Moyenne arithmético-géométrique, suites de Borchardt et applications

Version “rapporteurs”

11 janvier 2006

Changelog

Version "rapporteurs" du 11 décembre 2005

- L'introduction a été remaniée.
- Des remarques de Guillaume Hanrot sur le Chapitre 1 ont été prises en compte (en particulier, la Proposition 1.1 a été ajoutée).
- Des remarques de François Morain ont été prises en compte.

Version du 28 décembre 2005

- Une discussion a été ajoutée au début du Chapitre 8.
- Une Section 8.3 a été ajoutée.
- Une (courte) conclusion a été ajoutée.
- Les commentaires de John Boxall sur la version du 15 décembre ont été pris en compte.

Version du 15 décembre 2005

- Une introduction a été ajoutée.
- Un index a été ajouté.
- Mise en page pour D_2 et D_3.
- Manque (*a priori*) surtout la conclusion.

Version du 14 décembre 2005

- Manquent intro et conclusion.
- Au Chapitre 10, D_2 et D_3 sont à réécrire.
- Le début de 3.3 a été changé, ainsi que 3.3.3.
- Un nouveau dessin (Figure 9.1) a été ajouté.
- Certaines formules du Chapitre 8 ont été réécrites (factorisation des signes, ...).

Version du 9 décembre 2005

- L'introduction et la conclusion restent à rédiger.
- Le titre est encore provisoire.
- Certaines formules mathématiques sont à réécrire (factorisation par les signes au Chapitre 8, donnée de D_2 et D_3 au Chapitre 10).

Version du 31 octobre 2005

- Les premières versions des chapitres 1 à 8 sont terminées.
- Ajout de plusieurs propositions au Chapitre 4.

Version du 20 octobre 2005

- Les chapitres dont la première version est terminées sont les chapitres 1, 2, 3, 5, 6 et 7.
- Le chapitre 4 n'a pas changé depuis la version précédente : reste la section 4.4 a terminer.

Version du 14 octobre 2005

- Une grande partie du chapitre 4 est terminée (reste 4.4 à écrire).
- Le chapitre 5 est terminé.
- Quelques typos corrigées dans les chapitres 2 et 3.

Version du 28 septembre 2005

Les premiers jets des chapitres 1, 2, 3 et 7 sont terminés (et donc *a priori* lisibles).

Table des matières

Introduction **13**

1 Approximations et évaluation de fonctions **17**
1.1 Approximations et opérations élémentaires 17
1.1.1 Définitions 17
1.1.2 Opérations élémentaires et perte de précision 19
1.2 Évaluation de fonctions et perte de précision 22
1.2.1 Fonctions finiment décomposables 23
1.2.2 Fonctions itérées 26
1.3 Complexité de l'évaluation de fonctions élémentaires, itérations de Newton 28
1.3.1 Itérations de Newton 29

I Le genre 1 **37**

2 Formes et fonctions modulaires en genre 1, theta constantes **39**
2.1 Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré 39
2.1.1 Définitions et notations 39
2.1.2 Le domaine fondamental $\mathcal{F}$ 40
2.1.3 Polygones élémentaires et sous-groupes du groupe modulaire elliptique . . 42
2.2 Formes et fonctions modulaires en genre 1 47
2.2.1 Définitions 47
2.2.2 Les theta constantes 48
2.2.3 La fonction η de Dedekind 56
2.2.4 Construction de fonctions modulaires 57
2.2.5 Quelques résultats sur les fonctions modulaires 61
2.3 Polynômes modulaires 62
2.3.1 Définition 62
2.3.2 Polynômes modulaires pour $\Gamma^0(p)$ 62

3 Moyenne arithmético-géométrique et relation avec les theta constantes **67**
3.1 AGM sur les réels positifs 67
3.1.1 Définition 67
3.1.2 Historique 68
3.2 Définition de l'AGM sur les nombres complexes 69
3.3 Sur les limites des suites AGM 70
3.3.1 Schéma de la démonstration 71
3.3.2 Preuve détaillée 73
3.3.3 Le résultat de Gauss et les démonstrations de Cox et Geppert 76

3.3.4 Quelques remarques sur les suites AGM associées à des theta constantes . 79
3.4 Une fonction associée à l'AGM . . . 81
3.4.1 Définition . . . 81
3.4.2 Complexité de l'évaluation . . . 81
3.5 Évaluation du logarithme complexe . . . 87
3.5.1 Bornes explicites pour l'évaluation du logarithme *via* l'AGM . . . 87
3.5.2 Algorithmes . . . 92

4 Algorithmes d'évaluation de fonctions modulaires 95
4.1 Algorithme naïf . . . 95
4.2 Utilisation de l'AGM . . . 98
4.2.1 Principe général . . . 98
4.2.2 Un premier algorithme . . . 104
4.2.3 Variante et amélioration de la complexité . . . 106
4.2.4 Évaluation de k *via* l'égalité de Jacobi . . . 107
4.3 Évaluation d'autres fonctions modulaires . . . 108
4.3.1 Utilisation de polynômes modulaires . . . 108
4.3.2 Évaluation de la fonction η de Dedekind . . . 109
4.4 Applications . . . 109
4.4.1 Calcul de polynômes de classes . . . 110
4.4.2 Calcul de polynômes modulaires . . . 112
4.5 Résultats expérimentaux . . . 114
4.5.1 Précision nécessaire à l'initialisation des itérations de Newton . . . 114
4.5.2 Temps de calcul . . . 114

II Le genre 2 et au-delà 119

5 Theta constantes en genre supérieur 121
5.1 Définitions . . . 121
5.2 Le groupe symplectique $\mathrm{Sp}(2g, \mathbb{Z})$ et son action sur $\mathcal{H}_g$ . . . 122
5.2.1 Définition . . . 122
5.2.2 Le domaine fondamental $\mathcal{F}_g$ . . . 124
5.3 Les theta constantes comme formes modulaires . . . 125
5.4 Formules de duplication . . . 127

6 Le cas du genre 2 131
6.1 Le groupe Γ_2 et le domaine fondamental $\mathcal{F}_2$ . . . 131
6.1.1 Le groupe Γ_2 . . . 131
6.1.2 Le domaine fondamental $\mathcal{F}_2$ . . . 131
6.2 Theta constantes en genre 2 . . . 136
6.2.1 Valeurs des theta constantes sur le domaine fondamental $\mathcal{F}_2$ . . . 136
6.3 Action de Γ_2 sur les carrés des theta constantes . . . 143
6.3.1 Formules de transformation des theta constantes sous l'action de Γ_2 . . . 143
6.3.2 Les quotients de carrés de theta constantes comme fonctions modulaires de Siegel . . . 146
6.3.3 Invariants d'Igusa . . . 148
6.4 Équations modulaires . . . 149

7 Suites de Borchardt : définition et convergence 153
7.1 Définitions . . . 153
7.1.1 Historique . . . 154
7.2 Convergence . . . 154
7.3 Quelques remarques . . . 162
7.4 Une fonction associée à la moyenne de Borchardt . . . 163
7.4.1 Définition . . . 163
7.4.2 Évaluation . . . 164

8 Limites des suites de Borchardt de quatre éléments 167
8.1 Schéma de la démonstration . . . 168
8.2 Preuve détaillée . . . 170
8.2.1 Non-vacuité des ensembles T_n . . . 170
8.2.2 Le domaine fondamental $\mathcal{F}_b$ . . . 171
8.2.3 Limite de la suite $(\lambda(\tau_n))_{n\in\mathbb{N}}$ . . . 173
8.2.4 Conclusion de la démonstration . . . 179
8.3 Quelques remarques . . . 184
8.3.1 Généralisation au genre supérieur . . . 184
8.3.2 Domaine fondamental adapté à la fonction B_2 . . . 184

9 Matrices de Riemann de courbes hyperelliptiques 185
9.1 Courbes hyperelliptiques sur $\mathbb{C}$ . . . 185
9.1.1 Matrice de Riemann associée à une courbe hyperelliptique . . . 185
9.1.2 Les formules de Thomae . . . 189
9.2 Calcul de matrices de Riemann . . . 190
9.2.1 Méthodes utilisant l'intégration numérique . . . 191
9.2.2 L'algorithme de Richelot . . . 192
9.2.3 Méthode utilisant la moyenne de Borchardt . . . 192
9.2.4 Méthode de Mestre . . . 200
9.3 Résultats expérimentaux . . . 201

10 Évaluation des theta constantes en genre 2 207
10.1 Méthode naïve . . . 207
10.2 Méthode utilisant la moyenne de Borchardt et des itérations de Newton . . . 210
10.3 Résultats expérimentaux . . . 214
10.4 Applications . . . 215
10.4.1 Calcul de polynômes de classes . . . 215
10.4.2 Calcul de polynômes modulaires . . . 217

Conclusion 229

Bibliographie 230

Index 239

Table des figures

1.1 Arbre représentant la fonction $\phi : (y, z) \mapsto \sqrt{y + \frac{1}{z^2+3}}$ 24
1.2 Arbre représentant la fonction $z \mapsto z^k$ 26
1.3 Arbres représentant la fonction g 28

2.1 Pavage de $\mathcal{H}$ par les images du domaine fondamental $\mathcal{F}$ 44
2.2 Le domaine fondamental $\mathcal{F}_{k'}$ pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$ 58

3.1 Points de l'ensemble $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$ 70
3.2 Inverses des points de l'ensemble $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$ 71
3.3 Une itération AGM correspondant à un bon choix de racine 83

4.1 Précision initiale minimale nécessaire à l'Algorithme 7 en $\tau = 0.25 + y \cdot i$ 114
4.2 Temps de calcul pour l'évaluation de $k'(0.123456789 + 1.23456789 \cdot i)$ à faible précision 115
4.3 Temps de calcul pour l'évaluation de $k'(0.123456789 + 1.23456789 \cdot i)$ à haute précision 116
4.4 Temps de calcul pour 20 multiplications (fonction `mpc_mul`) 117
4.5 Ratio entre le temps de calcul de l'Algorithme 7 et $20\,\mathtt{M}(N)\log N$ 118

9.1 Construction de la surface de Riemann associée à $\mathcal{C} : y^2 = \prod_{j=1}^{6}(x - a_j)$ 187
9.2 Surface de Riemann associée à la courbe $y^2 = f(x)$: un tore à $g = 2$ trous 188
9.3 Une base du premier groupe d'homologie sur un tore à deux trous 188
9.4 Base canonique d'homologie associée aux formules de Thomae 190
9.5 Temps de calcul l'évaluation d'une matrice de Riemann associée à la courbe $\mathcal{C}$ . . 202
9.6 Ratio entre le temps de calcul des Algorithmes 12 et 14 et $(20\,\mathtt{M}(N)\log N)$ 203
9.7 Temps de calcul de la fonction `AnalyticJacobian` de MAGMA pour la courbe $\mathcal{C}$. 204
9.8 Ratio entre le temps de calcul de `AnalyticJacobian` et $20\,\mathcal{M}(N)N$ 205

10.1 Temps de calcul pour l'évaluation de $(b_j(\tau))$ par les Algorithmes 15 et 16 215
10.2 Ratio entre le temps de calcul de l' Algorithme 15 et $\frac{N}{100}\,\mathtt{M}(N)$ 216
10.3 Temps de calcul pour l'évaluation de $(b_j(\tau))$ par l'Algorithme 16 à haute précision 217
10.4 Ratio entre le temps de calcul de l' Algorithme 16 et $100\,\mathtt{M}(N)\log N$ 218

Liste des Algorithmes

1 Réduction dans l'ensemble fondamental $\mathcal{F}'$ 42
2 Domaine fondamental et générateurs pour un sous-groupe de Γ_1 46
3 Évaluation de la fonction M 86
4 Évaluation de π 93
5 Évaluation naïve des theta constantes 97
6 Évaluation naïve des theta constantes 98
7 Évaluation de k' *via* l'AGM et des itérations de Newton 105
8 Évaluation de k' (variante) 108
9 Réduction d'une matrice symétrique réelle au sens de Minkowski 133
10 Réduction dans le domaine fondamental $\mathcal{F}_2$ 134
11 Évaluation de la moyenne de Borchardt B_g 165
12 Évaluation des $b_j(\tau)$ associés à une courbe 194
13 Calcul de $\tau \in \mathcal{F}_2$ à partir des $b_j(\tau)$ 196
14 Calcul de $\tau \in \mathcal{F}_2$ à partir de $(b_1(\tau), b_2(\tau), b_3(\tau))$ 197
15 Évaluation "naïve" des theta constantes θ_j $(j \in [0, 3])$ 209
16 Évaluation des $(b_j)_{j\in[1,3]}$ par itérations de Newton 213

Introduction

L'idée d'utiliser des courbes elliptiques [Mil87, Kob87] puis hyperelliptiques [Kob89] en cryptologie a donné un nouvel intérêt à certaines questions concernant ces courbes en théorie algorithmique des nombres, comme le calcul de la cardinalités de leurs jacobiennes sur les corps finis ou la construction de telles courbes par multiplication complexe effective par exemple.

En ce qui concerne les courbes elliptiques, un certain nombre d'algorithmes efficaces sont aujourd'hui connus pour résoudre ces deux problèmes [BSS05, Chapter VI], [BS04, Eng05a, EM02]. On notera que l'algorithme le plus rapide connu actuellement pour calculer la cardinalité d'une courbe elliptique sur un corps fini premier, l'algorithme de Schoof–Elkies–Atkin (SEA) [Sch95, Elk98, Atk92], [BSS99, Chapter VII], nécessite (ceci peut être vu comme un précalcul) la connaissance de polynômes modulaires ; et que la principale étape de la construction de courbes par multiplication complexe est le calcul de polynômes de classe de Hilbert. Ces deux types de polynômes sont liés aux fonctions modulaires, et leur calcul peut se faire rapidement par des techniques d'évaluation/interpolation [Eng05a, Eng05b], nécessitant des algorithmes rapides d'évaluation numérique de fonctions modulaires. Ce problème a été la première motivation de nos travaux de thèse. Pour y apporter une solution, nous avons considéré la moyenne arithmético-géométrique (AGM).

Cette construction, découverte dès 1784 par Lagrange [Lag67] puis redécouverte par Gauss en 1791 (il n'était alors agé que de treize ans !), qui l'étudiera largement par la suite [Gau01], et par Legendre [Leg28] en 1825, présente en effet le double avantage d'être intimement liée à certaines fonctions modulaires et de converger très rapidement (quadratiquement). Historiquement, l'AGM sur les réels positifs a tout d'abord été utilisée pour évaluer efficacement des intégrales elliptiques. Le lien entre l'AGM et les fonctions modulaires (*via* les theta constantes) a été établi par Gauss lorsqu'il s'est intéressé à l'AGM sur les nombres complexes. En particulier, étant donné un nombre complexe z, Gauss savait comment (en utilisant l'AGM) déterminer $\tau \in \mathcal{H}$ tel que $z = k'(\tau)$, ce qui revient à inverser la fonction modulaire k'. Pour plus de détails, nous renvoyons à l'article de Cox [Cox84], qui donne un aperçu très complet de l'historique de l'AGM. Les travaux de Gauss sur l'AGM et sur les fonctions elliptiques n'ont malheureusement pas été publiés de son vivant (il semble qu'il en ait abandonné l'idée lorsque Abel et Jacobi ont publié leurs travaux sur la théorie des fonctions elliptiques), mais seulement entre 1868 et 1927 [Gau27]. Peu après cette publication, quelques articles [Gep28, vD28] ont été consacrés à l'AGM, démontrant des résultats entrevus par Gauss.

Il semble que l'AGM ait ensuite été peu étudiée, jusqu'à ce qu'en 1972, Salamin [BGS72] propose des algorithmes utilisant l'AGM pour le calcul de π et l'évaluation rapide de la fonction logarithme. L'AGM connaît alors un certain regain d'intérêt, et plusieurs articles [Bre76, Sal76, BB84] décrivent et étudient des algorithmes utilisant l'AGM pour le calcul de π et l'évaluation du logarithme. En 1987, Jonathan et Peter Borwein [BB87] publient un livre complet sur les relations entre l'AGM et π. L'intérêt principal de l'AGM en algorithmique est que la moyenne arithmético-géométrique de deux nombres s'évalue rapidement, notamment du fait de la convergence *quadratique* des suites associées.

On notera que l'AGM a récemment connu un regain d'intérêt en théorie algorithmique des nombres, depuis que Jean-François Mestre [Mes00, Mes02] a proposé un algorithme de comptage de points sur les courbes elliptiques en caractéristique 2 utilisant l'AGM (plus précisément, le fait que l'AGM s'interprète comme une 2-isogénie entre courbes elliptiques [BM88]).

Notre première idée a été d'utiliser des itérations de Newton pour, à partir de la fonction déjà considérée par Gauss permettant d'"inverser" la fonction modulaire k', obtenir un algorithme pour l'évaluation numérique de cette dernière. Il s'agit donc de combiner deux algorithmes particulièrement efficaces (l'AGM et les itérations de Newton convergent tous deux quadratiquement), l'algorithme obtenu étant quasi-optimal. On en déduit alors facilement des algorithmes rapides pour l'évaluation de nombre de fonctions modulaires, mais aussi des theta constantes. L'un des problèmes de ce type d'algorithmes est que l'on manipule des nombres réels et complexes, qui en pratique sont représentés de façon *finie*. Très vite se posent donc des problèmes de précision et d'approximation : nous avons donc dû fixer un cadre théorique à nos travaux, définissant bien ces notions ; et étudier relativement en détail les phénomènes de *perte de précision* qui peuvent survenir au cours des calculs. Nous avons alors pu étudier de façon précise la complexité de nos algorithmes, obtenant des résultats théoriques qui ont ensuite été validés par une implantation soignée en langage C (implantation utilisée par Andreas Enge [Eng05a] pour calculer des polynômes de classe de degré jamais encore atteint).

La plupart des autres travaux exposés dans ce mémoire ont été déclenchés par la suggestion faite par Pierrick Gaudry de chercher à généraliser ce type d'idées au genre 2. En effet, des polynômes de classe et polynômes modulaires peuvent être définis en genre 2, les premiers étant utilisés pour la multiplication complexe effective, les seconds pouvant peut-être (beaucoup de travail reste à faire) être utilisés pour généraliser l'algorithme SEA au genre 2. Comme dans le cas du genre 1, ces polynômes peuvent être calculés par évaluation/interpolation (on consultera les travaux de Weng [Wen01, Wen03] en ce qui concerne le calcul de polynômes de classe), ce qui nécessite des algorithmes rapides pour l'évaluation numérique des fonctions modulaires en genre 2. Une première piste pour concevoir de tels algorithmes, généralisant ceux que nous avons obtenus dans le cas du genre 1, a été de considérer l'algorithme de Richelot [BM88, Ric36], permettant l'évaluation rapide d'intégrales hyperelliptiques (en genre 2). Malheureusement, cet algorithme s'applique naturellement pour des courbes données par des équations de la forme $y^2 = f(x)$, le polynôme f étant de degré 6 *à racines réelles*. Nous nous sommes alors intéressé à des suites introduites par Carl-Wilhelm Borchardt [Bor76, Bor78] en 1858, que nous appelons donc *suites de Borchardt*. Ces suites peuvent être vues comme une généralisation de l'AGM en ce sens qu'elles sont liées aux theta constantes en genre 2 de la même façon que l'AGM l'est en genre 1 : les formules qui définissent les suites de Borchardt sont les formules de duplication des theta constantes. Borchardt s'intéressait en fait au départ à des équations différentielles associées à ces suites, qui généralisent là encore ce qui se passe avec l'AGM ; ce n'est qu'assez tardivement que les travaux de Weierstrass lui ont permis de faire le lien avec les theta constantes. Il semble que Borchardt se soit limité à l'étude des suites de Borchardt sur les réels positifs. Comme en ce qui concerne l'AGM, de nombreux problèmes surviennent lorsque l'on considère ces suites sur les nombres complexes, principalement du fait que leur définition fait intervenir des racines carrées, qui ne sont alors plus uniquement déterminées. Nous avons donc commencé par étudier les propriétés des suites de Borchardt sur les complexes : nous avons montré que toutes ces suites convergent —et même qu'elles convergent *quadratiquement* en général, ce qui fait leur intérêt algorithmique—, avons donné un critère permettant de déterminer quand la limite associée est nulle ou non, et avons prouvé que dans tous les cas où la limite est non nulle, la convergence est quadratique.

Nous avons ensuite utilisé le lien entre les suites de Borchardt et les theta constantes pour concevoir un algorithme permettant, à partir de certains invariants associés à une courbe hy-

perelliptique, de calculer rapidement une matrice de Riemann associée à cette courbe. Cet algorithme peut être vu comme une généralisation de la méthode utilisée par Gauss pour définir $\tau \in \mathcal{H}$ à partir de la valeur de $k'(\tau)$.

L'étape suivante a été, en genre 2, d'inverser formellement cet algorithme *via* des itérations de Newton pour obtenir un algorithme rapide d'évaluation de certaines fonctions modulaires (et des theta constantes).

Nous avons implanté ces algorithmes (en langage C), afin de vérifier expérimentalement les études de complexité que nous en avons fait. Afin d'illustrer l'intérêt de ces algorithmes, nous avons ensuite utilisé ces implantations pour calculer explicitement des polynômes modulaires (en genre 2) par évaluation et interpolation.

Enfin, nous nous sommes intéressé à un problème plus théorique, qui est celui de la détermination des limites possibles de suites de Borchardt. Dans le cas de l'AGM, si l'on fixe deux nombres complexes a et b et que l'on considère l'ensemble des limites de toutes les suites AGM initialisées par (a, b), il a été montré [Gep28, vD28, Cox84] que cet ensemble peut être déterminé explicitement (en particulier, les inverses des points de cet ensemble sont sur un réseau...). Nous avons généralisé ce résultat au cas du genre 2, en déterminant explicitement l'ensemble des limites de toutes les suites de Borchardt de quatre éléments initialisées en un quadruplet fixé de nombres complexes. On notera que les inverses des éléments de cet ensemble ne sont en général *pas* situés sur un réseau.

Plan

Ce mémoire comporte 10 chapitres, organisés en un chapitre isolé et deux parties.

Le premier chapitre (isolé donc) aborde des notions de représentation de nombres, d'approximation, de précision et de perte de précision. Nous y abordons aussi certains algorithmes bien connus, comme les itérations de Newton, que nous utilisons dans les chapitres suivants.

La première partie, consacrée exclusivement au genre 1, se décompose en trois chapitres. Le Chapitre 2 rappelle un certain nombre de propriétés des theta constantes et des fonctions modulaires en genre 1, en en donnant dans la plupart des cas des démonstrations complètes (en général classiques). Le Chapitre 3 est consacré à la moyenne arithmético-géométrique. Plusieurs résultats classiques concernant l'AGM sur les nombres complexes y sont prouvés (résultats de convergence, limites possibles), parfois par des méthodes originales (Section 3.3). On y étudie aussi la complexité de l'évaluation de l'AGM (Section 3.4.2) et l'utilisation de l'AGM pour la détermination du logarithme complexe (Section 3.5), sujets pour lesquels nous n'avons pas trouvé de référence précise dans la littérature. Le Chapitre 4 aborde l'utilisation de l'AGM et des itérations de Newton pour l'évaluation rapide de fonctions modulaires, et a fait l'objet d'un article [Dup05].

La seconde partie est consacrée principalement au genre 2, mais certains résultats sont valides en genre quelconque. Le Chapitre 5 donne un certains nombres de propriétés des theta constantes en genre quelconque (ainsi que leurs démonstrations). Le Chapitre 6 traite plus particulièrement des theta constantes en genre 2 ; y sont démontrés quelques lemmes techniques qui seront utilisés dans les chapitres suivants. Le Chapitre 7 est relativement indépendant, nous y définissons les suites de Borchardt, et démontrons leurs propriétés de convergence sur les complexes, que nous n'avons pas trouvées dans la littérature. Dans le Chapitre 8, nous étudions les limites des suites de Borchardt de quatre éléments associées à des carrés de theta constantes et démontrons le Théorème 8.1, qui généralise en partie les résultats de la Section 3.3. Dans le Chapitre 9, nous montrons comment les suites de Borchardt peuvent être utilisées pour évaluer rapidement une matrice de Riemann associée à une courbe hyperelliptique en genre quelconque. Enfin, le Chapitre 10 traite de l'utilisation de l'évaluation des theta constantes en genre 2. En particulier, nous y présentons un algorithme original utilisant les suites de Borchardt et les

itérations de Newton pour ce faire. À titre d'application, nous décrivons comment l'utilisation de cet algorithme nous a permis de calculer explicitement des polynômes modulaires en genre 2.

Chapitre 1

Approximations et évaluation de fonctions

Nous l'avons vu en introduction, une grande partie de ce mémoire est consacrée (directement ou indirectement) à l'étude d'algorithmes d'*évaluation de fonctions*. Typiquement, les fonctions auxquelles nous nous intéresserons sont des fonctions de variables complexes et à valeurs complexes. Se pose donc un problème de *représentation* des nombres complexes.

Le but de ce chapitre liminaire est de définir les représentations que nous avons choisi de manipuler (et que les programmes que nous avons écrits manipulent effectivement), ainsi que les notions d'approximation et de précision auxquelles nous nous intéressons. Nous nous pencherons aussi sur les phénomènes de *perte de précision* qui peuvent survenir lorsque l'on effectue des opérations élémentaires (typiquement des opérations arithmétiques, mais aussi l'extraction de racine carrée) sur des approximations. Enfin, nous donnerons la complexité d'algorithmes permettant d'effectuer ces opérations élémentaires : ces algorithmes, pour la plupart bien connues, sont en quelque sorte les briques de bases que nous utiliserons par la suite.

1.1 Approximations et opérations élémentaires

1.1.1 Définitions

Définition 1.1 (N-représentation d'un nombre) *Soit $z \in \mathbb{C} \setminus \{0\}$, alors en considérant le développement en binaire des parties réelle et imaginaire de z, on montre qu'il existe $E \in \mathbb{Z}$, $S_R, S_I \in \{0,1\}$ et $(R_n)_{n\geqslant 1}, (I_n)_{n\geqslant 1} \in \{0,1\}^{\mathbb{N}\setminus\{0\}}$ tels que $R_1 = 1$ ou $I_1 = 1$, qu'aucune des suites $(R_n)_{n\in\mathbb{N}}$ et $(I_n)_{n\in\mathbb{N}}$ ne converge vers 1, et que*

$$z = 2^E \left((-1)^{S_R} \sum_{n\geqslant 1} \frac{R_n}{2^n} + (-1)^{S_I} i \sum_{n\geqslant 1} \frac{I_n}{2^n} \right).$$

Pour $N \geqslant 0$, on définit la N-représentation de z, *notée* $\mathrm{Rep}_N(z)$, *par*

$$\mathrm{Rep}_N(z) = 2^E \left((-1)^{S_R} \sum_{n=1}^{N+2} \frac{R_n}{2^n} + (-1)^{S_I} i \sum_{n=1}^{N+2} \frac{I_n}{2^n} \right),$$

ainsi que l'ensemble $\mathcal{R}(N)$ des nombres N-représentables *:*

$$\mathcal{R}(N) = \{ z \in \mathbb{C} \setminus \{0\} : z = \mathrm{Rep}_N(z) \}.$$

Enfin, on dit qu'un nombre est finiment représentable *s'il appartient à l'ensemble*

$$\bigcup_{N\geqslant 0} \mathcal{R}(N).$$

L'intérêt de la notion de nombres finiment représentables est qu'un tel nombre peut être manipulé par un ordinateur : on code alors un élément $z \in \mathcal{R}(N)$ par les séquences $(R_n)_{n\in[1,N+2]}$ et $(I_n)_{n\in[1,N+2]}$ associées (que l'on appelle *mantisses*), les bits de signe S_I et S_R, et l'exposant E.

Lorsque, par la suite, nous analyserons des algorithmes opérant sur des représentations finies, nous supposerons toujours que les exposants des représentations manipulées sont tels que

$$|\log|E|| = O(N),$$

ce qui nous permettra d'utiliser comme unique paramètre pour les études de complexité la précision N (le nombre de bits nécessaire pour stocker un élément de $\mathcal{R}(N)$ étant alors en $O(N)$).

Bien sûr, le problème qui va se poser à nous est celui du traitement de nombres qui ne sont pas finiment représentables, que nous devrons nous restreindre à approcher par des nombres finiment représentables. Commençons par bien définir ce que nous appellerons par la suite une approximation :

Définition 1.2 (approximations en précision absolue et relative) *Soit $N \geqslant 0$ fixé.*

Soit $a \in \mathbb{C}\setminus\{0\}$, on dit que $\alpha \in \mathbb{C}$ est une approximation de a avec une précision absolue de N bits *si*

$$|a-\alpha| \leqslant \frac{1}{2^N},$$

et on dit que c'est une approximation de a avec une précision relative de N bits *si*

$$\left|\frac{a-\alpha}{a}\right| = \left|1-\frac{\alpha}{a}\right| \leqslant \frac{1}{2^N}.$$

Notons que pour tout $a \in \mathbb{C}\setminus\{0\}$ et pour tout $N \geqslant 0$, $\mathrm{Rep}_N(a)$ est une approximation de a avec une précision relative de N bits. En effet, si

$$a = 2^E\left((-1)^{S_R}\sum_{n\geqslant 1}\frac{R_n}{2^n} + (-1)^{S_I} i \sum_{n\geqslant 1}\frac{I_n}{2^n}\right),$$

où $E \in \mathbb{Z}$, $S_R, S_I \in \{0,1\}$, $(R_n)_{n\geqslant 1}, (I_n)_{n\geqslant 1} \in \{0,1\}^{\mathbb{N}\setminus\{0\}}$ et $R_1 = 1$ ou $I_1 = 1$, alors

$$2^{E-1} \leqslant |a| \leqslant 2^{E+1}$$

et

$$\begin{aligned}
\left|\frac{a-\mathrm{Rep}_N(a)}{a}\right| &= \frac{2^E}{|a|}\left|\sum_{n\geqslant 1}\frac{(-1)^{S_R}R_{n+N+2} + (-1)^{S_I}I_{n+N+2}i}{2^{n+N+2}}\right| \\
&\leqslant 2\sum_{n\geqslant 1}\frac{\left|(-1)^{S_R}R_{n+N+2} + (-1)^{S_I}I_{n+N+2}i\right|}{2^{n+N+2}} \\
&\leqslant \frac{1}{2^N}\sum_{n\geqslant 1}\frac{1}{2^n} \\
&\leqslant \frac{1}{2^N}.
\end{aligned}$$

C'est la raison pour laquelle on parle de N-représentations, bien que les mantisses soient codées sur $N+2$ bits.

1.1.2 Opérations élémentaires et perte de précision

Supposons que l'on se donne deux nombres complexes a et b de manière approchée par $\alpha = \mathrm{Rep}_N(a)$ et $\beta = \mathrm{Rep}_N(b)$, pour une certaine précision N, et que l'on souhaite calculer une approximation du produit ab. On peut naturellement calculer le produit $\alpha\beta$ de manière exacte (puisque $\alpha, \beta \in \mathcal{R}(N)$), mais ce n'est très certainement pas la façon la plus judicieuse de procéder. En effet, on a

$$\begin{aligned}\left|\frac{ab-\alpha\beta}{ab}\right| &= \left|\frac{a(b-\beta)+\beta(a-\alpha)}{ab}\right| \\ &\leqslant \left|\frac{b-\beta}{b}\right| + \left|\frac{\beta}{b}\right| \cdot \left|\frac{a-\alpha}{a}\right| \\ &\leqslant \left|\frac{b-\beta}{b}\right| + \left(1+\left|\frac{b-\beta}{b}\right|\right)\left|\frac{a-\alpha}{a}\right| \\ &\leqslant \left(2+\frac{1}{2^N}\right)\frac{1}{2^N},\end{aligned}$$

mais si l'on se contente de calculer $\mathrm{Rep}_N(\alpha\beta)$, alors

$$\left|\frac{\alpha\beta - \mathrm{Rep}_N(\alpha\beta)}{\alpha\beta}\right| \leqslant \frac{1}{2^N},$$

donc

$$\begin{aligned}\left|\frac{ab-\mathrm{Rep}_N(\alpha\beta)}{ab}\right| &\leqslant \left|\frac{ab-\alpha\beta}{ab}\right| + \left|\frac{\alpha\beta}{ab}\right| \cdot \left|\frac{\alpha\beta-\mathrm{Rep}_N(\alpha\beta)}{\alpha\beta}\right| \\ &\leqslant \left|\frac{ab-\alpha\beta}{ab}\right| + \left(1+\left|\frac{ab-\alpha\beta}{ab}\right|\right)\left|\frac{\alpha\beta-\mathrm{Rep}_N(\alpha\beta)}{\alpha\beta}\right| \\ &\leqslant \left(2+\frac{1}{2^N}\right)\frac{1}{2^N}.\end{aligned}$$

Comme le produit exact $\alpha\beta \in \mathcal{R}(2N+1)$ n'est pas en général une approximation de ab plus précise que $\mathrm{Rep}_N(\alpha\beta)$, il est préférable (pour des raisons de complexité) de calculer seulement $\mathrm{Rep}_N(\alpha\beta)$. Par ailleurs, ce calcul fait "perdre de la précision" : la meilleure approximation de ab que l'on puisse calculer en partant de α et β aura une précision relative plus faible que celle avec laquelle α et β approximaient a et b. En particulier, si l'on veut calculer une approximation de ab avec une précision relative de N bits, ce qui précède montre qu'il faut partir de $\mathrm{Rep}_{N+2}(a)$ et $\mathrm{Rep}_{N+2}(b)$, et calculer $\mathrm{Rep}_N\left(\mathrm{Rep}_{N+2}(a)\cdot\mathrm{Rep}_{N+2}(b)\right)$.

On dira que l'on *travaille à précision N (bits)* si l'on ne manipule que des éléments de $\mathcal{R}(N)$. Dans ce cadre, lorsque l'on doit effectuer une opération op sur des N-représentations $(\alpha_j)_{j\in J}$, on calcule en fait $\mathrm{Rep}_N\left(\mathrm{op}\left((\alpha_j)_{j\in J}\right)\right)$.

Dans ce qui suit, nous fixons $a, b \in \mathbb{C}\setminus\{0\}$, $A, B > 0$, $N \geqslant 0$ que l'on supposera grand devant $\log_2 A$ et $\log_2 B$, et $\alpha, \beta \in \mathcal{R}(N)$ tels que

$$\left|\frac{a-\alpha}{a}\right| \leqslant \frac{A}{2^N}$$

et

$$\left|\frac{b-\beta}{b}\right| \leqslant \frac{B}{2^N}.$$

Nous allons alors étudier, pour diverses opérations op, la précision relative avec laquelle $\mathrm{Rep}_N(\mathrm{op}(\alpha,\beta))$ approche $\mathrm{op}(\alpha,\beta)$. Notons que ceci est indépendant de la façon dont on calcule $\mathrm{Rep}_N(\mathrm{op}(\alpha,\beta))$, ou même de l'existence d'un algorithme pour effectuer ce calcul.

Nous nous restreignons à quatre opérations (la multiplication, l'inversion, l'addition, la soustraction et l'extraction de racine carrée), que nous appellerons dans la suite *opérations élémentaires*.

Cas de la multiplication

On note $p = \mathrm{Rep}_N(\alpha\beta)$, alors

$$\begin{aligned}\left|\frac{ab-p}{ab}\right| &\leqslant \left|\frac{ab-\alpha\beta}{ab}\right| + \left|\frac{\alpha\beta-p}{ab}\right| \\ &\leqslant \left|\frac{a(b-\beta)+\beta(a-\alpha)}{ab}\right| + \left|\frac{\alpha\beta}{ab}\right| \cdot \left|\frac{\alpha\beta-p}{\alpha\beta}\right| \\ &\leqslant \left|\frac{b-\beta}{b}\right| + \left|\frac{\beta}{b}\right| \cdot \left|\frac{a-\alpha}{a}\right| + \left|\frac{\alpha}{a}\right| \cdot \left|\frac{\beta}{b}\right| \cdot \left|\frac{\alpha\beta-p}{\alpha\beta}\right|,\end{aligned}$$

et en utilisant la majoration

$$\left|\frac{\alpha}{a}\right| \leqslant 1 + \left|\frac{a-\alpha}{a}\right|$$

(et de même pour $\left|\frac{\beta}{b}\right|$), on obtient finalement

$$\left|\frac{ab-p}{ab}\right| \leqslant \frac{1}{2^N}\left(A + B + \frac{AB}{2^N} + \left(1+\frac{A}{2^N}\right)\left(1+\frac{B}{2^N}\right)\right).$$

En supposant par exemple que $(A+B+3)^2 \leqslant 2^N$, on en déduit que

$$\left|\frac{ab-p}{ab}\right| \leqslant \frac{A+B+3}{2^N}.$$

Cas de l'inversion

On note $p = \mathrm{Rep}_N\left(\frac{1}{\alpha}\right)$, alors

$$\begin{aligned}\left|\frac{\frac{1}{a}-p}{\frac{1}{a}}\right| &\leqslant \left|\frac{\frac{1}{a}-\frac{1}{\alpha}}{\frac{1}{a}}\right| + \left|\frac{\frac{1}{\alpha}-p}{\frac{1}{a}}\right| \\ &\leqslant \left|\frac{a}{\alpha}\right| \cdot \left|\frac{a-\alpha}{a}\right| + \left|\frac{a}{\alpha}\right| \cdot \left|\frac{\frac{1}{\alpha}-p}{\frac{1}{\alpha}}\right| \\ &\leqslant \left(1+\left|\frac{a-\alpha}{a}\right|\right)\left(\left|\frac{a-\alpha}{a}\right| + \left|\frac{\frac{1}{\alpha}-p}{\frac{1}{\alpha}}\right|\right) \\ &\leqslant \left(1+\frac{A}{2^N}\right)\frac{A+1}{2^N},\end{aligned}$$

soit, en supposant que $A \leqslant 2^N$,

$$\left|\frac{\frac{1}{a}-p}{\frac{1}{a}}\right| \leqslant \frac{2A+2}{2^N}.$$

Cas de l'addition et de la soustraction

L'addition est l'opération élémentaire qui peut le plus poser problème, puisqu'elle peut faire perdre beaucoup de précision. S'en convaincre est facile : si $x = 1 + 2^{-(N+2)}$ et que $y = 1$, alors leurs N-approximations sont toutes les deux égales à 1, donc la différence de ces dernières est nulle, et toute la précision relative a été perdue. Notons cependant que l'addition se comporte beaucoup mieux vis-à-vis des approximations en précision *absolue*.

Fixons ici un entier $C \geqslant 0$ tel que

$$|a+b| \geqslant \frac{1}{2^C}\mathrm{Max}\left(|a|, |b|\right).$$

Par exemple, si les parties réelles et imaginaires de a et de b ont les même signes respectifs (ou plus généralement si a et b sont situés dans un même quart du plan complexe), alors on peut prendre $C = 0$.

En notant $p = \mathrm{Rep}_N(\alpha + \beta)$, on a

$$\begin{aligned}
\left|\frac{(a+b)-p}{a+b}\right| &\leqslant \left|\frac{(a+b)-(\alpha+\beta)}{a+b}\right| + \left|\frac{(\alpha+\beta)-p}{a+b}\right| \\
&\leqslant \left|\frac{(a+b)-(\alpha+\beta)}{a+b}\right| + \left|\frac{\alpha+\beta}{a+b}\right| \cdot \left|\frac{(\alpha+\beta)-p}{\alpha+\beta}\right| \\
&\leqslant \left|\frac{(a+b)-(\alpha+\beta)}{a+b}\right| + \left(1 + \left|\frac{(a+b)-(\alpha+\beta)}{a+b}\right|\right) \left|\frac{(\alpha+\beta)-p}{\alpha+\beta}\right|,
\end{aligned}$$

or

$$\begin{aligned}
\left|\frac{(a+b)-(\alpha+\beta)}{a+b}\right| &\leqslant \frac{1}{|a+b|}\left(|a-\alpha| + |b-\beta|\right) \\
&\leqslant \frac{|a|}{|a+b|}\left|\frac{a-\alpha}{a}\right| + \frac{|b|}{|a+b|}\left|\frac{b-\beta}{b}\right| \\
&\leqslant \frac{2^C(A+B)}{2^N},
\end{aligned}$$

donc on obtient finalement

$$\left|\frac{(a+b)-p}{a+b}\right| \leqslant \frac{1}{2^N}\left(2^C(A+B) + 1 + \frac{2^C(A+B)}{2^N}\right),$$

soit, en supposant que $2^C(A+B) \leqslant 2^N$,

$$\left|\frac{(a+b)-p}{a+b}\right| \leqslant \frac{2^C(A+B)+2}{2^N}.$$

On notera que le cas de la soustraction est tout à fait similaire.

Cas de l'extraction de racine carrée

Le calcul de racines carrées est particulièrement important lorsque l'on s'intéresse à la moyenne arithmético-géométrique, ou plus généralement aux moyennes de Borchardt, comme nous le verrons aux Chapitres 3 et 7.

