_1, d_2 passant par ces points. $S = d_1 d_2 \in \mathcal{S}$ et si $p = (d_1) \cap (d_2)$ $S_x(p) = S_y(p) = S_z(p) = 0$ donc $p \in E$.

Remarquons que la condition : p' appartient à la polaire par rapport à U en p étant symétrique pour une conique, on peut définir :

Définition 5.11
Les polaires par rapport aux coniques de $\mathcal{S}$ en un point p de E sont concourantes en un autre point de la jacobienne appelé point correspondant et noté $\overline{p}$.

Cette opération définit donc une involution sur E.

Remarque :
Matriciellement $\overline{p} = \ker \mathcal{J}(\mathcal{S})_p$.

5.2.2 Hessienne et cayleyenne

Nous allons donner un nouvel éclairage à ces notions. Soit donc S une cubique plane. On considère le réseau $\mathcal{S} =< S_x, S_y, S_z >$.

Proposition 5.12
On a $\mathcal{J}(\mathcal{S}) = \mathcal{H}(S)$. En particulier la hessienne de S est égale à la jacobienne de $\mathcal{S}$.

Démonstration :
On remarque tout simplement que $S_{x^2} = \frac{\partial}{\partial x} S_x$, ce qui identifie le terme en haut à gauche de la matrice jacobienne de S_x, S_y, S_z et de la matrice hessienne de S. De même pour les autres termes.

On note $E = \mathrm{H}(S)$.

Proposition 5.13
La conique polaire par rapport à S en un point (lisse) p de E se scinde en deux droites qui sont concourantes au point correspondant, $\overline{p}$, pour le réseau $\mathcal{S}$.

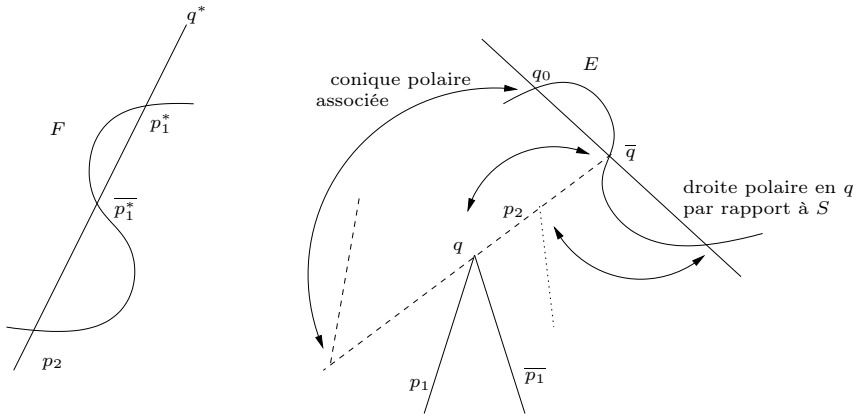
Démonstration :
Soit p un point lisse de E. Puisque $\mathcal{H}(S) = \mathcal{J}(\mathcal{S})$, $\mathcal{H}(S)_p$ est singulière de rang 2, c'est donc la matrice hessienne d'une conique singulière qui n'est autre que la conique polaire par rapport à S en p. Le point d'intersection des deux droites formant cette conique est égal à $\ker \mathcal{H}(S)_p$. Or on a vu que $\overline{p} = \ker \mathcal{J}(\mathcal{S})_p$. D'où le résultat par la proposition 5.12.

Soient $A, \overline{A}$ deux points correspondants de E. Comme A et $\overline{A}$ sont conjugués par rapport à toutes les coniques du réseau, la droite $(A\overline{A})$ est coupée harmoniquement par ces coniques qui définissent alors une involution sur cette droite pour laquelle A et $\overline{A}$ sont fixes. Considérons alors C le point d'intersection résiduel de $(A\overline{A})$ avec E. Il existe une conique dont le point singulier est C mais comme C n'est pas fixe pour l'involution, il faut qu'une des droites de la conique soit la droite $(A\overline{A})$. On a donc une correspondance biunivoque entre les droites reliant deux points correspondants et les paires de droites des coniques scindées de $\mathcal{S}$. On peut alors définir :

Définition 5.14
On appelle cayleyenne de S (ou du système $\mathcal{S}$) la courbe de $(\mathbb{P}^2)^*$ vue comme lieu des droites des coniques scindées de $\mathcal{S}$, ou comme lieu des droites reliant deux points correspondants de la hessienne de S. On note cette courbe $\mathrm{Cay}(S) = F$.

Remarque :
Sa courbe duale (qui est une «vraie» courbe de $\mathbb{P}^2$) est donc l'enveloppe de l'un ou l'autre des systèmes de droites ci-dessus.

FIG. 5.1 – F est de degré 3



Lemme 5.15
Cay(S) est une cubique.

Démonstration :
Considérons en effet un point $q \in \mathbb{P}^2$ qui est le représentant d'une droite q^* dans le plan dual (cf. figure 5.1). Un point $q_0 = (x_0 : y_0 : z_0)$ dont la conique polaire passe par q doit être sur la droite polaire en q par rapport à S (c'est l'écriture $x_0 S_x(q) + y_0 S_y(q) + z_0 S_z(q) = 0$) et cette conique est scindée si et seulement si q_0 est sur E d'où trois possibilités pour q_0.