Si l'on note $\sqrt{a}$ l'une des racines carrées de a, $\sqrt{\alpha}$ la racine de α la plus proche de $\sqrt{a}$ et $p = \mathrm{Rep}_N(\sqrt{\alpha})$, alors

$$\begin{aligned}
\left|\frac{\sqrt{a}-p}{\sqrt{a}}\right| &\leqslant \left|\frac{\sqrt{a}-\sqrt{\alpha}}{\sqrt{a}}\right| + \left|\frac{\sqrt{\alpha}}{\sqrt{a}}\right| \cdot \left|\frac{\sqrt{\alpha}-p}{\sqrt{\alpha}}\right| \\
&\leqslant \left|1 - \sqrt{\frac{\alpha}{a}}\right| + \left(1 + \left|1 - \sqrt{\frac{\alpha}{a}}\right|\right) \left|\frac{\sqrt{\alpha}-p}{\sqrt{\alpha}}\right|,
\end{aligned}$$

où $\sqrt{\frac{\alpha}{a}}$ désigne la racine carrée de $\frac{\alpha}{a}$ la plus proche de 1, que l'on peut aussi écrire

$$\sqrt{\frac{\alpha}{a}} = \sqrt{1 - \frac{a-\alpha}{a}}.$$

En considérant le développement de Taylor de la fonction $z \mapsto (1+z)^{\frac{1}{2}}$ au voisinage de zéro, on montre que pour tout $z \in \mathbb{C}$ tel que $|z| \leqslant \frac{1}{2}$, on a

$$\left|1 - \sqrt{1+z}\right| \leqslant |z|,$$

ce qui implique donc que

$$\left|1 - \sqrt{\frac{\alpha}{a}}\right| \leqslant \left|\frac{a-\alpha}{a}\right|,$$

et finalement que

$$\left|\frac{\sqrt{a} - p}{\sqrt{a}}\right| \leqslant \frac{1}{2^N}\left(A + 1 + \frac{A}{2^N}\right),$$

donc, si l'on suppose que $A \leqslant 2^N$, que

$$\left|\frac{\sqrt{a} - p}{\sqrt{a}}\right| \leqslant \frac{A+2}{2^N}.$$

1.2 Évaluation de fonctions et perte de précision

Nous considérons deux grands types de fonctions dans cette section. D'une part, les fonctions que nous appellerons *finiment décomposables*. Il s'agit de fonctions qui peuvent se décomposer en un nombre fini d'opérations élémentaires*. Par exemple, pour $k \geqslant 2$, la fonction $z \mapsto z^k$ est une fonction finiment décomposable. D'autre part, les fonctions que nous appellerons *itérées de fonctions finiment décomposables*, ou plus simplement *fonctions itérées*, qui sont définies comme suit :

Définition 1.3 (fonction itérée) *Soit $j \geqslant 1$, une fonction $f : U \to \mathbb{C}$ (où U est une partie de $\mathbb{C}^j$) est une* fonction itérée *si et seulement s'il existe*

- *$n \geqslant 1$;*
- *$\phi_1, \ldots, \phi_n : U \to \mathbb{C}$ des fonctions finiment décomposables ; et*
- *$g : V \to \mathbb{C}^n$ (où V est une partie de $\mathbb{C}^n$) une fonction finiment décomposable ;*

tels que, pour tout $z \in U$, si l'on pose

$$a^{(0)} = \left(a_1^{(0)}, \ldots, a_n^{(0)}\right) = (\phi_1(z), \ldots, \phi_n(z))$$

et

$$a^{(k+1)} = \left(a_1^{(k+1)}, \ldots, a_n^{(k+1)}\right) = g\left(a^{(k)}\right)$$

pour tout $k \geqslant 0$, alors

$$f(z) = \lim_{k \to +\infty} a_1^{(k)}.$$

*Dit autrement, les fonctions finiment décomposables de $x_1, \ldots, x_n$ forment la plus petite $\mathbb{C}$-algèbre contenant $\mathbb{C}(x_1, \ldots, x_n)$ et stable par racine carrée.

Par exemple, la fonction exponentielle est une fonction itérée : en reprenant les notations de la définition ci-dessus, on pose $n = 5$, $\phi_1(z) = \phi_2(z) = \phi_4(z) = 1$, $\phi_5(z) = 0$ et $\phi_3(z) = z$, puis

$$g(a, b, c, d, e) = \left(a + \frac{bc}{d(e+1)}, bc, c, d(e+1), e+1\right)$$

(qui est clairement finiment décomposable).

Pour $z \in \mathbb{C}$, si l'on pose

$$a^{(0)} = (\phi_1(z), \ldots, \phi_5(z)) = (1, 1, z, 1, 0),$$

alors une récurrence directe permet de montrer que, pour tout $k \geqslant 0$,

$$a^{(k)} = \left(\sum_{j=0}^{k} \frac{z^j}{j!}, z^k, z, k!, k\right).$$

En particulier, on a bien

$$\lim_{k \to +\infty} a_1^{(k)} = \exp(z).$$

1.2.1 Fonctions finiment décomposables

Soit f une fonction finiment décomposable, alors on peut représenter f par un arbre binaire dont les nœuds sont étiquetés par les opérations élémentaires, et dont les feuilles sont soit le ou les argument(s) de f, soit des constantes.

Par exemple, un arbre correspondant à la fonction $\phi : (y, z) \mapsto \sqrt{y + \frac{1}{z^2+3}}$ est donné en Figure 1.1.

On peut alors étiqueter récursivement les feuilles et les nœuds de l'arbre, en partant des feuilles, comme suit :

- les feuilles correspondant aux constantes finiment représentables sont étiquetées par 0 ;
- les feuilles correspondant aux autres constantes et aux variables sont étiquetées par 1 ;
- un nœud correspondant à une multiplication est étiqueté par $A + B + 3$, où A et B sont les entiers étiquetant ses deux fils ;
- un nœud correspondant à une inversion est étiqueté par $2A+2$, où A est l'entier étiquetant son fils ;
- un nœud correspondant à une addition (ou une soustraction) est étiqueté par $2^C(A+B)+2$, où A et B sont les entiers étiquetant ses deux fils, et où l'entier C est tel que, quels que soient les nombres x et y pouvant être sommés à ce nœud lors d'une 'evaluation de f, on ait
$$|x + y| \geqslant \frac{1}{2^C} \mathrm{Max}\left(|x|, |y|\right);$$
- un nœud correspondant à une racine carrée est étiqueté par $A + 2$, où A est l'entier étiquetant son fils.

L'étiquetage des nœuds correspondant à des additions ou soustractions pose souvent problème. On notera que l'on s'intéresse souvent à l'évaluation de fonctions sur des sous-ensembles de $\mathbb{C}$, ce qui peut simplifier les choses.

Par exemple, si l'on s'intéresse à l'évaluation de ϕ pour des couples (y, z) vérifiant $|y| \geqslant 1$ et $|z| \leqslant 1$, alors :

$$\left|z^2 + 3\right| \geqslant \frac{1}{2} \mathrm{Max}\left(3, \left|z^2\right|\right),$$

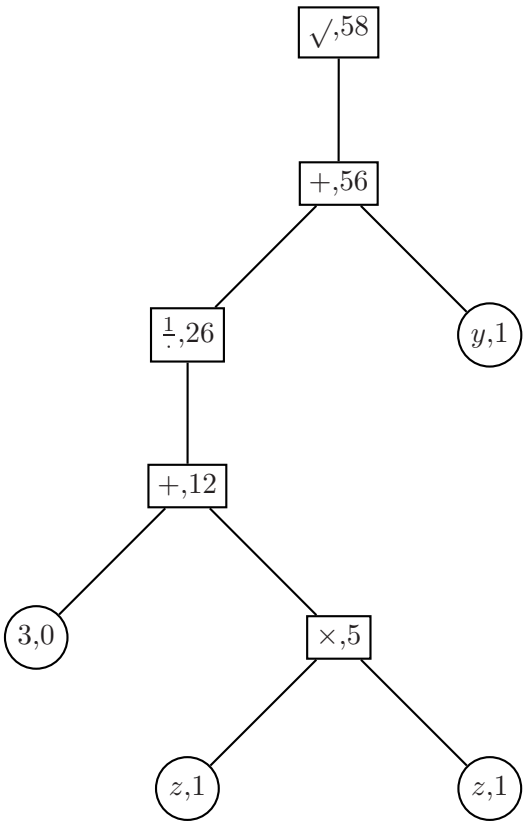

FIG. 1.1 – Arbre représentant la fonction $\phi : (y, z) \mapsto \sqrt{y + \frac{1}{z^2+3}}$

donc

$$\left|y+\frac{1}{z^2+3}\right| \geqslant |y| - \frac{1}{|z^2|+3} \geqslant |y| - \frac{1}{2} \geqslant \frac{1}{2}\mathrm{Max}\left(|y|, \left|\frac{1}{z^2+3}\right|\right).$$

En utilisant cette propriété, on voit que l'étiquetage par des entiers des feuilles et nœuds de l'arbre représenté à la Figure 1.1 correspond à la méthode d'étiquetage décrite plus haut.

On a alors le résultat suivant :

Proposition 1.1 *Soit X l'entier étiquetant la racine de l'arbre d'évaluation, et soit N un entier tel que*

$$X^2 \leqslant 2^N.$$

Si l'on part des N-représentations des constantes et des variables $(z_j)_{j\in J}$ correspondant aux feuilles de l'arbre et que l'on calcule, en travaillant à précision N et en suivant les chemins de l'arbre, une approximation $F \in \mathcal{R}(N)$ de $f((z_j)_{j\in J})$, on aura

$$\left|\frac{f((z_j)_{j\in J}) - F}{f((z_j)_{j\in J})}\right| \leqslant \frac{X}{2^N}.$$

Démonstration : Il s'agit d'une conséquence directe des résultats de la Section 1.1.2 et de l'algorithme utilisé pour étiqueter les nœuds et feuilles de l'arbre d'évaluation. □

En particulier, si l'on veut calculer une approximation de $f((z_j)_{j\in J})$ à précision relative N, il est suffisant de partir des M-représentations des z_j et des constantes intervenant dans f et de calculer une approximation en suivant les chemins de l'arbre et en travaillant toujours à précision M, où

$$M = N + \log_2 X.$$

On a ici implicitement supposé que M était assez grand pour que les constantes finiment représentables intervenant dans le calcul soient dans $\mathcal{R}(M)$. Si ce n'est pas le cas, on étiquette par 1 les feuilles de l'arbre correspondant à ces constantes, et l'on calcule comme plus haut l'entier étiquetant la racine.

Dans le cas de notre exemple, si l'on veut évaluer la fonction ϕ avec une précision relative de $N \geqslant 7$ bits, le raisonnement ci-dessus montre qu'en posant $M = N + \lceil \log_2 58 \rceil = N + 6$, en partant de $\mathrm{Rep}_M(y)$ et de $\mathrm{Rep}_M(z)$ et en travaillant toujours à précision M, on obtient finalement le résultat voulu.

Ce type d'étude peut rapidement devenir lourd pour des fonctions "compliquées", surtout du fait qu'il est nécessaire au préalable d'obtenir des bornes pour toutes les opérations d'addition pouvant survenir.

Nous traitons ci-dessous le cas (relativement simple) des fonctions puissance.

Fonctions puissance

Fixons un entier $k \geqslant 2$ et intéressons-nous à la fonction $z \mapsto z^k$. En raisonnant comme ci-dessus, on montre que l'arbre représenté à la Figure 1.2 est un arbre correspondant à l'évaluation de cette fonction, et que l'étiquetage de ses nœuds majore les pertes de précision pouvant affecter chaque résultat intermédiaire.

Pour calculer une approximation de z^k avec une précision relative de $N \geqslant 3 + \log_2 k$ bits, il suffit donc, en posant $M = N + 2 + \log_2 k$, de partir de $\mathrm{Rep}_M(z)$ et, en travaillant à précision M, d'effectuer les calculs correspondant aux branches de l'arbre. On obtient finalement un élément de $\mathcal{R}(M)$ qui est bien une approximation de z^k à précision relative N.

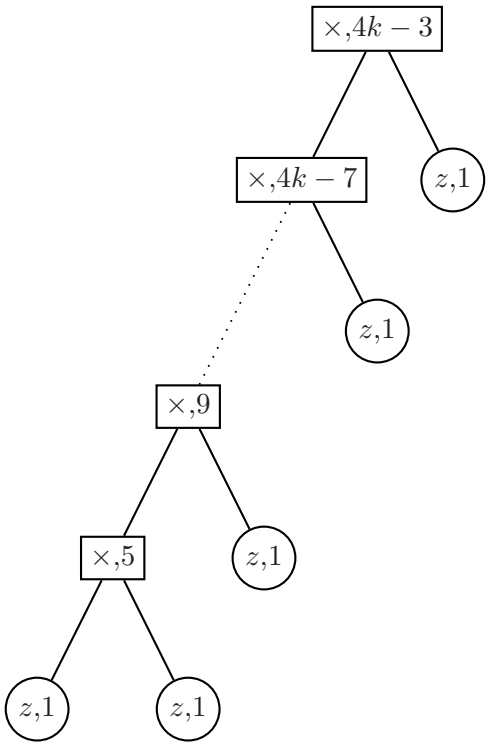

FIG. 1.2 – Arbre représentant la fonction $z \mapsto z^k$

1.2.2 Fonctions itérées

Dans cette section, on fixe f une fonction itérée, et l'on reprend les notations de la Définition 1.3.

Dans un premier temps, il convient de déterminer une fonction $B : \mathbb{N} \times U \to \mathbb{N}$ telle que, pour tous $N \in \mathbb{N}$ et $z \in U$, $a_1^{(B(N,z))}$ soit une approximation de $f(z)$ avec une précision relative de N bits.

On peut ensuite étudier (*via* par exemple une décomposition en arbre, comme dans la section précédente) les pertes de précision induites par la fonction g. Plus précisément, on tente de déterminer n fonctions $C_1, \ldots, C_n : \mathbb{N}^n \times V \to \mathbb{N}$ telles que, pour tous $N \in \mathbb{N}$ suffisamment grand, $z = (z_1, \ldots, z_n) \in V$, $A_1, \ldots, A_n \in \mathbb{N}$ et $Z = (Z_1, \ldots, Z_n) \in \mathcal{R}(N)^n$ tels que

$$\left| \frac{z_j - Z_j}{z_j} \right| \leqslant \frac{A_j}{2^N}$$

pour tout $j \in [1, n]$, si l'on note

$$(t_1, \ldots, t_n) = g(z)$$

et que $(T_1, \ldots, T_n) \in \mathcal{R}(N)^n$ désigne l'approximation de $g(z)$ obtenue en travaillant à précision N et en évaluant g *via* l'arbre la représentant à partir de Z, on ait

$$\left| \frac{t_j - T_j}{t_j} \right| \leqslant \frac{C_j(A_1, \ldots, A_n, z)}{2^N}$$

pour tout $j \in [1, n]$.

On peut alors, en utilisant ces fonctions C_j et en étudiant également, comme dans la section précédente, les fonctions ϕ_j, essayer de déterminer (typiquement par récurrence) une

fonction $C : \mathbb{N} \times U \to \mathbb{N}$ telle que $C(k, z)$ quantifie la perte de précision si l'on part de la $\mathrm{Rep}_N(z)$ et que l'on calcule $\alpha_k \in \mathcal{R}(N)$ approximant $a_1^{(k)}$ en travaillant toujours à précision N :

$$\left| \frac{a_1^{(k)} - \alpha_k}{a_1^{(k)}} \right| \leqslant \frac{C(k,z)}{2^N}.$$

Si l'on souhaite évaluer $f(z)$ avec une précision relative de N bits, on fixe alors

$$M = N + 2 + \lceil \log_2 C\left(B(N+2, z), z\right) \rceil,$$

et l'on calcule une $F \in \mathcal{R}(M)$ approximant $a_1^{(B(N+2,z))}$ en travaillant à précision M. D'après ce qui précède, on a alors

$$\left| \frac{a_1^{(B(N+2,z))} - F}{a_1^{(B(N+2,z))}} \right| \leqslant \frac{1}{2^{N+2}}$$

et

$$\left| \frac{f(z) - a_1^{(B(N+2,z))}}{f(z)} \right| \leqslant \frac{1}{2^{N+2}},$$

d'où l'on déduit finalement que

$$\left| \frac{f(z) - F}{f(z)} \right| \leqslant \frac{1}{2^N},$$

ce qui montre que F approche bien $f(z)$ avec la précision souhaitée.

Cette méthode exposée ici de façon relativement théorique s'avère fort pratique pour étudier en pratique la précision à laquelle doivent se faire les calculs si l'on souhaite évaluer une fonction avec une précision relative fixée. Nous illustrons ceci ci-dessous en traitant le cas de l'AGM.

Exemple : l'évaluation de l'AGM

La description relativement théorique qui précède est certainement plus compréhensible si elle est illustrée par un exemple. Nous allons donc traiter le cas de la fonction $M : \mathbb{C} \to \mathbb{C}$ (correspondant à la moyenne arithmético-géométrique, ou AGM, univariée), introduite à la Section 3.2. Plus précisément, nous allons reprendre, avec le formalisme introduit plus haut, le probléme de l'évaluation de $M(z)$ pour $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) \geqslant 0$.

En utilisant toujours les mêmes notations, on a alors $k = 1$, $n = 2$,

$$U = \{z \in \mathbb{C} : \mathrm{Re}(z) \geqslant 0\},$$

$V = U \times U$,

$$g : (a, b) \to \left(\frac{a+b}{2}, \sqrt{ab} \right)$$

(où l'on prend comme racine carrée celle ayant une partie réelle positive), ϕ_2 étant la fonction identité et ϕ_1 étant la fonction constante $z \mapsto 1$.

Nous montrerons (Propriété 3.3) qu'alors

$$B(N, z) = \mathrm{Max}\left(\lceil \log_2 |\log_2 |z|| \rceil, 1\right) + \lceil \log_2(N+2) \rceil + 2.$$

Par ailleurs, on peut représenter la fonction g par les arbres de la Figure 1.3, et on peut montrer que l'on peut alors prendre

$$C_1(A_1, A_2, z) = C_2(A_1, A_2, z) = A_1 + A_2 + 5.$$

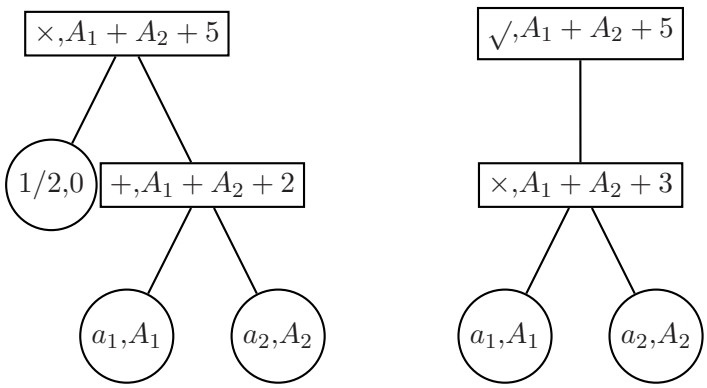

FIG. 1.3 – Arbres représentant la fonction g

Notons que l'on a utilisé le fait que pour toute addition entre deux opérandes x et y effectuée, x et y sont situés dans le même quart du plan complexe, donc

$$|x + y| \geqslant \mathrm{Max}\left(|x|, |y|\right).$$

On montre alors (par récurrence) que l'on peut prendre, pour $k \geqslant 4$,

$$C(k, z) = 3^k,$$

et l'on en déduit que, si l'on veut évaluer $M(z)$ avec une précision relative de N bits, il est suffisant de partir de $\mathrm{Rep}_M(z)$ et de travailler toujours à précision M, où

$$M = N + 2 + \lceil \log_2 C\left(B(N+2, z), z\right) \rceil = N + 2 + \lceil B(N+2, z) \log_2 3 \rceil.$$

1.3 Complexité de l'évaluation de fonctions élémentaires, itérations de Newton

L'objectif de cette section est de donner des résultats sur la complexité en temps de l'évaluation de certaines fonctions (et en particulier des opérations élémentaires). Pour cela, il est souvent nécessaire d'étudier relativement finement la gestion de la précision lors des calculs (donc les phénomènes de perte de précision), de façon a pouvoir garantir l'exactitude du résultat du calcul. Nous nous attacherons en particulier à montrer les classes de complexités pour l'évaluation de ces fonctions, en utilisant des notations en $O(\cdot)$. Des analyses plus fines (donnant en particulier des majorations des constantes apparaissant dans ces $O(\cdot)$) sont présentées par exemple dans [Bre75, Bre76] (cependant les questions de gestion de la précision n'y sont guère détaillées).

En ce qui concerne l'addition de deux N-représentations, elle se réduit à l'addition de leurs parties réelles et imaginaires, qui se réduisent elles-même à des additions d'entiers. Par un algorithme naïf, l'addition de deux entiers de taille N bits s'effectue en temps $O(N)$, on en déduit donc que le calcul de la N-représentation de la somme de deux N-représentations peut s'effectuer lui aussi en temps $O(N)$.

Si l'on considère la multiplication, comme l'on a supposé que les exposants que l'on manipule sont tous bornés, la multiplication de deux N-représentations se réduit à trois multiplications d'entiers de N bits et 6 additions, *via* la formule

$$(a + bi)(c + di) = ac - bd + \left((a + b)(c + d) - ac - bd\right) i.$$

En utilisant un algorithme naïf, la multiplication de deux entiers de taille N s'effectue en temps $O(N^2)$. Il existe cependant des algorithmes bien connus améliorant ce résultat. En particulier, l'algorithme de Karatsuba [KO63] à une complexité en temps en $O\left(N^{\log_2 3}\right)$ ($\log_2 3 \simeq 1.585$), et l'algorithme de Schönhage et Strassen [SS71], utilisant la transformation de Fourier rapide, a lui la meilleure complexité connue à ce jour pour la multiplication : il est en $O(N \log N \log\log N)$. Dans la suite de ce mémoire nous noterons $\mathcal{M}(N)$ le temps nécessaire pour multiplier deux entiers de N bits. On a donc

$$\mathcal{M}(N) = O\left(N \log N \log\log N\right) = O\left(N^{1+\varepsilon}\right)$$

(cette dernière notation signifie que pour tout $\varepsilon > 0$, on a $\mathcal{M}(N) = O\left(N^{1+\varepsilon}\right)$), et ce qui précède montre que le calcul de la N-représentation du produit de deux N-représentations se fait aussi en temps $O\left(\mathcal{M}(N)\right)$.

Dans le reste de cette section, nous allons nous intéresser aux *itérations de Newton*, qui peuvent être utilisées pour évaluer une grande classe de fonctions. En particulier, nous montrerons comment utiliser les itérations de Newton pour évaluer un inverse ou une racine carrée.

Nous mentionnerons enfin des algorithmes pour l'évaluation des fonctions logarithme et exponentielle.

1.3.1 Itérations de Newton

Principe général

Dans cette section, nous fixons $f : U \to \mathbb{C}$ une fonction analytique sur un ouvert U de $\mathbb{C}$ et supposons qu'il existe $\xi \in U$ tel que $f(\xi) = 0$ et $f'(\xi) \neq 0$.

On appelle alors *itérations de Newton* associées à f le processus consistant à partir d'une valeur $z_0 \in U$, puis à définir la suite $(z_n)_{n\in\mathbb{N}}$ par

$$z_{n+1} = N_f(z_n)$$

pour tout $n \geqslant 0$, où N_f est l'*opérateur de Newton associé à* f, défini dans un voisinage de ξ par

$$N_f(z) = z - \frac{f(z)}{f'(z)}.$$

Sous certaines conditions (en fait, si z_0 est suffisamment proche de ξ, comme nous allons le voir), la suite (z_n) converge *quadratiquement* vers ξ. Plus précisément, si l'on définit

$$\gamma(f,\xi) = \mathrm{Sup}_{n\geqslant 2} \left| \frac{f^{(n)}(\xi)}{f'(\xi) n!} \right|^{\frac{1}{n-1}}$$

(cette quantité est bien définie : comme f est analytique, la croissance des coefficients de son développement de Taylor en ξ ne peut être plus que géométrique, or le n-ème de ces coefficients vaut $\frac{f^{(n)}(\xi)}{n!}$), alors on a le résultat suivant :

Théorème 1.1 *Avec les notations précédentes, si*

$$|\xi - z_0| \leqslant \frac{3-\sqrt{7}}{2\gamma(f,\xi)},$$

alors pour tout $n \geqslant 0$,

$$|\xi - z_n| \leqslant \frac{1}{2^{2^n-1}} |\xi - z_0|.$$

Démonstration : Voir [BCSS97, pages 154–159]. □

Si l'on dispose d'un algorithme permettant l'évaluation de $z \mapsto f(z)/f'(z)$, on peut donc utiliser des itérations de Newton pour évaluer un zéro de f.

Toutefois, comme nous ne manipulons que des représentations finies des nombres, il n'est pas possible de calculer exactement la suite $(z_n)_{n\in\mathbb{N}}$, même si l'on dispose d'une représentation finie d'un nombre z_0 vérifiant

$$|\xi - z_0| \leqslant \frac{3-\sqrt{7}}{2\gamma(f,\xi)}.$$

Nous utiliserons donc la variante suivante du Théorème 1.1 :

Théorème 1.2 *Avec les notations précédentes, si $z_0 \in U$ et $A \in \mathbb{R}$ sont tels que*

$$|z_0 - \xi| \leqslant \frac{1}{2^A}$$

et

$$\frac{\gamma(f,\xi)}{2^A} \leqslant 2 - \sqrt{\frac{7}{2}},$$

et que $(z_n)_{n\in\mathbb{N}}$ est une suite telle que, pour tout $n \geqslant 0$,

$$|z_{n+1} - N_f(z_n)| \leqslant \frac{1}{2^{A+2^{n+1}}},$$

alors pour tout $n \geqslant 0$, on a

$$|z_n - \xi| \leqslant \frac{1}{2^{A+2^n-1}}.$$

Démonstration : La démonstration est relativement similaire à celle du Théorème 1.1. Nous la détaillons car les itérations de Newton jouent un rôle important dans la suite de ce mémoire.

Pour $z \in U$, nous notons

$$u(z) = \gamma(f,\xi)\,|z-\xi|\,.$$

Nous commençons par majorer la quantité $|f'(z) - f'(\xi)|$ lorsque $u(z) < 1$ comme suit :

$$\begin{aligned}
\left|f'(z) - f'(\xi)\right| &= \left|\sum_{k\geqslant 2} \frac{f^{(k)}(\xi)}{(k-1)!}(z-\xi)^{k-1}\right| \\
&\leqslant \sum_{k\geqslant 2} k\left|\frac{f^{(k)}(\xi)}{k!}(z-\xi)^{k-1}\right| \\
&\leqslant \left|f'(\xi)\right| \sum_{k\geqslant 2} k\gamma(f,\xi)^{k-1}\,|z-\xi|^{k-1} \\
&\leqslant \left|f'(\xi)\right| \sum_{k\geqslant 2} k u(z)^{k-1},
\end{aligned}$$

donc en utilisant l'égalité

$$\sum_{n\geqslant 1} n x^{n-1} = \frac{1}{(1-x)^2} \tag{1.1}$$

(ce qui est licite puisque $u(z) < 1$), on obtient

$$\left|f'(z) - f'(\xi)\right| \leqslant \left|f'(\xi)\right| \left(\frac{1}{\left(1-u(z)\right)^2} - 1\right).$$

On en déduit en particulier que, dans le cas où $u(z) < 1 - \frac{1}{\sqrt{2}}$, $f'(z) \neq 0$ et

$$\begin{aligned}
\left|\frac{f'(\xi)}{f'(z)}\right| &= \left|\frac{1}{1+\frac{f'(z)-f'(\xi)}{f'(\xi)}}\right| && (1.2)\\
&\leqslant \frac{1}{1-\left|\frac{f'(z)-f'(\xi)}{f'(\xi)}\right|} && (1.3)\\
&\leqslant \frac{1}{2-\frac{1}{(1-u(z))^2}} && (1.4)\\
&\leqslant \frac{(1-u(z))^2}{\psi(z)}, && (1.5)
\end{aligned}$$

où l'on a posé

$$\psi(z) = 1 - 4u(z) + 2u(z)^2.$$

Toujours dans le cas où $u(z) < 1 - \frac{1}{\sqrt{2}}$, on a aussi la majoration suivante :

$$\begin{aligned}
|N_f(z) - \xi| &= \frac{1}{|f'(z)|}\left|(z-\xi)f'(z) - f(z)\right|\\
&= \frac{1}{|f'(z)|}\left|\sum_{k\geqslant 1} f^{(k)}(\xi)\left(\frac{1}{(k-1)!} - \frac{1}{k!}\right)(z-\xi)^k\right|\\
&= \left|\frac{f'(\xi)}{f'(z)}\right| \cdot \left|\sum_{k\geqslant 1}(k-1)\frac{f^{(k)}(\xi)}{k!f'(\xi)}(z-\xi)^k\right|\\
&\leqslant \left|\frac{f'(\xi)}{f'(z)}\right| \sum_{k\geqslant 1}(k-1)\gamma(f,\xi)^{k-1}\left|z-\xi\right|^k,
\end{aligned}$$

et en utilisant à nouveau l'Équation (1.1), on obtient

$$|N_f(z) - \xi| \leqslant \left|\frac{f'(\xi)}{f'(z)}\right| \frac{u(z)}{(1-u(z))^2}\left|z-\xi\right|,$$

soit, *via* la majoration obtenue en (1.5) :

$$|N_f(z) - \xi| \leqslant \frac{u(z)}{\psi(z)}\left|z-\xi\right|. \tag{1.6}$$

Supposons maintenant que l'on ait une suite $(z_n)_{n\in\mathbb{N}} \in U^{\mathbb{N}}$ telle que $|z_0 - \xi| \leqslant \frac{1}{2^A}$ (donc que

$$u(z_0) \leqslant 2 - \sqrt{\frac{7}{2}} < 1 - \frac{1}{\sqrt{2}}$$

) et que, pour tout $n \geqslant 0$,

$$|z_{n+1} - N_f(z_n)| \leqslant \frac{1}{2^{A+2^{n+1}}}. \tag{1.7}$$

Nous allons montrer par récurrence sur n que, pour tout $n \in \mathbb{N}$,

$$|z_n - \xi| \leqslant \frac{1}{2^{A+2^n-1}}.$$

Ceci est vérifié, par hypothèse, pour $n = 0$. Supposons que ce le soit pour un certain $n \geqslant 0$, et montrons qu'alors, ça l'est encore pour $n+1$: d'après les Inégalités (1.6) et (1.7), on a

$$\begin{aligned} |z_{n+1} - \xi| &\leqslant |z_{n+1} - N_f(z_n)| + |N_f(z_n) - \xi| \\ &\leqslant \frac{1}{2^{A+2^{n+1}}} + \frac{u(z_n)}{\psi(z_n)} |z_n - \xi| \\ &\leqslant \frac{1}{2^{A+2^{n+1}}} + \frac{\gamma(f,\xi)}{\psi(z_n)} |z_n - \xi|^2, \end{aligned}$$

donc, en utilisant l'hypothèse de récurrence, on obtient

$$|z_{n+1} - \xi| \leqslant \frac{1}{2^{A+2^{n+1}}} + \frac{\gamma(f,\xi)}{\psi(z_n)} \frac{1}{2^{2A+2^{n+1}-2}}.$$

Comme la fonction $x \mapsto \frac{1}{1-4x+2x^2}$ est croissante sur $\left]0, 1 - \frac{1}{\sqrt{2}}\right[$, et que (d'après l'hypothèse de récurrence)

$$u(z_n) \leqslant \frac{\gamma(f,\xi)}{2^A} \leqslant 2 - \sqrt{\frac{7}{2}} < 1 - \frac{1}{\sqrt{2}},$$

on en déduit que

$$|z_{n+1} - \xi| \leqslant \frac{1}{2^{A+2^{n+1}}} + \frac{\gamma(f,\xi)}{2^A} \frac{1}{\psi\left(\frac{\gamma(f,\xi)}{2^A}\right)} \frac{1}{2^{A+2^{n+1}-2}}.$$

On utilise maintenant le fait que, pour $x \in \left]0, 2 - \sqrt{\frac{7}{2}}\right]$, on a

$$\frac{x}{1 - 4x + 2x^2} \leqslant \frac{1}{4}$$

pour (comme on a supposé que $\frac{\gamma(f,\xi)}{2^A} \leqslant 2 - \sqrt{\frac{7}{2}}$) finalement obtenir

$$|z_{n+1} - \xi| \leqslant \frac{1}{2^{A+2^{n+1}-1}},$$

ce qui conclut la démonstration. □

Voyons maintenant ce que signifie ce dernier théorème en terme de précisions relatives. Pour cela, toujours en gardant les mêmes notations, on suppose que l'on connaît un encadrement de $|\xi|$ de la forme

$$2^B \leqslant |\xi| \leqslant 2^C,$$

et l'on suppose de plus que $C \geqslant -A - 2$ (ce qui est toujours possible quitte à augmenter C).

Nous avons montré, dans la démonstration du théorème ci-dessus, que pour tout $n \geqslant 0$,

$$|N_f(z_n) - \xi| \leqslant \frac{1}{2^{A+2^{n+1}}} \leqslant 2^C,$$

donc

$$|N_f(z_n)| \leqslant |\xi| + |N_f(z_n) - \xi| \leqslant 2^{C+1}.$$

Posons maintenant, pour tout $n \in \mathbb{N}$,

$$p(n) = A + C + 1 + 2^n.$$

Si, pour $n \in \mathbb{N}$, on pose $z_{n+1} = \mathrm{Rep}_{p(n+1)}\left(N_f(z_n)\right)$, alors on a bien

$$|z_{n+1} - N_f(z_n)| \leqslant |N_f(z_n)| \cdot \left|\frac{z_{n+1} - N_f(z_n)}{N_f(z_n)}\right| \leqslant 2^{C+1}\frac{1}{2^{p(n+1)}} \leqslant \frac{1}{2^{A+2^{n+1}}},$$

comme requis.

Si l'on fixe un entier $N \in \mathbb{N}$ et que l'on veut calculer une approximation de ξ à précision relative N, il suffit donc de

– partir d'une première approximation z_0 de ξ telle que

$$|z_0 - \xi| \leqslant \frac{1}{2^A},$$

(par exemple $z_0 = \mathrm{Rep}_{A+C}(\xi)$ convient) ;

– calculer successivement les

$$z_{n+1} = \mathrm{Rep}_{p(n+1)}\left(N_f(z_n)\right);$$

– renvoyer le premier élément z_n tel que

$$2^n \geqslant N + 1 - A - B,$$

puisqu'alors, d'après le théorème, z_n est une approximation de ξ avec une précision relative de N bits.

On remarque ici un point important des itérations de Newton : *la précision à laquelle on travaille à chaque étape* pour le calcul de $N_f(z_n)$ (soit $p(n+1)$) *augmente* : modulo la constante $A + C + 1$, cette précision double à chaque étape.

Intéressons-nous à la complexité en temps des itérations de Newton. Supposons pour cela que la complexité de la k-ème itération est en $g\left(p(k)\right)$, où la fonction g est croissante et telle que, pour x suffisamment grand,

$$2g(x) \leqslant g(2x)$$

(ce sera très souvent le cas). Alors la complexité des n premières itérations est en

$$O\left(\sum_{k=1}^{n} g\left(p(k)\right)\right) = O\left(g\left(p(n)\right)\right).$$

On dit souvent que le coût en temps des itérations de Newton est proportionnel au coût de la dernière itération nécessaire.

Par ailleurs, on dit parfois que les itérations de Newton sont *auto-correctrices* : si l'on fait une erreur sur le calcul de l'un des termes de la suite $(z_n)_{n\in\mathbb{N}}$, alors (en supposant que cette erreur n'est pas trop importante, c'est-à-dire que l'on a encore $|z_n - \xi| \leqslant \frac{1}{A}$) la suite va tout de même converger vers ξ.

L'inversion

Soit $a \in \mathbb{C} \setminus \{0\}$, dont on souhait calculer l'inverse. Si l'on veut utiliser des itérations de Newton, on peut poser $f_a(z) = az - 1$, qui s'annule en $\frac{1}{a}$… mais alors $N_{f_a}(z) = \frac{1}{a}$, et l'on n'est pas très avancé.

Supposons maintenant que z_0 soit une approximation de $\frac{1}{a}$, et posons

$$I_a(z) = z - z(az - 1) = z(2 - az).$$

On a alors

$$\begin{aligned}\left|\frac{\frac{1}{a}-I_a(z_0)}{\frac{1}{a}}\right| &= |aI_a(z_0)-1| \\ &= |az_0 - az_0(az_0-1)-1| \\ &= |az_0-1|^2 \\ &= \left|\frac{\frac{1}{a}-z_0}{\frac{1}{a}}\right|,\end{aligned}$$

donc $I_a(z_0)$ approche $\frac{1}{a}$ avec une précision relative deux fois meilleure que z_0.

Notons que I_a est assez voisine de l'itération de Newton N_{f_a}, simplement on a remplacé le facteur $\frac{1}{f_a'(z)} = \frac{1}{a}$ par z (qui est justement censé approcher $\frac{1}{a}$). En général, on parle d'ailleurs encore d'itération de Newton pour I_a.

Le principal problème qui nous reste à résoudre est de trouver une valeur convenable pour z_0. Pour cela, notons que l'on peut se restreindre à $|a| \in \left[\frac{1}{2}, 1\right]$ (il suffit de diviser a par une puissance convenable de 2, ce qui est immédiat si l'on considère des représentations finies, et l'on devra alors multiplier le résultat calculé par la même puissance de 2). Par ailleurs, quitte à multiplier a par i, $-i$ ou -1, on peut aussi supposer que $|\mathrm{Arg}\,(a)| \leqslant \frac{\pi}{4}$ (il faudra alors aussi penser à modifier le résultat de l'inversion de façon idoine).

Un peu de trigonométrie montre que sous ces hypothèses, on a

$$|a-1| \leqslant \varepsilon = 2\sin\frac{\pi}{8} = \sqrt{2-\sqrt{2}}, \tag{1.8}$$

et en utilisant la formule

$$\frac{1}{a} = \sum_{n\geqslant 0}(1-a)^n,$$

on montre que pour tout $k \in \mathbb{N}$,

$$\left|\frac{1}{a} - \sum_{n=0}^{k}(1-a)^n\right| \leqslant \frac{\varepsilon^{k+1}}{1-\varepsilon}$$

donc

$$\left|\frac{\frac{1}{a} - \sum_{n=0}^{k}(1-a)^n}{\frac{1}{a}}\right| \leqslant \frac{2\varepsilon^{k+1}}{1-\varepsilon}.$$

En particulier, une application numérique montre que pour $k = 16$, on est sûr d'avoir ainsi une approximation de $\frac{1}{a}$ avec une précision relative de 3 bits, donc, si l'on pose

$$z_0 = \mathrm{Rep}_2\left(\sum_{n=0}^{16}(1-a)^n\right),$$

puis, pour $n \geqslant 0$,

$$z_{n+1} = \mathrm{Rep}_{2^n+2}\left(I_a(z_n)\right),$$

alors pour tout $n \geqslant 0$, z_n est une approximation de $\frac{1}{a}$ avec une précision relative de 2^n+1 bits.

Étudions maintenant la complexité de cet algorithme. Si l'on veut une précision relative de N bits, on devra aller jusqu'à l'indice $n = \lceil \log_2 N \rceil$. Par ailleurs, le calcul de

$z_{n+1} = \mathrm{Rep}_{2^{n+1}+2}\left(z_n(2 - az_n)\right)$ à partir de $z_n \in \mathcal{R}\left(2^n + 2\right)$ se fait en temps $O\left(\mathcal{M}(2^n)\right)$, donc la complexité en temps de cet algorithme d'inversion est en

$$O\left(\sum_{k=1}^{\log_2 N} \mathcal{M}(2^k)\right) = O\left(\mathcal{M}(N)\right),$$

indépendamment de la valeur de a (le fait de réduire le problème au cas où $|a| \in \left[\frac{1}{2}, 1\right]$ et $|\mathrm{Arg}\,(a)| \leqslant \frac{\pi}{4}$ est négligeable).

On notera que si a est très proche de 1 (par exemple si $|1 - a|^2 < \frac{1}{2^{N+2}}$), alors $2 - a$ approche $\frac{1}{a}$ avec une précision relative de N bits (on a en fait pris $k = 1$ dans le développement de Taylor utilisé ci-dessus pour obtenir z_0).

L'extraction de racine

Soit $a \in \mathbb{C} \setminus \{0\}$, dont on veut calculer la racine carrée. On peut, sans perte de généralité, supposer $\mathrm{Re}\,(a) \geqslant 0$ et calculer la racine de a ayant partie réelle strictement positive (que l'on notera $\sqrt{a}$).

Si l'on pose $f(z) = z^2 - a$, alors l'itération de Newton correspondante s'écrit

$$N_f(z) = \frac{1}{2}\left(z + \frac{a}{z}\right).$$

On a par ailleurs

$$\gamma\left(f, \sqrt{a}\right) = \frac{1}{2\sqrt{|a|}}.$$

On peut ici, quitte à multiplier a par la puissance de 4 idoine (et l'on multipliera alors le résultat par la puissance correspondante de $2 = \sqrt{4}$), supposer de plus que $|a| \in [1, 4]$. On a alors

$$\gamma\left(f, \sqrt{a}\right) \leqslant \frac{1}{2},$$

et si l'on pose $A = 2$ on a bien

$$\frac{\gamma\left(f, \sqrt{a}\right)}{2^A} \leqslant 2 - \sqrt{\frac{7}{2}}.$$

Comme par ailleurs, si l'on pose $B = 0$ et $C = 1$, on a

$$2^B \leqslant \left|\sqrt{a}\right| \leqslant 2^C,$$

le Théorème 1.2 et la discussion qui le suit montrent que si $z_0 = \mathrm{Rep}_3\left(\sqrt{a}\right)$ et que, pour $n \geqslant 0$, on pose $z_{n+1} = \mathrm{Rep}_{2^{n+1}+4}\left(z_n\right)$, alors $z_{\lceil \log_2 N \rceil}$ est une approximation de $\sqrt{a}$ avec une précision relative de N bits.