Remarque :
On peut aussi définir la cayleyenne comme le lieu des droites sur lesquelles $\mathcal{S}$ définit une involution. Sous cette forme, on peut donner une équation de Cay(S) (cf. [Sal69, p. 364]) :

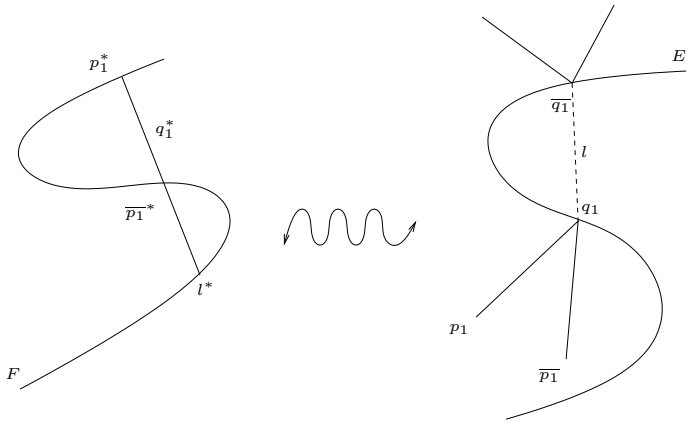
$$\begin{vmatrix} U_{x^2} & U_{y^2} & U_{z^2} & 2U_{yz} & 2U_{xz} & 2U_{xy} \\ V_{x^2} & V_{y^2} & V_{z^2} & 2V_{yz} & 2V_{xz} & 2V_{xy} \\ W_{x^2} & W_{y^2} & W_{z^2} & 2W_{yz} & 2W_{xz} & 2W_{xy} \\ x & 0 & 0 & 0 & z & y \\ 0 & y & 0 & z & 0 & x \\ 0 & 0 & z & y & x & 0 \end{vmatrix}$$

en notant $U = S_x$, $V = S_y$ et $W = S_z$.

Sur F on a aussi une involution (encore notée $\overline{\ }$) qui à un point de F représentant une des droites de la conique scindée associe la seconde.
Dans le cas où S est lisse, E et F le sont également. On peut alors considérer ces courbes comme des courbes elliptiques. Soient q_1 et $\overline{q_1}$ deux points correspondants sur E on considère la courbe elliptique $\tilde{E}$ isomorphe à E par ϕ qui est telle que $\phi(q_1) = O$. L'involution de E définit alors une translation par un point d'ordre 2 sur $\tilde{E}$, $\pi = \phi(\overline{q_1})$

et la courbe F est isomorphe au quotient E/π qui est 2-isogène à E (c'est la «chord construction» de [Leh02]). L'involution définie sur E/π par le point d'ordre 2 de $E[2]/<\pi>$ correspond à l'involution de F.

FIG. 5.2 – E et F



Comme on l'a vu la cayleyenne peut être définie par deux systèmes de droites différents. Si on se donne q_1 et $\overline{q_1}$, le premier système de droites définit les points p_1^* et $\overline{p_1}^*$ provenant de la conique scindée en q_1. Le deuxième système de droites définit un point $l^* \in F$ qui est le point correspondant à la droite $q_1\overline{q_1}$. Ce point qui est un point de F est aussi un point de q_1^*, c'est donc l'intersection résiduelle de $(p_1^*\overline{p_1}^*)$ avec F (voir figure 5.2).

5.2.3 Propriétés de tangences

Théorème 5.16
La droite polaire par rapport à la cubique S en un point de la hessienne est la tangente à la hessienne au point correspondant pour le réseau $\mathcal{S}$.

Lemme 5.17
La polaire d'un point A par rapport à S est la polaire de A par rapport à la conique polaire en A (par rapport à S).

Démonstration :
Notons $A = (a_1 : a_2 : a_3)$. La polaire par rapport à S en A est la droite $(S_x(A) : S_y(A) : S_z(A))$. La conique polaire est la courbe $a_1S_x + a_2S_y + a_3S_z = 0$ et la polaire en A par rapport à cette courbe est la droite $(a_1S_{x^2}(A) + a_2S_{xy}(A) + a_3S_{xz}(A) : \ldots)$. Or $a_1S_{x^2}(A) + a_2S_{xy}(A) + a_3S_{xz}(A) = a_1S_{x^2}(A) + a_2S_{yx}(A) + a_3S_{zx}(A) = 2S_x(A)$. De même pour les deux autres coordonnées. D'où le résultat.

Démonstration :
Nous allons montrer cela analytiquement. On peut supposer par un changement de coordonnées que $A = (0 : 0 : 1) \in E$, $\overline{A} = (x_0 : y_0 : z_0) \in E$ et que la conique polaire par rapport à S en $\overline{A}$ est $U = xy$. La polaire par rapport à U en $\overline{A}$ est $xy_0 + yx_0 = 0$. La définition de E comme la jacobienne du réseau montre que l'on peut supposer celui-ci de la forme $< U, V, W >$ avec U défini ci-dessus. Le point $\overline{A}$ est le point d'intersection des polaires par rapport à U, V, W en A. Il est donc défini par le système

$$\begin{cases} x_0 V_x(A) + y_0 V_y(A) + z_0 V_z(A) = 0 \\ x_0 W_x(A) + y_0 W_y(A) + z_0 W_z(A) = 0 \end{cases}$$

soit

$$x_0 = \begin{vmatrix} V_y(A) & V_z(A) \\ W_y(A) & W_z(A) \end{vmatrix},\ y_0 = \begin{vmatrix} V_z(A) & V_x(A) \\ W_z(A) & W_x(A) \end{vmatrix},\ z_0 = \begin{vmatrix} V_x(A) & V_y(A) \\ W_x(A) & W_y(A) \end{vmatrix}.$$

La cubique E a pour équation

$$E : \begin{vmatrix} y & V_x & W_x \\ x & V_y & W_y \\ 0 & V_z & W_z \end{vmatrix} = 0.$$

La tangente en A à E est le terme de degré 1 en x et en y de cette expression c'est-à-dire

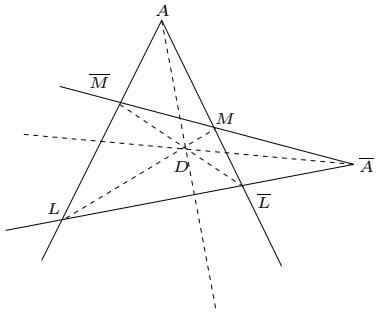
$$x \underbrace{(V_x(A)W_z(A) - W_x(A)V_z(A))}_{=y_0} - y \underbrace{(V_y(A)W_z(A) - W_y(A)V_z(A))}_{=x_0} = 0.$$

Ce qu'il fallait démontrer.

Corollaire 5.18
Les tangentes à la hessienne en des points correspondants sont concourantes en un point de la hessienne.