Reste donc à trouver un moyen de déterminer z_0. Ceci peut se faire *via* le développement de Taylor de la fonction $z \mapsto \sqrt{z}$ au voisinage de 1... mais il faut tout de même se ramener à ce voisinage. Pour cela, on peut par exemple poser $\alpha = \frac{5}{4}$, $\beta = \exp\frac{\pi i}{16}$, et (quitte à multiplier a par les bonnes puissances de α^2 et β^2) supposer de plus que $|a| \in \left[1, \frac{25}{16}\right]$ et $|\mathrm{Arg}\,(a)| \leqslant \frac{\pi}{8}$. Dans ce cas, $|a - 1|$ est majoré par une constante strictement plus petite que 1, par exemple on peut montrer que $|a - 1| \leqslant 0.7$. On peut alors utiliser les premiers termes du développement de Taylor pour obtenir z_0 (nous n'explicitons pas cette phase ici). Il reste ensuite à multiplier le z_0 obtenu par les bonnes puissances de α et β. Tous ces calculs se font à petite précision, et ont donc un coût négligeable.

Le coût global de l'algorithme s'étudie de la même façon que pour l'inversion, et l'on trouve là encore un temps de calcul en $O\left(\mathcal{M}(N)\right)$, indépendamment de la valeur de a.

Le logarithme et l'exponentielle

Dans les années 70, Salamin [BGS72] a présenté une méthode utilisant l'AGM pour l'évaluation rapide du logarithme d'un réel positif. Cette méthode a été analysée quantitativement par Borwein et Borwein [BB84], qui utilisent pour ce faire des majorations d'intégrales. Le fait que cette méthode puisse se généraliser au cas d'une variable complexe semble connu, mais aucune analyse de l'algorithme correspondant ne semble avoir été faite. Nous présentons à la Section 3.5 un tel algorithme, et montrons qu'il permet d'évaluer une détermination du logarithme complexe d'un nombre $z \in \mathbb{C} \setminus \{0\}$ avec une précision relative N en temps $O(\mathcal{M}(N) \log N)$, indépendamment de la valeur de z.

Par ailleurs, si l'on pose $a \in \mathbb{C}$ et que l'on veut évaluer $\exp(a)$, on peut utiliser des itérations de Newton sur la fonction $f(z) = \log z - a$. On a alors $N_f(z) = z(1 + a - \log z)$, et $\gamma(f, \exp(a)) = |\exp(a)|$. On peut alors utiliser le développement de Taylor de l'exponentielle pour initialiser les itérations de Newton avec la bonne précision. Il est utile de se réduire (*via* une multiplication par une puissance de 2 convenable) au voisinage de zéro (la série de Taylor converge alors rapidement, et l'on a une bonne majoration de $\gamma(f, \exp(a))$).

On obtient finalement une complexité pour l'évaluation de l'exponentielle avec une précision relative de N bits en $O(\mathcal{M}(N) \log N)$, indépendamment de la valeur de a.

Première partie

Le genre 1

Chapitre 2

Formes et fonctions modulaires en genre 1, theta constantes

Le but de ce chapitre est de définir les formes et fonctions modulaires en genre 1, ainsi que des fonctions qui nous intéresseront tout au long de ce mémoire connues sous le nom de theta constantes. En particulier, nous montrons comment ces dernières peuvent être utilisées pour construire des fonctions modulaires. Nous démontrons enfin un certain nombre de propriétés de ces fonctions, qui nous seront utiles par la suite.

2.1 Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré

2.1.1 Définitions et notations

Le demi-plan de Poincaré

Définition 2.1 (demi-plan de Poincaré $\mathcal{H}$) *Dans ce qui suit, on note $\mathcal{H}$ le demi-plan de Poincaré, défini par*

$$\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Si l'on considère $\mathcal{H}$ muni de la distance elliptique, alors son compactifié est $\widehat{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, où le point ∞ peut être vu comme le point situé à l'infini le long de l'axe des imaginaires.

Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré

Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathcal{H}$ *via*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

pour tous $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $\tau \in \mathcal{H}$.

On montre facilement que

$$\mathrm{Im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau\right) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

et il est alors aisé de vérifier que l'on a bien défini une action de groupe.

On notera que $(-I)\tau = \tau$, donc qu'il s'agit en fait d'une action du groupe

$$\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})/\langle -I \rangle$$

(ou *groupe modulaire elliptique*) sur $\mathcal{H}$.

On vérifie facilement que cette action se prolonge en une action sur $\widehat{\mathcal{H}}$, en posant, pour tous $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $\frac{p}{q} \in \mathbb{Q}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c} & \text{si } c \neq 0 \\ \infty & \text{si } c = 0, \end{cases}$$

et

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{p}{q} = \begin{cases} \frac{ap+bq}{cp+dq} & \text{si } cp+dq \neq 0 \\ \infty & \text{si } cp+dq = 0. \end{cases}$$

(en particulier, $\mathbb{Q}$ est l'orbite de ∞ sous l'action de Γ_1).

On pose maintenant $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a donc, pour $\tau \in \mathcal{H}$, $S\tau = -1/\tau$ et $T\tau = \tau + 1$. On notera que l'on a en particulier $S^2 = -I$ et $T^{-1} = S^3(TS)^2$. L'intérêt pour nous des matrices S et T vient du résultat classique suivant :

Proposition 2.1 *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par* S *et* T.

Démonstration : Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. On va montrer le résultat par récurrence sur $|a| + |c|$. Supposons qu'il existe $n \geqslant 1$ tel que toute matrice de $\mathrm{SL}_2(\mathbb{Z})$ de la forme $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $|\alpha|+|\gamma| \leqslant n$ soit engendrée par S et T. Si γ vérifie $|a|+|c| = n+1$, alors quitte à multiplier γ à gauche par S, on peut supposer $|a| \geqslant |c|$. On écrit alors la division euclidienne de a par c :

$$a = q.c + r,$$

avec $0 \leqslant r < |c|$. On a donc

$$T^{-q}\gamma = \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix}$$

qui est, d'après l'hypothèse de récurrence, engendrée par S et T.

Maintenant, si $|a|+|c| = 1$, alors quitte à multiplier à gauche par S, on peut supposer $|a| = 1$ et $|c| = 0$. Quitte à multiplier à gauche par $S^2 = -I$, on peut encore supposer $a = 1$. Alors la matrice est de la forme $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = T^c$, ce qui conclut la démonstration. □

2.1.2 Le domaine fondamental $\mathcal{F}$

On pose

$$\mathcal{F} = \left\{ \tau \in \mathcal{H} : |\tau| \geqslant 1, |\mathrm{Re}(\tau)| \leqslant \frac{1}{2} \right\}$$

et

$$\mathcal{F}' = \mathcal{F} \setminus \left(\delta\mathcal{F} \cap \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) > 0\} \right).$$

Définition 2.2 (domaine fondamental, ensemble fondamental) *Soit* G *un groupe agissant sur un ensemble* X *muni d'une topologie.*

Un ensemble $Y \subset X$ *est un* domaine fondamental *pour l'action de* G *sur* X *si,*

– *pour tout* $x \in X$, *il existe* $g \in G$ *et* $y \in Y$ *tels que* $y = g.x$; *et*

– *pour tous $y_1, y_2 \in Y$ et $g \in G \setminus \{1\}$ tels que $y_1 = g.y_2$, on a $y_1 \in \delta(Y)$ et $y_2 \in \delta(Y)$.*

Un ensemble $Y \subset X$ est un ensemble fondamental *pour l'action de G sur X si, pour tout $x \in X$, il existe un* unique *$y \in Y$ qui soit dans l'orbite de x sous l'action de G.*

Un ensemble fondamental est donc toujours un domaine fondamental (de même que sa clôture), mais la réciproque est fausse.

Proposition 2.2 *La région $\mathcal{F}'$ est un ensemble fondamental pour l'action de Γ sur $\mathcal{H}$ (donc $\mathcal{F}$ est un domaine fondamental pour cette même action). De plus, on a*

$$\mathrm{card}\left(\{\gamma \in \Gamma : \tau_0 = \gamma\tau\}\right) = \begin{cases} 2 \text{ si } \tau_0 = i; \\ 3 \text{ si } \tau_0 = \exp\left(\frac{2\pi i}{3}\right); \\ 1 \text{ sinon.} \end{cases}$$

Démonstration : Soit $\tau \in \mathcal{H}$, on lui associe l'ensemble

$$\begin{aligned} R(\tau) &= \{\mathrm{Im}(\gamma\tau) : \gamma \in \Gamma\} \\ &= \left\{ \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \right\}. \end{aligned}$$

Cet ensemble admet un élément minimal, donc il existe $\gamma_0 \in \Gamma$ tel que, pour tout $\gamma \in \Gamma$, $\mathrm{Im}(\gamma\tau) \leqslant \mathrm{Im}(\gamma_0\tau)$. Soient alors $u \in \mathbb{Z}$ et $v \in [-1/2, 1/2[$ tels que $\mathrm{Re}(\gamma_0\tau) = u + v$. On pose $\tau_0 = T^{-u}\gamma_0\tau$, de sorte que τ_0 soit encore de partie imaginaire maximale parmi les éléments équivalents à τ. Alors nécessairement, $|\tau_0| \geqslant 1$, car sinon on aurait

$$\begin{aligned} \mathrm{Im}(S\tau_0) &= \frac{\mathrm{Im}(\tau_0)}{|\tau_0|^2} \\ &> \mathrm{Im}(\tau_0). \end{aligned}$$

On en déduit que soit $\tau_0 \in \mathcal{F}'$, soit $|\tau_0| = 1$ et $\mathrm{Re}(\tau_0) > 0$, mais dans ce cas $S\tau_0 \in \mathcal{F}'$. On a donc montré que dans tous les cas, il existe $\tau_0 \in \mathcal{F}'$ qui est équivalent à τ modulo l'action de Γ.

Soient maintenant $\tau_1, \tau_2 \in \mathcal{F}'$ et $\gamma \in \Gamma$ tels que $\tau_2 = \gamma\tau_1$. Sans perte de généralité, on suppose $\mathrm{Im}(\tau_2) \geqslant \mathrm{Im}(\tau_1)$. Alors, si l'on écrit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en supposant (quitte à remplacer par $-\gamma$) que $c \geqslant 0$ et $d > 0$ si $c = 0$, on a

$$\mathrm{Im}(\tau_2) = \frac{\mathrm{Im}(\tau_1)}{|c\tau_1 + d|^2}.$$

Si l'on pose $\tau_1 = x_1 + y_1 i$ avec $x_1, y_1 \in \mathbb{R}$, alors

$$\begin{aligned} |c\tau_1 + d|^2 &= c^2 + d^2 + 2cdx_1 \\ &\geqslant c^2 + d^2 - |cd| \\ &\geqslant (|c| - |d|)^2 + |cd|, \end{aligned}$$

où l'on a utilisé le fait que $|x_1| \leqslant 1/2$ car $\tau_1 \in \mathcal{F}'$.

Comme c et d sont des entiers non tous deux nuls, $(|c| - |d|)^2 + |cd| \geqslant 1$, donc

$$\mathrm{Im}(\tau_2) = \frac{\mathrm{Im}(\tau_1)}{|c\tau_1 + d|^2} \leqslant \frac{\mathrm{Im}(\tau_1)}{(|c| - |d|)^2 + |cd|} \leqslant \mathrm{Im}(\tau_1) \leqslant \mathrm{Im}(\tau_2),$$

donc nécessairement, $(|c| - |d|)^2 + |cd| = 1$ et $\mathrm{Im}(\tau_1) = \mathrm{Im}(\tau_2)$.

Supposons alors que $c = 0$, alors $d = 1$ donc il existe $r \in \mathbb{Z}$ tel que $\gamma = T^r$. Mais r ne peut être non nul car alors $\mathrm{Re}(\tau_2) = \mathrm{Re}(\tau_1) + r \notin [-1/2, 1/2[$. Donc $r = 0$, et $\tau_1 = \tau_2$.

Reste donc le cas $c > 0$. On doit avoir $|cd| \leqslant 1$, donc $d \in \{-1, 0, 1\}$.

– Si $d = 0$, alors $c = 1$, et $\gamma = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$, donc $\tau_2 = a - 1/\tau_1$. De plus,

$$\mathrm{Im}(\tau_2) = \frac{\mathrm{Im}(\tau_1)}{|\tau_1|^2} = \mathrm{Im}(\tau_1),$$

donc $|\tau_1| = 1$ (et par un raisonnement similaire, $|\tau_2| = 1$). Par définition de $\mathcal{F}'$, les parties réelles de τ_1 et τ_2 sont dans $[-1/2, 0]$, et $\mathrm{Re}(\tau_2) = a - \mathrm{Re}(\tau_1)$. Les seuls cas possibles sont alors $a = 0$, *i.e.*, $\gamma = S$, $\tau_1 = \tau_2 = i$, et $a = -1$, *i.e.*, $\gamma = T^{-1}S$, $\tau_1 = \tau_2 = \exp(\frac{2\pi i}{3})$.

– Si $d = 1$, alors $c = 1$ et $|\tau_1 + 1| = 1$, ce qui implique $\tau_1 = \exp(\frac{2\pi i}{3})$. La matrice γ est alors soit $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, soit $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Dans le premier cas, on aurait $\tau_2 = \exp(\frac{\pi i}{3}) \notin \mathcal{F}'$, et dans le second, $\tau_1 = \tau_2 = \exp(\frac{2\pi i}{3})$ et $\gamma = ST$.

– Si $d = -1$, alors $c = 1$ et $|1 - \tau_1| = 1$ ne peut être vérifié.

On a donc montré que si τ_1 et τ_2 sont deux éléments de $\mathcal{F}'$ équivalents modulo l'action de Γ, alors nécessairement $\tau_1 = \tau_2$, et

$$\{\gamma \in \Gamma_1 : \tau_2 = \gamma\tau_1\} = \begin{cases} \{I, ST, T^{-1}S\} \text{ si } \tau_1 = \tau_2 = \exp(\frac{2\pi i}{3}); \\ \{I, S\} \text{ si } \tau_1 = \tau_2 = i; \\ \{I\} \text{ sinon.} \end{cases}$$

Soient maintenant $\tau \in \mathcal{H}$ et $\gamma \in \Gamma$ tels que $\tau_0 = \gamma\tau \in \mathcal{F}'$. Si $\gamma' \in \Gamma$ est tel que $\tau_0 = \gamma'\tau$, alors on a $\gamma^{-1}\tau_0 = \gamma'^{-1}\tau_0$, et la discussion ci-dessus permet de conclure. □

Par la suite, nous confondrons les éléments de $\mathrm{SL}_2(\mathbb{Z})$ avec leur classe dans Γ_1.

Algorithme de réduction dans l'ensemble fondamental $\mathcal{F}'$

On déduit de ce résultat l'Algorithme 1, permettant, étant donné $\tau \in \mathcal{H}$, de le réduire dans l'ensemble fondamental $\mathcal{F}'$:

Algorithme : `ReduceToFD`
Entrée : $\tau \in \mathcal{H}$
Sortie : $\gamma \in \Gamma_1$ et $\tau' \in \mathcal{F}'$ tels que $\tau' = \gamma\tau$

$\tau' \leftarrow \tau$, $\gamma \leftarrow I$;
$n \leftarrow \lfloor \mathrm{Re}(\tau') \rceil$;
$\tau' \leftarrow \tau' - n$, $\gamma \leftarrow T^{-n}$;
while $|\tau'| < 1$ **do**
  $\tau' \leftarrow -1/\tau'$, $\gamma \leftarrow S\gamma$;
  $n \leftarrow \lfloor \mathrm{Re}(\tau') \rceil$;
  $\tau' \leftarrow \tau' - n$, $\gamma \leftarrow T^{-n}$;
end
return τ', γ;

Algorithme 1: Réduction dans l'ensemble fondamental $\mathcal{F}'$

2.1.3 Polygones élémentaires et sous-groupes du groupe modulaire elliptique

Pour $a, b \in \mathbb{R}$, notons

$$\Delta_a = \{\tau \in \mathcal{H} : \mathrm{Re}(\tau) = a\}$$

et

$$\mathcal{C}_{a,b} = \left\{ \tau \in \mathcal{H} : \left| \tau - \frac{a+b}{2} \right| = \frac{|a-b|}{2} \right\}.$$

Il est aisé de vérifier que l'involution de $\mathcal{H}$ induite par S envoie Δ_0 sur Δ_0, Δ_a sur $\mathcal{C}_{0,-1/a}$ si $a \neq 0$, et $\mathcal{C}_{a,b}$ sur $\mathcal{C}_{-1/a,-1/b}$ si $ab \neq 0$.

Définition 2.3 (polygone élémentaire) *Un* polygone élémentaire *est un domaine fondamental connexe pour Γ_1, dont le bord est inclus dans une union* finie *d'ensembles de la forme Δ_a et $\mathcal{C}_{a,b}$.*

Le domaine fondamental $\mathcal{F}$ est un polygone élémentaire, on parlera même de triangle élémentaire puisque son bord est inclus dans

$$\Delta_{-\frac{1}{2}} \cup \Delta_{\frac{1}{2}} \cup \mathcal{C}_{-1,1}.$$

D'après ce qui prècède, il est facile de voir que l'image d'un polygone élémentaire par l'action d'un élément de Γ_1 est encore un polygone élémentaire (qui aura de plus le même nombre de côtés). En particulier, le demi-plan de Poincaré peut être pavé par un polygone élémentaire et ses images sous l'action de Γ_1. La Figure 2.1 représente ainsi le pavage de $\mathcal{H}$ par les images du domaine fondamental $\mathcal{F}$ sous l'action de Γ_1. Pour $\gamma \in \Gamma_1$, la région $\gamma\mathcal{F}$ y est identifiée par γ.

Soit $\mathcal{P}$ un polygone élémentaire ayant n côtés. Il existe alors n éléments distincts $(\gamma_j)_{j\in[1,n]} \in \Gamma_1^n$ tels que chacun des n côtés de $\mathcal{P}$ soit un côté commun avec un polygone $\gamma_j\mathcal{P}$. On dira alors que les polygones élémentaires $\gamma_j\mathcal{P}$ sont les *voisins* de $\mathcal{P}$. En particulier, les voisins du domaine fondamental $\mathcal{F}$ sont $T\mathcal{F}$, $T^{-1}\mathcal{F}$ et $S\mathcal{F}$. De plus, si $\mathcal{P}$ est un polygone élémentaire ayant pour voisins les $\gamma_j\mathcal{P}$ et que l'on fixe $\gamma \in \Gamma_1$, alors $\gamma\mathcal{P}$ est un polygone élémentaire ayant pour voisins les $\gamma_j\gamma\mathcal{P}$.

On en déduit facilement un algorithme permettant de calculer de proche en proche le graphe d'adjacence du pavage de $\mathcal{H}$ par des polygones élémentaires (et on notera que tous les sommets d'un tel graphe ont même arité, égale au nombre de côtés du polygone élémentaire que l'on considère).

Sous-groupes d'indice fini de Γ_1

Dans cette section, nous fixons $\mathcal{P}$ un polygone élémentaire à n côtés, $\{\gamma_j\}_{j\in[1,n]}$ l'ensemble des éléments de Γ_1 tels que les voisins de $\mathcal{P}$ soient les $\gamma_j\mathcal{P}$, et afin de simplifier les choses, nous désignerons par "polygones élémentaires" les éléments de l'orbite de $\mathcal{P}$ sous l'action de Γ_1 (et seulement ceux-ci).

Soit Γ un sous-groupe d'indice fini de Γ_1, et posons $\mu = [\Gamma_1 : \Gamma]$.

Si G_Γ est un ensemble de représentants pour les classes de $\Gamma\backslash\Gamma_1$, alors

$$\bigcup_{\gamma\in G_\Gamma} \gamma\mathcal{P}$$

est un domaine fondamental pour l'action de Γ sur $\mathcal{H}$.

Le calcul effectif de tels domaines fondamentaux repose sur le résultat suivant (principalement sur sa démonstration en fait) :

Proposition 2.3 *Il existe un domaine fondamental $\mathcal{P}_{\Gamma'}$ pour l'action de Γ' sur $\mathcal{H}$, connexe, et de la forme*

$$\mathcal{P}_{\Gamma'} = \bigcup_{j=1}^{\mu} \gamma_j\mathcal{P}.$$

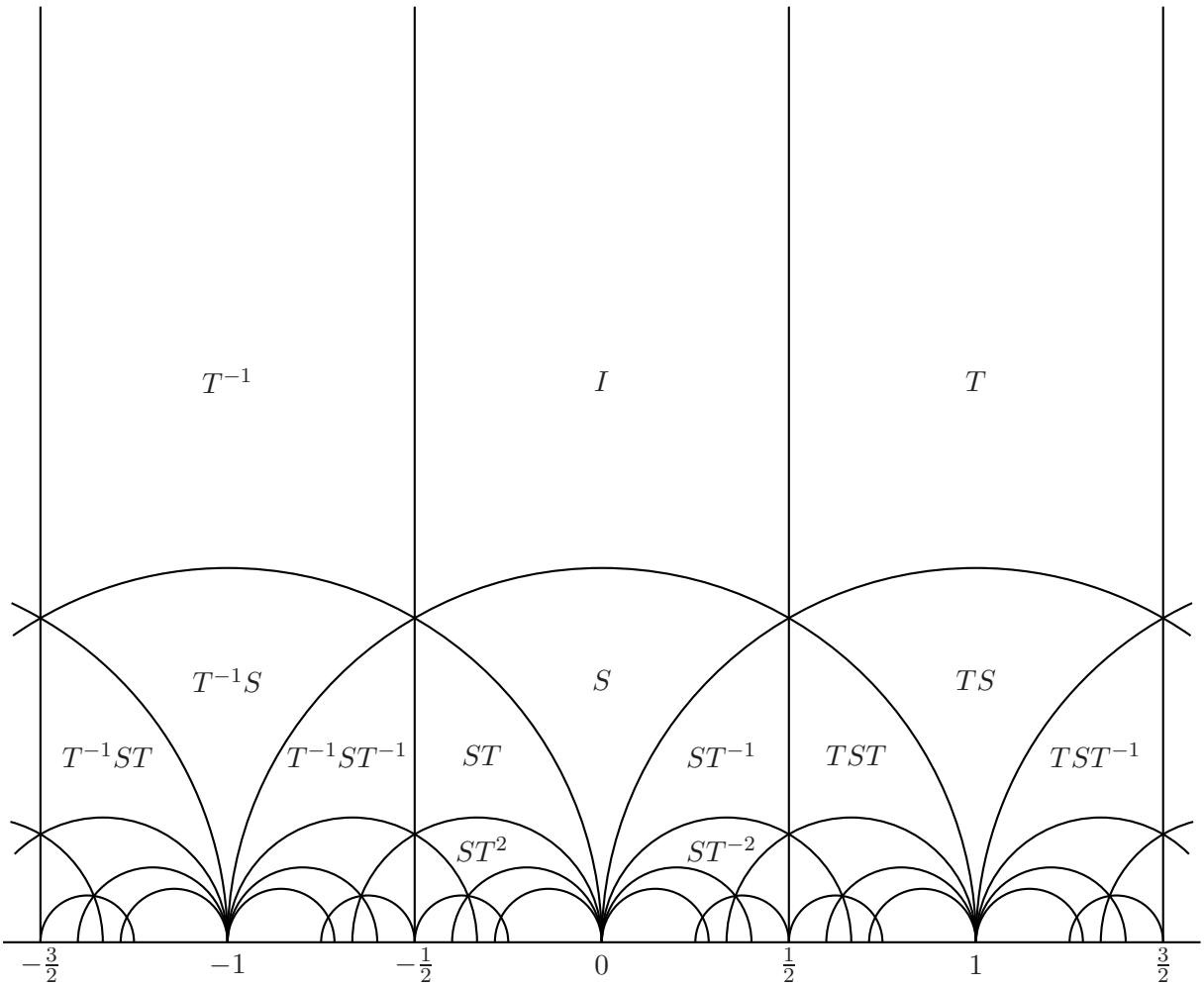

FIG. 2.1 – Pavage de $\mathcal{H}$ par les images du domaine fondamental $\mathcal{F}$

Démonstration : On construit itérativement un ensemble $\mathcal{S}$ comme suit : on part de $\mathcal{S} = \{I\}$, et s'il existe $\gamma \in \mathcal{S}$ et $j \in [1, n]$ tels que $\gamma\gamma_j \notin \mathcal{S}$ et que pour tout $\gamma' \in \mathcal{S}$, $\gamma\gamma_j\gamma'^{-1} \notin \Gamma$, alors on insère $\gamma\gamma_j$ dans $\mathcal{S}$. On réitère ce procédé jusqu'à ce que l'on ne puisse plus faire croître $\mathcal{S}$.

On pose alors

$$\mathcal{P}_\mathcal{S} = \bigcup_{\gamma\in\mathcal{S}} \gamma\mathcal{P}.$$

D'après ce que nous avons vu plus haut, si $\gamma \in \mathcal{S}$, alors les $\gamma\gamma_j\mathcal{P}$ sont les voisins du polygone élémentaire $\gamma\mathcal{P}$, ce qui prouve que $\mathcal{P}_\mathcal{S}$ est connexe.

Reste donc à montrer que $\mathcal{S}$ est un ensemble de représentants des classes de $\Gamma\backslash\Gamma_1$. Par construction, deux éléments distincts de $\mathcal{S}$ ne peuvent être équivalents modulo Γ, donc $\mathcal{P}_\mathcal{S}$ est un domaine fondamental pour l'action de Γ si et seulement si $\mathcal{S}$ contient μ éléments. Supposons que ce ne soit pas le cas, et soit γ un élément de Γ_1 qui ne soit équivalent à aucun élément de $\mathcal{S}$ modulo Γ. Par construction de $\mathcal{S}$, le polygone élémentaire $\gamma\mathcal{P}$ n'est pas dans $\mathcal{P}_\mathcal{S}$ et n'a aucun de ses n voisins dans $\mathcal{P}_\mathcal{S}$. Soit alors x (resp. y) un point intérieur de $\mathcal{P}_\mathcal{S}$ (resp. de $\gamma\mathcal{P}$). On peut relier x à y par un chemin polygonal dans $\mathcal{H}$, et si l'on suit ce chemin en partant de x, alors le premier polygone élémentaire image de $\mathcal{P}$ que l'on rencontre qui n'est pas dans $\Gamma\mathcal{P}_\mathcal{S}$ est nécessairement équivalent modulo l'action de Γ à un polygone élémentaire image de $\mathcal{P}$ ayant un voisin dans $\mathcal{P}_\mathcal{S}$, ce qui contredit la contruction de $\mathcal{S}$.

Soient maintenant $\gamma_1, \gamma_2 \in \Gamma_1$ tels que

- $\gamma_1 \in \mathcal{S}$;
- le polygone élémentaire $\gamma_1\mathcal{P}$ a un côté en commun avec un polygone élémentaire image de $\mathcal{P}$ non-inclus dans $\mathcal{P}_\mathcal{S}$;
- $\gamma_2 \notin \mathcal{S}$; et
- le polygone élémentaire $\gamma_2\mathcal{P}$ a un côté en commun avec un polygone élémentaire de $\mathcal{P}_\mathcal{S}$.

Dans ces conditions, on dit que $\gamma_1\gamma_2^{-1}$ est une *substitution de bords*. D'après la définition de $\mathcal{S}$, il est clair qu'une substitution de bords est un élément de Γ. Par ailleurs, l'image de $\mathcal{P}_\mathcal{S}$ par une substitution de bord est un domaine fondamental pour l'action de Γ ayant un côté en commun avec $\mathcal{P}_\mathcal{S}$ (et tous les tels domaines fondamentaux sont ainsi caractérisés). On en déduit (et c'est ce qui fait leur intérêt) que les substitutions de bords engendrent le groupe Γ. □

Cette proposition est une généralisation de résultats sur les domaines fondamentaux exposés dans [Sch74], qui est beaucoup plus complet sur le sujet.

La démonstration de cette proposition conduit naturellement à l'Algorithme 2, qui, étant donné le groupe Γ (plus précisément, on utilise un test permettant de décider si un élément de Γ_1 est ou non dans Γ), permet de calculer :

- un ensemble $\mathcal{S}$ de représentants des classes de $\Gamma\backslash\Gamma_1$ (et en particulier son cardinal μ), tel que $\bigcup_{\gamma\in\mathcal{S}} \gamma\mathcal{P}$ soit un domaine fondamental connexe pour l'action de Γ sur $\mathcal{H}$;
- un ensemble fini $\mathcal{G}$ de générateurs du groupe Γ.

Si l'on note, pour $\mathcal{X} \subset \Gamma_1$,

$$\mathcal{P}_\mathcal{X} = \{\gamma\mathcal{P} : \gamma \in \mathcal{X}\},$$

alors lors de l'exécution de l'algorithme, $\mathcal{P}_\mathcal{D}$ contient les polygones élémentaires qui ont déjà été considérés ($\mathcal{D}$ pour *done*), et $\mathcal{P}_\mathcal{V}$ contient les voisins de $\mathcal{P}_\mathcal{S}$ qui n'ont pas encore été considérés.

Au final, le nombre total d'éléments de Γ_1 qui vont avoir appartenu à l'ensemble $\mathcal{V}$ est égal au cardinal final de $\mathcal{S}$ (soit μ), plus le nombre de voisins de $\mathcal{S}$, qui est au plus en $(n-1)\mu$, moins un (puisque l'élément I n'appartient jamais à $\mathcal{V}$). On en déduit que la boucle "*while*" de l'algorithme est appelée au plus $n\mu$ fois. Le temps d'exécution d'une de ces boucles est directement proportionnel au nombre d'éléments dans l'ensemble $\mathcal{S}$ courant, soit au plus μ. On en déduit donc une complexité dans le pire des cas en

$$O(n\mu^2).$$

Algorithme : `ComputeFDAndGenerators`

Entrée : $\Gamma \subset \Gamma_1$

Sortie : un ensemble $\mathcal{S}$ de représentants des classes de $\Gamma\backslash\Gamma_1$, et un ensemble fini $\mathcal{G}$ de générateurs de Γ

$\mathcal{S} \leftarrow \{I\}$;
$\mathcal{D} \leftarrow \{I\}$;
$\mathcal{V} \leftarrow \{\gamma_j\}_{j\in[1,n]}$;
$\mathcal{G} \leftarrow \emptyset$;
while $\mathcal{V} \neq \emptyset$ **do**
  choisir $\gamma \in \mathcal{V}$;
  $t \leftarrow$ true;
  for $\gamma' \in \mathcal{S}$ **do**
    if $\gamma'\gamma^{-1} \in \Gamma$ **then**
      $t \leftarrow$ false;
      $\mathcal{G} \leftarrow \mathcal{G} \cup \{\gamma'\gamma^{-1}\}$;
    end
  end
  if t **then**
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{\gamma\}$;
    $\mathcal{V} \leftarrow \mathcal{V} \cup (\{\gamma\gamma_j : j \in [1,n]\} \setminus \mathcal{D})$;
  end
  $\mathcal{V} \leftarrow \mathcal{V} \setminus \{\gamma\}$;
  $\mathcal{D} \leftarrow \mathcal{D} \cup \{\gamma\}$;
end
return $(\mathcal{S}, \mathcal{G})$;

Algorithme 2: Domaine fondamental et générateurs pour un sous-groupe de Γ_1

2.2 Formes et fonctions modulaires en genre 1

2.2.1 Définitions

Fixons dans cette section Γ un sous-groupe d'indice fini de Γ_1. Notons qu'alors, il existe nécessairement un entier $r > 0$ tel que $T^r \in \Gamma$. Pour voir cela, il suffit de considérer les classes de T, T^2,... dans $\Gamma\backslash\Gamma_1$: comme Γ est d'indice fini dans Γ_1, le quotient est fini, donc il existe deux entiers r_1 et r_2 tels que T^{r_1} et T^{r_2} soient équivalents modulo l'action à gauche de Γ, et il suffit alors de poser $r = |r_1 - r_2|$.

Définition 2.4 (forme modulaire) *Une* forme modulaire *de poids k pour Γ est une fonction $f : \mathcal{H} \to \mathbb{C}$ telle que*

1. *pour tous* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *et* $\tau \in \mathcal{H}$,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau);$$

2. *f est holomorphe sur $\mathcal{H}$;*
3. *f est holomorphe aux pointes.*

Explicitons la condition (3) : soit f une fonction vérifiant les conditions (1) et (2) ci-dessus. Nous avons vu plus haut que le groupe Γ contient nécessairement un élément de la forme T^r ($r > 0$), donc f est en particulier r-périodique, et admet un développement de Fourier de la forme

$$f(\tau) = \sum_{n \in \mathbb{Z}} f_n \exp\left(\frac{2\pi i \tau n}{r}\right).$$

La fonction f est dite *holomorphe à l'infini* si $f_n = 0$ pour $n < 0$.

Les *pointes* (de Γ) sont les images de $\mathbb{Q} \cup \{\infty\}$ (l'orbite de ∞ par Γ_1) dans $\Gamma\backslash\widehat{\mathcal{H}}$. Soit alors $\frac{a}{c} \in \mathbb{Q}$, il existe un élément de Γ_1 de la forme $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et l'on a $\frac{a}{c} = \gamma\infty$. La fonction

$$\begin{array}{rccc} f_\gamma : & \mathcal{H} & \to & \mathbb{C} \\ & \tau & \mapsto & (c\tau + d)^{-k} f(\gamma\tau) \end{array}$$

vérifie les conditions (1) et (2) ci-dessus pour le groupe $\gamma\Gamma\gamma^{-1}$, et on dit que f est *holomorphe en* $\frac{a}{c}$ (plus précisément en la pointe correspondant à $\frac{a}{c}$) si la fonction f_γ est holomorphe à l'infini.

Notons que toute forme modulaire de poids impair est identiquement nulle*. En effet, supposons que f soit une forme modulaire de poids impair k pour un sous-groupe $\Gamma \subset \Gamma_1$. Soit alors $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que son image dans Γ_1 soit dans Γ (il s'agit justement d'un cas où il est peu commode d'identifier, comme nous le faisons par ailleurs, les éléments de $\mathrm{SL}_2(\mathbb{Z})$ avec leur classe dans Γ_1). Alors on a bien sûr $\gamma\tau = (-\gamma)\tau$, donc

$$f\left((-\gamma)\tau\right) = (-c\tau - d)^k f(\tau) = -(c\tau + d)^k f(\tau) = -f(\gamma\tau),$$

ce qui implique la nullité de f.

*Ceci est vrai pour la définition que nous avons donnée des formes modulaires, qui sont modulaires relativement à des sous-groupes de Γ_1 et non de $\mathrm{SL}_2(\mathbb{Z})$. Il existe des définitions plus générales des formes modulaires qui impliquent l'existence de formes de poids impair, voire de formes de poids fractionnaire.

Définition 2.5 (fonction modulaire) *Une* fonction modulaire *pour* Γ *est une fonction*

$$f : \mathcal{H} \to \mathbb{C}$$

telle que

1. *pour tous* $\gamma \in \Gamma$ *et* $\tau \in \mathcal{H}$,
$$f(\gamma\tau) = f(\tau)$$
(on dit que f *est invariante sous l'action de* Γ*) ;*
2. f *est méromorphe sur* $\mathcal{H}$ *;*
3. f *est méromorphe aux pointes de* Γ*.*

La dernière condition est tout à fait similaire à celle d'holomorphie aux pointes vue dans la définition précédente. Soit $r > 0$ tel que $T^r \in \Gamma$ et soit f une fonction vérifiant les conditions 1. et 2. ci-dessus : elle est r-périodique, donc admet un développement de Fourier de la forme

$$f(\tau) = \sum_{n\in\mathbb{Z}} f_n \exp\left(\frac{2\pi i\tau n}{r}\right).$$

La fonction f est dite *méromorphe en l'infini* s'il existe $n_0 \in \mathbb{Z}$ tel que $f_n = 0$ pour $n < n_0$.

Soit maintenant $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$. La fonction $f_\gamma : \tau \mapsto f(\gamma\tau)$ vérifie encore les conditions 1. et 2. pour le groupe $\gamma\Gamma\gamma^{-1}$, et on dit que que f *est méromorphe en* $\frac{a}{c}$ si la fonction f_γ est méromorphe à l'infini.

Notons que si $\{\gamma_j\}_{j\in J}$ est un ensemble de représentants des classes de $\Gamma\backslash\Gamma_1$ et que l'on note $\gamma_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$, alors f est holomorphe (resp. méromorphe) aux pointes de Γ si et seulement si elle l'est à l'infini et en les $\frac{a_j}{c_j}$, pour $j \in J$.

2.2.2 Les theta constantes

Définition

Définition 2.6 (theta constantes) *Nous appellerons* theta constantes *les trois fonctions* θ_0, θ_1 *et* θ_2, *de* $\mathcal{H}$ *dans* $\mathbb{C}$, *définies par*

$$\theta_0(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2},$$

$$\theta_1(\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}$$

et

$$\theta_2(\tau) = \sum_{n\in\mathbb{Z}} q^{\left(n+\frac{1}{2}\right)^2},$$

pour tout $\tau \in \mathcal{H}$, *avec* $q = \exp(\pi i\tau)$[†].

[†]Notons que beaucoup utilisent plutôt la notation $q = \exp(2\pi i\tau)$: notre choix semble cependant plus adapté pour travailler avec les theta constantes, c'est d'ailleurs historiquement ce qui a d'abord été utilisé.

Notons que, plus généralement, on définit *la fonction theta* comme suit :

$$\begin{array}{rccl} \theta: & \mathbb{C}\times\mathcal{H} & \to & \mathbb{C} \\ & (z,\tau) & \mapsto & \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z). \end{array}$$

Les theta constantes, en général, sont définies à un facteur près comme les valeurs, à τ fixé, de la fonction θ en les points $z \in \frac{1}{\ell}\mathbb{Z} + \frac{\tau}{\ell}\mathbb{Z}$ pour un entier ℓ fixé (ce sont donc des fonctions de τ uniquement). On parle alors de theta constantes (puisque l'argument z ne varie pas) de caractéristique $\frac{1}{\ell}$. Les plus connues (celles que nous avons introduites), sont les theta constantes de caractéristique $\frac{1}{2}$, et parle alors souvent simplement de theta constantes, en omettant la caractéristique. On vérifie en effet facilement que :

$$\theta_0(\tau) = \theta(0,\tau),$$

$$\theta_1(\tau) = \theta\left(\frac{1}{2},\tau\right)$$

et

$$\theta_2(\tau) = \exp\left(\frac{\pi i\tau}{4}\right)\theta\left(\frac{\tau}{2},\tau\right).$$

Le fait que, pour tout $\tau\in\mathcal{H}$, la fonction $z\mapsto\theta(z,\tau)$ soit 1-périodique et que

$$\theta(z+\tau,\tau) = \exp(\pi i\tau + 2\pi i z)\theta(z,\tau)$$

explique que l'on se restreint, pour les theta constantes de caractéristiques $\frac{1}{\ell}$, aux valeurs de z de la forme $\frac{a+b\tau}{\ell}$, avec $a,b\in[0,\ell-1]$.

On pourrait par ailleurs définir une quatrième theta constante de caractéristique $\frac{1}{2}$ par

$$\theta_3(\tau) = \exp\left(\frac{\pi i\tau}{4}\right)\theta\left(\frac{1+\tau}{2},\tau\right),$$

mais cette fonction est identiquement nulle (Proposition 5.1).

Le terme "theta constante" en français est relativement mal choisi. C'est une traduction littérale de l'anglais *theta constants*, dont le sens est expliqué plus haut (ce sont, à un facteur près, des valeurs de la fonction $z\mapsto\theta(z,\tau)$ en des points bien déterminés). On les désigne aussi parfois sous leur nom allemand de *Thetanullwerte*.

Propriétés

La fonction θ (et ses dérivés, dont les theta constantes) est omniprésente en théorie des nombres. Elle vérifie un nombre relativement impressionnant de propriétés, parfois surprenantes. Le but de cette section n'est certainement pas d'être exhaustif, mais d'introduire certaines de ces propriétés qui nous semblent importantes, et que l'on réutilisera par la suite. Pour des références beaucoup plus complètes, nous renvoyons à [Web02, Mum84a, Igu72].

On commencera par noter que la convergence des theta constantes définies par des séries en q est uniforme sur tout compact de $\mathcal{H}$, et les theta constantes sont toutes trois analytiques sur le demi-plan de Poincaré.

Nous nous intéressons maintenant à l'action des éléments du groupe modulaire elliptique Γ_1 sur les (carrés des) theta constantes.