Démonstration :
Soit A et $\overline{A}$ deux points correspondants de E de coniques polaires respectives (AL, AM) et $(\overline{AL}, \overline{A}\,\overline{M})$ où $L, M, \overline{L}, \overline{M}$ sont les quatre pôles de la droite $(A\overline{A})$ par rapport à S (voir la figure 5.3). Rappelons qu'un pôle d'une droite d par rapport à S est un point p tel que la polaire en p par rapport à S soit d. Ce sont donc les points d'intersection de toutes les coniques polaires par rapport à S en les points de la droite d.

FIG. 5.3 – Tangentes à la hessienne

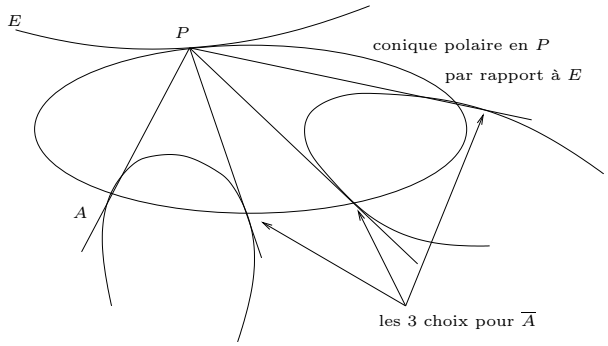


Si on considère la conique scindée formée des deux droites (LM) et $(\overline{L}\,\overline{M})$ c'est une conique du système $\mathcal{S}$ donc $D = (LM) \cap (\overline{L}\,\overline{M})$ est un point de la jacobienne E. De plus cette conique est la conique polaire du point correspondant $\overline{D}$ qui est sur $(A\overline{A})$ (par définition des pôles d'une droite). D'après le théorème 5.16, la tangente en $\overline{A}$ à E est la polaire en A par rapport à la cubique S et donc aussi, d'après le lemme 5.17, la polaire en A par rapport à la conique polaire en A (par rapport à S). Donc ici par rapport à $(\overline{AL}, \overline{AM})$. Par les propriétés harmoniques du quadrilatère c'est donc la droite $(\overline{A}D)$. De même la tangente en A est la droite $(\overline{A}D)$. Ces deux droites sont donc concourantes en D qui est un point de E.

Remarque :
Ce corollaire est évident lorsqu'on considère des cubiques lisses puisqu'avec l'interprétation elliptique : $\overline{A} = A + \pi$ avec $\pi \in E[2]$. Alors $-2\overline{A} = -2A$ est le point d'intersection des tangentes en A et $\overline{A}$.

Etant donné un point A de E, il existe trois points de E pouvant être le correspondant de A pour une certaine cubique S : en effet si on considère P le point d'intersection de la tangente en A avec E, ces trois points sont les points d'intersection (différents de A et P) de la conique polaire en P par rapport à E (voir figure 5.4).

FIG. 5.4 – Trois choix pour S



Etant donnée une cubique E, il existe donc génériquement trois cubiques S telles que $E = \mathrm{H(S)}$. En effet une cubique et sa hessienne ont mêmes points d'inflexion, ce qui équivaut à 8 conditions indépendantes sur les coefficients de S. On peut donc écrire $S = E + \lambda \mathrm{H(E)}$. On a alors trois déterminations de λ qui expriment la condition que la polaire en A par rapport à S est la tangente en un des trois points correspondants possibles. Dans le cas lisse, ceci correspond au choix d'un élément non nul de $E[2]$.

Proposition 5.19
Soit E une cubique et p, p' deux points de E dont les tangentes à E sont concourantes en un point de E. Alors il existe une unique cubique S telle que $E = \mathrm{H}(S)$ et $p' = \overline{p}$ pour le réseau $< S_x, S_y, S_z >$.

Remarque :
A isomorphisme près toute cubique lisse peut s'écrire $S : x^3+y^3+z^3+6mxyz = 0$. Sous cette forme $\mathrm{H}(S) : m^2(x^3 + y^3 + z^3) - (1 + 2m^3)xyz = 0$.

5.2.4 Réseau de coniques et quartique plane

Soit C une quartique plane lisse définie par $V^2 - UW = 0$ où U, V, W sont des coniques. C étant lisse $U \cap V \cap W = \emptyset$.

On considère le réseau $\mathcal{S} =< U, V, W >$ et le système

$$\mathcal{Q} = \{Q(\lambda) = \lambda^2 U + 2\lambda V + W\,, \lambda \in \mathbb{P}^1\} \subset \mathcal{S}.$$

On pose $E = \mathrm{J}(\mathcal{S})$. Le déterminant d'une matrice générique de $\mathcal{Q}$ étant un polynôme de degré 6 en λ, il existe 6 valeurs $\lambda_1, \ldots, \lambda_6$ distinctes pour lesquelles les coniques $Q(\lambda_i) = x_i u_i$ sont scindées. Les points $q_i = (x_i) \cap (u_i)$ sont des points de E (d'après la remarque suivant le théorème 5.10).

Lemme 5.20
Il existe une cubique S telle que :

– $E = \mathrm{H}(S)$.
– $< S_x, S_y, S_z >= \mathcal{S}$.
– $u_i^* = \overline{x_i^*}$ *sur la cayleyenne de* S.

Démonstration :
Soit F la cayleyenne du système $\mathcal{S}$. Par définition de F, les 12 points x_i^*, u_i^* sont sur F. Le couplage x_1^*, u_1^* définit une involution sur F qui permet d'associer à q_1 un point correspondant : il s'agit de l'unique point q de E tel que les tangentes en q_1 et en q soient concourantes en un point de E et tel que $(q_1 q)^*$ soit le point d'intersection résiduelle de $(x_1^* u_1^*)$ avec F. Cette involution définit alors de manière unique la courbe S d'après la proposition 5.19. Vérifions que $< S_x, S_y, S_z >= \mathcal{S}$. Par définition de l'involution, la conique polaire en $\overline{q_i} = (a_i : b_i : c_i)$ par rapport à S est $a_i S_x + b_i S_y + c_i S_z$ mais c'est aussi $x_i u_i = \lambda_i^2 U + 2\lambda_i V + W$. On peut donc exprimer U, V, W en fonction de S_x, S_y, S_z puisque la matrice

$$\begin{pmatrix} \lambda_1^2 & 2\lambda_1 & 1 \\ \lambda_2^2 & 2\lambda_2 & 1 \\ \lambda_3^2 & 2\lambda_3 & 1 \end{pmatrix}$$

est inversible. Enfin, d'après la proposition 5.12, on a aussi $E = \mathrm{H}(S)$.

Lemme 5.21
Il existe une conique $\overline{Q}$ *telle que, quelque soit* $p \in C$, *la droite* $xS_x(p)+yS_y(p)+zS_z(p) = 0$ *est tangente à* $\overline{Q}$.

Démonstration :
Soit P la matrice inversible telle que ${}^t(U, V, W) = P\ {}^t(S_x, S_y, S_z)$. Si $p \in C$, on a $U^2(p) - V(p)W(p) = 0$ soit si on pose

$$M = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 1 & 0 \\ -2 & 0 & 0 \end{pmatrix}$$

la relation $(U(p), V(p), W(p))\ M^{-1}\ {}^t(U(p), V(p), W(p)) = 0$ d'où

$$(S_x(p), S_y(p), S_z(p))\ {}^t P M^{-1} P\ {}^t(S_x(p), S_y(p), S_z(p)) = 0.$$

Cette relation montre que la droite $(S_x(p) : S_y(p) : S_z(p))^*$ est tangente à la conique $\overline{Q}$ dont la matrice hessienne est $P^{-1} M\ {}^t P^{-1}$.

Corollaire 5.22
La quartique C *est l'enveloppe des coniques polaires par rapport à* S *à la conique* $\overline{Q}$.

Démonstration :
Reprenons les notations de la démonstration précédente et effectuons le changement de coordonnées par la matrice P. On suppose les objets donnés dans cette base. On a alors en particulier $S_x = U, S_y = V, S_z = W$ et $\overline{Q} : y^2 - 4xz = 0$. Soit $p = (\mu^2 : 2\mu : 1)$ avec

$\mu \in \mathbb{P}^1$ un point de $\overline{Q}$. La conique polaire par rapport à S en p est $\mu^2 S_x + 2\mu S_y + S_z = \mu^2 U + 2\mu V + W = Q(\mu)$. Or l'enveloppe de cette famille de coniques est le discriminant en λ de $Q(\lambda)$ c'est-à-dire la courbe $V^2 - UW = 0$. C'est la courbe C.

Remarque :
Cette construction est l'analogue en degré double de la construction des coniques comme enveloppe de droites. Par exemple, lorsque les coordonnées sont arbitraires, l'enveloppe des coniques polaires par rapport à S à la conique

$$\overline{Q} = ax^2 + by^2 + cz^2 + 2fyz + 2gxz + 2hxy = 0$$

est donnée par le même type de formule (cf. [Sal69, p.260]) c'est-à-dire

$$(bc-f^2)S_x^2+(ca-g^2)S_y^2+(ab-h^2)S_z^2+2(gh-af)S_yS_z+2(hf-bg)S_xS_z+2(fg-ch)S_xS_y = 0.$$

Les points de contact de l'enveloppe avec C sont les points d'intersection de

$$\begin{cases} \lambda U + V = 0 \\ \lambda V + W = 0 \end{cases}$$

Les 6 points d'intersection de $\overline{Q}$ avec E sont connus : en effet si q est l'un de ces points, sa conique polaire est de la forme $Q(\lambda)$ et elle est scindée donc $q = \overline{q_i}$ pour une valeur de i.

5.3 Application aux courbes de genre 3

On reprend les notations de Lehavi introduites dans le paragraphe 5.1.

5.3.1 De (C, α) à (E, Q, π)

Soit C une courbe de genre 3 non hyperelliptique et $\alpha \in \mathrm{Jac}(C)[2] \setminus \{0\}$. On considère alors le groupe de α dont on note les éléments $([\sqrt{x_i}], [\sqrt{u_i}])$ pour $i = 1 \dots 6$. Relativement à ce groupe, on peut donc écrire C sous la modèle de Riemann (cf. corollaire 3.44) $\sqrt{x_1u_1} + \sqrt{x_2u_2} + \sqrt{x_3u_3} = 0$ soit encore par exemple

$$C : V^2 - UW = 0$$

avec $U = 2x_1u_1$, $W = 2x_2u_2$ et $V = x_3u_3 - x_1u_1 - x_2u_2$.

On peut facilement identifier les points de Σ : ils correspondent aux thêta caractéristiques impaires ϵ telles que $\epsilon + \alpha$ est encore impaire. Ce sont donc exactement les paires du groupe de α. On peut noter $p_i^* = x_i^*$ et $\overline{p_i}^* = u_i^*$. On a alors, d'après la proposition 5.7 :

Lemme 5.23
F est l'unique cubique de $(\mathbb{P}^2)^*$ passant par les points x_i^* et u_i^*.

D'autre part, si on considère $\mathcal{S} =< U, V, W >$ et

$$\mathcal{Q} = \{Q(\lambda) = \lambda^2 U + 2\lambda V + W, \lambda \in \mathbb{P}^1\} \subset \mathcal{S}$$

nous avons vu lors de la construction du système d'Aronhold (cf. paragraphe 3.5) que les six $Q(\lambda)$ qui sont des coniques scindées correspondent exactement aux $x_i u_i$. La cayleyenne de $\mathcal{S}$ étant le lieu des droites des coniques scindées on obtient :

Proposition 5.24
La cubique F est la cayleyenne du réseau $\mathcal{S}$.

Notons $q_i = (x_i) \cap (u_i)$, $i = 1 \dots 6$. L'involution de F, $i : p_i^* \mapsto \overline{p_i}^*$, définit un point d'ordre 2, π^*, et E est réalisée dans $\mathbb{P}^2$ comme l'intersection de p_i et $\overline{p_i}$ d'après la proposition 5.7. Mais c'est également par définition le cas pour la jacobienne du réseau $\mathcal{S}$. D'où :

Proposition 5.25
La cubique E est la jacobienne du réseau $\mathcal{S}$.