Proposition 2.4 *Pour tout $\tau\in\mathcal{H}$, on a*

$$\begin{array}{rcl} \theta_0^2(T\tau) & = & \theta_1^2(\tau), \\ \theta_1^2(T\tau) & = & \theta_0^2(\tau), \\ \theta_2^2(T\tau) & = & i\theta_2^2(\tau), \end{array}$$

et

$$\begin{aligned}\theta_0^2(S\tau) &= -i\tau\theta_0^2(\tau),\\ \theta_1^2(S\tau) &= -i\tau\theta_2^2(\tau),\\ \theta_2^2(S\tau) &= -i\tau\theta_1^2(\tau).\end{aligned}$$

DÉMONSTRATION : Les formules de transformation des theta constantes sous l'action de T se montrent directement à partir de leur définition comme séries en q. Pour l'action de S, plusieurs démonstrations existent. La manière la plus classique de procéder est certainement d'utiliser la formule de sommation de Poisson, comme illustré ci-dessous (cette méthode est par exemple exposée dans [Mum84a, pages 28–33]). Une technique alternative de démonstration est exposée dans [Cou03].

Pour ce qui concerne θ_1^2 par exemple, pour tout $\tau \in \mathcal{H}$ on a (d'après la formule de Poisson) :

$$\begin{aligned}\theta_1(S\tau) &= \sum_{n\in\mathbb{Z}} \exp\left(-\frac{\pi i n^2}{\tau} - \pi i n\right)\\ &= \sum_{n\in\mathbb{Z}} \int_{\mathbb{R}} \exp\left(-\frac{\pi i x^2}{\tau} - \pi i x - 2\pi i n x\right) dx\\ &= \sum_{n\in\mathbb{Z}} \int_{\mathbb{R}} \exp\left(-\frac{\pi i}{\tau}(x^2 + 2n\tau x + x\tau)\right) dx.\end{aligned}$$

Via les changements de variable $y = x + \left(n + \frac{1}{2}\right)\tau$, on a donc

$$\begin{aligned}\theta_1(S\tau) &= \sum_{n\in\mathbb{Z}} \int_{\mathbb{R}} \exp\left(-\frac{\pi i}{\tau}\left(y^2 - \left(n+\frac{1}{2}\right)^2 \tau^2\right)\right) dy\\ &= \left(\int_{\mathbb{R}} \exp\left(-\frac{\pi i y^2}{\tau}\right) dy\right) \sum_{n\in\mathbb{Z}} \exp\left(\pi i \left(n+\frac{1}{2}\right)^2 \tau\right)\\ &= \left(\int_{\mathbb{R}} \exp\left(-\frac{\pi i y^2}{\tau}\right) dy\right) \theta_2(\tau).\end{aligned}$$

Pour finir, le calcul est classique :

$$\left(\int_{\mathbb{R}} \exp\left(-\frac{\pi i y^2}{\tau}\right) dy\right)^2 = \int_{\mathbb{R}^2} \exp\left(-\frac{\pi i}{\tau}(x^2+y^2)\right) dxdy,$$

donc en coordonnées polaires

$$\begin{aligned}\left(\int_{\mathbb{R}} \exp\left(-\frac{\pi i y^2}{\tau}\right) dy\right)^2 &= \int_0^{2\pi}\int_0^{+\infty} \exp\left(-\frac{\pi i r^2}{\tau}\right) r dr d\phi\\ &= \frac{2\tau}{i}\int_0^{+\infty} R\exp(-R^2) dR\\ &= -i\tau,\end{aligned}$$

ce qui prouve donc que $\theta_1^2(S\tau) = -i\tau\theta_2^2(\tau)$. Les autres formules se prouvent de façon similaire. □

La Proposition 5.4, beaucoup plus générale, permet de calculer la formule de transformation des carrés de theta constantes sous l'action d'un élément quelconque de Γ_1, *à une racine quatrième de l'unité près.*

Notons maintenant que si, pour $k \geqslant 1$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$, on pose

$$e_{k,\gamma}(\tau) = (c\tau + d)^k,$$

alors pour tous $\gamma_1, \gamma_2 \in \Gamma_1$, $k \geqslant 1$ et $\tau \in \mathcal{H}$, on a

$$e_{k,\gamma_1\gamma_2}(\tau) = e_{k,\gamma_1}(\gamma_2\tau)e_{k,\gamma_2}(\tau).$$

D'après ce qui précède, pour tous $\tau \in \mathcal{H}$ et $j \in [0,2]$,

$$\theta_j^2(S\tau) = -ie_{1,S}(\tau)\theta^2_{\sigma_S(j)}(\tau)$$

et

$$\theta_j^2(T\tau) = e_{1,T}(\tau)\theta^2_{\sigma_T(j)}(\tau),$$

où σ_S et σ_T sont des bijections de $[0,2]$. Donc, comme S et T engendrent le groupe Γ_1, on en déduit que pour tout $\gamma \in \Gamma_1$, il existe une racine quatrième de l'unité ω_γ et une bijection σ_γ de $[0,2]$ telles que, pour tout $\tau \in \mathcal{H}$,

$$\theta_j^2(\gamma\tau) = \omega_\gamma e_{1,\gamma}(\tau)\theta^2_{\sigma_\gamma(j)}(\tau).$$

Nous allons maintenant expliciter la bijection σ_γ. Pour cela, nous introduisons une nouvelle notation pour les theta constantes (qui correspond plus aux notations habituelles). Nous les indexons par deux éléments de $\mathbb{Z}/2\mathbb{Z}$ comme suit : $\theta_0 = \theta_{0,0}$, $\theta_1 = \theta_{0,1}$ et $\theta_2 = \theta_{1,0}$. Avec cette notation, σ_γ devient une bijection de $(\mathbb{Z}/2\mathbb{Z})^2$, qui peut être déterminée explicitement *via* le résultat suivant :

Proposition 2.5 *Pour tous* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$ *et* $(x,y) \in (\mathbb{Z}/2\mathbb{Z})^2$, *on a*

$$\sigma_\gamma\,(x,y) = (x + cd, y + ab)\gamma$$

(où la multiplication de droite est une simple multiplication matricielle, et où l'on considère les coefficients de γ *comme des éléments de* $\mathbb{Z}/2\mathbb{Z}$*).*

Démonstration : Comme S et T sont des générateurs de Γ_1, il suffit de vérifier que la règle de calcul pour la bijection $\sigma_{\cdot\cdot}$ donnée dans l'énoncé vérifie bien, pour tout $\gamma \in \Gamma_1$,

$$\sigma_{S\gamma} = \sigma_\gamma \circ \sigma_S$$

et

$$\sigma_{T\gamma} = \sigma_\gamma \circ \sigma_T,$$

ce qui se fait facilement. □

Nous nous intéressons maintenant aux valeurs prises par les theta constantes sur le domaine fondamental $\mathcal{F}$. Nous commençons par le résultat (trivial) suivant, dont nous ferons largement usage dans le reste de ce mémoire :

Lemme 2.1 *Pour tous* $x \in [0,1[$ *et* $N \in \mathbb{N}$, *si* $f : \mathbb{N} \to \mathbb{R}$ *est une fonction telle que*

$$f(n+1) - f(n) \geqslant 1$$

pour $n \geqslant N$, *alors*

$$\sum_{n \geqslant N} x^{f(n)} \leqslant \frac{x^{f(N)}}{1-x}.$$

Démonstration : On a $f(n+k) \geqslant f(n)+k$ pour tout $k \geqslant 0$, d'où

$$\sum_{n \geqslant N} x^{f(n)} \leqslant \sum_{k \geqslant 0} x^{f(N)+k} \leqslant \frac{x^{f(N)}}{1-x}.$$

□

Proposition 2.6 *Pour tout $\tau \in \mathcal{H}$ tel que $\mathrm{Im}\,(\tau) \geqslant \frac{\sqrt{3}}{2}$ (en particulier pour $\tau \in \mathcal{F}$), on a*

$$|\theta_j(\tau) - 1| \leqslant 0.141$$

pour $j \in \{0,1\}$, et

$$\left| \frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - 1 \right| \leqslant 0.005.$$

Démonstration : Soit $\tau \in \mathcal{H}$ tel que $\mathrm{Im}\,(\tau) \geqslant \frac{\sqrt{3}}{2}$, et soit $\varepsilon \in \{0,1\}$, alors

$$\begin{aligned} |\theta_\varepsilon(\tau) - 1| &= \left| 2 \sum_{n \geqslant 1} (-1)^\varepsilon q^{n^2} \right| \\ &\leqslant 2 \sum_{n \geqslant 1} |q|^{n^2} \\ &\leqslant 2 \sum_{n \geqslant 1} |q|^{n} \\ &\leqslant \frac{2\,|q|}{1-|q|}, \end{aligned}$$

et comme $|q| \leqslant \exp\left(-\pi\frac{\sqrt{3}}{2}\right)$, un calcul numérique montre que

$$|\theta_\varepsilon(\tau) - 1| < 0.141.$$

Par ailleurs, on a aussi

$$\begin{aligned} \theta_2(\tau) &= 2 \sum_{n \geqslant 0} q^{\left(n+\frac{1}{2}\right)^2} \\ &= 2q^{\frac{1}{4}} \left(1 + \sum_{n \geqslant 1} q^{n^2+n} \right), \end{aligned}$$

donc

$$\begin{aligned} \left| \frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - 1 \right| &= \left| \sum_{n \geqslant 1} q^{n^2+n} \right| \\ &\leqslant \sum_{n \geqslant 2} |q|^{n} \\ &\leqslant \frac{|q|^2}{1-|q|}, \end{aligned}$$

et comme plus haut, un calcul numérique montre que

$$\left| \frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - 1 \right| < 0.005.$$

□

Cette proposition implique directement qu'aucune des θ_j ($j \in [0,2]$) ne s'annule sur $\mathcal{F}$.

Proposition 2.7 *Aucune des trois theta constantes ne s'annule sur $\mathcal{H}$.*

Démonstration : Soient $\tau \in \mathcal{H}$ et $j \in [0,2]$, alors il existe $\gamma \in \Gamma_1$ et $\tau' \in \mathcal{F}$ tels que $\tau = \gamma\tau'$, donc d'après la remarque qui précède,

$$\begin{aligned} \theta_j^2(\tau) &= \theta_j^2(\gamma\tau') \\ &= \omega_\gamma e_{1,\gamma}(\tau)\theta^2_{\sigma_\gamma(j)}(\tau'). \end{aligned}$$

Il est clair que $e_{1,\gamma}(\tau) \neq 0$, et la Proposition 2.6 montre que $\theta^2_{\sigma_\gamma(j)}(\tau') \neq 0$, ce qui conclut. □

Proposition 2.8 *La fonction θ_0^8 est une forme modulaire de poids 4 pour le groupe*

$$\Gamma_{1,2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : ab \equiv 0 \bmod 2, cd \equiv 0 \bmod 2 \right\}.$$

Les fonctions θ_1^8 et θ_2^8 sont des formes modulaires de poids 4 pour les groupes $\gamma_1^{-1}\Gamma_{1,2}\gamma_1$ et $\gamma_2^{-1}\Gamma_{1,2}\gamma_2$, avec $\gamma_1 = T$ et $\gamma_2 = STS$.

Démonstration : La preuve la plus simple consiste à calculer un ensemble de générateurs de $\Gamma_{1,2}$ (*via* l'Algorithme 2 par exemple). En décomposant ces générateurs en produits de S et T et en utilisant la Proposition 2.4, il est facile de montrer que la fonction θ_0^8 est invariante sous l'action de chacun de ces générateurs, donc (d'après la remarque qui précède), elle est invariante sous l'action de $\Gamma_{1,2}$. Cette invariance est aussi un corollaire direct de la Proposition 5.4

Il est par ailleurs clair que θ_0^8 est holomorphe sur $\mathcal{H}$, et la condition d'holomorphie aux pointes peut se tester "à la main" (en utilisant des représentants des classes de $\Gamma_{1,2}\backslash\Gamma_1$ que l'on peut encore calculer *via* l'Algorithme 2 par exemple).

Le résultat pour θ_1^8 (resp. pour θ_2^8) est une conséquence directe du fait (aisément vérifiable *via* la Proposition 2.4) que pour tout $\tau \in \mathcal{H}$,

$$\theta_0^8(\gamma_1\tau) = \theta_1^8(\tau) = e_{4,\gamma_1}(\tau)\theta_1^8(\tau)$$

et

$$\theta_0^8(\gamma_2\tau) = (\tau - 1)^4\theta_2^8(\tau) = e_{4,\gamma_2}(\tau)\theta_2^8(\tau).$$

□

Une autre propriété importante pour nous est la suivante :

Proposition 2.9 (formules de duplication) *Pour tout $\tau \in \mathcal{H}$, on a*

$$\begin{aligned} \theta_0^2(2\tau) &= \tfrac{\theta_0^2(\tau)+\theta_1^2(\tau)}{2}, \\ \theta_1^2(2\tau) &= \theta_0(\tau)\theta_1(\tau), \\ \theta_2^2(2\tau) &= \tfrac{\theta_0^2(\tau)-\theta_1^2(\tau)}{2}. \end{aligned}$$

DÉMONSTRATION : Ceci peut être prouvé directement à partir des définitions des theta constantes. C'est aussi un cas particulier ($g = 1$) de la Proposition 5.5, dont la démonstration est tout aussi élémentaire. □

Cette dernière propriété était déjà connue de Gauss (qui utilisait les notations $p = \theta_0$, $q = \theta_1$ et $r = \theta_2$) [Gau27, pages 361–403], et même de Jacobi [Jac91].

Proposition 2.10 (égalité de Jacobi) *Pour tout $\tau \in \mathcal{H}$,*

$$\theta_0^4(\tau) = \theta_1^4(\tau) + \theta_2^4(\tau).$$

DÉMONSTRATION : C'est une conséquence directe de la formule de duplication (Proposition 2.9). En effet, cette formule montre que pour tout $\tau \in \mathcal{H}$,

$$\begin{aligned} \theta_1^4(\tau) + \theta_2^4(\tau) &= \theta_0^2\left(\frac{\tau}{2}\right)\theta_1^2\left(\frac{\tau}{2}\right) + \left(\frac{\theta_0^2\left(\frac{\tau}{2}\right) - \theta_1^2\left(\frac{\tau}{2}\right)}{2}\right)^2 \\ &= \left(\frac{\theta_0^2\left(\frac{\tau}{2}\right) + \theta_1^2\left(\frac{\tau}{2}\right)}{2}\right)^2 \\ &= \theta_0^4(\tau). \end{aligned}$$

□

Proposition 2.11 *Pour tout $\tau \in \mathcal{H}$, on a*

$$\begin{aligned} \theta_0^2\left(\tfrac{\tau}{2}\right) &= \theta_0^2(\tau) + \theta_2^2(\tau), \\ \theta_1^2\left(\tfrac{\tau}{2}\right) &= \theta_0^2(\tau) - \theta_2^2(\tau), \\ \theta_2^2\left(\tfrac{\tau}{2}\right) &= 2\theta_0(\tau)\theta_2(\tau). \end{aligned}$$

DÉMONSTRATION : En posant $\tau' = 2\tau$, les deux premières égalités se prouvent aisément en faisant la somme et la différence des première et troisième égalités énoncées dans la Proposition 2.9. La troisième égalité découle alors de l'égalité de Jacobi (Proposition 2.10), l'indétermination dans le signe pouvant être levée en considérant les développements en q. □

Lemme 2.2 *Pour tout $\tau \in \mathcal{H}$,*

$$\lim_{n\to+\infty} \theta_0(2^n\tau) = \lim_{n\to+\infty} \theta_1(2^n\tau) = 1,$$

et

$$\lim_{n\to+\infty} \theta_2(2^n\tau) = 0.$$

DÉMONSTRATION : Soit $\tau \in \mathcal{H}$, alors $q(2^n\tau) = \exp(\pi i 2^n \tau)$, donc $\lim_{n\to+\infty} |q(2^n\tau)| = 0$, et comme nous avons vu dans la démonstration de la Proposition 2.6 que, pour $j \in [0, 1]$,

$$|\theta_j(\tau) - 1| \leqslant \frac{2\,|q|}{1 - |q|},$$

ceci suffit à montrer les deux premières limites. La troisième s'en déduit directement *via* l'égalité de Jacobi (Proposition 2.10). □

Nous prouvons maintenant le lemme suivant, qui nous sera utile au Chapitre 8 :

Lemme 2.3 *Pour tout compact K inclus dans $\mathcal{F}$, il existe une constante $\varepsilon_K > 0$ telle que, pour tout $(\omega, j, k) \in \big\{(x, y, z) \in \{\pm i, \pm 1\} \times [0, 3]^2 : y < z\big\} \setminus \{(1, 1, 2)\}$,*

$$\mathrm{Max}_{\tau \in K} \left|\omega\theta_j^2(\tau) - \theta_k^2(\tau)\right| \geqslant \varepsilon_K.$$

Démonstration : Nous allons en fait montrer que, pour tout $(\omega, j, k) \in \{\pm i, \pm 1\} \times [0, 3]^2$ tel que $j < k$, la fonction $\omega\theta_j^2 - \theta_k^2$ ne s'annule dans $\mathcal{F}$ que si $(\omega, j, k) = (1, 1, 2)$, ce qui suffit pour montrer le lemme.

Soient $j, k \in [0, 3]$ tels que $j < k$, on distingue alors plusieurs cas :

- Si $k = 3$ (donc $\theta_k = 0$), on a vu plus haut que θ_j^2 ne s'annule pas sur $\mathcal{F}$.
- Si $j = 0$ et $k = 1$, alors l'égalité de Jacobi et le fait que θ_2 ne s'annule pas sur $\mathcal{F}$ montrent que $\theta_0^2 - \theta_1^2$ ne s'annule pas non plus sur $\mathcal{F}$. Par ailleurs, la Proposition 2.6 montre que pour $u \in \{0, 1\}$ et $\tau \in \mathcal{F}$,

  $$|\mathrm{Arg}\,(\theta_u(\tau))| \leqslant \mathrm{Arcsin}(0.141) < \frac{\pi}{20},$$

  donc

  $$\left|\mathrm{Arg}\left(\theta_u^2(\tau)\right)\right| < \frac{\pi}{10}. \tag{2.1}$$

  On en déduit directement que pour $\omega \in \{\pm i, -1\}$, la fonction $\omega\theta_0^2 - \theta_1^2$ ne s'annule pas sur $\mathcal{F}$.
- Si $j = 0$ et $k = 2$, alors comme ci-dessus, l'égalité de Jacobi et le fait que θ_1 ne s'annule pas sur $\mathcal{F}$ montrent que $\theta_0^2 - \theta_2^2$ ne s'annule pas sur $\mathcal{F}$. Par ailleurs, la Proposition 2.6 montre que

  $$\left|\mathrm{Arg}\left(\frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - 1\right)\right| < \mathrm{Arcsin}(0.005),$$

  et comme $\tau \in \mathcal{F}$, on a $|\mathrm{Re}\,(\tau)| \leqslant \frac{1}{2}$ donc $\left|\mathrm{Arg}\left(2q^{\frac{1}{4}}\right)\right| \leqslant \frac{\pi}{8}$ et

  $$|\mathrm{Arg}\,(\theta_2(\tau))| \leqslant \frac{\pi}{8} + \mathrm{Arcsin}(0.005) < \frac{\pi}{7}.$$

  Comme $\frac{\pi}{7} + \frac{\pi}{10} < \frac{\pi}{4}$, ceci montre avec (2.1) que si $\omega \in \{\pm i, -1\}$ la fonction $\omega\theta_0^2 - \theta_2^2$ ne s'annule pas sur $\mathcal{F}$.
- Si $j = 1$ et $k = 2$, le même argument que ci-dessus permet de montrer que pour $\omega \in \{\pm i, -1\}$, la fonction $\omega\theta_1^2 - \theta_2^2$ ne s'annule pas sur $\mathcal{F}$.

□

On notera que la fonction $\theta_1^2 - \theta_2^2$, elle, s'annule en $\tau = i$. Pour le voir, il suffit de considérer l'action de S sur les theta constantes (Proposition 2.4), ainsi que le fait que $Si = i$.

Nous énonçons enfin un dernier résultat sur les theta constantes, qui nous sera utile au Chapitre 4 :

Proposition 2.12 *Pour tout $\tau \in \mathcal{H}$,*

$$4\frac{d}{d\tau}\log\frac{\theta_{10}}{\theta_{01}}(\tau) = i\pi\theta_{00}^4(\tau),$$

$$4\frac{d}{d\tau}\log\frac{\theta_{00}}{\theta_{01}}(\tau) = i\pi\theta_{10}^4(\tau),$$

et

$$4\frac{d}{d\tau}\log\frac{\theta_{10}}{\theta_{00}}(\tau) = i\pi\theta_{01}^4(\tau).$$

Démonstration : Nous ne connaissons pas de démonstration "élémentaire" de ce résultat. Nous renvoyons à [Web02, page 82], qui utilise des propriétés de la fonction θ de deux variables. □

2.2.3 La fonction η de Dedekind

La fonction η de Dedekind est définie, pour $\tau \in \mathcal{H}$, par

$$\eta(\tau) = q^{\frac{1}{12}} \prod_{n \geqslant 1} (1 - q^{2n}),$$

ou, de manière équivalente, par

$$\eta(\tau) = q^{\frac{1}{12}} \left(1 + \sum_{n \geqslant 1} (-1)^{n+1} \left(q^{n(3n-1)} + q^{n(3n+1)} \right) \right),$$

où l'on rappelle que $q = \exp(\pi i \tau)$. Le théorème prouvant l'équivalence entre ces deux définitions porte le nom de théorème des nombres pentagonaux d'Euler [Eul14], et on peut en trouver une démonstration plus moderne, utilisant des propriétés de la fonction θ (de deux variables), dans [Mum84a, pages 70–71].

Cette fonction est liée aux theta constantes par les relations suivantes :

Proposition 2.13 *Pour tout $\tau \in \mathcal{H}$,*

$$\theta_0(\tau) = q^{-\frac{1}{12}} \frac{\eta^2\left(\frac{\tau+1}{2}\right)}{\eta(\tau)},$$

$$\theta_1(\tau) = \frac{\eta^2\left(\frac{\tau}{2}\right)}{\eta(\tau)},$$

$$\theta_2(\tau) = 2\frac{\eta^2(2\tau)}{\eta(\tau)}$$

et

$$\eta^3(\tau) = \frac{\theta_0(\tau)\theta_1(\tau)\theta_2(\tau)}{2}.$$

Démonstration : Nous renvoyons à [Web02, pages 112–116]. □

Nous ne nous étendrons pas plus sur la fonction η, qui ne jouera pas un rôle central par la suite. Comme elle est parfois utilisée pour définir des fonctions modulaires (voir la Section 2.3.2 par exemple), et que notre travail porte sur l'évaluation de ces fonctions, il importe surtout de noter que, d'après la quatrième des égalités ci-dessus, un algorithme permettant d'évaluer les theta constantes donne un algorithme permettant d'évaluer η (il faut extraire une racine troisième, ce qui peut se faire rapidement par des itérations de Newton, la bonne racine pouvant être choisie en calculant une approximation de la valeur de η à faible précision en utilisant son développement en q, ce qui permet aussi d'initialiser les itérations de Newton).

2.2.4 Construction de fonctions modulaires

Les fonctions k et k'

On définit les fonctions k et k' de $\mathcal{H}$ dans $\mathbb{C}$ par

$$k(\tau) = \frac{\theta_2^2(\tau)}{\theta_0^2(\tau)}$$

et

$$k'(\tau) = \frac{\theta_1^2(\tau)}{\theta_0^2(\tau)}$$

pour tout $\tau \in \mathcal{H}$.

L'égalité de Jacobi 2.10 implique directement que

$$k^2 + k'^2 = 1. \tag{2.2}$$

La Proposition 2.7 montre que les fonctions k et k' ne s'annulent pas sur $\mathcal{H}$, et l'égalité ci-dessus montre par ailleurs que ni k ni k' ne prend la valeur 1 sur $\mathcal{H}$.

Par ailleurs, les formules de transformation des carrés des theta constantes (Proposition 2.4) montrent que, pour tout $\tau \in \mathcal{H}$,

$$k(T\tau) = i\frac{k(\tau)}{k'(\tau)}, \qquad k'(T\tau) = \frac{1}{k'(\tau)},$$

$$k(S\tau) = k'(\tau) \quad \text{et} \quad k'(S\tau) = k(\tau),$$

D'après ce qui précède, on peut se restreindre à l'étude d'une seule de ces deux fonctions k et k'. Nous allons en fait privilégier k', car nous verrons au chapitre suivant que cette fonction est intimement liée à la moyenne arithmético-géométrique.

On définit le sous-groupe $\Gamma_{k'}$ de Γ_1 par

$$\Gamma_{k'} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : b \equiv 0 \bmod 2, c \equiv 0 \bmod 4 \right\}.$$

Lemme 2.4 *L'ensemble*

$$\mathcal{G}_{k'} = \left\{ I, T, S, ST, T^{-1}S, ST^{-1}, TST, ST^2, TST^2, STS, ST^{-2}S, ST^2ST \right\}$$

est un ensemble de représentants des classes de $\Gamma_{k'}\backslash\Gamma_1$, et l'ensemble

$$\mathcal{F}_{k'} = \left\{ \tau \in \mathcal{H} : -1 \leqslant \mathrm{Re}\,(\tau) < 1, \left|\tau + \frac{3}{4}\right| \geqslant \frac{1}{4}, \left|\tau + \frac{1}{4}\right| > \frac{1}{4}, \left|\tau - \frac{1}{4}\right| \geqslant \frac{1}{4} \text{ et } \left|\tau - \frac{3}{4}\right| > \frac{1}{4} \right\}$$

(voir Figure 2.2) est un ensemble fondamental pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$. De plus, le groupe $\Gamma_{k'}$ est engendré par

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, ST^4S = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \text{ et } TST^4ST = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}.$$

Démonstration : Montrer que $\mathcal{G}_{k'}$ est un ensemble de représentants des classes de $\Gamma_{k'}\backslash\Gamma_1$ peut se faire "à la main" : on commence par montrer que pour tous $\gamma_1, \gamma_2 \in \mathcal{G}_{k'}$, $\gamma_1\gamma_2^{-1} \in \Gamma_{k'}$ implique que $\gamma_1 = \gamma_2$, ce qui montre bien que les éléments de $\mathcal{G}_{k'}$ sont dans des classes distinctes modulo l'action à gauche de $\Gamma_{k'}$. Il faut ensuite montrer que toutes les classes de $\Gamma_{k'}\backslash\Gamma_1$ ont

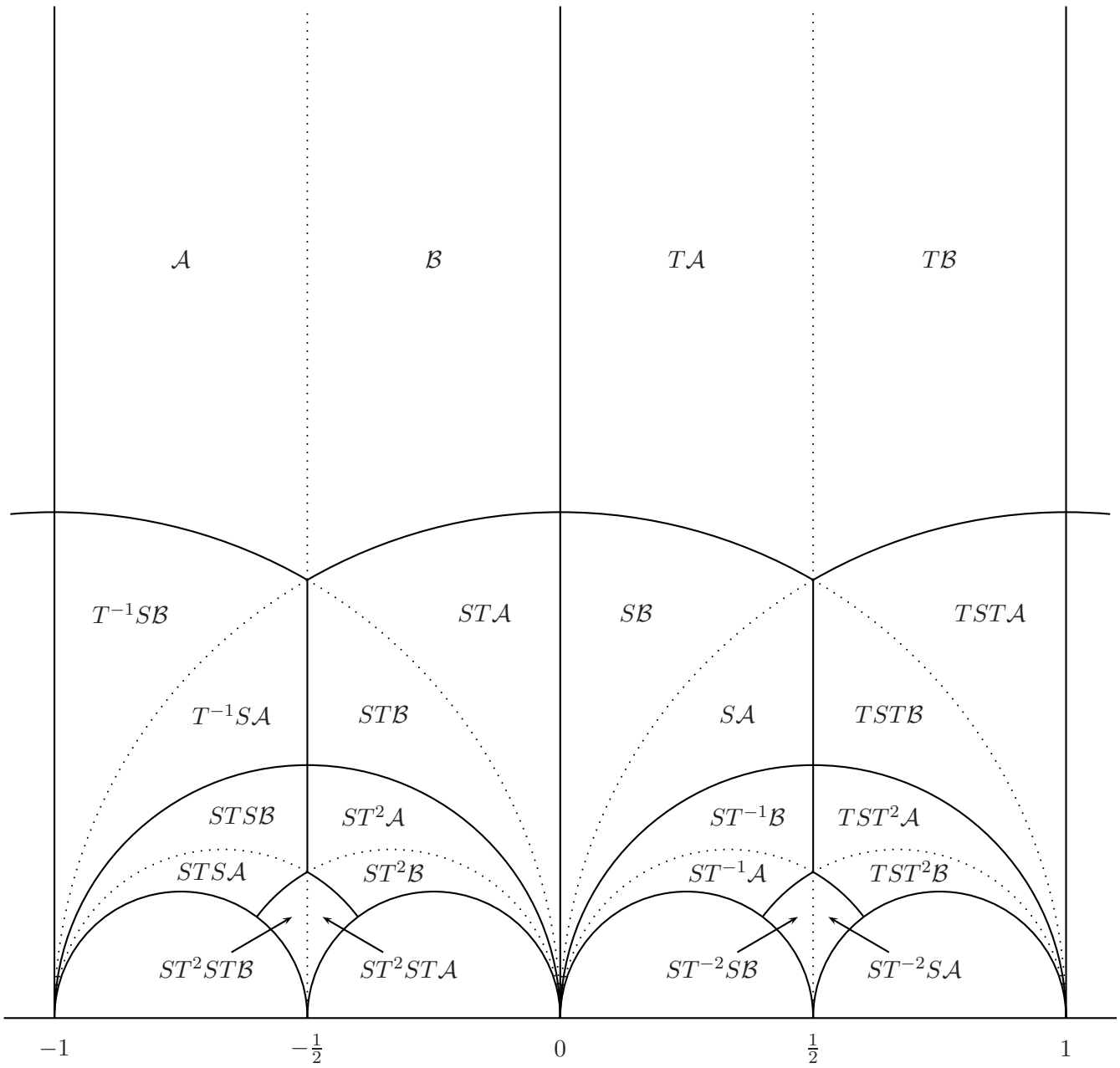

FIG. 2.2 – Le domaine fondamental $\mathcal{F}_{k'}$ pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$

bien un représentant dans $\mathcal{G}_{k'}$. Pour cela, il suffit (comme S et T engendrent Γ_1) de vérifier que pour tout $\gamma \in \mathcal{G}_{k'}$, il existe $\gamma_S, \gamma_T \in \mathcal{G}_{k'}$ tels que

$$S\gamma\gamma_S^{-1} \in \Gamma_{k'}$$

et

$$T\gamma\gamma_T^{-1} \in \Gamma_{k'}.$$

Pour montrer que $\mathcal{F}_{k'}$ est un ensemble fondamental, on commence par remarquer que si l'on définit les ensembles $\mathcal{A}$ et $\mathcal{B}$ par

$$\mathcal{A} = \left\{ \tau \in \mathcal{H} : -1 \leqslant \mathrm{Re}\,(\tau) < -\frac{1}{2} \text{ et } |\tau| \geqslant 1 \right\},$$

et

$$\mathcal{B} = \left\{ \tau \in \mathcal{H} : -\frac{1}{2} \leqslant \mathrm{Re}\,(\tau) < 0 \text{ et } |\tau| \geqslant 1 \right\}$$

alors $\mathcal{A} \cup T\mathcal{B} = \mathcal{F}'$ est un ensemble fondamental pour l'action de Γ_1 sur $\mathcal{H}$, donc si l'on pose

$$\mathcal{C} = \mathcal{A} \cup \mathcal{B},$$

alors $\mathcal{C}$ est aussi un ensemble fondamental pour l'action de Γ_1 sur $\mathcal{H}$, donc

$$\bigcup_{\gamma \in \mathcal{G}_{k'}} \gamma\mathcal{C}$$

est un ensemble fondamental pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$.

On vérifie alors facilement qu'en posant

$$\mathcal{D} = \{-1 + \lambda i : 0 < \lambda < 1\},$$

on a

$$\mathcal{F}_{k'} = \left(\bigcup_{\gamma \in \mathcal{G}_{k'}} \gamma\mathcal{C} \right) \cup \mathcal{D} \setminus T^2\mathcal{D},$$

ce qui prouve le résultat puisque $\mathcal{D}$ est équivalent à $T^2\mathcal{D}$ modulo l'action de $\Gamma_{k'}$.

Enfin, pour montrer que les trois éléments donnés sont bien des générateurs de $\Gamma_{k'}$, il suffit de remarquer qu'avec leurs inverses, ils engendrent les substitutions de bords. □

Nous pouvons maintenant prouver le résultat suivant :

Proposition 2.14 *La fonction k' est une fonction modulaire pour le groupe $\Gamma_{k'}$.*

Démonstration : On commence par vérifier que k' est invariante sous l'action de $\Gamma_{k'}$. Ceci est aisé : il suffit, en utilisant les formules de transformation des carrés des theta constantes sous l'action de S et T (Proposition 2.4), de prouver que k' est invariante sous l'action des trois générateurs de $\Gamma_{k'}$ exhibés dans le Lemme 2.4.

Il est alors facile, en utilisant les développements en q des theta constantes, de voir que k' est méromorphe sur $\mathcal{H}$, et en utilisant les représentants des classes de $\Gamma_{k'}\backslash\Gamma_1$ exhibés dans le Lemme 2.4, on montre que k' est aussi méromorphe aux pointes. □

D'après ce qui précède, la fonction k est elle modulaire pour le groupe $\Gamma_k = S\Gamma_{k'}S$, et le Lemme 2.4 permet d'obtenir des informations sur ce groupe (représentants des classes, domaine fondamental et générateurs).

Le résultat qui suit nous sera utile au Chapitre 3 :

Proposition 2.15 *Pour tout $x \in \mathbb{C} \setminus \{-1, 0, 1\}$, il existe un unique $\tau \in \mathcal{F}'_{k'}$ tel que $k'(\tau) = x$.*

Démonstration : En utilisant les mêmes techniques que pour la démonstration du Lemme 2.4, on montre que la fonction k'^2 est modulaire pour le groupe

$$\Gamma(2) = \left\{ \gamma \in \Gamma_1 : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2 \right\},$$

que l'ensemble

$$\mathcal{G}_2 = \left\{ I, T, S, ST, T^{-1}S, TST \right\},$$

est un ensemble de représentants des classes de $\Gamma(2)\backslash\Gamma_1$, et que

$$\mathcal{F}'_{\Gamma_2} = \bigcup_{\gamma \in \mathcal{G}_2} \gamma \mathcal{C}$$

est un ensemble fondamental pour l'action de $\Gamma(2)$ sur $\mathcal{H}$.

Nous renvoyons maintenant à [WW27, pages 481–484] pour une démonstration du fait que, pour tout $x \in \mathbb{C} \setminus \{0, 1\}$, il existe un unique $\tau \in \mathcal{F}'_{\Gamma_2}$ tel que $k^2(\tau) = x$ (on notera que les notations utilisées dans [WW27] sont $f = k^2$ et $g = k'^2$). L'ingrédient principal utilisé est le théorème des résidus, et l'intégration sur des contours bien choisis, ce qui rend cette démonstration relativement technique et peu éclairante. On en déduit le même résultat pour la fonction k'^2 (puisque $k^2 + k'^2 = 1$).

Remarquons que $\{I, ST^{-2}S\}$ est un ensemble de représentants des classes de $\Gamma_{k'}\backslash\Gamma_2$. En utilisant la Proposition 2.4, on montre que pour tout $\tau \in \mathcal{H}$,

$$k'(ST^{-2}S\tau) = -k'(\tau).$$

On en déduit que pour tout $x \in \mathbb{C}\backslash\{-1, 0, 1\}$, il existe un unique $\tau \in \mathcal{F}'_{\Gamma_2}$ tel que $k'^2(\tau) = x^2$, donc soit $x = k'(\tau)$, soit $x = -k'(\tau) = k'(ST^{-2}S\tau)$ (ces deux cas étant exclusif l'un de l'autre puisque k' ne s'annule pas sur $\mathcal{H}$). On en déduit le résultat. □

La fonction modulaire elliptique j

Définition 2.7 (fonction modulaire elliptique j) *La fonction $j : \mathcal{H} \to \mathbb{C}$ est définie*[‡] *par*

$$j(\tau) = 256 \frac{\left(1 - k'^2(\tau) + k'^4(\tau)\right)^3}{k'^4(\tau)\left(1 - k'^2(\tau)\right)^2}.$$

L'inégalité de Jacobi pour les fonctions k et k' (Équation (2.2)) montre que l'on a aussi

$$j(\tau) = 256 \frac{\left(1 - k^2(\tau) + k^4(\tau)\right)^3}{k^4(\tau)\left(1 - k^2(\tau)\right)^2}.$$

Toujours d'après l'Équation (2.2), le dénominateur peut se réécrire

$$k'^4(\tau)\left(1 - k'^2(\tau)\right)^2 = \left(k(\tau)k'(\tau)\right)^4,$$

[‡]Ce n'est sûrement pas la manière la plus standard de la définir, mais certains textes utilisent aussi cette définition, comme [BB87]. Pour une définition plus "standard" de la fonction j, on pourra consulter [Ser70] par exemple.

et comme nous avons vu plus haut que les fonctions k et k' ne s'annulent pas sur $\mathcal{H}$, on en déduit que j est holomorphe sur $\mathcal{H}$.

On peut aussi calculer le début du développement en q de la fonction j :

$$j(\tau) = \frac{1}{q^2} + 744 + 196884q^2 + 21493760q^4 + \dots$$

(attention au fait que nous notons $q = \exp(\pi i \tau)$, sans le facteur 2 habituel).

En particulier, ceci montre que j a un pôle simple en ∞.

Proposition 2.16 *La fonction j est une fonction modulaire pour le groupe Γ_1.*

DÉMONSTRATION : D'après ce qui précède, il suffit de vérifier l'invariance de j sous l'action de Γ_1, ou bien (plus simplement), sous l'action des générateurs S et T de Γ_1. Ceci se fait facilement à partir de la définition de j que nous avons donnée, en utilisant les formules de transformation pour k et k' données à la section précédente, ainsi que l'Équation (2.2). □

2.2.5 Quelques résultats sur les fonctions modulaires

Le résultat le plus important concernant les fonctions modulaires pour Γ_1 est très certainement le théorème suivant :

Théorème 2.1 *Pour toute fonction f modulaire pour Γ_1, il existe une fraction rationnelle $F(X) \in \mathbb{C}(X)$ telle que, pour tout $\tau \in \mathcal{H}$,*

$$f(\tau) = F\left(j(\tau)\right).$$

DÉMONSTRATION : Soit f une fonction modulaire pour le groupe Γ_1. Elle est donc méromorphe sur $\mathcal{H}$ et en ∞, donc admet un nombre fini de pôles et de zéros sur $\mathcal{F}' \cup \{\infty\}$. On note $\{\alpha_j\}_{j\in J}$ (resp. $\{\beta_k\}_{k\in K}$) l'ensemble des zéros (resp. des pôles) de f sur $\mathcal{F}' \cup \{\infty\}$, et $\{m_j\}_{j\in J}$ (resp. $\{n_k\}_{k\in K}$) leurs multiplicités. On définit alors la fonction F par

$$F(\tau) = \frac{\prod_{k\in K} \left(j(\tau) - j(\beta_k)\right)^{n_k}}{\prod_{j\in J} \left(j(\tau) - j(\alpha_j)\right)^{m_j}} f(\tau),$$

où, dans le cas où $x = \infty$, on a remplacé $(j(\tau) - j(x))$ par 1.

La fonction F est alors une fonction modulaire pour Γ_1 n'ayant ni pôle ni zéro sur $\widehat{\mathcal{H}}$: c'est donc une constante, ce qui prouve le résultat. □

Ce théorème montre que la fonction j est entièrement déterminée par le fait qu'elle est holomorphe sur $\mathcal{H}$, a un pôle simple en ∞, est modulaire pour Γ_1 et a le premier coefficient non nul de son développement en q égal à 1. C'est pourquoi l'on fait souvent référence à j comme à *la* fonction modulaire elliptique.

Proposition 2.17 *Soient Γ un sous-groupe d'indice fini de Γ_1 et f une fonction modulaire pour Γ_1. Alors il existe un polynôme $P(X, Y) \in \mathbb{C}[X, Y]$, de degré $[\Gamma_1 : \Gamma]$ en X, tel que pour tout $\tau \in \mathcal{H}$,*

$$P\left(f(\tau), j(\tau)\right) = 0.$$

DÉMONSTRATION : Soit Γ un sous-groupe d'indice fini μ de Γ_1, et soit $\{\gamma_j\}_{j\in[1,\mu]}$ un ensemble de représentants des classes de $\Gamma\backslash\Gamma_1$. Soit maintenant f une fonction modulaire pour Γ. Considérons les fonctions $(c_j)_{j\in[0,\mu-1]}$ de $\mathcal{H}$ dans $\mathbb{C}$ définies par

$$\prod_{j\in[1,\mu]} (X - f(\gamma_j\tau)) = X^\mu + \sum_{j=0}^{\mu-1} c_j(\tau)X^j,$$

pour tout $\tau \in \mathcal{H}$.

Ces fonctions sont symétriques en les $\tau \mapsto f(\gamma_j\tau)$, et comme f est modulaire pour Γ et que les γ_j forment un ensemble des représentants des classes de $\Gamma\backslash\Gamma_1$, les c_j sont invariantes sous l'action de Γ_1, et sont méromorphes sur $\mathcal{H}$ et en ∞, donc ce sont des fonctions modulaires pour Γ_1.

Le Théorème 2.1 montre alors qu'il existe des fractions rationnelles $(F_j)_{j\in[0,\mu-1]}$ telles que, pour tout $\tau \in \mathcal{H}$,

$$c_j(\tau) = F_j\left(j(\tau)\right).$$

On en déduit directement le résultat. □

2.3 Polynômes modulaires

2.3.1 Définition

Définition 2.8 (polynôme modulaire) *Soient Γ_x et Γ_y deux sous-groupes d'indice fini de Γ_1, et soient f_x et f_y deux fonctions modulaires pour Γ_x et Γ_y respectivement. Alors la Proposition 2.17 montre qu'il existe un polynôme non nul $\Phi_{f_x,f_y}(X,Y) \in \mathbb{C}[X,Y]$ tel que, pour tout $\tau \in \mathcal{H}$,*

$$\Phi\left(f_x(\tau), f_y(\tau)\right) = 0.$$

Un tel polynôme est appelé polynôme modulaire *ou* équation modulaire.

Notons que la Proposition 2.17 montre qu'un tel polynôme existe dans le cas où f_x (ou f_y) est la fonction j. Dans le cas général, il suffit de considérer le résultant de deux tels polynômes, pour éliminer j.

D'après cette définition, un polynôme modulaire est donc une relation algébrique entre deux fonctions modulaires quelconques.

Nous avons déjà rencontré quelques polynômes modulaires :

$$\Phi_{k,k'}(X,Y) = X^2 + Y^2 - 1$$

est un polynôme modulaire liant k et k', et

$$\Phi_{j,k'}(X,Y) = XY^4(1-Y^2)^2 - 256(1-Y^2+Y^4)^3$$

est un polynôme modulaire liant j et k'.

2.3.2 Polynômes modulaires pour $\Gamma^0(p)$

Définition

Pour tout nombre entier $N \geqslant 0$, on définit le groupe

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : N \mid b \right\}.$$

C'est un sous-groupe d'indice fini de Γ_1. Dans la suite, nous ne nous intéresserons qu'au cas où N est un nombre premier, que l'on notera alors ℓ.

Proposition 2.18 *Pour tout nombre premier ℓ, $\Gamma^0(\ell)$ est d'indice $\ell+1$ dans Γ_1, et*

$$\left\{\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} : j \in [0, \ell-1]\right\} \cup \left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right\}$$

est un ensemble de représentants des classes de $\Gamma^0(\ell)\backslash\Gamma_1$.

Démonstration : Soit ℓ un nombre premier, notons alors $\mathcal{S}_\ell$ l'ensemble défini dans l'énoncé de la proposition. Pour montrer que $\mathcal{S}_\ell$ est bien un ensemble de représentants des classes du groupe quotient, il suffit de montrer d'une part que deux éléments distincts de $\mathcal{S}_\ell$ ne peuvent être équivalents modulo l'action de $\Gamma^0(\ell)$, d'autre part que tout élément de Γ_1 est équivalent à un élément de $\mathcal{S}_\ell$ modulo cette même action.

Commençons par le premier point : soient $j, k \in [0, \ell-1]$, alors

$$\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & j-k \\ 0 & 1 \end{pmatrix},$$

et cette matrice n'est dans $\Gamma_0(\ell)$ que si $j = k$. On a aussi

$$S\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -j \end{pmatrix} \notin \Gamma_0(\ell),$$

ce qui prouve le premier point.

Par ailleurs, comme ${}^tT = ST^{-1}S$, le groupe Γ_1 est engendré par S et ${}^tT$. Comme ${}^tT \in \Gamma^0(\ell)$, alors pour tout $j \in [0, \ell-1]$, $T\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ est dans la classe de $\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ et TS est dans la classe de S, et on vérifie facilement que $S\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ est dans la classe de S, alors que $SS = I$, ce qui montre qu'il ne peut exister plus que les $\ell+1$ classes dont nous avons donnés des représentants. □

Polynômes modulaire classiques

Soit ℓ un nombre premier. Il est facile de voir que la fonction $j_\ell : \tau \mapsto j\left(\frac{\tau}{\ell}\right)$ est modulaire pour le groupe $\Gamma^0(\ell)$: la seule chose à vérifier est son invariance sous l'action du groupe. Soit $\begin{pmatrix} a & \ell b \\ c & d \end{pmatrix} \in \Gamma^0(\ell)$, alors on a aussi $\begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \Gamma_1$, et pour tout $\tau \in \mathcal{H}$,

$$\begin{aligned} j_\ell\left(\begin{pmatrix} a & \ell b \\ c & d \end{pmatrix}\tau\right) &= j\left(\frac{1}{\ell}\frac{a\tau+\ell b}{c\tau+d}\right) \\ &= j\left(\begin{pmatrix} a & b \\ \ell c & d \end{pmatrix}\frac{\tau}{\ell}\right) \\ &= j\left(\frac{\tau}{\ell}\right) \\ &= j_\ell(\tau), \end{aligned}$$

où l'on a utilisé la modularité de j.

La démonstration de la Proposition 2.17 montre alors qu'il existe un polynôme $\Phi_\ell(X,Y) \in \mathbb{C}[X,Y]$ tel que, pour tout $\tau \in \mathcal{H}$,

$$\Phi_\ell\left(X, j(\tau)\right) = \left(X - f_\ell\left(-\frac{1}{\tau}\right)\right) \prod_{k=0}^{\ell-1} \left(X - f_\ell\left(\tau + k\right)\right).$$

C'est ce polynôme Φ_ℓ que l'on appelle le polynôme modulaire classique (d'indice ℓ).

Théorème 2.2 *Soit ℓ un nombre premier, alors*
- $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$,
- *le polynôme $\Phi_\ell(X,Y)$, considéré comme un polynôme en X, est irréductible,*
- $\Phi_\ell(X,Y) = \Phi_\ell(Y,X)$,
- $\Phi_\ell(X,Y) \equiv (X^\ell - Y)(X - Y^\ell) \bmod \ell\mathbb{Z}[X,Y]$.

Démonstration : Voir [Cox89, pages 231–234]. □

Notons que les coefficients de ces polynômes croissent relativement rapidement avec l'indice ℓ. Plus précisément, si l'on note $h(\Phi_\ell)$ le logarithme népérien de la valeur absolue du plus grand coefficient de Φ_ℓ, Paula Cohen [Coh84] a montré que

$$h(\Phi_\ell) = 6(\ell+1)\left(\left(1 - \frac{2}{\ell}\right)\log \ell + O(1)\right),$$

donc en particulier $h(\Phi_\ell) = O\left(\ell^{1+\varepsilon}\right)$.

À titre d'exemple, on a

$$\begin{aligned}\Phi_3(X,Y) \;=\; & (X^4+Y^4) + 2232(X^3Y^2 + X^2Y^3) - 1069956(X^3Y + XY^3) - X^3Y^3 + 2587918086X^2Y^2 \\ & +36864000(X^3+Y^3) + 8900222976000(X^2Y + XY^2) + 452984832000000(X^2+Y^2) \\ & -770845966336000000XY + 1855425871872000000000(X+Y).\end{aligned}$$

Nous aborderons à la Section 4.4.2 la principale utilisation que nous connaissons de ces polynômes en théorie algorithmique des nombres, et exposerons brièvement des algorithmes pour les calculer.

Autres types de polynômes modulaires

Le principal inconvénient de l'utilisation des polynômes modulaires classiques est la taille de leur coefficients. De ce point de vue, il est intéressant de considérer des fonctions modulaires pour $\Gamma^0(\ell)$ autres que les fonctions j_ℓ définies plus haut. Nous décrivons ici brièvement deux autres familles de fonctions modulaires pour $\Gamma^0(\ell)$ (cette description n'est pas limitative !).

Dans [Elk98], Elkies considère un certain nombre de fonctions modulaires pouvant être utilisées à la place de j et de j_ℓ.

Par exemple, les fonctions parfois appelées "fonctions de Weber généralisées", définies par

$$f_\ell(\tau) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s},$$

où $s = \frac{12}{\mathrm{pgcd}(12,\ell-1)}$. On note alors $\Phi_\ell^c(X,Y)$ le polynôme modulaire liant la fonction f_ℓ à j, ce polynôme est parfois appelé *polynôme modulaire canonique* d'indice ℓ. On trouvera plus de détails sur ces fonctions (ainsi que des algorithmes pour les calculer) dans [Mor95]. En

particulier, le polynôme $\Phi_\ell^c(X, Y)$ est encore à coefficients entiers (et son degré en X reste égal à $\ell + 1$), mais il n'est plus symétrique, et son degré en Y est en général plus petit que $\ell + 1$.

À titre d'exemple, on a

$$\Phi_3^c(X, Y) = X^4 + 36X^3 + 270X^2 - XY + 756X + 729,$$

ce qui illustre bien le fait que les coefficients de Φ_ℓ^c sont plus petits que ceux de Φ_ℓ. Si l'on souhaite calculer des polynômes modulaires par évaluation et interpolation, la précision à laquelle on doit travailler croît en fonction de la hauteur des coefficients [Eng05b], ce qui fait que plus les coefficients sont petits, plus les polynômes peuvent être calculés rapidement par cette méthode.

Dans [BB87, pages 126–133], Jonathan et Peter Borwein étudient d'autres polynômes modulaires liant les fonctions k et $\tau \mapsto k(\ell\tau)$, ayant des coefficients relativement petits (comparés à ceux de Φ_ℓ) et des propriétés intéressantes. Par exemple, le polynôme d'indice 3 liant ces fonctions est

$$\Omega_3(X, Y) = X^4 + 2X^3Y^3 - 2XY - Y^4,$$

ce qui est relativement compact.

Notons que dans les applications comme le comptage de points par l'algorithme SEA, la compacité des polynômes modulaires n'est pas l'unique critère entrant en ligne de compte dans le choix des fonctions modulaires que l'on va utiliser. En effet, une fois une racine du polynôme instancié en j calculée, il reste à déterminer le noyau de l'isogénie associée à cette racine, et la complexité de cette phase dépend de la fonction modulaire utilisée. Une étude menée avec Andreas Enge, Pierrick Gaudry et François Morain a par exemple montré qu'il nétait pas intéressant d'utiliser les polynômes $\Omega_\ell(X, Y)$, malgré leur compacité.

Chapitre 3

Moyenne arithmético-géométrique et relation avec les theta constantes

Dans ce chapitre, nous nous intéressons à la moyenne arithmético-géométrique (ou AGM) de deux nombres complexes. Nous verrons plus tard comment l'AGM peut se généraliser *via* ce que l'on appelle la moyenne de Borchardt (Chapitre 7). Un certain nombre de résultats concernant l'AGM ne sont pas démontrés dans ce chapitre car nous en donnons des démonstrations dans le cadre des suites de Borchardt au Chapitre suscité.

3.1 AGM sur les réels positifs

3.1.1 Définition

Soient a et b deux nombres réels positifs. On définit la suite $(a_n, b_n)_{n\in\mathbb{N}}$ en posant $a_0 = a$, $b_0 = b$, et pour tout $n \geqslant 0$,

$$a_{n+1} = \frac{a_n + b_n}{2}$$

et

$$b_{n+1} = \sqrt{a_n b_n}.$$

L'élément a_{n+1} est donc la moyenne arithmétique de a_n et b_n, alors que b_{n+1} est leur moyenne géométrique. On dit que la suite (a_n, b_n) est la *suite AGM* associée à (a, b).

Supposons maintenant que $a \geqslant b$, et notons $(a_n^{(0)}, b_n^{(0)})_{n\in\mathbb{N}}$ la suite AGM associée à (a, b) et $(a_n^{(1)}, b_n^{(1)})_{n\in\mathbb{N}}$ la suite AGM associée à (b, a). On montre alors facilement, par récurrence, que

1. pour tout $n \geqslant 0$,
$$a_n^{(0)} \geqslant b_n^{(0)},$$
2. pour tout $n \geqslant 0$,
$$(a_n^{(1)}, b_n^{(1)}) = \begin{cases} (a_n^{(0)}, b_n^{(0)}) & \text{si } n \text{ est impair,} \\ (b_n^{(0)}, a_n^{(0)}) & \text{si } n \text{ est pair.} \end{cases}$$

En particulier les suites $(a_n^{(0)})$ et $(b_n^{(0)})$ sont adjacentes, donc convergent. La définition de ces suites implique qu'elles ont la même limite, qui est aussi celle des suites $(a_n^{(1)})$ et $(b_n^{(1)})$, et qui sera appelée *moyenne arithmético-géométrique* (ou AGM) de a et b, et notée $\mathrm{AGM}(a, b)$.

Notons tout d'abord quelques propriétés élémentaires de l'AGM : pour tous $a, b \geqslant 0$, on a

$$\mathrm{AGM}(a, b) = \mathrm{AGM}(b, a),$$

$$\mathrm{AGM}(a,0)=0$$

et

$$\mathrm{AGM}(a,b)=a\mathrm{AGM}\left(1,\frac{b}{a}\right).$$

En particulier, cette dernière propriété (que l'on peut qualifier d'homogénéité de l'AGM) montre que l'on peut, pour étudier l'AGM, se restreindre à l'étude de la fonction $M:\mathbb{R}^+\to\mathbb{R}^+$ définie, pour tout $x\geqslant 0$, par

$$M(x)=\mathrm{AGM}(1,x).$$

Cette fonction est croissante, et pour tout $x\geqslant 0$, on a

$$M(x)\in[0,x].$$

L'une des propriétés importantes de l'AGM est que si $(a_n,b_n)_{n\in\mathbb{N}}$ est une suite AGM, alors les suites (a_n) et (b_n) convergent *de manière quadratique* vers $\mathrm{AGM}(a_0,b_0)$ si cette dernière limite est non nulle. Ceci est un cas particulier de la Propriété 7.1.

3.1.2 Historique

La moyenne arithmético-géométrique a été introduite en 1784 par Lagrange [Lag67], puis redécouverte et largement étudiée à partir de 1791 par Gauss [Gau01, pages 361–403]. L'un des problèmes à l'époque était le calcul numérique des intégrales elliptiques, et l'AGM a apporté une solution élégante à ce problème. Par exemple, si l'on note, pour $k\in[0,1]$,

$$K(k)=\int_0^{\frac{\pi}{2}}\frac{d\psi}{\sqrt{1-k^2\sin^2\psi}}$$

(on dit que $K(k)$ est l'*intégrale elliptique complète de première espèce de module* k), alors on a l'égalité

$$K(k)=\frac{\pi}{2\mathrm{AGM}\left(1,\sqrt{1-k^2}\right)}.$$

Gauss était en fait allé beaucoup plus loin en développant à partir semble-t-il de l'AGM une théorie des fonctions elliptiques qu'il ne publia pas de son vivant. En particulier, il construisait les theta constantes (ainsi que certaines fonctions modulaires) *à partir* de l'AGM, une approche relativement originale que l'on pourra retrouver par exemple dans [vD28].

On notera que Legendre [Leg28] (en particulier le Chapitre XIX du premier volume et le Chapitre II du second volume), pour calculer des intégrales elliptiques, utilisait une méthode relativement proche de l'AGM (en particulier convergeant à la même vitesse, c'est-à-dire quadratiquement, comme nous le verrons par la suite) : il considérait les suites définies par des récurrences du type

$$u_{n+1}=\frac{1+u_n}{2\sqrt{u_n}},$$

ce qui revient à considérer, si (a_n,b_n) est une suite AGM, la suite des quotients $\left(\frac{a_n}{b_n}\right)$ (Legendre considérait aussi les suites données par des récurrences de type

$$u_n=\frac{1+u_{n+1}}{2\sqrt{u_{n+1}}},$$

ce qui revient à considérer une suite AGM "à l'envers").

Pour un historique beaucoup plus détaillé de l'AGM, nous renvoyons à l'article très complet de Cox [Cox84], qui expose aussi un certain nombre de problèmes de mécanique ou de géométrie à la résolution desquels le calcul d'intégrales elliptiques était nécessaire (le premier volume de [Leg28] expose par ailleurs aussi ces problèmes).

3.2 Définition de l'AGM sur les nombres complexes

Définition 3.1 (itéré AGM) *Soient $x, y \in \mathbb{C}$, on dit que (X, Y) est un* itéré AGM *de (x, y) si*

$$X = \frac{x+y}{2}$$

et

$$Y^2 = xy.$$

On notera que si x et y sont non-nuls, alors le couple (x, y) a deux itérés AGM distincts. Par ailleurs, le couple (y, x) a les mêmes itérés AGM que le couple (x, y).

Définition 3.2 (suite AGM) *Soient $a, b \in \mathbb{C}$, on dit que $(a_n, b_n)_{n\in\mathbb{N}}$ est une* suite AGM *associée à (a, b) si $a_0 = a$, $b_0 = b$ et que, pour tout $n \in \mathbb{N}$, le couple (a_{n+1}, b_{n+1}) est un itéré AGM du couple (a_n, b_n).*

Une suite AGM n'est donc pas uniquement déterminée par la donnée du couple (a_0, b_0), mais aussi par les déterminations successives des b_n (si a_n et b_n sont fixés, alors a_{n+1} est uniquement déterminé, tandis que b_{n+1} l'est au signe près seulement).

Notons tout de suite que si l'on fixe $\tau \in \mathcal{H}$, alors la Proposition 2.9 montre que la suite

$$\left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right)_{n\in\mathbb{N}}$$

est une suite AGM, et le Lemme 2.2 montre même que cette suite converge vers 1. Ceci explique le lien étroit existant entre l'AGM et les theta constantes.

Définition 3.3 (bon et mauvais choix de racines) *Si $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM et si $n_0 \geqslant 1$, on dit que b_{n_0} est* le bon choix *(de racine) (parmi b_{n_0} et $-b_{n_0}$) si*

$$|a_{n_0} - b_{n_0}| \leqslant |a_{n_0} + b_{n_0}|,$$

avec de plus $\operatorname{Im}\left(\frac{b_{n_0}}{a_{n_0}}\right) > 0$ *lorsque l'inégalité ci-dessus est une égalité. Dans le cas contraire, on parle (logiquement) de* mauvais choix *(de racine).*

Il est montré (c'est un cas particulier du Théorème 7.1, mais on peut, pour une démonstration plus simple, consulter [Cox84, Proposition 2.1]) que si $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM, alors il existe $A \in \mathbb{C}$ tel que

$$\lim_{n\to+\infty} a_n = \lim_{n\to+\infty} b_n = A,$$

et que $A \neq 0$ si et seulement si le nombre de mauvais choix de la suite AGM est fini. Enfin, la Proposition 7.1 montre que dans le cas où $A \neq 0$, la convergence est quadratique.

Notons qu'une suite AGM associée à deux réels *strictement* positifs, comme définie à la Section 3.1.1, ne contient que des bons choix de racines.

Soit $(a_n, b_n)_{n\in\mathbb{N}}$ une suite AGM et soit $\lambda \in \mathbb{C} \setminus \{0\}$, alors la suite $(\lambda a_n, \lambda b_n)_{n\in\mathbb{N}}$ est encore une suite AGM, et si l'on fixe un indice $n \geqslant 0$, alors $(\lambda a_n, \lambda b_n)$ est un bon choix si et seulement si (a_n, b_n) en est un.

Si $(a_n, b_n)_{n\in\mathbb{N}}$ est une suite AGM, et qu'il existe un indice $n \geqslant 0$ tel que $a_n = 0$ ou $b_n = 0$, alors pour tout $m \geqslant n$, on a $b_m = 0$ (et en particulier (a_m, b_m) est un mauvais choix).

Définition 3.4 (fonction M) *On définit une fonction $M : \mathbb{C} \to \mathbb{C}$ comme suit : pour $z \neq 0$, on définit $M(z)$ comme étant la limite de* la *suite AGM associée à $(1, z)$ ne comportant* que des bons choix*, et on pose $M(0) = 0$.*

D'après ce qui précède, ceci généralise bien la fonction M introduite à la Section 3.1.1.

Définition 3.5 (ensemble $\mathcal{B}_1(a,b)$) *Pour tous $a, b \in \mathbb{C}$, on définit l'ensemble $\mathcal{B}_1(a,b)$ comme étant l'ensemble des limites des suites AGM associées à (a,b).*

La lettre $\mathcal{B}$ est ici employée comme initiale de Borchardt, puisqu'au Chapitre 7 nous utiliserons encore cette lettre pour désigner l'ensemble des limites de suites de Borchardt, et que l'AGM est un cas particulier de suite de Borchardt (voir la définition des suites de Borchardt, Section 7.1).

On notera que pour tous $a, b \in \mathbb{C}$ et $\lambda \in \mathbb{C} \setminus \{0\}$, on a

$$\mathcal{B}_1(\lambda a, \lambda b) = \{\lambda x : x \in \mathcal{B}_1(a,b)\}\,.$$

À titre d'illustration, la Figure 3.1 représente une partie des points de l'ensemble $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$ (il manque les points vers l'origine, qui seraient de plus en plus denses). Les points semblent situés à l'intersection de cercles dont les centres sont situés sur deux axes s'intersectant en l'origine. Ceci peut faire penser à considérer les inverses de ces points. La Figure 3.2 montre que ces inverses sont situés sur un réseau. Ce phénomène sera démontré à la section suivante (Section 3.3).

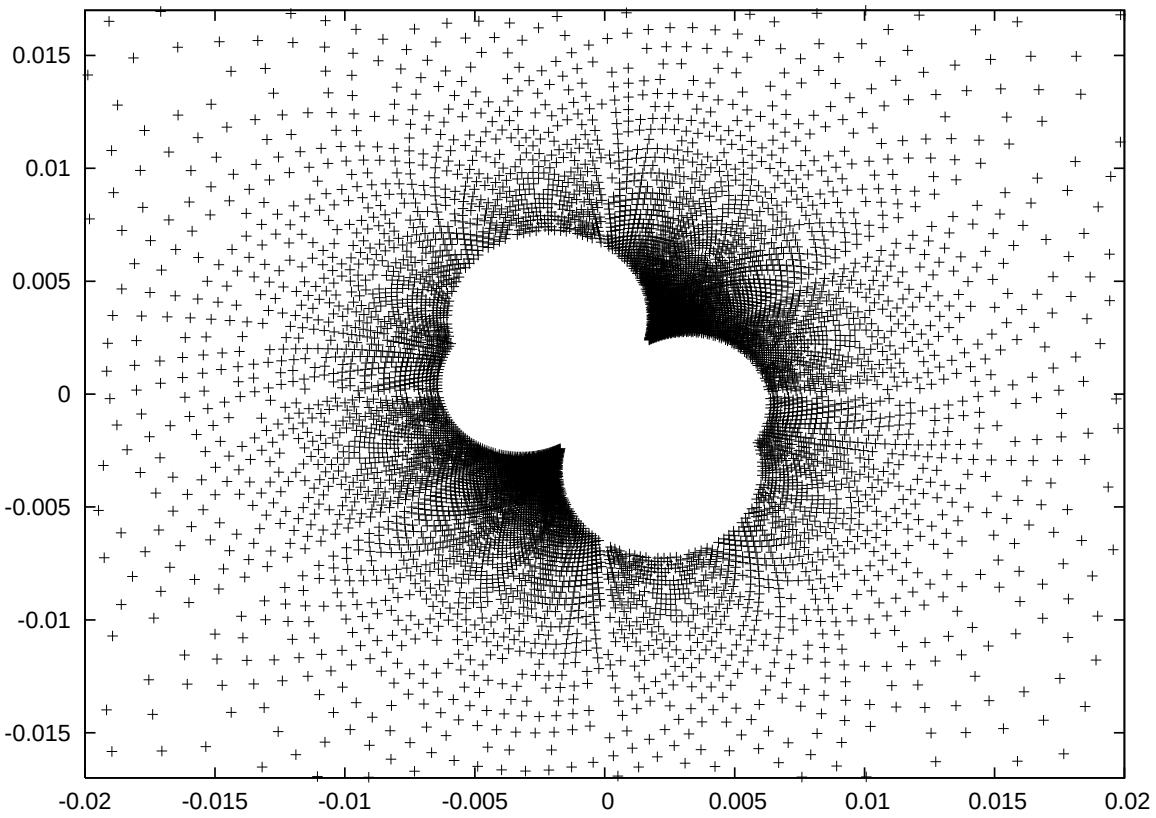

FIG. 3.1 – Points de l'ensemble $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$

3.3 Sur les limites des suites AGM

Le but de cette section est de montrer le résultat suivant, déjà en partie connu (sous une autre forme) par Gauss [Gau27, pages 467–468 et 477–478] :

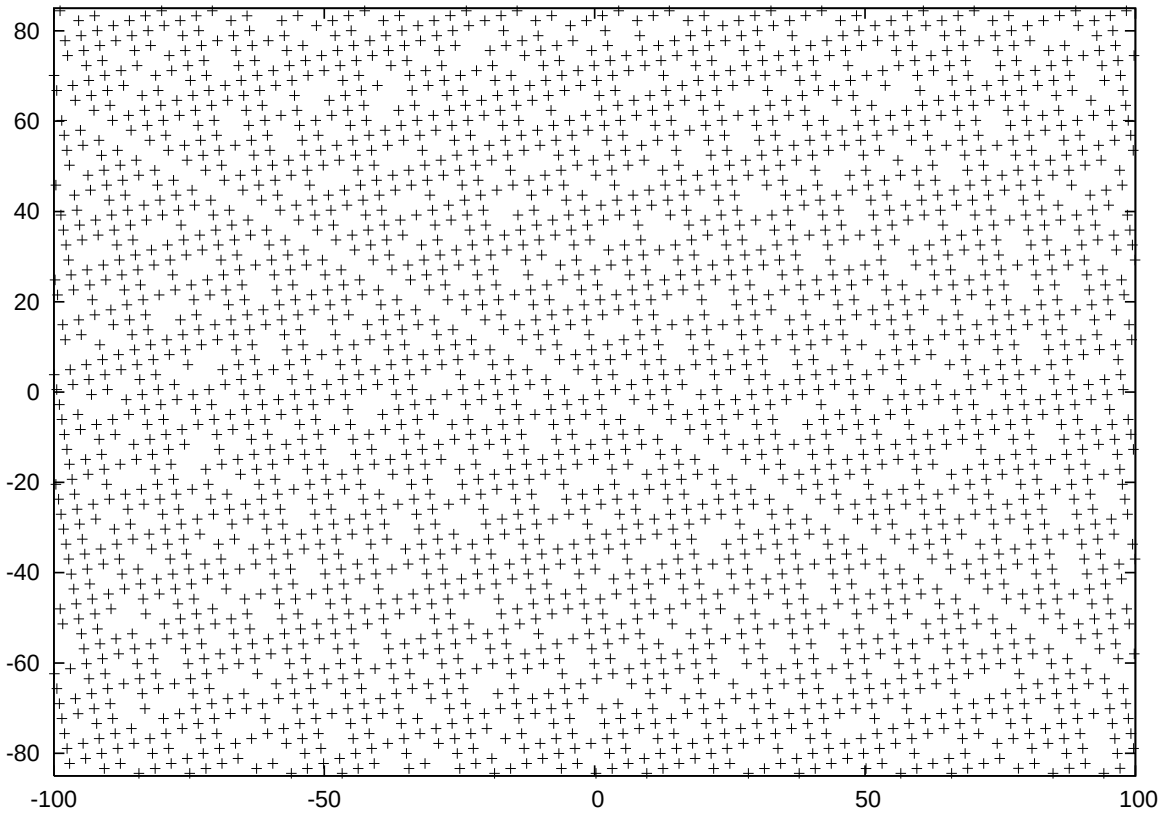

FIG. 3.2 – Inverses des points de l'ensemble $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$

Théorème 3.1 *Pour tout $\tau \in \mathcal{H}$, on a*

$$\mathcal{B}_1\left(\theta_0^2(\tau), \theta_1^2(\tau)\right) = \left\{ \frac{\theta_0^2(\tau)}{\theta_0^2(\gamma\tau)} : \gamma \in \Gamma_{k'} \right\} \cup \{0\}.$$

Nous verrons à la Section 3.3.3 que ce théorème a un corollaire (Théorème 3.2) qui, en fonction des valeurs de $a, b \in \mathbb{C}$ uniquement, permet de décrire $\mathcal{B}_1(a, b)$. C'est du Théorème 3.2 que Gauss était proche, et ce théorème a été démontré pour la première fois en 1928, indépendamment par Geppert [Gep28] et par von David [vD28] (par deux méthodes différentes). Une preuve assez proche de celle de Geppert a été publiée plus récemment par Cox [Cox84].

Nous commençons (Sections 3.3.1 et 3.3.2) par donner une démonstration (en partie) originale du Théorème 3.1, puis (Section 3.3.3) nous énonçons le Théorème 3.2, donnons une description de sa preuve et expliquons en quoi les démonstrations données dans la littérature diffèrent de la nôtre.

Pour le reste de cette Section, nous fixons $\tau_0 \in \mathcal{H}$ et notons $(a_0, b_0) = \left(\theta_0^2(\tau_0), \theta_1^2(\tau_0)\right)$.

3.3.1 Schéma de la démonstration

On commence par montrer l'inclusion

$$\left\{ \frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)} : \gamma \in \Gamma_{k'} \right\} \cup \{0\} \subset \mathcal{B}_1(a_0, b_0). \tag{3.1}$$

Il est facile de voir que l'on peut construire une suite AGM associée à (a_0, b_0) ayant un

nombre infini de mauvais choix. Une telle suite, d'après le Théorème 7.1, converge vers zéro, donc $\mathcal{B}_1(a_0, b_0)$ contient zéro.

Par ailleurs, la formule de duplication des theta constantes (Proposition 2.9) montre que la suite

$$\left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right)_{n\in\mathbb{N}}$$

est une suite AGM associée à (a_0, b_0), et comme, d'après le Lemme 2.2,

$$\lim_{n\to+\infty} \theta_j^2(2^n\tau) = 1$$

pour tous $\tau \in \mathcal{H}$ et $j \in \{0, 1\}$, on a prouvé que l'ensemble $\mathcal{B}_1(a_0, b_0)$ contient 1.

Soit maintenant $\gamma \in \Gamma_{k'}$. Comme k' est modulaire pour Γ'_k (Proposition 2.14), on a

$$(a_0, b_0) = \frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)} \left(\theta_0^2(\gamma\tau_0), \theta_1^2(\gamma\tau_0)\right),$$

donc

$$\mathcal{B}_1(a_0, b_0) = \left\{ \frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)} x : x \in \mathcal{B}_1\left(\theta_0^2(\gamma\tau_0), \theta_1^2(\gamma\tau_0)\right) \right\}.$$

D'après ce qui précède, $1 \in \mathcal{B}_1\left(\theta_0^2(\gamma\tau_0), \theta_1^2(\gamma\tau_0)\right)$, donc

$$\frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)} \in \mathcal{B}_1(a_0, b_0),$$

ce qui termine la démonstration de l'inclusion (3.1).

Pour prouver l'autre inclusion, on pose $(a_n, b_n)_{n\in\mathbb{N}}$ une suite AGM associée à (a_0, b_0) convergeant vers une limite $A \neq 0$. On introduit alors, pour tout $n \geqslant 0$, l'ensemble

$$T_n = \left\{ \tau \in \mathcal{H} : k'(\tau) = \frac{b_n}{a_n} \right\}.$$

Dans un premier temps, on montrera qu'aucun de ces ensembles T_n ne peut être vide. On en déduira alors qu'il existe une suite $(\tau_n)_{n\in\mathbb{N}}$ telle que pour tout $n \geqslant 0$, $\tau_n \in T_n \cap \mathcal{F}_{k'}$ (où $\mathcal{F}_{k'}$ est le domaine fondamental pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$ introduit au Lemme 2.4).

Comme les deux suites (a_n) et (b_n) convergent vers la même limite A non nulle, alors $k'(\tau_n)$ converge vers 1. En utilisant le fait que $\tau_n \in \mathcal{F}_{k'}$, nous en déduirons que $\mathrm{Im}\,(\tau_n)$ tend vers l'infini, et qu'il existe alors un indice $N \geqslant 0$ tel que, pour tout $n \geqslant 0$,

$$(a_{N+n}, b_{N+n}) = A\left(\theta_0^2(2^n\tau_N), \theta_1^2(2^n\tau_N)\right).$$

Nous montrerons ensuite qu'il existe $\tau'_0 \in \mathcal{H}$ tel que

$$(a_0, b_0) = A\left(\theta_0^2(\tau'_0), \theta_1^2(\tau'_0)\right),$$

ce qui implique par ailleurs que

$$A = \frac{\theta_0^2(\tau_0)}{\theta_0^2(\tau'_0)},$$

avec $k'(\tau'_0) = k'(\tau_0)$.

D'après la Proposition 2.15, cette dernière égalité implique l'existence d'une matrice $\gamma \in \Gamma_{k'}$ telle que $\tau'_0 = \gamma\tau_0$, ce qui montre finalement la seconde inclusion et le théorème.

3.3.2 Preuve détaillée

La première inclusion a été prouvée dans la section précédente, donc nous exposons ici la démonstration de la seconde inclusion.

Soit $(a_n, b_n)_{n\in\mathbb{N}}$ une suite AGM associée à (a_0, b_0) convergeant vers une limite $A \neq 0$. Nous allons montrer que A s'écrit $\frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)}$, avec $\gamma \in \Gamma_{k'}$.

Pour tout $n \geqslant 0$, on pose

$$T_n = \left\{ \tau \in \mathcal{H} : \frac{b_n}{a_n} = k'(\tau) \right\}.$$

(On notera que cet ensemble est bien défini, puisque si la limite A est non nulle, alors aucun des termes de (a_n) ni de (b_n) ne peut s'annuler).

Nous allons montrer que pour tout $n \geqslant 0$, l'ensemble T_n est non vide. C'est en fait une conséquence directe du Lemme suivant :

Lemme 3.1 *Pour tout $\tau \in \mathcal{H}$, si (a, b) est une itérée AGM de $\left(\theta_0^2(\tau), \theta_1^2(\tau)\right)$, alors*

$$\frac{b}{a} \in \left\{ k'(2G_0\tau), k'(2G_1\tau) \right\}$$

où $G_0 = I$ et $G_1 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$.

Démonstration : Soit $\tau \in \mathcal{H}$, et soit (a, b) une itérée AGM de $\left(\theta_0^2(\tau), \theta_1^2(\tau)\right)$, alors par définition d'une itérée AGM, on a

$$(a, b) = \left(\theta_0^2(2\tau), \pm\theta_1^2(2\tau)\right),$$

et

$$\frac{b}{a} = \pm k'(2\tau).$$

La formule de tranformation des theta constantes sous l'action des éléments de Γ_1 (Proposition 2.4) permet de montrer que

$$k'(2G_1\tau) = k'\left(\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} 2\tau\right) = k'\left(ST^{-2}S(2\tau)\right) = -k'(2\tau),$$

ce qui termine la démonstration. □

Par hypothèse, $T_0 \neq \emptyset$, donc une récurrence directe utilisant le Lemme 3.1 permet de montrer que pour tout $n \geqslant 0$, $T_n \neq \emptyset$.

Comme $\mathcal{F}_{k'}$ est un domaine fondamental pour l'action de $\Gamma_{k'}$ sur $\mathcal{H}$, on a aussi montré que pour tout $n \geqslant 0$, $T_n \cap \mathcal{F}_{k'} \neq \emptyset$. Il existe donc une suite $(\tau_n)_{n\geqslant 1}$ telle que, pour tout $n \geqslant 1$, $\tau_n \in T_n \cap \mathcal{F}_{k'}$. De plus, comme les suites (a_n) et (b_n) convergent toutes deux vers $A \neq 0$, alors

$$\lim_{n\to+\infty} k'(\tau_n) = \lim_{n\to+\infty} \frac{b_n}{a_n} = 1.$$

Nous allons maintenant montrer que

$$\lim_{n\to+\infty} \mathrm{Im}\,(\tau_n) = +\infty.$$

Pour cela, on commence par fixer une constante $B > 0$ telle que, pour tout $\tau \in \mathcal{H}$ tel que $\mathrm{Im}\,(\tau) \geqslant B$, on ait

$$\left|\theta_j^2(\tau) - 1\right| \leqslant \frac{1}{10} \tag{3.2}$$

pour $j \in \{0, 1\}$ et

$$\left|\theta_2^2(\tau)\right| \leqslant \frac{1}{10}. \tag{3.3}$$

(L'existence d'une telle constante est assurée par la démonstration du Lemme 2.2).

On définit maintenant

$$\mathcal{C}_{B^-} = \{\tau \in \mathcal{C} : \mathrm{Im}\,(\tau) \leqslant B\}$$

et

$$\mathcal{C}_{B^+} = \{\tau \in \mathcal{C} : \mathrm{Im}\,(\tau) \geqslant B\},$$

où $\mathcal{C}$ est le domaine fondamental pour l'action de Γ_1 sur $\mathcal{H}$ introduit dans la démontration du Lemme 2.4. La clôture de $\mathcal{C}_{B^-}$ est un compact inclus dans $\mathcal{C}$, donc celle de $\bigcup_{\gamma\in\Gamma_{k'}} \gamma\mathcal{C}_{B^-}$ est un compact de $\mathcal{H}$ et (comme la fonction $\tau \to k'(\tau) - 1$ ne s'annule pas sur $\mathcal{H}$) il existe une constante $\varepsilon_1 > 0$ telle que, pour tout $\tau \in \bigcup_{\gamma\in\mathcal{G}_{k'}} \gamma\mathcal{C}_{B^-}$,

$$\left|k'(\tau) - 1\right| \geqslant \varepsilon_1. \tag{3.4}$$

La Proposition 2.4 permet de montrer que, pour tout $\tau \in \mathcal{H}$,

$$\begin{array}{llll}
k'(T^{-1}S\tau) &= \frac{1}{k(\tau)}, & k'(ST\tau) &= i\frac{k(\tau)}{k'(\tau)},\\
k'(S\tau) &= k(\tau), & k'(TST\tau) &= -i\frac{k'(\tau)}{k(\tau)},\\
k'(STS\tau) &= i\frac{k'(\tau)}{k(\tau)}, & k'(ST^2\tau) &= -k(\tau),\\
k'(ST^{-1}\tau) &= -i\frac{k(\tau)}{k'(\tau)}, & k'(TST^2\tau) &= \frac{-1}{k(\tau)},\\
k'(ST^2ST\tau) &= \frac{-1}{k'(\tau)}, & k'(ST^{-2}S\tau) &= -k'(\tau).
\end{array}$$

En utilisant les informations que nous avons sur les valeurs des theta constantes sur $\mathcal{C}_{B^+}$ (Équations (3.2) et (3.3)), on montre alors qu'il existe une constante $\varepsilon_2 > 0$ telle que, pour tous $\tau \in \mathcal{C}_{B^+}$ et $\gamma \in \mathcal{G}_{k'} \setminus \{I, T\}$,

$$\left|k'(\tau) - 1\right| \geqslant \varepsilon_2. \tag{3.5}$$

(Notons que la constante ε_2 est explicitable, mais le calcul présente peu d'intérêt).

On déduit des Équations (3.4) et (3.5) l'existence d'un indice $N_B \geqslant 0$ tel que, pour tout $n \geqslant N_B$, $\tau_n \in \mathcal{C}_{B^+} \cup T\mathcal{C}_{B^+}$. En particulier, $\mathrm{Im}\,(\tau_n) \geqslant B$ pour $n \geqslant N_B$.

Tout ceci reste vrai si l'on augmente la valeur de B, ce qui montre que $\mathrm{Im}\,(\tau_n)$ tend vers l'infini.