Q est facilement identifiée : c'est l'unique conique passant par les q_i. Quant à π, c'est le point de E qui définit l'involution duale de celle de F. Pour le déterminer, on procède comme suit : soit l^* le point d'intersection résiduel de $(p_1^* \overline{p_1}^*)$. Alors $\overline{q_1}$ est l'unique point de $l \cap E$ tel que les tangentes à E en $\overline{q_1}$ et en q_1 soient concourantes en un point de E (corollaire 5.18). On pose $\pi = q_1 - \overline{q_1}$.

5.3.2 De (E, Q, π) à (C, α)

Soit $(q_i)_{i=1\dots6}$ les six points d'intersection de E et Q et $\pi = q - q'$. On considère S l'unique cubique telle que $E = \mathrm{H}(S)$ et telle que la polaire par rapport à S en q soit la tangente à E en q' (proposition 5.19). Rappelons que l'on peut construire S explicitement en exprimant $S = E + \lambda \mathrm{H}(E)$ et en utilisant la condition de tangence pour déterminer λ. S détermine alors une involution $\bar{}$ sur E pour laquelle $q' = \overline{q}$. On construit les points $\overline{q_i}$.

Lemme 5.26
Il existe une conique $\overline{Q}$ telle que $\{\overline{q_i}\} = E \cap \overline{Q}$.

Démonstration :
En effet les q_i étant les points d'intersection de E et de Q on a $\sum q_i = 2K_{\mathbb{P}^2|E}$. Alors $\sum \overline{q_i} = \sum (q_i + \pi) = \sum q_i + 6\pi = \sum q_i = 2K_{\mathbb{P}^2|E}$.

Théorème 5.27
C est isomorphe à la quartique obtenue comme enveloppe des coniques polaires par rapport à S en les points de la conique $\overline{Q}$. Si $x_i u_i$ est la conique polaire en $\overline{q_i}$ par rapport à S on a $\alpha = \frac{1}{2}((x_i \cdot C) - (u_i \cdot C))$.

Démonstration :
Soit C' la courbe enveloppe et on fixe les coordonnées telles que $\overline{Q} : y^2 = 4xz$. On a alors $C' : S_y^2 = S_x S_z$ d'après le corollaire 5.22. On note $\alpha' = \frac{1}{2}((x_i \cdot C') - (u_i \cdot C'))$. Comme dans la construction 5.3.1 on associe alors à C' le réseau $\mathcal{S}' =< S_x, S_y, S_z >$ et le système $\mathcal{Q}' = \{Q(\lambda) = \lambda^2 S_x + 2\lambda S_y + S_z\}$. La jacobienne du réseau $\mathcal{S}'$ est E. Les coniques scindées de la famille $\mathcal{Q}'$ sont les coniques polaires par rapport à S en des points de E de la forme $(\lambda^2 : 2\lambda : 1)$. Ce sont donc les points d'intersection de E et $\overline{Q}$. Elles se coupent aux points q_i et définissent une conique $Q' = Q$ et un point d'ordre 2, $\pi' = \pi$. La configuration plane associée à (C', α') par la construction 5.3.1 est donc la même que pour (C, α). L'équivalence du théorème 5.8 montre que C' est isomorphe à C.

5.3.3 De $(C, \mathcal{L})$ à $(C', \mathcal{L}')$

Soit $\mathcal{L}$ un sous-groupe isotrope maximal. On considère alors une base symplectique (e_i, f_i) de $\mathrm{Jac}(C)[2]$ telle que $\mathcal{L} =< e_1, e_2, e_3 >$ avec $\mathcal{L}_1 =< e_1 >$ et $\mathcal{L}_2 =< e_1, e_2 >$.
On se donne également un système d'Aronhold (β_i) ayant pour caractéristiques

$$[\sqrt{\beta_1}] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad [\sqrt{\beta_2}] = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad [\sqrt{\beta_3}] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad [\sqrt{\beta_4}] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$
$$[\sqrt{\beta_5}] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad [\sqrt{\beta_6}] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad [\sqrt{\beta_7}] = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

On a alors $[e_1] = [\sqrt{\beta_1}] + [\sqrt{\beta_2}] + [\sqrt{\beta_3}]$, $[e_2] = [\sqrt{\beta_1}] + [\sqrt{\beta_4}] + [\sqrt{\beta_5}]$ et $[e_3] = [\sqrt{\beta_3}] + [\sqrt{\beta_5}] + [\sqrt{\beta_7}]$.
On pose

$$\begin{array}{llllll} (x_1) = \beta_1 & (x_2) = \beta_2 & (x_3) = \beta_3 & (x_4) = \beta_{45} & (x_5) = \beta_{46} & (x_6) = \beta_{47} \\ (u_1) = \beta_{23} & (u_2) = \beta_{13} & (u_3) = \beta_{12} & (u_4) = \beta_{67} & (u_5) = \beta_{57} & (u_6) = \beta_{56} \end{array}$$

et on suppose C définie par $\sqrt{x_1 u_1} + \sqrt{x_2 u_2} + \sqrt{x_3 u_3} = 0$. Les constructions précédentes et les propriétés du théorème 5.9 permettent de construire $(C', \mathcal{L}')$ comme suit :

Théorème 5.28

1. *Construire (E, Q, π) et les points $q_i = (x_i) \cap (u_i)$ comme au paragraphe 5.3.1.*
2. *Construire t le point d'intersection résiduel de (q_1, q_4) avec E.*
3. *Construire l'unique cubique E' qui passe par t et qui est tangente à (tq_i) en q_i pour $i = 2, 3, 5, 6$.*
4. *Soit Q' la conique passant par*
   - *les deux autres points d'intersection (en dehors de t) de (tq_1) avec E'. On appelle ces deux points q'_1, q'_4.*
   - *Les quatre points d'intersection de la conique polaire en t par rapport à E (en dehors de t). Ces points sont les points de ramification de τ. Ils sont appariés par l'involution. On les note q'_2, q'_3, q'_5, q'_7 de telle sorte que q'_3 et q'_7 soient correspondants.*

5. *E' ayant pour tangente en q_i, $i = 2, 3, 5, 6$, la droite (tq_i), le choix de deux de ces points définit une involution sur E'. On pose $\pi' = q_3 - q_5$.*
6. *C' est la quartique donnée par (E', Q', π') suivant le paragraphe 5.3.2.*
7. *Le sous-groupe isotrope maximal $\mathcal{L}' =< f_1, f_2, f_3 >$ de $\mathrm{Jac}(C')[2]$ tel que $\mathrm{Jac}(C) \simeq \mathrm{Jac}(C')/\mathcal{L}'$ peut être décrit par (on note $'$ les objets construits au paragraphe 5.3.2 et associés à (E', Q', π'))*
   - $f_3 = \frac{1}{2}((x'_i) \cdot C' - (u'_i) \cdot C')$ *pour tout i.*
   - $f_2 = \frac{1}{2}((x'_1) \cdot C' - (x'_4) \cdot C')$.
   - $f_1 = \frac{1}{2}((x'_3) \cdot C' - (u'_5) \cdot C')$.

L'algorithme décrit ci-dessus a été implanté en MAGMA version 2.9 sur $\overline{\mathbb{Q}}$.

Exemple :
Considérons par exemple la quartique définie sur $\mathbb{Q}$ par les six paramètres (cf. paragraphe 3.6)

$$\alpha_1 = \frac{5}{2},\ \alpha_2 = 2,\ \alpha_3 = -3,\ \alpha'_1 = -2,\ \alpha'_2 = 4,\ \alpha'_3 = -\frac{3}{4}.$$

On a $C : \sqrt{x_1 u_1} + \sqrt{x_2 u_2} + \sqrt{x_3 u_3} = 0$ avec

$$\begin{array}{ll} x_1 = x & u_1 = -605/56x + 45/28y + 565/56z \\ x_2 = y & u_2 = 171/28x - 59/14y - 159/28z \\ x_3 = z & u_3 = 207/56x + 45/28y - 303/56z \end{array}$$

Les calculs s'effectuent dans des extensions quadratiques de $\mathbb{Q}$ puis on obtient pour C' l'équation suivante (temps de calcul : 1.78 seconde)

$$\begin{aligned} C' \ : \ & x^4 + 187935030487874734346386 96/254843509821260096281985 97x^3y + \\ & 308478552338965912320941 2/254843509821260096281985 97x^3z + \\ & 262062516821192303326040 9672/252295074723047495319166 1103x^2y^2 + \\ & 726359258775202331881787224/102786882294574905500401007 9x^2yz - \\ & 102540172984710789089921466 22/925081940651174149503609 0711x^2z^2 + \\ & 298358857944743264314933609 6/277524582195352244851082721 33xz^3 - \\ & 522456846039332759089542916 64/277524582195352244851082721 33xy^2z - \\ & 144671717380155653417022408 904/277524582195352244851082721 33xyz^2 - \\ & 248253800614584539600593544 68/925081940651174149503609 0711xz^3 + \\ & 572757570343831549194704848/277524582195352244851082721 33y^4 - \\ & 864444609946446337815485737 6/277524582195352244851082721 33y^3z + \\ & 314978377998818538562115222 96/277524582195352244851082721 33y^2z^2 + \\ & 105386280868424402920031709 592/277524582195352244851082721 33yz^3 + \\ & 745473082725557161845314439 97/277524582195352244851082721 33z^4 = 0 \end{aligned}$$

Remarque :
Bien qu'élégante, cette méthode nous semble difficile à mettre en œuvre de manière itérative pour deux raisons :
Premièrement l'itération de cette construction demande la détermination sur C' de bitangentes relatives à un élément de $\mathrm{Jac}(C')[2]/\mathcal{L}'$. Les bitangentes qu'on obtient facilement par la construction précédente sont des bitangentes relatives à $f_3 \in \mathcal{L}'$. En effet, si on écrit

$$\begin{aligned}[f_3] &= \beta'_2 + \beta'_{57} \\ &= \beta'_5 + \beta'_{27} \\ &= \beta'_7 + \beta'_{25} \\ &= \beta'_{13} + \beta'_{46} \\ &= \beta'_{14} + \beta'_{36} \\ &= \beta'_{16} + \beta'_{34}\end{aligned}$$

ces bitangentes correspondent aux bitangentes x'_i et u'_i (par exemple $x'_1 = \beta'_{16}$). On trouve le groupe correspondant à $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ en considérant les coniques scindées de

$$\left(\lambda\sqrt{\beta'_2\beta'_{13}} + \sqrt{\beta'_{57}\beta'_{46}}\right)^2 = 0.$$

L'itération de l'A.G.M. demande alors la détermination de $\beta'_2, \beta'_{13}, \beta'_{57}$ et β'_{46}. Or même lorsque la courbe C possède toute ses bitangentes définies sur $\mathbb{Q}$, la détermination de ces nouvelles bitangentes doit s'effectuer dans des extensions quadratiques diverses. Les calculs deviennent donc assez rapidement pénibles.
Le deuxième problème semble plus profond : en effet si on réduit modulo p les deux courbes C et C', elles n'ont pas toujours le même nombre de points sur $\mathbb{F}_p$ mais seulement sur $\mathbb{F}_{p^2}$. Leurs jacobiennes ne sont donc pas isogènes sur $\mathbb{Q}$ mais uniquement sur une extension de $\mathbb{Q}$. Un tel phénomène est effectivement possible. C'est une illustration du résultat suivant de Serre [Ser01] qui découle d'une version précise du théorème de Torelli :

Théorème 5.29
Soit C_1 une courbe non hyperelliptique sur un corps fini k_1 et k une sous-extension de k_1. On suppose que la jacobienne principalement polarisée de C_1, (J_1, a_1), admet une k-structure c'est-à-dire qu'il existe un couple (J, a) où J est une variété abélienne sur k munie d'une polarisation a définie sur k et un isomorphisme de (J_1, a_1) avec $(J, a)/k_1$. Il existe alors une k-structure C sur C_1 compatible avec sa k_1-structure et un homomorphisme $\varepsilon : \mathrm{Gal}(k_1/k) \to \{\pm 1\}$ tel que la jacobienne de C soit isomorphe à la tordue de (J, a) par la torsion galoisienne relative à ε.