Soit maintenant $N \geqslant 0$ tel que $\mathrm{Im}\,(\tau_N) \geqslant B$ (où B est toujours tel que l'Équation (3.2) soit vérifiée) et que, pour tout $n \geqslant N$, $|a_n - A| \leqslant \frac{|A|}{10}$ et $|b_n - A| \leqslant \frac{|A|}{10}$. Alors

$$(a_N, b_N) = \frac{a_N}{\theta_0^2(\tau_N)} \left(\theta_0^2(\tau_N), \theta_1^2(\tau_N)\right),$$

et d'après la démonstration du Lemme 3.1,

$$(a_{N+1}, b_{N+1}) = \frac{a_N}{\theta_0^2(\tau_N)} \left(\theta_0^2(2\tau_N), \pm\theta_1^2(2\tau_N)\right).$$

Par ailleurs, on a la majoration suivante :

$$\begin{aligned}
\left|\frac{a_N\theta_1^2(2\tau_N)}{A\theta_0^2(\tau_N)}-1\right| &\leqslant \left|\frac{a_N}{A}\right|\cdot\left|\frac{\theta_1^2(2\tau_N)}{\theta_0^2(\tau_N)}-1\right|+\left|\frac{a_N}{A}-1\right| \\
&\leqslant \left|\frac{a_N}{A}\right|\cdot\frac{1}{\left|\theta_0^2(\tau_N)\right|}\left(\left|\theta_1^2(2\tau_N)-1\right|+\left|\theta_0^2(\tau_N)-1\right|\right)+\frac{1}{10} \\
&\leqslant \frac{2}{10}\left|\frac{a_N}{A}\right|\frac{1}{\left|\theta_0^2(\tau_N)\right|}+\frac{1}{10} \\
&\leqslant \frac{2}{10}\left(1+\left|\frac{a_N}{A}-1\right|\right)\frac{1}{1-\left|\theta_0^2(\tau)-1\right|}+\frac{1}{10} \\
&\leqslant \frac{2}{10}\left(1+\frac{1}{10}\right)\frac{1}{1-\frac{1}{10}}+\frac{1}{10} \\
&\leqslant \frac{31}{90},
\end{aligned}$$

donc

$$\begin{aligned}
\left|A+\frac{a_N}{\theta_0^2(\tau_N)}\theta_1^2(2\tau_N)\right| &\geqslant |A|\left(2-\left|\frac{a_N\theta_1^2(2\tau_N)}{A\theta_0^2(\tau_N)}-1\right|\right) \\
&\geqslant \frac{149}{90}|A|.
\end{aligned}$$

Comme, par hypothèse, $|b_{N+1}-A|\leqslant\frac{|A|}{10}$, ceci montre que nécessairement,

$$(a_{N+1},b_{N+1})=\frac{a_N}{\theta_0^2(\tau_N)}\left(\theta_0^2(2\tau_N),\theta_1^2(2\tau_N)\right).$$

Bien sûr, on a $\operatorname{Im}(2\tau)\geqslant B$, et une récurrence directe sur n montre que, pour tout $n\geqslant 0$,

$$(a_{N+n},b_{N+n})=\frac{a_N}{\theta_0^2(\tau_N)}\left(\theta_0^2(2^n\tau_N),\theta_1^2(2^n\tau_N)\right).$$

D'après le Lemme 2.2, on en déduit que

$$A=\frac{a_N}{\theta_0^2(\tau_N)}.$$

Pour terminer la démonstration, nous allons utiliser le résultat suivant :

Lemme 3.2 *Pour tout $\tau\in\mathcal{H}$, l'ensemble des paires (a,b) telles qu'il existe une itération AGM de (a,b) à $\left(\theta_0^2(\tau),\theta_1^2(\tau)\right)$ est*

$$\left\{\left(\theta_0^2\left(\frac{\tau+c}{2}\right),\theta_1^2\left(\frac{\tau+c}{2}\right)\right):c\in\{0,2\}\right\}.$$

DÉMONSTRATION : Une démonstration de ce résultat est contenue dans l'article de Cox [Cox84]. Nous la reproduisons ici afin d'exposer une démonstration complète du Théorème 3.1.

Soit $\tau\in\mathcal{H}$, alors (par définition d'une itération AGM) il existe une itération AGM de (a,b) à $\left(\theta_0^2(\tau),\theta_1^2(\tau)\right)$ si et seulement si $\theta_0^2(\tau)=\frac{a+b}{2}$ et $\theta_1^4(\tau)=ab$, donc a et b sont nécessairement racines de l'équation

$$X^2-2\theta_0^2(\tau)X+\theta_1^4(\tau)=0.$$

En utilisant l'égalité de Jacobi, il est facile de voir que les deux solutions de cette équation sont $\theta_0^2(\tau)\pm\theta_1^2(\tau)$, et en utilisant la Proposition 2.11, on montre que ces deux racines sont

$x = \theta_0^2\left(\frac{\tau}{2}\right)$ et $y = \theta_1^2\left(\frac{\tau}{2}\right)$. La formule de duplication (Proposition 2.9) montre que (x, y) et (y, x) sont bien tous deux susceptibles de mener à $\left(\theta_0^2(\tau), \theta_1^2(\tau)\right)$ par une itération AGM, et la formule de transformation (Proposition 2.4) montre que

$$x = \theta_1^2\left(\frac{\tau+2}{2}\right)$$

et

$$y = \theta_0^2\left(\frac{\tau+2}{2}\right),$$

ce qui permet de conclure. □

En appliquant ce Lemme à (a_N, b_N), on montre qu'il existe $\tau'_{N-1} \in \left\{\frac{\tau_N}{2}, \frac{\tau_N+2}{2}\right\}$ tel que

$$(a_{N-1}, b_{N-1}) = A\left(\theta_0^2(\tau'_{N-1}), \theta_1^2(\tau'_{N-1})\right),$$

et une récurrence directe montre finalement qu'il existe τ'_0 tel que

$$(a_0, b_0) = A\left(\theta_0^2(\tau'_0), \theta_1^2(\tau'_0)\right),$$

donc que

$$A = \frac{\theta_0^2(\tau_0)}{\theta_0^2(\tau'_0)},$$

avec $k'(\tau_0) = k'(\tau'_0)$.

En utilisant la Proposition 2.15, on en déduit qu'il existe $\gamma \in \Gamma_{k'}$ tel que

$$A = \frac{\theta_0^2(\tau_0)}{\theta_0^2(\gamma\tau_0)},$$

ce qui conclut la démonstration du Théorème 3.1.

3.3.3 Le résultat de Gauss et les démonstrations de Cox et Geppert

Dans cette section, nous décrivons brièvement la démonstration du Théorème 3.1 donnée par Cox dans [Cox84]. Les points importants de cette démonstration sont les mêmes que ceux de la démonstration de Geppert [Gep28].

Nous reprenons les notations utilisées dans la section précédente.

La différence significative entre notre démonstration et celle de Cox est que cette dernière utilise la propriété suivante de la fonction k', dont nous n'avons pas fait usage :

Proposition 3.1 *Pour tout $\tau \in \mathcal{F}_{k'}$, on a $\mathrm{Re}\,(k'(2\tau)) \geqslant 0$, et si $\mathrm{Re}\,(k'(2\tau)) = 0$, alors $\mathrm{Im}\,(k'(2\tau)) > 0$.*

Démonstration : Soit $\tau \in \mathcal{F}_{k'}$. Le fait que $\mathrm{Re}\,(k'(2\tau)) \geqslant 0$ est le Lemme 2.8 de [Cox84], et le fait que si $\mathrm{Re}\,(k'(2\tau)) = 0$, alors $\mathrm{Im}\,(k'(2\tau)) > 0$ est contenu dans la démonstration du Lemme 2.9 de [Cox84]. □

L'intérêt de cette propriété est qu'elle permet de montrer le résultat suivant, établissant une relation entre le domaine fondamental $\mathcal{F}_{k'}$ et une suite AGM particulière (correspondant à la fonction M) :

Proposition 3.2 *Pour tout $\tau \in \mathcal{F}_{k'}$,*

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)}.$$

DÉMONSTRATION : Soit $\tau \in \mathcal{F}_{k'}$, et soit $(a_n, b_n)_{n\in\mathbb{N}}$ la suite AGM associée à $(1, k'(\tau))$ ne contenant que des bons choix au sens de la Section 3.2.

D'après les formules de duplication des theta constantes (Proposition 2.9), on sait que

$$(a_1, b_1) = \frac{1}{\theta_0^2(\tau)}\left(\theta_0^2(2\tau), \pm\theta_1^2(2\tau)\right).$$

En particulier, on a $\frac{b_1}{a_1} = \pm k'(2\tau)$, et comme tous les choix sont bons, la Propriété 3.1 montre que $\frac{b_1}{a_1} = k'(2\tau)$, donc

$$(a_1, b_1) = \frac{1}{\theta_0^2(\tau)}\left(\theta_0^2(2\tau), \theta_1^2(2\tau)\right).$$

Mais alors 2τ appartient soit à $\mathcal{F}_{k'}$, soit à un de ses translatés d'un multiple de 2, et comme la fonction k' est 2-périodique, on en déduit de même que

$$(a_2, b_2) = \frac{1}{\theta_0^2(\tau)}\left(\theta_0^2(4\tau), \theta_1^2(4\tau)\right),$$

et une récurrence directe permet de montrer que pour tout $n \geqslant 0$,

$$(a_n, b_n) = \frac{1}{\theta_0^2(\tau)}\left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right).$$

Le Lemme 2.2 permet alors de conclure. □

Le raisonnement utilisé par Cox est alors le suivant : soit $(a_n, b_n)_{n\in\mathbb{N}}$ une suite AGM convergeant vers une limite $A \neq 0$. D'après le Théorème 7.1, cette suite n'a qu'un nombre fini de mauvais choix de racines.

Soit alors $N \geqslant 0$ tel que la suite (a_n, b_n) n'ait aucun mauvais choix pour les indices $n \geqslant N$. Comme $A \neq 0$, on peut supposer a_N et b_N non nuls et $a_N + b_N \neq 0$. On peut par ailleurs supposer $a_N \neq b_N$ (nous renvoyons à l'article de Cox pour les détails) : la Proposition 2.15 montre qu'alors il existe $\tau_N \in \mathcal{F}_{k'}$ tel que

$$\frac{b_N}{a_N} = k'(\tau_N).$$

Comme il n'y a pas de mauvais choix pour les indices $n \geqslant N$, la Proposition 3.2 et sa démonstration montrent que, pour tout $n \geqslant 0$,

$$(a_{N+n}, b_{N+n}) = A\left(\theta_0^2(2^n\tau_N), \theta_1^2(2^n\tau_N)\right).$$

Cox utilise alors le même raisonnement que celui utilisé dans la démonstration donnée en Sections 3.3.1 et 3.3.2 pour conclure.

Le théorème auquel était arrivé Gauss (et qui est démontré par Geppert, von David et Cox dans leurs articles) est en fait le suivant :

Théorème 3.2 *Soient $a, b \in \mathbb{C} \setminus \{0\}$ tels que $a \neq \pm b$ et $|a| \geqslant |b|$. Alors, si l'on pose*

$$\lambda = aM\left(\frac{b}{a}\right)$$

et

$$\mu = (a+b)M\left(\frac{a-b}{a+b}\right),$$

on a

$$\mathcal{B}_1(a,b) = \left\{ \left(\frac{d}{\mu} + \frac{ic}{\lambda}\right)^{-1} : c, d \in \mathbb{Z}, \operatorname{pgcd}(c,d) = 1, c \equiv 0 \bmod 4, d \equiv 1 \bmod 4 \right\}.$$

Démonstration : Soient $a, b \in \mathbb{C} \setminus \{0\}$ tels que $a \neq \pm b$ et $|a| \geqslant |b|$. Alors, d'après la Proposition 2.15, il existe $\tau \in \mathcal{F}_{k'}$ tel que $\frac{b}{a} = k'(\tau)$.

On a de plus, d'après les Propositions 2.9 et 2.4,

$$\frac{a-b}{a+b} = k(2\tau) = k'(S2\tau).$$

C'est ici qu'intervient la condition $|a| \geqslant |b|$: elle implique en effet que nécessairement, $S2\tau \in \mathcal{F}_{k'}$ (voir [Cox84] pour les détails).

La Proposition 3.2 montre alors que

$$aM\left(\frac{b}{a}\right) = \frac{a}{\theta_0^2(\tau)},$$

et

$$(a+b)M\left(\frac{a-b}{a+b}\right) = \frac{a+b}{\theta_0^2(S2\tau)}.$$

En utilisant la Proposition 2.4, on obtient

$$\theta_0^2(S2\tau) = -2i\tau\theta_0^2(2\tau),$$

et comme, d'après la formule de duplication de θ_0^2 (Proposition 2.9), on a

$$a+b = \frac{2a\theta_0^2(2\tau)}{\theta_0^2(\tau)},$$

on en déduit finalement que

$$(a+b)M\left(\frac{a-b}{a+b}\right) = \frac{i}{\tau}\frac{a}{\theta_0^2(\tau)} = \frac{i}{\tau}aM\left(\frac{b}{a}\right).$$

Une étude détaillée de l'action des éléments de $\Gamma_{k'}$ sur θ_0^2 (voir [Cox84]) permet de conclure : pour tous $\gamma = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \Gamma_{k'}$ et $\tau \in \mathcal{H}$, on a en effet

$$\frac{\theta_0^2(\gamma\tau)}{\theta_0^2(\tau)} = (-1)^{\frac{t-1}{2}}(z\tau + t),$$

par ailleurs tout élément de $\Gamma_{k'}$ admet un représentant de la forme $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ avec $t \equiv 1 \bmod 4$, z divisible par 4 et t et z premiers entre eux. Réciproquement, si $z, t \in \mathbb{Z}$ sont

premiers entre eux et tels que z est divisible par 4 et $t \equiv 1 \bmod 4$, alors il existe $x, y \in \mathbb{Z}$ tels que $\begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \Gamma_{k'}$. On en déduit le résultat. □

Interprétons le résultat que nous venons de démontrer : si l'on fixe un élément $z \in \mathbb{C} \setminus \{-1, 0, 1\}$, alors il existe $\tau \in \mathcal{H}$ tel que $z = k'(\tau)$, et

$$\mathcal{B}_1(1, z) = \left\{ \frac{1}{(4(c\tau + d) + 1)\,\theta_0^2(\tau)} : c, d \in \mathbb{Z}, \operatorname{pgcd}(c, 4d + 1) = 1 \right\}.$$

Les inverses des points de $\mathcal{B}_1(1, z)$ sont donc inclus dans les points du réseau de $\mathbb{Z}$-base

$$\left[4\theta_0^2(\tau), \tau\theta_0^2(\tau)\right],$$

entièrement paramétré par τ, et l'on peut même déterminer quels sont les points de ce réseau dont les inverses sont dans $\mathcal{B}_1(1, z)$. Ceci permet d'expliquer les Figures 3.1 et 3.2, le réseau apparaissant dans cette dernière correspondant à τ tel que $k'(\tau) = \frac{1}{2} + i$, une telle valeur étant (par exemple) donnée par

$$\tau \simeq -0.53377658198 + 0.61947192232 \cdot i.$$

On a alors

$$\theta_0^2(\tau) \simeq 0.86100156912 + 0.55199942434 \cdot i,$$

ce qui permet de déterminer le réseau contenant les inverses des points de $\mathcal{B}_1\left(1, \frac{1}{2} + i\right)$.

Nous voyons que l'argument clé dans les démonstrations de Cox et Geppert est la Proposition 3.1. C'est en essayant en vain d'obtenir un résultat similaire en genre 2 que nous avons eu l'idée de la démonstration exposée en Sections 3.3.1 et 3.3.2.

Notons que la démonstration donnée par von David [vD28] du Théorème 3.2 est substantiellement différente de celles de Geppert et Cox. En particulier, von David *définit* les theta constantes à partir de l'AGM. Cette façon de faire correspond d'ailleurs à ce qui a été fait historiquement par Gauss.

3.3.4 Quelques remarques sur les suites AGM associées à des theta constantes

Première remarque

Fixons un élément $\tau \in \mathcal{H}$, et définissons comme précédemment la suite

$$(a_n, b_n)_{n \in \mathbb{N}} = \left(\theta_0^2(2^n\tau), \theta_1^2(2^n\tau)\right)_{n \in \mathbb{N}}.$$

Comme le montre le Lemme 2.2, cette suite converge vers 1.

Fixons maintenant $\gamma = \begin{pmatrix} a & 2b \\ 4c & d \end{pmatrix} \in \Gamma_{k'}$. On a donc

$$(a_0, b_0) = \frac{a_0}{\theta_0^2(\gamma\tau_0)} \left(\theta_0^2(\gamma\tau), \theta_1^2(\gamma\tau)\right),$$

et le Lemme 3.1 montre qu'il existe alors $j_0 \in \{0, 1\}$ tel que

$$(a_1, b_1) = \frac{\theta_0^2(2\tau)}{\theta_0^2(2G_{j_0}\gamma\tau)} \left(\theta_0^2(2G_{j_0}\gamma\tau), \theta_1^2(2G_{j_0}\gamma\tau)\right),$$

où G_0 et G_1 sont définies dans le Lemme 3.1.

D'après la Proposition 2.15, les points 2τ et $2G_{j_0}\gamma\tau$ doivent donc être équivalents modulo l'action de $\Gamma_{k'}$. Or

$$2G_{j_0}\gamma\tau = \frac{2a\tau + 4b}{4(j_0 a + c)\tau + 8j_0 b + d},$$

et si $j_0 a + c \equiv 0 \bmod 2$, alors

$$\begin{pmatrix} a & 4b \\ 2(j_0 a + c) & 8j_0 b + d \end{pmatrix} \in \Gamma_{k'}.$$

Ceci permet donc de déterminer j_0 (qui ne dépend que de γ).

Par récurrence directe, on montre l'existence d'une suite $(j_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ telle que, pour tout $n \geqslant 1$,

$$(a_n, b_n) = \frac{a_n}{\theta_0^2(\tau_n)} \left(\theta_0^2(\tau_n), \theta_1^2(\tau_n)\right),$$

où

$$\tau_n = \frac{2^n \gamma\tau}{4\left(\sum_{k=0}^{n-1} 2^k j_k\right)\gamma\tau + 1}.$$

Les mêmes arguments que ci-dessus impliquent que les points $2^n\tau$ et τ_n doivent être équivalents modulo l'action de $\Gamma_{k'}$. Ceci est le cas lorsque la condition

$$c + a\sum_{k=0}^{n-1} 2^k j_k \equiv 0 \bmod 2^n \tag{3.6}$$

est vérifiée, puisqu'alors on a

$$\tau_n = \gamma_n 2^n \tau,$$

avec

$$\gamma_n = \begin{pmatrix} a & 2^{n+1}b \\ 4\frac{c + a\sum_{k=0}^{n-1} 2^k j_k}{2^n} & d + 8b\sum_{k=0}^{n-1} 2^k j_k \end{pmatrix} \in \Gamma_{k'}.$$

Notons que la Condition (3.6) suffit à définir la suite (j_n) de façon unique (comme le développement 2-adique de $-c/a$), puisque si N est le plus petit indice ne vérifiant pas cette condition, alors

$$a_N k'(\tau_N) = -b_N,$$

ce qui contredit la définition de τ_N.

Seconde remarque

Soit $\tau_0 \in \mathcal{H}$, et posons $(a_0, b_0) = \left(\theta_0^2(\tau_0), \theta_1^2(\tau_0)\right)$. On peut alors considérer l'ensemble des modules des éléments de $\mathcal{B}_1(a_0, b_0)$. On a vu que les éléments de cet ensemble sont de la forme $\frac{1}{|c\tau + d|}$, avec c et d premiers entre eux, et c multiple de 4. Cet ensemble admet donc un élément maximal, que l'on notera $\mathcal{L}(\tau_0)$. On a $\mathcal{L}(\tau_0) \geqslant 1$.

Supposons maintenant que $\tau_0 \in \mathcal{F}$: en particulier, pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$, $|c\tau_0 + d| \geqslant 1$, ce qui montre que $\mathcal{L}(\tau_0) = 1$.

Enfin, $\mathcal{L}(S\tau_0)$ est de la forme $\left|-\frac{c}{\tau_0} + d\right|^{-1}$, avec c et d premiers entre eux et c divisible par 4. Si $\mathcal{L}(S\tau_0) > 1$, alors nécessairement $c \neq 0$, et

$$|d\tau_0 - c| < |\tau_0|.$$

Ceci ne peut pas être possible si $|d| = 1$, car $|\mathrm{Re}\,(\tau_0)| \leqslant \frac{1}{2}$. Sinon $|d| \geqslant 3$ et on voit facilement (en utilisant le fait que $\tau_0 \in \mathcal{F}$) que $|\mathrm{Im}\,(d\tau_0 - c)| > |\tau_0|$. On en déduit que $\mathcal{L}(S\tau_0) = 1$.

3.4 Une fonction associée à l'AGM

3.4.1 Définition

Notre objectif dans cette section est de définir une fonction $M : \mathbb{C} \to \mathbb{C}$ à partir de l'AGM *univariée*.

Soit $z \in \mathbb{C} \setminus \{-1, 0, 1\}$, on pose $a_0 = 1$, $b_0 = z$, et l'on considère la suite AGM associée $(a_n, b_n)_{n\in\mathbb{N}}$ ne contenant *que des bons choix de racines* (ce qui est toujours possible avec les suppositions que l'on a faites sur z). Alors cette suite converge vers une valeur non nulle que l'on définit comme étant $M(z)$. On pose par ailleurs $M(-1) = M(0) = 0$ et $M(1) = 1$.

On a la propriété suivante : pour tout $z \in \mathbb{C} \setminus \{0\}$,

$$M(z) = zM\left(\frac{1}{z}\right).$$

3.4.2 Complexité de l'évaluation

Notre objectif dans cette section est de déterminer une fonction $B : \mathbb{N} \times \mathbb{C} \to \mathbb{N}$ telle que, pour tous $N \in \mathbb{N}$ et $z \in \mathbb{C}$, si l'on désigne par $(a_n, b_n)_{n\in\mathbb{N}}$ la suite AGM associée au calcul de $M(z)$, alors $a_{B(N,z)}$ est une approximation de $M(z)$ avec une précision relative de N bits.

Notons dès à présent que

- si $z = 1$, alors $M(z) = 1$ et pour tout $n \in \mathbb{N}$, $a_n = b_n = 1$,
- si $z = 0$, alors $M(z) = 0$ et pour tout $n \in \mathbb{N}$, $a_n = \frac{1}{2^n}$ et $b_n = 0$,
- si $z = -1$, alors $M(z) = 0$ et pour tout $n \geqslant 2$, $a_n = \frac{i}{2^{n-1}}$ et $b_n = 0$.

Nous fixons donc pour le reste de cette section $z \in \mathbb{C} \setminus \{0, -1, 1\}$, et notons $(a_n, b_n)_{n\in\mathbb{N}}$ la suite AGM associée au calcul de $M(z)$. Nous introduisons aussi les quantités auxilliaires suivantes :

- la suite $(m_n)_{n\in\mathbb{N}}$ définie par
$$m_n = \mathrm{Min}\left(|a_n|, |b_n|\right)$$
pour tout $n \in \mathbb{N}$,
- la suite $(M_n)_{n\in\mathbb{N}}$ définie par
$$M_n = \mathrm{Max}\left(|a_n|, |b_n|\right)$$
pour tout $n \in \mathbb{N}$,
- la suite $(c_n)_{n\in\mathbb{N}}$ définie par
$$c_n = \mathrm{Max}\left(\left|\frac{a_n}{b_n}\right|, \left|\frac{b_n}{a_n}\right|\right) = \frac{M_n}{m_n}$$
pour tout $n \in \mathbb{N}$,
- la suite $(\psi_n)_{n\in\mathbb{N}}$, où ψ_n désigne l'angle *non orienté* entre a_n et b_n (voir la Figure 3.3).

Quelques propriétés de la suite $(a_n, b_n)_{n\in\mathbb{N}}$ et des quantités associées

Les propriétés qui sont données ici sont la plupart prouvées et utilisées dans [Cox84] pour montrer la convergence des suites AGM. La Propriété (5) montre le caractère quadratique de la convergence des suites AGM.

1. La suite $(M_n)_{n\in\mathbb{N}}$ est décroissante.
2. Pour tout $n \in \mathbb{N}$ tel que $\psi_n < \pi$ (en fait, d'après la Propriété (3) ci-dessous, on ne peut avoir $\psi_n = \pi$ que pour $n = 0$), on a
$$c_{n+1} \leqslant \frac{\sqrt{c_n}}{\cos\frac{\psi_n}{2}}.$$

En effet, on a

$$\left|\frac{a_{n+1}}{b_{n+1}}\right|^2 = \frac{|a_n+b_n|^2}{4\,|a_nb_n|} \leqslant \frac{(2M_n)^2}{4m_nM_n} = c_n$$

d'une part, et

$$\left|\frac{b_{n+1}}{a_{n+1}}\right|^2 = \frac{4\,|a_nb_n|}{|a_n+b_n|^2} \leqslant \frac{4M_nm_n}{4m_n^2\cos^2\psi_n} = \frac{c_n}{\cos^2\frac{\psi_n}{2}}$$

d'autre part, où l'on a utilisé le fait que

$$|a_n+b_n|^2 = |a_n|^2+|b_n|^2+2\,|a_nb_n|\cos\psi_n \geqslant 2m_n^2\,(1+\cos\psi_n) = 4m_n^2\cos^2\frac{\psi_n}{2}.$$

En particulier, si $\psi_n \leqslant \frac{\pi}{2}$, alors $c_{n+1} \leqslant \sqrt{2c_n}$.

3. Pour tout $n \in \mathbb{N}$,

$$\psi_{n+1} \leqslant \frac{\psi_n}{2}.$$

Pour voir ceci, on notera que a_{n+1}, moyenne arithmétique de a_n et b_n, est situé dans le secteur angulaire défini par a_n et b_n (et qui a pour angle d'ouverture ψ_n). Par ailleurs, comme tous les choix de la suite AGM sont bons, alors b_{n+1} est situé sur la bissectrice du même secteur angulaire. Donc finalement, a_{n+1} est situé soit dans le secteur angulaire définie par a_n et b_{n+1}, soit dans celui défini par b_n et b_{n+1}, et comme tous deux ont pour angle d'ouverture $\psi_n/2$, on en déduit le résultat. Ceci est illustré par la Figure 3.3 (la zone hachurée correspond au demi-plan contenant le mauvais choix correspondant à $-b_{n+1}$, qui est déterminé par a_{n+1}).

4. Pour tout $n \in \mathbb{N}$,

$$m_{n+1} \geqslant m_n\cos\frac{\psi_n}{2}.$$

Pour voir ceci, notons que $m_n \leqslant |b_{n+1}|$, et que

$$|a_{n+1}|^2 = \frac{1}{4}\left(|a_n|^2+|b_n|^2+2\,|a_nb_n|\cos\psi_n\right) \geqslant m_n^2\frac{1+\cos\psi_n}{2} = \left(m_n\cos\frac{\psi_n}{2}\right)^2.$$

5. Pour tout $n \in \mathbb{N}$,

$$|a_{n+1}-b_{n+1}| \leqslant \frac{1}{4m_n}\,|a_n-b_n|^2\,.$$

Pour voir ceci, notons α_n (resp. β_n) une racine carrée de a_n (resp. de b_n), telles que $\alpha_n\beta_n = b_{n+1}$. Alors

$$|a_{n+1}-b_{n+1}| = \frac{1}{2}\,|\alpha_n-\beta_n|^2 = \frac{1}{2\,|\alpha_n+\beta_n|^2}\,|a_n-b_n|^2\,,$$

et comme l'angle non-orienté entre α_n et β_n vaut $\frac{\psi_n}{2} \leqslant \frac{\pi}{2}$ (puisque tous les choix de la suite AGM sont bons), alors

$$|\alpha_n+\beta_n| \geqslant \sqrt{2}\mathrm{Min}\,(|\alpha_n|\,,|\beta_n|) = \sqrt{2m_n},$$

d'où le résultat.

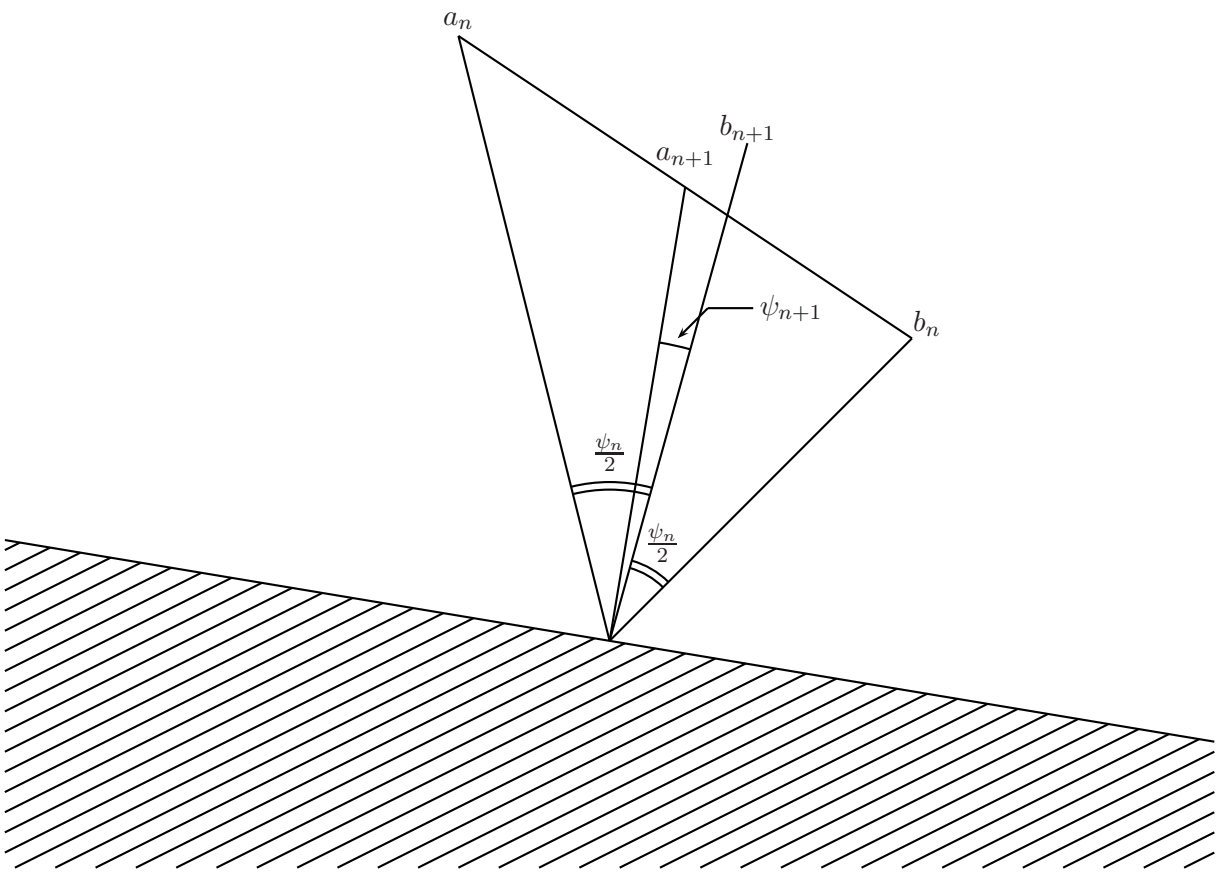

FIG. 3.3 – Une itération AGM correspondant à un bon choix de racine

6. Pour tout $n \in \mathbb{N}$,
$$|a_{n+1} - b_{n+1}| \leqslant \frac{1}{2} |a_n - b_n| .$$
Pour voir ceci, on introduit α_n et β_n comme ci-dessus : comme tous les choix sont bons, alors en particulier on a
$$|\alpha_n - \beta_n| \leqslant |\alpha_n + \beta_n| ,$$
donc
$$|a_{n+1} - b_{n+1}| = \frac{1}{2} |\alpha_n - \beta_n|^2 \leqslant \frac{1}{2} |\alpha_n - \beta_n| \cdot |\alpha_n + \beta_n| = \frac{1}{2} |a_n - b_n| .$$

Cas où $\mathrm{Re}\,(z) \geqslant 0$

Ceci est équivalent à la condition $\psi_0 \leqslant \frac{\pi}{2}$.
D'après la Propriété (2) ci-dessus on a alors, pour tout $n \geqslant 0$,
$$\log_2 c_{n+1} \leqslant \frac{1 + \log_2 c_n}{2},$$
soit, *via* une récurrence directe,
$$\log_2 c_n \leqslant \frac{\log_2 c_0 + 2^n - 1}{2^n}.$$
Comme $\log_2 c_0 = |\log_2 |z||$, on en déduit donc que si $n \geqslant \log_2 |\log_2 |z||$, alors $\log_2 c_n \leqslant 1$ donc $c_n \leqslant 2$.

Soient maintenant $n \in \mathbb{N}$ et $k \geqslant 1$, alors d'après la Propriété (5),

$$|a_{n+k+1} - b_{n+k+1}| \leqslant \frac{1}{4m_{n+k}} |a_{n+k} - b_{n+k}|^2 ,$$

et comme d'après une récurrence directe utilisant la Propriété (4), on a

$$m_{n+k} \geqslant \left(\prod_{j=0}^{k-1} \cos \frac{\psi_{n+j}}{2} \right) m_n,$$

et même (*via* la Propriété (3))

$$m_{n+k} \geqslant \left(\prod_{j=1}^{k} \cos \frac{\psi_n}{2^j} \right) m_n,$$

on utilise alors la minoration

$$\prod_{j=1}^{k} \cos \frac{\psi_n}{2^j} \geqslant \prod_{j \geqslant 1} \cos \frac{\psi_n}{2^j} = \frac{\sin \psi_n}{\psi_n}$$

(voir [GR65, page 38] pour une démonstration de l'égalité de droite) pour finalement obtenir

$$|a_{n+k+1} - b_{n+k+1}| \leqslant \frac{1}{4\frac{\sin \psi_n}{\psi_n} m_n} |a_{n+k} - b_{n+k}|^2 .$$

Si l'on pose $d_n = \log_2 |a_n - b_n|$ et $e_n = \log_2 \left(4\frac{\sin \psi_n}{\psi_n} m_n \right)$, alors d'après ce qui précède, pour tous $n \in \mathbb{N}$ et $k \geqslant 0$,

$$d_{n+k+1} \leqslant 2d_{n+k} - e_n$$

(le fait que cela soit aussi vrai pour $k = 0$ découle directement de la Propriété (5)). Une récurrence directe montre alors que pour tout $k \geqslant 0$,

$$d_{n+k} \leqslant 2^k (d_n - e_n) + e_n. \tag{3.7}$$

Cherchons maintenant à majorer la quantité

$$\frac{|M(z) - a_n|}{|M(z)|}.$$

On a

$$|a_{n+1} - a_n| = \frac{1}{2} |a_n - b_n| ,$$

donc pour tout $k \geqslant 1$,

$$|a_{n+k} - a_n| \leqslant \sum_{j=0}^{k-1} |a_{n+j+1} - a_{n+j}| \leqslant \frac{1}{2} \sum_{j=0}^{k-1} |a_{n+j} - b_{n+j}| ,$$

et comme, par une récurrence directe utilisant la Propriété (6), on a

$$|a_{n+j} - b_{n+j}| \leqslant \frac{1}{2^j} |a_n - b_n| ,$$

on en déduit que

$$|a_{n+k} - a_n| \leqslant \sum_{j=1}^{k} \frac{1}{2^j} |a_n - b_n| \leqslant |a_n - b_n| .$$

En faisant tendre k vers l'infini, on en déduit que

$$|M(z) - a_n| \leqslant |a_n - b_n| .$$

Par ailleurs, pour tous $n \in \mathbb{N}$ et $k \geqslant 1$, on a

$$|a_{n+k}| \geqslant m_{n+k} \geqslant \frac{\sin \psi_n}{\psi_n} m_n,$$

donc en faisant tendre k vers l'infini, on en déduit que

$$|M(z)| \geqslant \frac{\sin \psi_n}{\psi_n} m_n.$$

Nous avons donc prouvé que pour tous $n, k \in \mathbb{N}$,

$$\frac{|M(z) - a_{n+k}|}{M(z)} \leqslant \frac{|a_{n+k} - b_{n+k}|}{\frac{\sin \psi_n}{\psi_n} m_n} = 2^{d_{n+k} - e_n + 2}.$$

On en déduit que pour que a_{n+k} soit une approximation de $M(z)$ avec une précision relative de N bits, il suffit que $N + 2 \leqslant e_n - d_{n+k}$.

Posons maintenant $n_1 = \mathrm{Max}\left(\lceil \log_2 |\log_2 |z|| \rceil, 1\right)$: d'après ce que nous avons vu plus haut, on a alors $c_{n_1} \leqslant 2$ et $\psi_{n_1} \leqslant \frac{\pi}{4}$. En particulier,

$$\frac{|a_{n_1} - b_{n_1}|}{m_{n_1}} \leqslant \frac{1}{m_{n_1}} \left(|a_{n_1}| + |b_{n_1}|\right) \leqslant 1 + c_{n_1} \leqslant 3,$$

donc si l'on pose $n_2 = n_1 + 2$, on a

$$\frac{|a_{n_2} - b_{n_2}|}{m_{n_2}} \leqslant \frac{|a_{n_1} - b_{n_1}|}{4 m_{n_2}} \leqslant \frac{|a_{n_1} - b_{n_1}|}{4 \cos \frac{\psi_{n_1}}{2} \cos \frac{\psi_{n_1}}{4} m_{n_1}} \leqslant \frac{3}{4 \cos \frac{\pi}{8} \cos \frac{\pi}{16}} < 1.$$

Par ailleurs,

$$\frac{\sin \psi_{n_2}}{\psi_{n_2}} \geqslant \frac{\sin \frac{\pi}{16}}{\frac{\pi}{16}} \geqslant 0.99,$$

donc on obtient

$$\frac{|a_{n_2} - b_{n_2}|}{4 \frac{\sin \psi_{n_2}}{\psi_{n_2}} m_{n_2}} \leqslant \frac{1}{2},$$

c'est-à-dire $d_{n_2} - e_{n_2} \leqslant -1$.

D'après ce qui précède (Équation (3.7)), pour tout $k \geqslant 0$, on a alors

$$d_{n_2+k} \leqslant 2^k (d_{n_2} - e_{n_2}) + e_{n_2} \leqslant -2^k + e_{n_2},$$

donc si l'on pose $k = \lceil \log_2(N + 2) \rceil$, alors

$$e_{n_2} - d_{n_2+k} \geqslant 2^k \geqslant N + 2,$$

ce qui garantit que a_{n_2+k} est une approximation de $M(z)$ avec une précision relative de N bits.

Nous avons donc prouvé le résultat suivant :

Proposition 3.3 *Pour tout $z \in \mathbb{C} \setminus \{0,1\}$ ayant partie réelle positive ou nulle, si l'on note $(a_n, b_n)_{n\in\mathbb{N}}$ la suite AGM associée au calcul de $M(z)$ et que l'on pose*

$$B(N,z) = \mathrm{Max}\left(\lceil \log_2 |\log_2 |z|| \rceil, 1\right) + \lceil \log_2(N+2) \rceil + 2,$$

alors $a_{B(N,z)}$ est une approximation de $M(z)$ avec une précision relative de N bits.

Notons que le fait que $B(N,z) = B\left(N, \frac{1}{z}\right)$ était attendu, puisque $M(z) = zM\left(\frac{1}{z}\right)$.

La complexité de l'évaluation de $M(z)$ a déjà été abordée en exemple à la Section 1.2.2. On y a montré que pour calculer une approximation de $M(z)$ avec une précision relative de N bits, en posant

$$N' = \lceil N + 2 + B(N+2,z) \log_2 3 \rceil,$$

il est suffisant de partir de $\mathrm{Rep}_{N'}(z)$ et d'effectuer $B(N+2,z)$ itérations d'AGM en travaillant toujours à précision N', d'où (puisque le temps d'évaluation d'une racine carrée est proportionnel à celui d'une multiplication) une complexité en $O\left(\mathcal{M}(N')B(N+2,z)\right)$, soit

$$O\left(\mathcal{M}\left(N + \log|\log|z||\right)\left(\log N + \log|\log|z||\right)\right).$$

Dans le cas particulier où l'on suppose que

$$0 < B_1 \leqslant |z| \leqslant B_2,$$

cette complexité devient

$$O\left(\mathcal{M}(N) \log N\right)$$

(indépendamment de z).

Tout ceci montre que l'Algorithme 3 peut être utilisé pour évaluer la fonction M.

Algorithme : `EvaluateM`
Entrée : $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) \geqslant 0$, $N \in \mathbb{N}$
Sortie : m tel que $\left|\frac{M(z)-m}{M(z)}\right| \leqslant \frac{1}{2^N}$

if $z = 0$ **then**
  return 0;
end
if $z = 1$ **then**
  return 1;
end
$B \leftarrow B(N+2, z)$;
$a_n \leftarrow 1$;
$b_n \leftarrow z$;
for $n = 1$ **to** B **do**
  $c \leftarrow (a_n + b_n)/2$;
  $b_n \leftarrow \sqrt{a_n b_n}$;
  $a_n \leftarrow c$;
end
return a_n;

Algorithme 3: Évaluation de la fonction M

D'après ce que nous avons vu, dans cet algorithme, on doit toujours travailler à la précision

$$N + 2 + B(N + 2, z) \log_2 3.$$

C'est l'un des points importants de l'AGM : le processus n'est pas auto-correctif, comme le sont par exemple les itérations de Newton (voir la Section 1.3), et toutes les itérations doivent donc se faire à la précision maximale.

Cas où $\mathrm{Re}\,(z) < 0$

Dans le cas où $\psi_0 < \pi$, en utilisant le même raisonnement que précédemment, on montre que

$$c_1 \leqslant \frac{\sqrt{c_0}}{\cos \psi_0},$$

puis (comme $\psi_n \leqslant \frac{\pi}{2}$ dès que $n \geqslant 1$, d'après la Propriété (3)) que

$$\log_2 c_{n+1} \leqslant \frac{2^n - 1 + \log_2 c_1}{2^n} \leqslant \frac{2^n - 1 + \frac{1}{2} \log_2 c_0 - \log_2 \cos \psi_0}{2^n}$$

La condition

$$2^n \geqslant \frac{1}{2} \left|\log_2 |z|\right| - \log_2 \cos \psi_0$$

suffit donc à garantir que $c_{n+1} \leqslant 2$.

Le reste est inchangé, ce qui prouve que dans le cas où $\psi_0 \in \left]\frac{\pi}{2}, \pi\right[$, si l'on pose

$$B(N, z) = \left\lceil \log_2 \left(\frac{1}{2} \left|\log_2 |z|\right| - \log_2 \cos \phi_0 \right) \right\rceil + \lceil \log_2 (N + 2) \rceil + 3,$$

alors $a_{B(N,z)}$ est une approximation de $M(z)$ avec une précision relative de N bits.