Conclusion

Nous présentons ici quelques sujets de réflexion autour de la thématique de l'A.G.M. :

1. En genre 1, l'A.G.M. permet non seulement d'obtenir le nombre de points de la courbe mais également de déterminer l'invariant j du relèvement canonique (et donc ce dernier). Dans notre cas, il est fort possible d'obtenir un résultat semblable, à partir des équations définissant l'espace des modules. En particulier, les formules permettant de relier les thêta constantes aux moduli α_i, α'_i (paragraphe 3.6) sont présentes chez Weber, et pourraient certainement conduire à la construction d'une «courbe canonique», point de départ pour des travaux similaires à ceux d'A. Weng sur les courbes CM hyperelliptiques (cf. [Wen01]).
2. Nous envisageons un certain nombre d'améliorations possibles pour l'algorithme que nous proposons. Il serait par exemple agréable d'avoir une condition de rationnalité sur les points de 4-torsion, visible sur la rationnalité des thêta constantes (cf. l'exemple du paragraphe 4.2.3). Plus déterminante serait l'obtention du polynôme caractéristique de la courbe sans utiliser LLL. Nous avons vu dans le cas du genre 1 (paragraphe 2.1.3) que l'on peut déterminer, sur les modèles de Mumford, une différentielle invariante pour laquelle le rapport des thêta constantes intervient naturellement. En dimension supérieure, l'action sur une base de ces différentielles pourrait fournir tout le polynôme caractéristique. Nous n'avons pu trouver trace dans la littérature de telles expressions. Une autre piste en genre 3 non hyperelliptique consiste peut-être à analyser l'action des formules de duplication non pas sur les thêta constantes mais sur la valeur en 0 des dérivées des fonctions thêta caractéristiques impaires, ces dernières étant naturellement reliées aux différentielles.
3. D'autres idées de l'analyse complexe attendent encore leur utilisation dans le cadre p-adique. Signalons par exemple le cas des fonctions thêta de Schottky (cf. [RF74, chap.VI]) introduites dans l'étude des revêtements doubles non ramifiés. Lors «d'expériences informatiques», nous avons pu tester leur pertinence pour le calcul du polynôme caractéristique d'un tel revêtement.
4. La confrontation des points de vue géométrique (évoqué au chapitre 5) et analytique sera certainement très profitable. En particulier, on peut espérer comprendre la loi de groupe sur la jacobienne d'une courbe de genre 3 par des opérations sur la conique et la cubique qui lui sont associées par l'équivalence 5.8. En contrepartie, l'utilisation des techniques développées dans les chapitre 4 et 5 permet de simplifier certaines constructions de Lehavi.

5. Les méthodes A.G.M. ne se limitent pas au cadre 2-adique. Il serait par exemple intéressant de les étendre aux cas d'autres corps résiduels, travaux entrepris dans le cas du genre 1 par D. Kohel et R. Carls. Enfin, en revenant aux sources de l'inspiration A.G.M. (le cas réel), l'algorithme proposé ici permettrait le calcul d'une matrice de Riemann d'une courbe de genre 3 non hyperelliptique avec une convergence quadratique, calcul utile entre autres dans la théorie des équations différentielles de type KdV.

Bibliographie

[Alb66] H.H Alberstam & K.F. Roth, *Sequences*, **Vol. 1**, Oxford, (1966).

[BM89] J.-B. Bost & J.-F. Mestre, Moyenne Arithmético-géométrique et Périodes des courbes de genre 1 et 2, Gaz. Math., S.M.F. **38** (1989) , 36-64.

[CS00] L. Caporaso & E. Sernesi : Recovering plane curves from their bitangents, `http://arxiv.org/abs/math.AG/0008239`, (2000).

[Car02] R. Carls : Approximation of canonical lifts, in preparation, (2002) disponible sur `http://www.math.leidenuniv.nl/~carls/`.

[Cas86] J.W.S. Cassels : *Local fields*, London Math. Soc. Student texts **3**, (1986).

[Cha86] C.-L. Chai : Siegel moduli schemes and their compactification over $\mathbb{C}$, dans *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag. (1986).

[Coh93] H. Cohen : *A course in Computational Algebraic Number Theory*, **138**, Springer-Verlag, (1993).

[Cox84] D. Cox, The arithmetic-geometric mean of Gauss, Enseign. Math. **30** (1984), 275-330.

[Deb99] O. Debarre : *tores et variétés abéliennes complexes*, Cours spécialisés **6**, collection SMF, (1999).

[Del69] P. Deligne : variétés abéliennes ordinaires sur un corps fini, Inv. math. **8**, (1969), 238-243.

[Deu41] M. Deuring, Die Typen der Multiplikatoringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ Hamburg **14** (1941), 197-272.

[Don92] R. Donagi : the fibers of the Prym map, Cont. Math. **136**, (1992), 55-125.

[Fay73] J.D. Fay : *Theta Functions on Riemann Surfaces*, Lecture Notes in Math. **352**, Springer-Verlag, (1973).

[FGH00] M. Fouquet, P. Gaudry & R. Harley : an extension of Satoh's algorithm and its implementation, J. Ramanujan Math. Soc. (2000).

[GH00] P. Gaudry & R. Harley : counting points on hyperelliptic curves over finite fields, ANTS-IV (W. Bosma,ed.) Lecture notes in comput. sci., **1838**, Springer-Verlag, (2000), 313-332.

[GH01] P. Gaudry & R. Harley : records disponibles sur `http://www.xent.com/~harley/Records.html`.

[Gau70] C.F. Gauss : *Werke*, Vol. **12**, Göttingen, (1870-1927).

[Gon98] J. González : on the p-rak of an abelian variety ant its endomorphism algebra, Publicacions Mate. **42**, (1998), 119-130.

[GH78] P. A. Griffiths & J. Harris : *Principles of algebraic geometry*, New York NY ; Chichester ; Brisbane : J. Wiley, (1978).

[GH01] B.H. Gross & J. Harris : On some geometric constructions related to theta characteristics, prépublication disponible sur `http://abel.math.harvard.edu/~gross/preprints/` (2001).

[Har75] R. Hartshorne : *Algebraic geometry*, Providence RI : American Mathematical Society (1975).

[HM89] G, Henniart & J.-F. Mestre : moyenne arithmético-géométrique p-adique, C. R. Acad. Sci. Paris, t. **308**, Série I (1989), 391-395.

[Hup67] B. Huppert : *Endliche Gruppen I*, Springer-Verlag, (1967).

[Igu72] J.-I. Igusa : *Theta functions*, die Grundlehren der mathematischen Wissenschaften, **194**, Springer Verlag, (1972).

[Lag67] J.L. Lagrange : *Oeuvres*, Vol. **14**, Gauthiers-Villars, Paris (1867-1892).

[Lan70] S. Lang : *Algebraic Number Theory*, Reading, Mass, Addison-Wesley Pub (1970).

[Lau02] A.-G.-B Lauder and D. Wan : Counting points on varieties over finite fields of small characteristic, prépublication disponible sur `http://web.comlab.ox.ac.uk/oucl/work/alan.lauder/` (2002).

[Leh02] D. Lehavi : *Bitangents and two level structure for curves of genus* 3, thèse disponible sur `http://www.ma.huji.ac.il/~dlehavi/` (2002).

[LL02] R. Lercier & D. Lubicz : Calcul du nombre de points d'une courbe elliptique définie sur $F_{2^{100002}}$, disponible sur `http://www.medicis.polytechnique.fr/~lercier/` (2002).

[LL03] R. Lercier & D. Lubicz : Cardinalité d'une courbe hyperelliptique de genre 2 sur $F_{2^{32770}}$, disponible sur `http://www.medicis.polytechnique.fr/~lercier/` (2003).

[LST64] J. Lubin & J.-P. Serre & J. Tate, *Elliptic Curves and formal groups*, notes disponibles sur `http://ma.utexas.edu/users/voloch/lst.html`, (1964).

[Mes72] W. Messing : *The crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes*, Lect. Notes in Math., **264**, Berin-Heidelberg-New-York, Springer (1972).

[Mes00] J.-F. Mestre : lettre à Gaudry et Harley, disponible sur `http://www.institut.math.jussieu.fr/`, (2000).

[Mes02] J.-F. Mestre : Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, disponible sur `www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps` (2002).

[Mil86] J.S. Milne : Abelian varieties, dans *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag (1986).

[Mum66] D. Mumford : On the equations defining abelian varieties. I, Invent. Math. **1**, (1966), 287-354.

[Mum71] D. Mumford : Theta characteristics of an algebraic curve, Ann. Sci. École Norm. Sup. **4**, (1971), 181-192.

[Mum74] D. Mumford : Prym varieties. I, contributions to analysis (a collection of papers dedicated to Lipman Bers), Academic Press, New York, (1974), 325-350.

[Mum83] D. Mumford : *Tata Lectures on Theta*, Vol **1,2**, Birkhäuser, (1983).

[Oor97] F. Oort : canonical liftings and dense sets of CM-points, Arithmetic Geometry (Cortona, 1994), Sympos. Math., XXXVII, Cambridge Univ. Press, Cambridge, (1997), 228-234.

[RF74] H.E. Rauch & H.M. Farkas, *Theta functions with applications to Riemann surfaces* Baltimore MD : Williams & Wilkins, (1974).

[Rie98] B. Riemann : sur la théorie des fonctions abéliennes, Oeuvres de Riemann, deuxième édition, p. 487, (1898).

[Rit03] C. Ritzenthaler : Méthode A.G.M. pour les courbes ordinaires de genre 3 non hyperelliptiques sur F_{2^N}, prépublication, `http://arXiv.org/abs/math.NT/0303072` (2003).

[Ros86] M. Rosen : Abelian varieties over $\mathbb{C}$, dans *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[Sal69] G. Salmon : *A treatise on conic sections*, sixième édition, Chelsea, (1869).

[Sal79] G. Salmon : *A treatise on the higher plane curves*, troisième édition, Chelsea, (1879).

[Sat00] T. Satoh : the canonical lift of an ordinary elliptic curve over a finite field and its point counting, J. Ramanujan Math. Soc. **15**, (2000), 247-270.

[Sch95] R. Schoof : Counting points on elliptic curves over finite fields, J. théorie des nombres Bordeaux **7**, (1995), 219-254.

[Ser01] : J.-P. Serre : lettre à K. Lauter, 8 février 1998, citée dans Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, J. of Algebraic Geometry 10 (2001), 19-36.

[Ser58] J.-P. Serre, sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., Mexico City, (1958), 24-53 (ou *Oeuvres* **1**, 501-530).

[Shi98] G. Shimura : *Abelian varieties with complex multiplication and modular functions*, Princ. Univ. Press, NJ, (1998).

[Sil92] J.H Silverman : *The Arithmetic of Elliptic Curves*, **106**, Springer, (1992).

[Sil94] J.H Silverman : *Advanced topics in the arithmetic of elliptic curves* Springer-Verlag, **94**, (1994).

[Sin38] J. Singer : a theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc., **43**, (1938), 377-385.

[SV87] K.-0. Stöhr & J.-F. Voloch : A formula for the Cartier operator on plane algebraic Curves, J. für die Reine und Ang. Math., **377**, (1987), 49-64.

[VPV01] F. Vercauteren, B. Preneel, J. Vandewalle : A memory efficient version of Satoh's algorithm, Adv. in Cryptology, Eurocrypt (2001) (Innsbruck, Austria, Mai 2001), Lect. Notes in Comput. Sci. **2045**, 1-13, ed. Pfitzmann, Berlin, Heidelberg : Springer-Verlag (2001).

[Wal95] C.T.C Wall : Quartic curves in characteristic 2, Math. Proc. Cambridge Phil. Soc. **117**, (1995), 393-414.

[Web76] H. Weber : *Theorie der abelschen Functionen vom Geschlecht 3*, (1876).

[Wen01] A. Weng : hyperelliptic CM-curves of genus 3, Journal of the Ramanujan Math. Soc. **16**, (2001), 339-372.

Index

– **S** –

– **T** –

– **V** –