Reste enfin à traiter le cas où $z = -x$ ($x > 0$, $x \neq 1$). Comme $M(z) = zM\left(\frac{1}{z}\right)$, on peut de plus supposer que $x < 1$. On a alors

$$M(z) = \frac{1 - x}{2} M\left(\frac{2i\sqrt{x}}{1 - x} \right),$$

et l'on est ramené au cas où $\mathrm{Re}\,(z) \geqslant 0$, donc on peut appliquer la Proposition 3.3.

Nous ne détaillons pas plus la complexité de l'évaluation de $M(z)$ dans le cas $\mathrm{Re}\,(z) < 0$: par la suite, nous nous ramènerons toujours explicitement au cas où la partie réelle de z est positive.

3.5 Évaluation du logarithme complexe

3.5.1 Bornes explicites pour l'évaluation du logarithme *via* l'AGM

Le but de cette section est de montrer le résultat suivant :

Théorème 3.3 *Soit $z \in \mathbb{C} \setminus \{0\}$ tel que $|z| \leqslant \frac{1}{2^{10}}$ et que $|\mathrm{Arg}\,(z)| \leqslant \frac{\pi}{4}$. Alors*

$$\left| \log \frac{z}{4} + \frac{\pi}{2M(z)} \right| \leqslant 0.26 \, |z|^2 \left(1 + \left| \log \frac{z}{4} \right| \right),$$

où la détermination du logarithme est choisie de façon à ce que sa partie imaginaire soit dans $\left[-\frac{\pi}{4}, \frac{\pi}{4}\right]$.

Dans le cas où z est un réel strictement positif, de tels bornes sont bien connues et s'obtiennent typiquement en considérant des intégrales elliptiques, comme expliqué dans [BB84] par exemple.

Nous utiliserons dans la démonstration de ce théorème le résultat suivant :

Proposition 3.4 *Soient $A(x) = 1 + \sum_{n\geqslant 1} a_n x^n$ et $B(x) = 1 + \sum_{n\geqslant 1} b_n x^n$ deux séries à coefficients complexes, et $\alpha, \beta > 0$ tels que, pour tout $n \geqslant 1$, on ait $|a_n| \leqslant \alpha^n$ et $|b_n| \leqslant \beta^n$.*

Alors on peut écrire

$$A(x).B(x) = 1 + \sum_{n\geqslant 1} c_n x^n$$

et

$$\frac{1}{A(x)} = 1 + \sum_{n\geqslant 1} d_n x^n,$$

où, pour tout $n \geqslant 1$,

$$|c_n| \leqslant (2\mathrm{Max}(\alpha, \beta))^n$$

et

$$|d_n| \leqslant (2\alpha)^n.$$

Démonstration : L'existence des séries pour $A.B$ et pour $\frac{1}{A}$ est claire. Pour simplifier, on pose $a_0 = b_0 = c_0 = d_0 = 1$.

Commençons par le cas du produit : si l'on pose $\gamma = \mathrm{Max}(\alpha, \beta)$, alors pour tout $n \geqslant 0$, on a

$$\begin{aligned}
|c_n| &= \left|\sum_{k=0}^{n} a_k b_{n-k}\right| \\
&\leqslant \sum_{k=0}^{n} |a_k b_{n-k}| \\
&\leqslant \sum_{k=0}^{n} \alpha^k \beta^{n-k} \\
&\leqslant \sum_{k=0}^{n} \gamma^n \\
&\leqslant (n+1)\gamma^n \\
&\leqslant (2\gamma)^n.
\end{aligned}$$

Pour traiter le cas de l'inverse, nous allons procéder par récurrence : soit $n \geqslant 1$ tel que, pour tout $k \in [0, n-1]$, on ait $|d_k| \leqslant (2\alpha)^k$, alors

$$\sum_{k=0}^{n} a_k d_{n-k} = 0,$$

donc

$$\begin{aligned} |d_n| &= \left| \sum_{k=1}^{n} a_k d_{n-k} \right| \\ &\leqslant \sum_{k=1}^{n} |a_k| \, |d_{n-k}| \\ &\leqslant \sum_{k=1}^{n} \alpha^k (2\alpha)^{n-k} \\ &\leqslant \alpha^n \sum_{k=0}^{n-1} 2^k \\ &\leqslant (2\alpha)^n, \end{aligned}$$

ce qui conclut la démonstration. □

Démonstration (du théorème) : En considérant les q-séries des theta constantes et en utilisant la Propriété 3.4, on montre que

$$\frac{k(\tau)}{4q^{\frac{1}{2}}} = \left(\frac{\theta_2(\tau)}{2q^{\frac{1}{4}}\theta_0(\tau)} \right)^2 = 1 + \sum_{n \geqslant 1} r_n q^n,$$

avec $|r_n| \leqslant 16^n$ pour tout $n \geqslant 1$.

Soit $z \in \mathbb{C} \setminus \{0\}$ tel que $|z| \leqslant \frac{1}{2^{10}}$ et $|\mathrm{Arg}\,(z)| \leqslant \frac{\pi}{4}$. D'après la Proposition 2.15 (et le fait que $k(S\tau) = k'(\tau)$), il existe $\tau_z \in \mathcal{H}$ tel que $z = k(\tau_z)$. Par ailleurs, en utilisant le Lemme 2.4 et le fait que k est modulaire pour le groupe $\Gamma_k = S\Gamma_k' S$, on montre que si l'on pose

$$\mathcal{G}_k = \left\{ T^{-1}, I, T, T^2, T^{-2}S, T^{-1}S, S, TS, T^{-1}ST, ST, TST, T^2ST \right\},$$

alors

$$\mathcal{F}_k = \bigcup_{\gamma \in \mathcal{G}_k} \gamma \mathcal{C}$$

est un domaine fondamental pour l'action de Γ_k sur $\mathcal{H}$. On peut donc supposer que $\tau_z \in \mathcal{F}_k$, et l'on pose $q_z = \exp(\pi i \tau_z)$.

Si $\tau \in \mathcal{C}$, alors en particulier $\mathrm{Im}\,(\tau) \geqslant \frac{\sqrt{3}}{2}$, et la Propriété 2.6 permet de montrer que

$$\frac{1}{2} < \left(\frac{1 - 0.141}{1 + 0.141} \right)^2 \leqslant \left| k'(\tau) \right| \leqslant \left(\frac{1 + 0.141}{1 - 0.141} \right)^2 < 2, \tag{3.8}$$

et que

$$|k(\tau)| \leqslant 4 \left(\frac{1 + 0.005}{1 - 0.141} \right)^2 \exp\left(-\pi \frac{\sqrt{3}}{4} \right) < \frac{3}{2}. \tag{3.9}$$

Les formules de transformation des theta constantes sous l'action de S et de T (Proposition 2.4) montrent que, pour tout $\tau \in \mathcal{H}$,

$$\begin{array}{llll} k(T^2ST\tau) &= \frac{-1}{k'(\tau)}, & k(T^{-2}S\tau) &= -k'(\tau), \\ k(T^{-1}S\tau) &= -i\frac{k'(\tau)}{k(\tau)}, & k(S\tau) &= k'(\tau), \\ k(TS\tau) &= i\frac{k'(\tau)}{k(\tau)}, & k(T^{-1}ST\tau) &= \frac{-1}{k(\tau)}, \\ k(ST\tau) &= \frac{1}{k'(\tau)}, & k(TST\tau) &= \frac{1}{k(\tau)}. \end{array}$$

En utilisant ces formules et les bornes données par (3.8) et (3.9), on montre aisément que pour tous $\tau \in \mathcal{C}$ et $\gamma \in \mathcal{G}_k \setminus \{T^{-2}, T^{-1}, I, T\}$, on a

$$|k(\gamma\tau)| \geqslant \frac{1}{3},$$

donc (comme $|k(\tau_z)| = |z| \leqslant \frac{1}{2^{10}}$), on en déduit que

$$\tau_z \in T^{-2}\mathcal{C} \cup T^{-1}\mathcal{C} \cup \mathcal{C} \cup T\mathcal{C},$$

et en particulier que $\operatorname{Im}(\tau_z) \geqslant \frac{\sqrt{3}}{2}$.

Notons maintenant que si l'on suppose que $\operatorname{Im}(\tau_z) \leqslant H$ pour une certaine constante H, alors $|q_z| \geqslant \exp(-\pi H)$ et, en utilisant à nouveau la Propriété 2.6, on montre que

$$|k(\tau_z)| \geqslant 4\left(\frac{1-0.005}{1+0.141}\right)^2 \exp\left(-\pi\frac{H}{2}\right) = f(H).$$

En particulier, $2^{10} f(5) > 1$, ce qui montre que nécessairement, $\operatorname{Im}(\tau_z) \geqslant 5$.

On a alors

$$\left|\sum_{n\geqslant 1} r_n q_z^n\right| \leqslant \sum_{n\geqslant 1} (16\exp(-5\pi))^n \leqslant \frac{16\exp(-5\pi)}{1-16\exp(-5\pi)} = C_1,$$

d'où l'on déduit que

$$|q_z| = \left|\frac{k(\tau_z)}{4\left(1+\sum_{n\geqslant 1} r_n q_z^n\right)}\right| \leqslant \frac{|k(\tau_z)|^2}{16(1-C_1)^2} = C_2\,|k(\tau_z)|^2,$$

ce qui, au passage, fournit une meilleure majoration de $|q_z|$ que $\exp(-5\pi)$.

Notons aussi que

$$\left|\frac{k(\tau_z)}{4q_z^{\frac{1}{2}}} - 1\right| = \left|\sum_{n\geqslant 1} r_n q_z^n\right| \leqslant C_1,$$

donc

$$\left|\operatorname{Arg}\left(\frac{k(\tau_z)}{q_z^{\frac{1}{2}}}\right)\right| \leqslant \operatorname{Arcsin}(C_1),$$

et

$$|\operatorname{Re}(\tau_z)| = \frac{1}{\pi}\,|\operatorname{Arg}(q_z)| \leqslant \frac{1}{\pi}\left(2\,|\operatorname{Arg}(k(\tau_z))| + 2\operatorname{Arcsin}(C_1)\right) < \frac{1}{2}$$

(puisque $|\operatorname{Arg}(z)| \leqslant \frac{\pi}{4}$).

En particulier, $\tau_z \in \mathcal{F}$, donc $S\tau_z \in \mathcal{F}_{k'}$ et la Proposition 3.2 montre que

$$M\left(k'(S\tau_z)\right) = \frac{1}{\theta_0^2(\tau_z)},$$

d'où

$$M(k(\tau_z)) = \frac{i}{\tau_z\theta_0^2(\tau_z)}$$

(en utilisant la Propriété 2.4).

Nous sommes maintenant prêts à établir la borne annoncée : en utilisant l'égalité précédente, on a

$$\begin{aligned}
\left|\log\frac{z}{4}+\frac{\pi}{2M(z)}\right| &= \left|\log\frac{k(\tau_z)}{4}-\frac{i\pi\tau_z\theta_0^2(\tau_z)}{2}\right| && (3.10)\\
&\leqslant \left|\log\frac{k(\tau_z)}{4q^{\frac{1}{2}}}\right|+\frac{1}{2}\left|\log q_z-i\pi\tau_z\theta_0^2(\tau_z)\right| && (3.11)\\
&\leqslant \left|\log\left(1+\sum_{n\geqslant 1}r_nq_z^n\right)\right|+\frac{\pi\left|\tau_z\right|}{2}\left|1-\theta_0^2(\tau_z)\right|. && (3.12)
\end{aligned}$$

Un rapide calcul montre que $r_1=-4$, par ailleurs

$$\left|\sum_{n\geqslant 2}r_nq_z^n\right|\leqslant\sum_{n\geqslant 2}(16q_z)^n\leqslant 16C_1\left|q_z\right|,$$

donc

$$\left|\sum_{n\geqslant 1}r_nq_z^n\right|\leqslant(4+16C_1)\left|q_z\right|=C_3\left|q_z\right|.$$

En utilisant le développement de Taylor de la fonction logarithme au voisinage de 1, on montre alors que

$$\begin{aligned}
\left|\log\left(1+\sum_{n\geqslant 1}r_nq_z^n\right)\right| &\leqslant \sum_{n\geqslant 1}\left(C_3\left|q_z\right|\right)^n && (3.13)\\
&\leqslant \frac{C_3}{1-C_3\exp(-5\pi)}\left|q_z\right| && (3.14)\\
&\leqslant \frac{C_2C_3}{1-C_3\exp(-5\pi)}\left|z\right|^2=C_4\left|z\right|^2. && (3.15)
\end{aligned}$$

Comme de plus

$$\log\frac{k(\tau_z)}{4q_z^{\frac{1}{2}}}=\log\frac{k(\tau_z)}{4}-\frac{\pi i\tau_z}{2},$$

la majoration (3.15) implique que

$$\frac{\pi\left|\tau_z\right|}{2}\leqslant\left|\log\frac{k(\tau_z)}{4}\right|+\left|\log\frac{k(\tau_z)}{4q_z^{\frac{1}{2}}}\right|\leqslant\left|\log\frac{z}{4}\right|+C_4\left|z\right|^2. \qquad (3.16)$$

Enfin, la Proposition 3.4 montre que

$$\theta_0^2(\tau_z)-1=\sum_{n\geqslant 1}s_nq_z^n,$$

avec $|s_n|\leqslant 4^n$ pour tout $n\geqslant 1$, donc

$$\begin{aligned}
\left|\theta_0^2(\tau_z)-1\right| &\leqslant \sum_{n\geqslant 1}\left(4\left|q_z\right|\right)^n && (3.17)\\
&\leqslant \frac{4}{1-4\exp(-5\pi)}\left|q_z\right| && (3.18)\\
&\leqslant \frac{4C_2}{1-4\exp(-5\pi)}\left|z\right|^2=C_5\left|z\right|^2. && (3.19)
\end{aligned}$$

On déduit finalement de (3.12), (3.15), (3.16) et (3.19) que

$$\left|\log\frac{z}{4}+\frac{\pi}{2M(z)}\right| \leqslant |z|^2\left(C_4+C_5\left(\left|\log\frac{z}{4}\right|+C_4\,|z|^2\right)\right),$$

et une application numérique (en utilisant le fait que $|z| \leqslant \frac{1}{2^{10}}$) permet finalement de conclure. □

3.5.2 Algorithmes

Évaluation de π

L'une des applications les plus connues de l'AGM est sans doute le calcul de π. Nous abordons ce problème ici car π intervient dans l'évaluation du logarithme.

La référence la plus complète concernant les méthodes de calcul de π (et plus particulièrement celles utilisant l'AGM) est certainement [BB87]. Nous décrivons ci-dessous une méthode due (indépendamment) à Brent [Bre76] et à Salamin [Sal76] (nous renvoyons à ces références pour une démonstration).

Si l'on pose $a_0 = 1$, $b_0 = \frac{1}{\sqrt{2}}$, que l'on définit la suite AGM associée $(a_n, b_n)_{n\in\mathbb{N}}$ et que l'on introduit la suite intermédiaire $(c_n)_{n\in\mathbb{N}}$ définie par

$$c_n = a_n^2 - b_n^2$$

pour tout $n \geqslant 0$, alors la quantité

$$\pi_n = \frac{2a_{n+1}^2}{1-\sum_{k=0}^{n} 2^k c_k}$$

converge quadratiquement vers π. Plus précisément, on a

$$|\pi - \pi_n| \leqslant \frac{1}{2^{2^n}},$$

et on en déduit directement l'Algorithme 4 permettant dévaluer une approximation de π avec une précision relative de N bits en temps $O(\mathcal{M}(N)\log N)$. Les meilleurs algorithmes pour le calcul de π décrits dans [BB87] ont la même complexité asymptotique.

On notera que dans [Bor88], Borchardt donnait deux algorithmes proches de l'AGM permettant de calculer π. Le premier consistait à partir de (a_0, b_0) et à définir

$$a_{n+1} = \frac{a_n + b_n}{2}$$

et

$$b_{n+1} = \sqrt{a_{n+1}b_n}.$$

Comme dans le cas de l'AGM, ces deux suites convergent vers une limite commune, et si l'on part de $a_0 = \frac{1}{4}$ et $b_0 = \frac{1}{2\sqrt{2}}$, cette limite vaut $\frac{1}{\pi}$. Le second algorithme consistait à utiliser les itérations

$$b_{n+1} = \sqrt{a_n b_n}$$

et

$$a_{n+1} = \frac{a_n + b_{n+1}}{2}.$$

Dans ce cas encore, les deux suites convergent vers une limite commune, qui vaut $\frac{1}{\pi}$ lorsque $a_0 = \frac{1}{4}$ et $b_0 = \frac{1}{2}$. Malheureusement, la convergence de ces deux algorithmes n'est pas quadratique mais seulement linéaire, ce qui les rend peu attractifs.

Algorithme : `EvaluatePi`
Entrée : $N \in \mathbb{N}$
Sortie : p tel que $|\pi - p| \leqslant \frac{1}{2^N}$

$a \leftarrow 1$;
$b \leftarrow \frac{1}{\sqrt{2}}$;
$t \leftarrow \frac{1}{4}$;
$x \leftarrow 1$;
while $a - b > \frac{1}{2^N}$ **do**
  $y \leftarrow a$;
  $a \leftarrow \frac{a+b}{2}$;
  $b \leftarrow \sqrt{by}$;
  $t \leftarrow t - x(a-y)^2$;
  $x \leftarrow 2x$;
end
return $\frac{(a+b)^2}{4t}$;

Algorithme 4: Évaluation de π

Évaluation de $\log 2$

Soit $n \geqslant 12$ et $z = \frac{1}{2^n}$, alors le Théorème 3.3 montre que

$$\left| \log z + \frac{\pi}{2M\left(4z\right)} \right| \leqslant 16 \times 0.26\, z^2 \left(1 + |\log z|\right),$$

donc, puisque $\log z = -n \log 2$, on a en particulier

$$\left| \frac{\log z + \frac{\pi}{2M(4z)}}{\log z} \right| \leqslant \frac{1}{2^{2n-3}}.$$

On en déduit donc que $\frac{-\pi}{2M(4z)}$ est une approximation de $\log z = -n \log 2$ avec une précision relative de $2n - 3$ bits.

Si l'on veut calculer une approximation de $\log_2$ avec une précision relative de $N \geqslant 20$ bits, il suffit donc poser $n = \left\lceil \frac{N+4}{2} \right\rceil$, et de calculer

$$\mathrm{Rep}_{N+1}\left(-\frac{\pi}{2nM\left(\frac{1}{2^n-2}\right)} \right),$$

qui est bien une approximation de $\log 2$ avec une précision relative de N bits.

Les résultats de la Section 3.4.2 montrent que ce calcul peut se faire en temps $O\left(\mathcal{M}(N) \log N\right)$ (y compris le calcul de π, d'après la section qui précède).

Évaluation du logarithme d'un nombre complexe

Soit $z \in \mathbb{C} \setminus \{0\}$ dont on souhaite évaluer une détermination du logarithme. Quitte à le multiplier par une puissance de i (auquel cas il faudra ajouter ou soustraire un multiple de $i\frac{\pi}{2}$ au résultat), on peut supposer que $|\mathrm{Arg}\,(z)| \leqslant \frac{\pi}{4}$. On s'intéresse alors à la détermination de $\log z$ dont la partie imaginaire est dans l'intervalle $\left]-\frac{\pi}{4}, \frac{\pi}{4}\right]$.

Supposons que l'on veuille déterminer $\log z$ avec une précision relative de $N \geqslant 20$ bits. Quitte à multiplier z par la puissance de 2 adéquate (auquel cas il faudra ajouter au résultat le multiple correspondant de $\log 2$), on suppose que

$$\frac{1}{2^M + 1} \leqslant |z| \leqslant \frac{1}{2^M},$$

avec $M = \left\lceil \frac{N+4}{2} \right\rceil$.

Le Théorème 3.3 montre alors que $\frac{-\pi}{2M(4z)}$ est une approximation de $\log z$ avec une précision relative de $N + 1$ bits, donc

$$\mathrm{Rep}_{N+1}\left(\frac{-\pi}{2M(4z)}\right)$$

est une approximation de $\log z$ avec une précision relative de N bits.

Les résultats de la Section 3.4.2 montrent alors que ce calcul prend un temps en $O\left(\mathcal{M}(N) \log N\right)$ (y compris le calcul de π et de $\log 2$, comme le montrent les sections précédentes).

Chapitre 4

Algorithmes d'évaluation de fonctions modulaires

Le principal objectif de ce chapitre est de décrire des algorithmes pour l'évaluation rapide de fonctions modulaires. Dans les deux premières sections, nous nous intéressons à l'évaluation des fonctions k et k' : par un algorithme "naïf" tout d'abord, puis par un algorithme utilisant l'AGM, ayant une complexité quasi-optimale. La troisième section traite de l'évaluation d'autres fonctions modulaires. Enfin, la quatrième section donne des applications de ce type d'algorithmes au calcul de polynômes de classe et de polynômes modulaires.

4.1 Algorithme naïf

Commençons par remarquer que les formules de transformation des fonctions k et k' sous l'action de S et T sont connues (nous les avons données Section 2.2.4). Nous avons par ailleurs décrit des algorithmes permettant d'écrire un élément $\tau \in \mathcal{H}$ quelconque sous la forme $\tau = \gamma\tau'$, avec $\gamma \in \Gamma_1$ et $\tau' \in \mathcal{F}$ (Algorithme 1), et de décomposer un élément quelconque $\gamma \in \Gamma_1$ en un produit des générateurs S et T (l'algorithme est en fait la preuve de la Proposition 2.1). On ne perd donc pas de généralité à se restreindre à l'évaluation de k et k' sur le domaine fondamental $\mathcal{F}$. Pour ce faire, la méthode la plus directe est sans doute de revenir à la définition que nous avons donnée de ces fonctions comme (carrés de) quotients de theta constantes. Le problème peut donc se ramener à celui de l'évaluation des theta constantes, dont les séries en q sont connues et peuvent donc être utilisées.

Rappelons que ces séries, particulièrement simples, sont données par

$$\theta_0(\tau) = 1 + 2\sum_{n\geqslant 1} q^{n^2},$$

$$\theta_1(\tau) = 1 + 2\sum_{n\geqslant 1} (-1)^n q^{n^2}$$

et

$$\theta_2(\tau) = 2q^{\frac{1}{4}} \sum_{n\geqslant 0} q^{n^2+n}.$$

Introduisons, pour tout $B \geqslant 0$, les sommes partielles

$$S_{j,B}(\tau) = \begin{cases} 1 & \text{si } B = 0 \\ 1 + 2\sum_{n=1}^{B} (-1)^{jn} q^{n^2} & \text{sinon,} \end{cases}$$

(pour $j \in \{0,1\}$) et

$$S_{2,B}(\tau) = \sum_{j=0}^{B} q^{n^2+n}.$$

On a alors, pour tous $B \geqslant 0$, $\tau \in \mathcal{F}$ et $j \in \{0,1\}$:

$$\begin{aligned} |\theta_j(\tau) - S_{j,B}(\tau)| &= 2\left|\sum_{n>B} (-1)^{jn} q^{n^2}\right| \\ &\leqslant 2\sum_{n>B} |q|^{n^2} \\ &\leqslant 2\sum_{n\geqslant (B+1)^2} |q|^{n} \\ &\leqslant 2\frac{|q|^{(B+1)^2}}{1-|q|} \\ &\leqslant 3\,|q|^{(B+1)^2}, \end{aligned}$$

où l'on a utilisé le fait que $|q| \leqslant \exp\left(-\pi\frac{\sqrt{3}}{2}\right)$. La même technique permet de montrer que l'on a aussi

$$\left|\frac{\theta_2(\tau)}{2q^{\frac{1}{4}}} - S_{2,B}(\tau)\right| \leqslant 2\,|q|^{(B+1)^2+B+1}.$$

En utilisant la Proposition 2.6, on montre alors que pour tous $B \geqslant 0$ et $\tau \in \mathcal{F}$,

$$\left|\frac{\theta_j(\tau) - S_{j,B}(\tau)}{\theta_j(\tau)}\right| \leqslant 4\,|q|^{(B+1)^2}$$

pour $j \in \{0,1\}$, et

$$\left|\frac{\theta_2(\tau) - 2q^{\frac{1}{4}} S_{2,B}(\tau)}{\theta_2(\tau)}\right| \leqslant 4\,|q|^{(B+1)^2+B+1}.$$

On pose alors

$$B(N,\tau) = \left\lceil \sqrt{\frac{N+2}{\pi \log_2 e \mathrm{Im}\,(\tau)}} - 1 \right\rceil,$$

de sorte que pour tous $N \geqslant 0$ et $\tau \in \mathcal{F}$, $S_{0,B(N,\tau)}(\tau)$ (resp. $S_{1,B(N,\tau)}(\tau)$, resp. $2q^{\frac{1}{4}} S_{2,B(N,\tau)}(\tau)$) soit une approximation de $\theta_0(\tau)$ (resp. de $\theta_1(\tau)$, resp. de $\theta_2(\tau)$) avec une précision relative de N bits. On en déduit que l'Algorithme 5 peut être utilisé pour évaluer les theta constantes sur $\mathcal{F}$.

Une récurrence directe permet de montrer que pour toute valeur de n *à la fin* de la boucle "for", on a $q_a = q^{n^2}$, $q_b = q^{n^2+n}$, $q_c = q^{2n+1}$, $q_d = q^2$,

$$T_0 = \sum_{k=1}^{n} q^{k^2},$$

$$T_1 = \sum_{k=1}^{n} (-1)^k q^{k^2}$$

et

$$T_2 = \sum_{k=0}^{n} q^{n^2+n}.$$

Algorithme : `EvaluateThetasNaive`
Entrée : $\tau \in \mathcal{F}$, $N \in \mathbb{N}$
Sortie : (T_0, T_1, T_2) tel que $|T_j/\theta_j(\tau) - 1| \leqslant 2^{-N}$ pour $j \in \{0, 1, 2\}$

$r_4 \leftarrow \exp\left(i\pi\frac{\tau}{4}\right)$;
$q \leftarrow r_4^4$;
$q_a \leftarrow q$;
$q_b \leftarrow q^2$;
$q_c \leftarrow q$;
$q_d \leftarrow q_b$;
$T_0 \leftarrow q$;
$T_1 \leftarrow -q$;
$T_2 \leftarrow 1 + q_d$;
$B \leftarrow B(N + 2, \tau)$;
for $n = 2$ **to** B **do**
  $q_c \leftarrow q_c \cdot q_d$;
  $q_a \leftarrow q_a \cdot q_c$;
  $q_b \leftarrow q_b \cdot q_c \cdot q$;
  $T_0 \leftarrow T_0 + q_a$;
  $T_1 \leftarrow T_1 + (-1)^n q_a$;
  $T_2 \leftarrow T_2 + q_b$;
end
$T_0 \leftarrow 1 + 2T_0$;
$T_1 \leftarrow 1 + 2T_1$;
$T_2 \leftarrow 2r_4 \cdot T_2$;
return (T_0, T_1, T_2)

Algorithme 5: Évaluation naïve des theta constantes

Ceci montre donc la validité de l'algorithme. Reste à étudier la précision à laquelle il convient de travailler à chaque étape. En utilisant les résultats du Chapitre 1 et en notant que, comme $|q| \leqslant \exp\left(-\pi\frac{\sqrt{3}}{2}\right)$, il ne peut y avoir de grosse perte de précision lors des additions (ou soustractions), on montre qu'il est suffisant de toujours travailler avec une précision en $O(N)$ (il est possible de détailler plus, ce qui est d'ailleurs nécessaire pour l'implantation, mais cela devient vite très technique et n'est guère éclairant). On en déduit donc que la complexité en temps de cet algorithme est en

$$O\left(\mathcal{M}(N)\sqrt{\frac{N}{\operatorname{Im}(\tau)}}\right),$$

donc en particulier en $O\left(\mathcal{M}(N)\sqrt{N}\right) = O\left(N^{1.5+\varepsilon}\right)$.

On en déduit directement l'Algorithme 6 permettant d'évaluer les fonctions k et k' sur $\mathcal{F}$, avec la même complexité.

Algorithme : `EvaluatekAndkpNaive`
Entrée : $\tau \in \mathcal{F}$, $N \in \mathbb{N}$
Sortie : (a, b) tel que $|a/k(\tau) - 1| \leqslant 2^{-N}$ et $|b/k'(\tau) - 1| \leqslant 2^{-N}$

$(x, y, z) \leftarrow$`EvaluateThetasNaive`$(\tau, N + 5)$;
return $\left((y/x)^2, (z/x)^2\right)$;

Algorithme 6: Évaluation naïve des theta constantes

Remarques

Le fait que les séries en q des theta constantes soient creuses (plus précisément, que les puissances de q augmentent comme des carrés) est crucial dans l'obtention d'un algorithme en $O\left(N^{1.5+\varepsilon}\right)$: avec des séries non creuses, on aurait obtenu une complexité en $O\left(N^{2+\varepsilon}\right)$. C'est pourquoi, pour évaluer k et k', on ne calcule pas leurs séries en q : ces séries ne sont plus creuses ! Par ailleurs, on profite aussi ici du fait que les coefficients non nuls des séries que l'on manipule sont particulièrement simples.

L'évaluation conjointe de θ_0 et de θ_1 a un coût sensiblement égal à celui de l'évaluation d'une seule de ces deux fonctions (la seule différence étant dans les additions). Si par contre on veut aussi évaluer θ_2, alors le temps de calcul sera approximativement doublé (puisqu'à chaque itération, il faudra alors effectuer 4 multiplication contre 2 sinon).

On notera enfin que l'on peut mettre à profit l'égalité de Jacobi (Proposition 2.10) pour se restreindre à l'évaluation de deux des theta constantes et en déduire la troisième *via* une extraction de racine quatrième. Ceci peut induire une perte de précision, et la complexité exacte de cette méthode est discutée à la Section 4.2.4. On retiendra que cette technique est intéressante lorsque la précision requise est grande devant $\operatorname{Im}(\tau)$.

4.2 Utilisation de l'AGM

4.2.1 Principe général

L'une des applications classiques de l'AGM est le calcul des périodes des courbes elliptiques (principalement sur celles définies par une équation réelle, comme décrit par exemple dans [BM88]). En particulier, étant donné $k'(\tau)$ (par exemple), l'AGM permet de calculer

numériquement τ. L'idée est la suivante : supposons que l'on connaisse la valeur de $k'(\tau)$ pour un certain $\tau \in \mathcal{F}$. Alors, d'après la Proposition 3.2, on a

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)},$$

mais (comme $S\tau \in \mathcal{F}_{k'}$), la même proposition montre aussi que

$$M\left(k'(S\tau)\right) = \frac{1}{\theta_0^2(S\tau)},$$

ce qui, d'après la Proposition 2.4, s'écrit aussi

$$M\left(k(\tau)\right) = \frac{i}{\tau\theta_0^2(\tau)}.$$

On en déduit que

$$\tau = i\frac{M\left(k'(\tau)\right)}{M\left(k(\tau)\right)},$$

et la valeur de $k(\tau)$ peut se déduire de celle de $k'(\tau)$ en utilisant l'égalité de Jacobi :

$$k(\tau) = \sqrt{1 - k'^2(\tau)},$$

et la Proposition 3.1 qui permet montrer que $\mathrm{Re}\left(k(\tau)\right) > 0$.

Dans la suite de cette section, afin de simplifier les notations, nous désignerons par $\mathbb{C}^{r+}$ l'ensemble des nombres complexes à partie réelle strictement positive, et lorsque $z \in \mathbb{C}^{r+}$, nous noterons $\sqrt{z}$ l'unique racine carrée de z dans $\mathbb{C}^{r+}$.

Fixons maintenant $\tau \in \mathcal{F}$, et introduisons la fonction

$$\begin{array}{rccl} f_\tau : & \mathbb{C}^{r+} & \to & \mathbb{C} \\ & z & \mapsto & iM(z) - \tau M\left(\sqrt{1-z^2}\right). \end{array}$$

D'après ce qui précède, on a $f_\tau\left(k'(\tau)\right) = 0$. On peut donc penser que des itérations de Newton sur la fonction f_τ vont nous permettre d'évaluer $k'(\tau)$. Pour montrer que cela va être possible, nous allons commencer par montrer un certain nombre de résultats concernant cette fonction f_τ.

Remarquons tout d'abord que f_τ est analytique sur $\mathbb{C}^{r+} \setminus \{1\}$. Ceci est une conséquence directe de sa définition et de la proposition suivante :

Proposition 4.1 *La fonction $M : \mathbb{C}^{r+} \to \mathbb{C}$ est analytique.*

Démonstration : Nous commençons par montrer que le théorème des fonctions implicites peut être appliqué à k' en tout point de $\mathcal{F}_{k'}$: ceci vient du fait que k' est analytique sur $\mathcal{H}$, et que pour tout $\tau \in \mathcal{F}_{k'}$,

$$\frac{dk'}{d\tau}(\tau) = \frac{-i\pi\theta_1^2(\tau)\theta_2^4(\tau)}{2\theta_0^2(\tau)} \neq 0$$

(où l'on a utilisé la Proposition 2.12 pour obtenir l'expression de la dérivée de k'). Par ailleurs, la fonction $1/\theta_0^2(\tau)$ est aussi analytique sur $\mathcal{F}_{k'}$, et pour tout $\tau \in \mathcal{F}_{k'}$,

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)}$$

(d'après la Proposition 3.2). Comme k' est surjective de $\mathcal{F}_{k'}$ dans $\mathbb{C}^{r+}\setminus\{1\}$, on en déduit que M est analytique sur $\mathbb{C}^{r+}\setminus\{1\}$, et comme elle est continue en 1, on en déduit qu'elle est analytique sur $\mathbb{C}^{r+}$. □

Les deux propositions qui suivent vont nous renseigner sur la dérivée de la fonction f_τ en $k'(\tau)$.

Proposition 4.2 *Pour tout $\tau \in \mathcal{F}_{k'}$, on a*

$$\frac{dM}{dz}\left(k'(\tau)\right) = \frac{\theta_0'(\tau)}{i\pi\theta_0(\tau)\theta_1^2(\tau)\theta_2^4(\tau)},$$

où $\theta_0' = \frac{d\theta_0}{d\tau}$.

Démonstration : Soit $\tau \in \mathcal{F}_{k'}$. D'après la Proposition 3.2, on a

$$M\left(k'(\tau)\right) = \frac{1}{\theta_0^2(\tau)},$$

et en dérivant cette égalité par rapport à τ, on obtient

$$2k'(\tau)\left(\frac{d}{d\tau}\log\frac{\theta_1}{\theta_2}(\tau)\right)\frac{dM}{dz}\left(k'(\tau)\right) = -\frac{2\theta_0'(\tau)}{\theta_0^3(\tau)},$$

soit, en utilisant la Propriété 2.12,

$$\frac{dM}{dz}\left(k'(\tau)\right) = \frac{\theta_0'(\tau)}{i\pi\theta_0(\tau)\theta_1^2(\tau)\theta_2^4(\tau)}.$$

□

Proposition 4.3 *Pour tout $\tau \in \mathcal{F}$, on a*

$$\frac{df_\tau}{dz}\left(k'(\tau)\right) = \frac{-2}{\pi\tau\theta_1^2(\tau)\theta_2^4(\tau)}.$$

Démonstration : En dérivant la définition de f_τ, on obtient

$$\frac{df_\tau}{dz}(z) = i\frac{dM}{dz}(z) + \frac{\tau z}{\sqrt{1-z^2}}\frac{dM}{dz}\left(\sqrt{1-z^2}\right),$$

d'où

$$\frac{df_\tau}{dz}\left(k'(\tau)\right) = i\frac{dM}{dz}\left(k'(\tau)\right) + \tau\frac{k'(\tau)}{k'(S\tau)}\frac{dM}{dz}\left(k'(S\tau)\right),$$

où l'on a utilisé le fait que $k^2 + k'^2 = 1$ et que $k'(S\tau) = k(\tau)$.

L'égalité prouvée à la Proposition 4.2 permet alors d'écrire

$$\frac{df_\tau}{dz}\left(k'(\tau)\right) = \frac{4\theta_0'(\tau)}{\pi\theta_0(\tau)\theta_1^2(\tau)\theta_2^4(\tau)} + \frac{4\tau k'(\tau)\theta_0^2(S\tau)}{i\pi k'(S\tau)\theta_0(S\tau)\theta_1^2(S\tau)\theta_2^4(S\tau)}. \tag{4.1}$$

Si l'on dérive maintenant l'égalité

$$\theta_0^2(S\tau) = -i\tau\theta_0^2(\tau)$$

(Proposition 2.4), on obtient

$$2\theta_0(S\tau)\theta_0'(S\tau) = -i\tau^2\theta_0(\tau)\left(\theta_0(\tau) + 2\tau\theta_0'(\tau)\right).$$

En injectant cette dernière égalité dans (4.1) et en utilisant la formule de transformation des theta constantes sous l'action de S (Proposition 2.4), on obtient finalement le résultat anoncé. □

Cette dernière proposition montre en particulier que la dérivée de f_τ en $k'(\tau)$ est non nulle, donc (d'après le Théorème 1.2 par exemple) que l'on va effectivement pouvoir utiliser des itérations de Newton sur la fonction f_τ pour évaluer $k'(\tau)$. Pour ce faire, il est *a priori* nécessaire de savoir évaluer la dérivée de f_τ. Plusieurs techniques sont alors utilisables, par exemple :

– se ramener à deux évaluations successives de f_τ : si ε est assez petit, alors

$$\frac{f_\tau(z+\varepsilon) - f_\tau(z)}{\varepsilon} = \frac{df_\tau}{dz}(z) + O(\varepsilon)$$

(cette manière de procéder est étudiée par exemple dans [Bre75]),

– utiliser directement un algorithme permettant l'évaluation de la dérivée de la fonction M (plusieurs tels algorithmes sont décrits dans [BB87]).

Nous allons en fait utiliser une technique alternative (et, accessoirement, plus rapide) : introduisons la fonction

$$\begin{array}{rccc} g: & \mathbb{C}^{r+} \setminus \{1\} & \to & \mathbb{C} \\ & z & \mapsto & \frac{M(z)^3}{z(1-z^2)}. \end{array}$$

Cette fonction g est analytique sur $\mathbb{C}^{r+} \setminus \{1\}$ (d'après la Proposition 4.1), et (d'après la Proposition 3.2)

$$g\left(k'(\tau)\right) = \frac{1}{\theta_1^2(\tau)\theta_2^4(\tau)},$$

d'où (d'après la Proposition 4.2)

$$\frac{df_\tau}{dz}\left(k'(\tau)\right) = \frac{-2}{\pi\tau} g\left(k'(\tau)\right).$$

Posons maintenant, pour simplifier les notations, $\xi = k'(\tau)$. Si l'on considère la démonstration du Théorème 1.2, on voit que le résultat de convergence des itérations est inchangé si l'on considère des itérations de la forme

$$z_{n+1} = z_n - \frac{f_\tau(z_n)}{f_\tau'(\xi)} = z_n + \frac{\pi\tau f_\tau(z_n)}{2g(\xi)}$$

(le résultat étant d'ailleurs plus simple à obtenir dans ce cas). Le problème dans notre cas est que l'on ne connaît pas la valeur de $g(\xi)$. Cependant, comme z_n est censé être déjà une approximation de ξ et que g est analytique, on peut alors considérer des itérations de la forme

$$N_{f_\tau}(z) = z + \frac{\pi\tau f_\tau(z)}{2g(z)}.$$

Si l'on pose

$$F(\tau) = \sup_{n \geqslant 2} \left| \frac{f_\tau^{(n)}(\xi)}{n! f_\tau'(\xi)} \right|^{\frac{1}{n-1}},$$

$$G(\tau) = \sup_{n \geqslant 1} \left| \frac{g^{(n)}(\xi)}{n! g'(\xi)} \right|^{\frac{1}{n}}$$

et

$$H(\tau) = \mathrm{Max}\left(F(\tau), G(\tau)\right),$$

alors on a la variante suivante du Théorème 1.2 :

Théorème 4.1 *Soient $\tau \in \mathcal{F}$, et $\xi = k'(\tau)$. En conservant les notations ci-dessus, si $z_0 \in \mathbb{C}^{r+} \setminus \{1\}$ est tel que*

$$|z_0 - \xi| \leqslant \frac{1}{2^A}$$

pour une constante A vérifiant

$$\frac{H}{2^A} \leqslant \frac{1}{9},$$

et que la suite $(z_n)_{n \in \mathbb{N}} \in \mathbb{C}^{r+} \setminus \{1\}$ vérifie

$$|z_{n+1} - N_{f_\tau}(z_n)| \leqslant \frac{1}{2^{A+2^{n+1}}}$$

pour tout $n \geqslant 0$, alors

$$|z_n - \xi| \leqslant \frac{1}{2^{A+2^n-1}}$$

pout tout $n \geqslant 0$.

Démonstration : Soit $z \in \mathbb{C}^{r+} \setminus \{1\}$ tel que $H(\tau)\,|z-\xi| \leqslant \frac{1}{9}$, alors

$$\begin{aligned}
|N_{f_\tau}(z) - \xi| &= \left|\frac{\pi\tau}{2g(z)}\right| \cdot \left| f_\tau(z) - \left(\frac{-2g(z)}{\pi\tau}\right)(z-\xi) \right| && (4.2)\\
&\leqslant \left|\frac{\pi\tau}{2g(z)}\right| \left(\left| f_\tau(\xi) - f'_\tau(\xi)(z-\xi) \right| + \left| f'_\tau(\xi) - \left(\frac{-2g(z)}{\pi\tau}\right) \right| \cdot |z-\xi| \right) && (4.3)\\
&\leqslant \left|\frac{\pi\tau}{2g(z)}\right| \cdot \left| f_\tau(\xi) - f'_\tau(\xi)(z-\xi) \right| + \left| \frac{g(\xi)-g(z)}{g(z)} \right| \cdot |z-\xi|\,. && (4.4)
\end{aligned}$$

En utilisant les mêmes techniques que pour la démonstration du Théorème 1.2, on montre par ailleurs que

$$\left| f_\tau(\xi) - f'_\tau(\xi)(z-\xi) \right| \leqslant \left| f'_\tau(\xi) \right| \frac{F(\tau)}{1 - F(\tau)\,|z-\xi|} |z-\xi|^2\,, \tag{4.5}$$

et que

$$|g(\xi) - g(z)| \leqslant |g(\xi)| \frac{G(\tau)}{1 - G(\tau)\,|z-\xi|} |z-\xi|\,. \tag{4.6}$$

En combinant les majorations (4.4), (4.5) et (4.6), on obtient

$$|N_{f_\tau}(z) - \xi| \leqslant \left|\frac{g(\xi)}{g(z)}\right| \left(\frac{F(\tau)}{1 - F(\tau)\,|z-\xi|} + \frac{G(\tau)}{1 - G(\tau)\,|z-\xi|} \right) |z-\xi|^2\,. \tag{4.7}$$

La majoration (4.6) permet de montrer que

$$\left|\frac{g(\xi)}{g(z)}\right| = \frac{1}{1 + \frac{g(z)-g(\xi)}{g(\xi)}} \leqslant \frac{1}{1 - \frac{G(\tau)|z-\xi|}{1-G(\tau)|z-\xi|}} \leqslant \frac{1 - G(\tau)\,|z-\xi|}{1 - 2G(\tau)\,|z-\xi|},$$

ce qui, combiné avec (4.7), donne

$$|N_{f_\tau}(z)-\xi| \leqslant 1\frac{1-G(\tau)\,|z-\xi|}{1-2G(\tau)\,|z-\xi|}\left(\frac{F(\tau)}{1-F(\tau)\,|z-\xi|}+\frac{G(\tau)}{1-G(\tau)\,|z-\xi|}\right)|z-\xi|^2\,. \tag{4.8}$$

Notons maintenant que
– la fonction $x \mapsto \frac{1-x}{1-2x}$ est croissante sur $\left]0,\frac{1}{2}\right[$, et vaut 2 en $x=\frac{1}{3}$,
– la fonction $x \mapsto \frac{x}{1-x}$ est croissante sur $]0,1[$.
On déduit donc de (4.8) la nouvelle majoration

$$|N_{f_\tau}(z)-\xi| \leqslant 4\frac{H(\tau)\,|z-\xi|^2}{1-H(\tau)\,|z-\xi|}. \tag{4.9}$$

Supposons que $z_0 \in \mathbb{C}^{r+}\setminus\{1\}$ soit tel que $|z_0-\xi| \leqslant \frac{1}{2^A}$, avec A une constante telle que

$$\frac{H(\tau)}{2^A} \leqslant \frac{1}{9},$$

et que la suite $(z_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{C}^{r+}\setminus\{1\}$ vérifie

$$|z_{n+1}-N_{f_\tau}(z_n)| \leqslant \frac{1}{2^{A+2^{n+1}}}$$

pour tout $n \geqslant 0$.

Nous allons montrer le résultat voulu par récurrence : supposons que, pour un certain $n\in\mathbb{N}$, on ait

$$|z_n-\xi| \leqslant \frac{1}{2^{A+2^n-1}}.$$

En particulier, on a

$$H(\tau)\,|z_n-\xi| \leqslant \frac{1}{9},$$

donc, *via* la majoration (4.9), on a

$$\begin{aligned} |N_{f_\tau}(z_n)-\xi| &\leqslant 4\frac{H(\tau)\,|z_n-\xi|^2}{1-H(\tau)\,|z_n-\xi|} &(4.10)\\ &\leqslant 4\frac{H(\tau)}{1-H(\tau)\,|z_n-\xi|}\frac{1}{2^{2A+2^{n+1}-2}}. &(4.11)\end{aligned}$$

Comme la fonction $x\mapsto\frac{1}{1-x}$ est croissante sur $]0,1[$ (et que $|z_n-\xi|\leqslant\frac{1}{2^A}$, ceci implique que

$$|N_{f_\tau}(z_n)-\xi| \leqslant 4\frac{\frac{H(\tau)}{2^A}}{1-\frac{H(\tau)}{2^A}}\frac{1}{2^{A+2^{n+1}-2}} \leqslant \frac{1}{2^{A+2^{n+1}}},$$

où l'on a utilisé le fait que $x\mapsto\frac{x}{1-x}$ vaut $\frac{1}{8}$ en $x=\frac{1}{9}$.

On a donc

$$|z_{n+1}-\xi| \leqslant |z_{n+1}-N_{f_\tau}(z_n)|+|N_{f_\tau}(z_n)-\xi| \leqslant \frac{1}{2^{A+2^{n+1}-1}},$$

ce qui conclut. □

Ce résultat montre que la variante des itérations de Newton que nous avons introduite pour la fonction f_τ va effectivement pouvoir être utilisée pour évaluer $k'(\tau)$.

4.2.2 Un premier algorithme

Intéressons-nous maintenant aux précisions de calcul nécessaires : posons pour cela

$$h_\tau = 4 + \lceil \log_2 H(\tau) \rceil,$$

alors le théorème peut s'appliquer avec $A = h_\tau$. On supposera par ailleurs que l'on pose

$$z_{n+1} = \mathrm{Rep}_{h_\tau + 2^{n+1}} \left(N_{f_\tau}(z_n) \right). \tag{4.12}$$

Notons que, comme $\tau \in \mathcal{F}$, l'Inégalité (3.8) donne un encadrement de $|k'(\tau)|$:

$$\frac{1}{2} < \left| k'(\tau) \right| < 2,$$

donc si l'on veut évaluer $k'(\tau)$ avec une précision relative de N bits, il est suffisant de le faire avec une précision *absolue* de $N+1$ bits. En particulier, si (z_n) est une suite vérifiant les hypothèses du théorème (avec $A = h_\tau$), et que l'on pose

$$n(N) = \lceil \log_2 (N + 2 - h_\tau) \rceil,$$

alors $z_{n(N)}$ est une approximation de $k'(\tau)$ avec une précision relative de N bits.

Pour tout $n \geqslant 0$, on a (d'après (4.12) et le théorème)

$$\left| \frac{\pi \tau f_\tau(z_n)}{2 g(z_n)} \right| \leqslant \frac{1}{2^{h_\tau + 2^n}},$$

et cette quantité doit être évaluée avec une précision *absolue* de $h_\tau + 2^{n+1}$ bits, donc une précision *relative* de 2^n bits. En tenant compte des pertes de précision pouvant intervenir, il est suffisant d'évaluer $f_\tau(z_n)$ et $g(z_n)$ avec une précision relative de $2^n + 5$ bits. Le problème restant est que l'évaluation de $f_\tau(z_n)$ comporte une soustraction entraînant une importante perte de précision. Pour contourner ce problème, nous allons plutôt nous intéresser à la précision *absolue* avec laquelle il faut approcher $f_\tau(z_n)$. Notons pour commencer que, d'après la Propriété 2.6, on a

$$\frac{1}{32\,|q|} \leqslant |g(\xi)| \leqslant \frac{1}{8\,|q|}. \tag{4.13}$$

D'après la démonstration du Théorème 4.1 (Inégalité (4.6)), on a aussi

$$\left| \frac{g(z_n) - g(\xi)}{g(\xi)} \right| \leqslant \frac{H(\tau)\,|z_n - \xi|}{1 - H(\tau)\,|z_n - \xi|} \leqslant \frac{1}{8},$$

donc, d'après (4.13) :

$$\frac{1}{64\,|q|} \leqslant |g(z_n)| \leqslant \frac{1}{4\,|q|}.$$

Ceci montre qu'il est suffisant d'évaluer $f_\tau(z_n)$ avec une précision absolue de

$$h_\tau + 2^{n+1} - \log_2 \left(64 \frac{|q|}{|\tau|} \right) \leqslant h_\tau + 2^{n+1} + 5\mathrm{Im}\,(\tau)$$

bits. Comme les additions (ou soustractions) ne peuvent provoquer d'importante perte de précision *absolue*, ceci donne donc aussi la précision absolue à laquelle $M(z_n)$ et $M\left(\sqrt{1 - z_n^2}\right)$ doivent être évalués. Notons enfin que, comme

$$|M(z)| \geqslant \mathrm{Min}\,(1, \mathrm{Re}\,(z))$$

Algorithme : `Evaluatekp1`
Entrée : $\tau \in \mathbb{F}$, $N \in \mathbb{N}$, $h_\tau \in \mathbb{N}$
Sortie : k'_a tel que $|k'_1/k'(\tau) - 1| \leqslant 2^{-N}$

$z \leftarrow$`EvaluatekpNaive`(τ, h_τ);
$n_N \leftarrow \lceil \log_2(N + 2 - h_\tau) \rceil$;
for $n = 1$ **to** n_N **do**
  $a \leftarrow$`EvaluateM`$(z, \lceil 2^{n+1} + h_\tau + 5\mathrm{Im}\,(\tau) - \alpha(z) \rceil)$;
  $b \leftarrow$`EvaluateM`$(\sqrt{1-z^2}, \lceil 2^{n+1} + h_\tau + 5\mathrm{Im}\,(\tau) - \alpha\left(\sqrt{1-z^2}\right) \rceil)$;
  $z \leftarrow z + \frac{\pi\tau z(1-z^2)(ia-\tau b)}{2a^3}$;
end
return z;

Algorithme 7: Évaluation de k' *via* l'AGM et des itérations de Newton

(d'après 7.3), alors si l'on pose

$$\alpha(z) = \mathrm{Min}\,(0, \log_2 \mathrm{Re}\,(z))\,,$$

une approximation de $M(z)$ avec une précision *relative* de $N - \alpha(z)$ bits est aussi une approximation avec une précision *absolue* de N bits.

On en déduit finalement que l'Algorithme 7 peut être utilisé pour évaluer $k'(\tau)$.

Si l'on travaille à τ fixé et que l'on étudie la complexité de l'algorithme lorsque N tend vers l'infini, les choses sont relativement simples : le coût des itérations de Newton, classiquement, et proportionnel au coût de la dernière itération, et l'on obtient directement une complexité en $O\,(\mathcal{M}(N) \log N)$. Nous avons donc montré le résultat suivant :

Théorème 4.2 *Pour tout $\tau \in \mathcal{F}$, il existe un algorithme permettant, pour tout $N \geqslant 0$, d'évaluer $k'(\tau)$ avec une précision relative de N bits en temps*

$$O\,(\mathcal{M}(N) \log N)\,.$$

Notons cependant que ceci suppose que l'on connaît une majoration de h_τ, ce qui en pratique est problématique.

Si l'on s'intéresse à l'évolution de la complexité lorsque l'on fait varier à la fois N et τ, les choses se compliquent :

- la valeur de h_τ semble augmenter linéairement avec $\mathrm{Im}\,(\tau)$; en fait, le calcul de la dérivée seconde de f_τ en $k'(\tau)$ permet de montrer que h_τ augmente au moins en
$$-\log_2 |q| = \pi \log_2 e \mathrm{Im}\,(\tau)\,;$$
ceci n'est pas catastrophique puisque l'algorithme naïf (Algorithme 6) nécessite un nombre *constant* de multiplications pour évaluer $k'(\tau)$ à une précision linéaire en $\mathrm{Im}\,(\tau)$,
- lorsque $\mathrm{Im}\,(\tau) \to +\infty$, $k'(\tau)$ tend vers 1 et $\sqrt{1-k'^2(\tau)} = k(\tau)$ tend vers 0, donc l'évaluation de $M\left(\sqrt{1-z_n^2}\right)$ nécessaire pour évaluer $f_\tau(z_n)$ lors des itérations de Newton prendra un temps de plus en plus important : une étude précise montre que le nombre d'itérations nécessaire sera en $O\,(\log \mathrm{Im}\,(\tau) + 2^n) = O\,(\log \mathrm{Im}\,(\tau) + N)$.

On notera donc au final que, si l'on fixe une constante $C > 0$, alors dans les cas où $N \leqslant C\mathrm{Im}\,(\tau)$, l'algorithme naïf permet d'évaluer $k'(\tau)$ avec une précision relative de N bits en temps $O\,(\mathcal{M}(N) \log N)$, et dans les cas où $N \geqslant C\mathrm{Im}\,(\tau)$, la discussion ci-dessus montre que l'Algorithme 7 permet d'atteindre la même complexité, *en supposant que h_τ augmente bien linéairement avec* $\mathrm{Im}\,(\tau)$.

4.2.3 Variante et amélioration de la complexité

Le but de cette section est de prouver le résultat suivant :

Théorème 4.3 *Il exite un algorithme permettant, pour tous $\tau \in \mathcal{F}$ et $N \geqslant 0$, d'évaluer $k'(\tau)$ avec une précision relative de N bits en temps*

$$O\left(\mathcal{M}(N)\log N\right).$$

Notons que c'est ici l'ordre des mots qui est important : alors que, dans le Théorème 4.2, la valeur de τ était fixée, elle est ici quelconque. L'intérêt de ce théorème est donc de montrer que la complexité de l'évaluation de $k'(\tau)$ *ne dépend pas de la valeur de* τ.

Le principal ingrédient que nous allons utiliser est le résultat suivant :

Proposition 4.4 *Soit U un ouvert de $\mathbb{C}$, h une fonction analytique sur U et K un sous-ensemble compact de U tel que h ne s'annule pas sur K. Alors la fonction H définie pour $z \in U$ par*

$$H(z) = \sup_{n\geqslant 1}\left|\frac{h^{(n)}(z)}{n!h(z)}\right|^{\frac{1}{n}}$$

est bornée sur K.

Démonstration : Comme $K \subset U$, il existe une constante $\varepsilon > 0$ telle que, pour tous $z \in K$ et $z' \in \mathbb{C}$,

$$\left|z - z'\right| \leqslant \varepsilon \Rightarrow z' \in U.$$

Alors, par application du théorème des résidus, pour tous $z \in K$ et $n \geqslant 1$,

$$h^{(n)}(z) = \frac{1}{2\pi i}\int_{C(z,\varepsilon)} \frac{h(t)}{(t-z)^{n-1}}dt,$$

où $C(z,\varepsilon)$ est le cercle de centre z et de rayon ε. Si l'on note h_m (resp. h_M) le minimum (resp. le maximum) de $|h(z)|$ sur K, alors

$$\left|\frac{h^{(n)}(z)}{n!h(z)}\right| \leqslant \frac{h_M}{n!\varepsilon^n h_m} \leqslant \frac{h_M}{\varepsilon^n h_m}$$

pour tout $n \geqslant 1$, donc

$$H(z) \leqslant \frac{1}{\varepsilon}\sup_{n\geqslant 1}\left(\frac{h_M}{h_m}\right)^{\frac{1}{n}} \leqslant \frac{h_M}{\varepsilon h_m},$$

ce qui conclut la démonstration. □

Fixons maintenant $r > 1$, et posons

$$\mathcal{F}_r = \{\tau \in \mathcal{F} : |\tau| \leqslant r\}$$

(qui est un compact). La Proposition 4.4 montre alors qu'il existe H_r tel que, pour tout $\tau \in \mathcal{F}_r$, $h_\tau \leqslant H_r$. Notons par ailleurs que sur $\mathcal{F}_r$, la distance de $k'(\tau)$ à 1 est minorée, de même que la distance de $k(\tau) = \sqrt{1-k'^2(\tau)}$ à 0. La discussion à la fin de la section précédente montre alors qu'il existe un algorithme qui, pour tous $\tau \in \mathcal{F}_r$ et $N \geqslant 0$, permet d'évaluer $k'(\tau)$ avec une précision relative de N bits en temps $O\left(\mathcal{M}(N)\log N\right)$, indépendamment de la valeur de τ.

Le principe est maintenant relativement simple : soient $\tau \in \mathcal{F}$ et $N \geqslant 0$, alors si $N \leqslant 10\,\mathrm{Im}\,(\tau)$, l'algorithme naïf (Algorithme 6) permet d'évaluer $k'(\tau)$ avec une précision relative de N bits et il a la complexité requise. Sinon, il existe un entier n tel que $\frac{\tau}{2^n} \in \mathcal{F}_2$. On peut alors évaluer $k'\left(\frac{\tau}{2^n}\right)$ en utilisant l'Algorithme 7 vu à la section précédente, puis calculer

$$\theta_0^2\left(\frac{\tau}{2^n}\right) = \frac{1}{M\left(k'\left(\frac{\tau}{2^n}\right)\right)}$$

et

$$\theta_1^2\left(\frac{\tau}{2^n}\right) = k'\left(\frac{\tau}{2^n}\right)\theta_0^2\left(\frac{\tau}{2^n}\right).$$

Ensuite, la Proposition 2.9 et le fait que, d'après la Proposition 2.6, les valeurs des theta constantes θ_0 et θ_1 sur $\mathcal{F}$ soient relativement proches de 1 (et en particulier aient partie réelle strictement positive) montrent que

$$\theta_0^2\left(\frac{\tau}{2^{n-1}}\right) = \frac{\theta_0^2\left(\frac{\tau}{2^n}\right) + \theta_1^2\left(\frac{\tau}{2^n}\right)}{2}$$

et

$$\theta_1^2\left(\frac{\tau}{2^{n-1}}\right) = \sqrt{\theta_0^2\left(\frac{\tau}{2^n}\right)\theta_1^2\left(\frac{\tau}{2^n}\right)},$$

et ce procédé peut être itéré. Ainsi, en n itérations AGM (pour lesquelles on connaît les choix de racines), on obtient $\theta_0^2(\tau)$ et $\theta_1^2(\tau)$, donc $k'(\tau)$, qui est leur quotient.

Si l'on veut évaluer $k'(\tau)$ avec une précision relative de N bits, les résultats de la Section 3.4.2 montrent qu'il faut évaluer les carrés des theta constantes en $\frac{\tau}{2^n}$ avec une précision relative de $N' = N + n\log_2 3$ bits, et que pour cela il conviendra d'abord d'évaluer k' en $\frac{\tau}{2^n}$ avec une précision relative de

$$N' + 2 + B\left(N' + 2, k'\left(\frac{\tau}{2^n}\right)\right)\log_2 3$$

bits, avec

$$\begin{aligned} B\left(N' + 2, k'\left(\frac{\tau}{2^n}\right)\right) &= \mathrm{Max}\left(1, \left\lceil \log_2\left|\log_2\left|k'\left(\frac{\tau}{2^n}\right)\right|\right|\right\rceil\right) + 2 + \lceil \log_2(N'+2)\rceil \\ &= 3 + \log_2\left(N + 2 + n\log_2 3\right). \end{aligned}$$

Comme par ailleurs on est dans le cas où $N \geqslant 10\mathrm{Im}\,(\tau)$, on a $n \leqslant \log_2 N$, et finalement on peut montrer qu'il est suffisant d'évaluer k' en $\frac{\tau}{2^n}$ avec une précision relative de

$$N + 7 + 15\log_2 N$$

bits.

On en déduit que l'Algorithme 8 peut être utilisé pour évaluer k', avec une complexité en $O\left(\mathcal{M}(N)\log N\right)$ indépendante de la valeur de τ, ce qui démontre finalement le Théorème 4.3.

4.2.4 Évaluation de k *via* l'égalité de Jacobi

Notons que lorsque $\tau \in \mathcal{F}$, la Proposition 2.6 permet de montre que $\mathrm{Re}\,(k(\tau)) > 0$ donc, en utilisant l'égalité de Jacobi, on peut déduire $k(\tau)$ de $k'(\tau)$ puisque

$$k(\tau) = \sqrt{1 - k'^2(\tau)}.$$

On notera cependant que cette méthode de calcul peut induire une perte de précision conséquente (due à la soustraction). En effet, la Proposition 2.6 permet de montrer que pour tout $\tau \in \mathcal{F}$,

$$8\,|q| \leqslant \left|k^2(\tau)\right| = \left|1 - k'^2(\tau)\right| \leqslant 32\,|q|.$$

Algorithme : `Evaluatekp2`
input : $\tau \in \mathbb{F}$, $N \in \mathbb{N}$, $H_2 \in \mathbb{N}$
output : k'_a such that $|k'(\tau) - k'_a| / |k'(\tau)| \leqslant \frac{1}{2^N}$

if $N \leqslant 10\mathrm{Im}(\tau)$ **then**
  return `EvaluatekpNaive`(τ, N);
end
$n \leftarrow 1 + \lceil \log_2 |\tau| \rceil$;
$\tau' \leftarrow \tau / 2^n$;
$N' \leftarrow N + 7 + \lceil 15 \log_2 N \rceil$;
$c \leftarrow$`Evaluatekp1`(τ', N', H_2);
$d \leftarrow$`EvaluateM`(c, N');
$b \leftarrow cd$;
$a \leftarrow 1/d$;
while $n > 0$ **do**
  $c \leftarrow a + b$;
  $b \leftarrow \sqrt{ab}$;
  $a \leftarrow c/2$;
  $n \leftarrow n - 1$;
end
return a/b;

Algorithme 8: Évaluation de k' (variante)

Comme, par ailleurs,

$$\frac{1}{4} \leqslant k'^2(\tau) \leqslant 4,$$

on en déduit que l'on perd $O(\mathrm{Im}(\tau))$ bits de précision dans cette soustraction. Plus précisément, ce qui précède permet de montrer que si l'on pose

$$C = \lceil \pi \log_2 e \mathrm{Im}(\tau) \rceil - 1,$$

alors on a toujours

$$\left|1 - k'^2(\tau)\right| \geqslant \frac{1}{2^C} \mathrm{Max}\left(1, \left|k'^2(\tau)\right|\right).$$

Les résultats de la Section 1.1.2 montrent alors que pour évaluer $k(\tau)$ avec une précision relative de N bits, il est suffisant de partir d'une approximation de $k'(\tau)$ avec une précision relative de $N + C + 5 = O(N + \mathrm{Im}(\tau))$ bits. Comme précédemment, on peut choisir d'utiliser l'algorithme naïf dans les cas où $N \leqslant 10\mathrm{Im}(\tau)$ par exemple, et l'Algorithme 8 dans les autres cas. On en déduit dans tous les cas que l'évaluation de k sur $\mathcal{F}$ a la même complexité asymptotique que celle de k'.

4.3 Évaluation d'autres fonctions modulaires

4.3.1 Utilisation de polynômes modulaires

Soit f une fonction modulaire pour un sous-groupe d'indice fini $\Gamma \subseteq \Gamma_1$. La Proposition 2.17 montre qu'il existe un polynôme $\Phi_{k',f}(X, Y) \in \mathbb{C}[X, Y]$ tel que, pour tout $\tau \in \mathcal{H}$,

$$\Phi_{k',f}\left(k'(\tau), f(\tau)\right) = 0.$$

Pour beaucoup de fonctions modulaires f "usuelles", le polynôme $\Phi_{k',f}$ est en fait à coefficients dans $\mathbb{Z}$, $\mathbb{Q}$ ou dans un corps de nombres. Si l'on suppose ce polynôme connu de façon exacte, alors une méthode pour évaluer f en un certain $\tau \in \mathcal{H}$ consiste à :

– évaluer $k'(\tau)$ en utilisant les algorithmes vus dans les sections précédentes ;

– utiliser des itérations de Newton sur la fonction $z \mapsto \Phi_{k',f}\left(k'(\tau), z\right)$ pour évaluer $f(\tau)$.

L'algorithme décrit ci-dessus a encore une complexité en $O\left(\mathcal{M}(N)\log N\right)$ (lorsque τ est fixé).

L'utilisation de l'égalité de Jacobi pour déduire $k(\tau)$ de $k'(\tau)$ (Section 4.2.4) peut être vue comme un cas (très) particulier de cette méthode.

Traitons ici par exemple du cas de la fonction j : nous l'avons définie par

$$j(\tau) = 256\frac{\left(1-k'^2(\tau)+k'^4(\tau)\right)^3}{k'^4(\tau)\left(1-k'^2(\tau)\right)^2}.$$

Les résultats concernant la complexité de l'évaluation des fonctions k et k' vus plus haut montrent que la fonction j peut s'évaluer en $O\left(\mathcal{M}(N)\log N\right)$, indépendamment de la valeur de $\tau \in \mathcal{F}$.

4.3.2 Évaluation de la fonction η de Dedekind

La fonction η de Dedekind est souvent utilisée pour construire des fonctions modulaires, ou encore pour construire des invariants de classe dans la théorie de la multiplication complexe, et nous verrons à la Section 4.4 que certains problèmes nécessitent l'évaluation rapide de telles fonctions à grande précision. C'est pourquoi nous donnons ici un algorithme permettant l'évaluation rapide de η.

On notera qu'un sous-produit de l'Algorithme 8 est un algorithme permettant l'évaluation de θ_0^2 et θ_1^2 sur $\mathcal{F}$ avec une complexité en $O\left(\mathcal{M}(N)\log N\right)$, indépendamment de la valeur de τ.

Il est montré dans [Web02, pages 112–114] que

$$\theta_0(\tau) = \eta(\tau) f^2(\tau),$$

où f est une fonction modulaire vérifiant l'équation modulaire

$$f^{24}k'^2k^2 = 16.$$

On a donc

$$\eta^{12}(\tau) = \frac{k^2(\tau)k'^2(\tau)\theta_0^2(\tau)}{16},$$

et le développement en q de η peut être utilisé pour déterminer quelle est la bonne racine douzième. En utilisant des itérations de Newton, on peut donc évaluer $\eta(\tau)$ en temps

$$O\left(\mathcal{M}(N)\log N\right),$$

indépendamment de la valeur de τ.

4.4 Applications

Nous avons choisi, dans ce mémoire, de ne pas aborder en détail les courbes elliptiques, et en particulier les courbes elliptiques sur $\mathbb{C}$ et leurs relations avec les fonctions modulaires. Pour plus de détails sur ce (vaste) sujet, nous renvoyons aux classiques [Sil86, Sil94], ou encore à [Cox89], qui traite entre autres précisément de polynômes modulaires et de polynômes de classe.

4.4.1 Calcul de polynômes de classes

Théorie de la multiplication complexe

Soit E une courbe elliptique définie sur $\mathbb{C}$, alors son anneau d'endomorphismes est soit isomorphe à $\mathbb{Z}$, soit isomorphe à un ordre dans un corps quadratique imaginaire : on dit alors que E a *multiplication complexe* par cet ordre.

Soient $D < 0$ un discriminant, et $\mathcal{O}_D$ l'ordre de discriminant D dans le corps quadratique imaginaire $\mathbb{Q}\left(\sqrt{D}\right)$. Si l'on note R_D l'ensemble des racines dans $\mathcal{H}$ des formes quadratiques réduites de discriminant D (leur nombre, que l'on notera h_D, est appelé *nombre de classes*), alors le polynôme

$$H_D(X) = \prod_{\tau \in R_D} (X - j(\tau))$$

est appelé *polynôme de classes*. Il est à coefficients entiers, et ses racines correspondent à l'ensemble des j-invariants des courbes elliptiques ayant multiplication complexe par $\mathcal{O}_D$.

Soit maintenant $\mathbb{F}_q$ un corps fini de caractéristique p ne divisant pas D. Dans le cas où il existe deux entiers t, V tels que

$$4q = t^2 + DV^2,$$

alors $H_D(X)$ est scindé sur $\mathbb{F}_q$, et, d'après le théorème de réduction de Deuring [Deu41], ses racines sont exactement les j-invariants des courbes elliptiques définies sur $\mathbb{F}_q$ ayant un anneau d'endomorphismes isomorphe à $\mathcal{O}_D$ (on dit encore que ces courbes ont multiplication complexe par $\mathcal{O}_D$). Le nombre de points d'une telle courbe est de la forme $q + 1 \pm t$.

Ce lien entre la cardinalité d'une courbe définie sur $\mathbb{F}_q$ et son anneau d'endomorphismes peut être utilisé pour construire *via* la multiplication complexe des courbes elliptiques ayant des propriétés particulières. Cette technique, que l'on appelle *multiplication complexe effective*, est utilisée par exemple en preuve de primalité [AM93] ou dans la construction de courbes elliptiques utilisables dans des cryptosystèmes basés sur l'identité [MNT01, DEM05, BLS03, BW05].

Multiplication complexe effective

Soit D un discriminant et soit p un nombre premier ne divisant pas D. D'après ce qui précède, pour construire une courbe elliptique sur $\mathbb{F}_p$ ayant $\mathcal{O}_D$ comme anneau d'endomorphismes, il suffit de

1. calculer $H_D(X) \in \mathbb{Z}[X]$;
2. déterminer une racine J de H_D modulo p (par exemple par l'algorithme de Cantor–Zassenhaus, dont on trouvera une description dans [GG99, p. 358–365]) ;
3. construire une courbe elliptique sur $\mathbb{F}_p$ ayant J pour j-invariant (dans le cas où $J \notin \{0, 1728\}$, on peut par exemple prendre la courbe d'équation affine

$$y^2 = x^3 - \frac{3J}{J - 1728}x + \frac{2J}{J - 1728}$$

).

Nous nous intéressons ici uniquement au premier point, à savoir le calcul de $H_D(X)$. Commençons par donner des bornes sur la *taille* de ce polynôme : tout d'abord, d'après le théorème de Siegel [Sie35], son degré est $h_D = O\left(|D|^{\frac{1}{2}+\varepsilon}\right)$. Par ailleurs, il est montré dans [Eng05a, Theorem 2] que la hauteur logarithmique de ses coefficients est en $O\left(\sqrt{|D|}\log_2|D|\right)$. L'espace nécessaire pour stocker une représentation de $H_D(X)$ est donc en $O\left(|D|^{1+\varepsilon}\right)$.

Un algorithme permettant de déterminer l'ensemble des formes quadratiques réduites de discriminant D en temps $O\left(|D|^{\frac{3}{4}+\varepsilon}\right)$ est décrit dans [Eng05a]. Si $Ax^2+Bxy+Cy^2$ est une telle forme quadratique, on lui associe un élément $\tau = \frac{-B+i\sqrt{-D}}{2A} \in \mathcal{H}$. Il suffit alors d'évaluer numériquement la fonction j en les h_D éléments de $\mathcal{H}$ ainsi déterminés, puis de reconstruire le polynôme à partir de ses racines : si l'on a travaillé à une précision suffisante, il suffira d'arrondir le résultat pour obtenir $H_D(X)$. D'après ce qui précède, il est suffisant de travailler à une précision en $O\left(\sqrt{|D|}\log^2|D|\right)$, donc chaque évaluation de j a un coût en

$$O\left(\mathcal{M}\left(\sqrt{|D|}\log^2|D|\right)\log|D|\right) = O\left(|D|^{\frac{1}{2}+\varepsilon}\right),$$

et h_D telles évaluations sont nécessaires, ce qui porte la complexité totale de l'évaluation des racines de $H_D(X)$ à $O\left(|D|^{1+\varepsilon}\right)$. Reconstruire $H_D(X)$ à partir de ses racines se fait, en utilisant [Eng05a, Algorithm 1], en temps $O\left(|D|^{1+\varepsilon}\right)$.

Ceci montre le résultat suivant :

Théorème 4.4 *Pour tout discriminant D, le polynôme de classe $H_D(X)$ peut être calculé en temps $O\left(|D|^{1+\varepsilon}\right)$.*

Ce résultat a en fait été prouvé par Enge (toujours dans [Eng05a]), mais en utilisant une méthode permettant d'évaluer *simultanément* la fonction j en les h_D éléments de $\mathcal{H}$ rapidement.

On notera que cette méthode d'approximation des racines sur les complexes n'est pas la seule existante pour le calcul de polynômes de classe. Une approche p-adique a été décrite par Couveignes et Hénocq [CH02], et implantée par Bröker et Stevenhagen [BS04]. Ce type de méthodes a aussi une complexité en $O\left(|D|^{1+\varepsilon}\right)$.

On construit parfois des polynômes de classe en utilisant d'autres fonctions que j comme invariants de classe, ceci afin d'obtenir des polynômes dont les coefficients ont une hauteur moindre (on peut ainsi diviser la hauteur des coefficients par une constante). Cette théorie est développée dans [EM02, ES04, Sch02], et virtuellement tous les invariants qui sont utilisés sont définis *via* la fonction η de Dedekind, ce qui explique pourquoi nous nous sommes intéressé à son évaluation.

Andreas Enge [Eng05a] a comparé différentes approches pour le calcul de polynômes de classe. En particulier, en utilisant du code C que nous lui avons fourni pour évaluer numériquement la fonction η de Dedekind, il a réussi à calculer explicitement un polynôme de classe de degré $h = 100000$ (ce qui implique de travailler à une précision de l'ordre de 260000 bits), ce qui constitue à ce jour un record. Les résultats qu'il a obtenus montrent d'une part que la méthode d'évaluation simultanée de la fonction η en h valeurs distinctes, bien qu'asymptotiquement plus rapide que l'évaluation "naïve", n'est pas utilisable (car beaucoup trop lente) dans le cas où $h = 100000$; et d'autre part que pour cette même valeur de h, notre méthode d'évaluation rapide de η par l'AGM ne permet qu'un gain de vitesse d'environ 6% par rapport à la méthode classique utilisant la série en q creuse de η. La théorie rejoint donc la pratique, puisque la méthode asymptotiquement rapide devient effectivement plus rapide en pratique. On peut s'étonner qu'il faille aller jusqu'à un tel nombre de classe pour obtenir un gain par notre méthode. Un certain nombre de facteurs entrent en jeu pour expliquer cela :

- Enge utilise pour l'évaluation de η par sa série en q une chaîne d'addition *ad hoc* (en ce sens qu'il la détermine expérimentalement jusqu'à un certain rang, mais n'a pas de résultat asymptotique sur de telles chaînes), particulièrement rapide ;
- avec notre méthode, l'évaluation de η est légèrement plus coûteuse que celle de k' (et même que celle des theta constantes) ;

– enfin, nous avons vu que lorsque la partie imaginaire de τ est grande notre méthode est moins performante, or de tels cas apparaissent dans le calcul de polynômes de classe.

4.4.2 Calcul de polynômes modulaires

L'algorithme SEA

L'algorithme de Schoof [Sch95] permet de compter le nombre de points sur une courbe elliptique définie sur un corps fini. Dans le cas où ce dernier est un corps premier*, des améliorations ont été apportées à l'algorithme de base par Elkies [Elk98] et Atkin [Atk92] afin d'en améliorer la complexité, pour aboutir à un algorithme connu sous le nom de Schoof–Elkies–Atkin, ou SEA.

Si E est une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, son cardinal est de la forme $q+1-t$ où l'entier t, appelé *trace*, est dans l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$. Le principe de l'algorithme de Schoof "de base" est de calculer t modulo plusieurs nombres premiers p distincts, puis d'utiliser le théorème des restes chinois pour reconstruire t. Pour calculer t modulo ℓ, on utilise le fait que si P est un point de ℓ-torsion, et si ϕ désigne l'endomorphisme de Frobenius, alors on doit avoir

$$\phi^2(P) - [t]_\ell \phi(P) + [q]_\ell P = 0,$$

où $[x]_\ell$ désigne le représentant dans $[0, \ell-1]$ de $x \bmod \ell$. Pour travailler dans la ℓ-torsion, on travaille en fait modulo le polynôme de ℓ-division, dont le degré est quadratique en ℓ.

L'amélioration majeure de l'algorithme SEA consiste à ne plus travailler modulo *toute* la ℓ-torsion, mais modulo un groupe d'ordre ℓ que l'on fait apparaître comme le noyau d'une ℓ-isogénie. C'est à ce niveau qu'interviennent les polynômes modulaires : si J désigne le j-invariant de la courbe E, alors l'ensemble des j-invariants des courbes ℓ-isogènes à E est l'ensemble des racines de l'équation

$$\Phi_\ell(J, X) = 0.$$

Nous n'entrerons ici pas plus dans les détails de l'algorithme SEA, et renvoyons le lecteur à [BSS99, Chapter VII, Schoof's algorithm and extentions, pages 109–148] par exemple pour une présentation plus approfondie.

Les polynômes modulaires Φ_ℓ sont donc des ingrédients nécessaires à la mise en œuvre de l'algorithme SEA (qui peuvent bien entendu être précalculés). La hauteur logarithmique des coefficients de ces polynômes est en $O\left(\ell^{1+\varepsilon}\right)$, et, comme dans le cas des polynômes de classe, on utilise souvent d'autres polynômes que les Φ_ℓ (reliant toujours des fonctions modulaires pour des groupes de la forme $\Gamma^0(\ell)$), afin de réduire la hauteur des coefficients.

On notera que le record actuel de comptage de points par l'algorithme SEA [Mor05] concerne une courbe dont le cardinal est de l'ordre de 2000 chiffres décimaux, et nécessite l'utilisation de polynômes modulaires pour ℓ allant jusqu'à environ 6000. Les hauteurs des coefficients de polynômes utilisés vont jusqu'à environ 12000 bits.

Calcul de polynômes modulaires par manipulation de séries en q

Une première méthode de calcul de polynômes modulaires, décrite par Atkin dans [Atk88, Atk92] (on pourra aussi consulter [Mor95]), consiste à considérer les développements en q des fonctions utilisées. En effet, si le développement en q de j s'écrit

$$j(\tau) = \sum_{n \geqslant -2} j_n q^n,$$

*Il suffit en fait que la caractéristique soit grande devant le logarithme du nombre d'éléments du corps.

alors, comme (d'après la Section 2.3.2)

$$\Phi_\ell\left(X, j(q)\right) = \left(X - j\left(\frac{-\ell}{\tau}\right)\right) \prod_{k=0}^{\ell-1} \left(X - j\left(\frac{\tau+k}{\ell}\right)\right),$$

on peut calculer Φ_ℓ en procédant comme suit :

1. précalculer le développement en q de $j(\tau)$, par exemple en utilisant la définition que nous avons donnée de j et en manipulant des séries formelles (d'autres solutions sont présentées dans [BK01]) ;
2. en utilisant l'égalité ci-dessus, écrire formellement le polynôme $\Phi_\ell\left(X, j(\tau)\right)$ comme un polynôme en X dont les coefficients sont des séries en q ;
3. exprimer chacun des coefficients obtenus au point 2. comme un polynôme en la série $j(\tau)$, pour cela on précalcule les séries en q des différentes puissances de $j(\tau)$, et le fait que la q-valuation de $j(\tau)^k$ vaut $-2k$ rend la reconstruction des polynômes aisée.

Au final (nous n'entrons pas dans les détails ici), on obtient un algorithme permettant de calculer $\Phi_\ell(X, Y)$ en temps $O\left(\ell^{4+\varepsilon}\right)$. Cet algorithme s'adapte facilement pour le calcul de polynômes modulaires entre d'autres types de fonctions modulaires pour $\Gamma^0(\ell)$ (avec la même complexité).

Calcul de polynômes modulaires par évaluation et interpolation

Nous décrivons ici rapidement une autre famille d'algorithmes pour le calcul de polynômes modulaires, dont l'idée semble revenir à Jonathan et Peter Borwein [BB87, p. 132–133], et qui ont récemment été étudiés plus en détail et implantés par Enge [Eng05b].

Il s'agit de calculer, pour $\ell + 1$ valeurs de τ distinctes (et non-équivalentes modulo l'action de Γ_1) les valeurs de

$$j(\tau), j\left(\frac{-\ell}{\tau}\right), j\left(\frac{\tau}{\ell}\right), j\left(\frac{\tau+1}{\ell}\right), \ldots, j\left(\frac{\tau+p-1}{\ell}\right),$$

soit $(\ell+1)(\ell+2) = O\left(\ell^2\right)$ évaluations de j. On reconstruit alors le polynôme modulaire par interpolation.

Notons qu'il est suffisant de travailler à une précision correspondant à la hauteur des coefficients de Φ_ℓ, soit $O\left(\ell^{1+\varepsilon}\right)$. En utilisant les méthodes rapides d'évaluation de j vues plus haut, la phase d'évaluation peut se faire en temps $O\left(\ell^{3+\varepsilon}\right)$. Le calcul de Φ_ℓ par cette technique se fait finalement en temps $O\left(\ell^{3+\varepsilon}\right)$, ce qui est quasi-optimal. Nous renvoyons à [Eng05b] pour une analyse plus détaillée de la complexité, ainsi que pour une généralisation à d'autres types de polynômes modulaires.

On notera que cette méthode semble la plus rapide actuellement, mais que les précisions nécessaires (de l'ordre de 12000 bits pour ℓ de l'ordre de 6000 par exemple) ne justifient pas l'utilisation d'algorithmes asymptotiquement rapides pour l'évaluation de fonctions modulaires.

Il ne faut pas confondre la méthode que nous venons d'exposer avec la méthode exposée à la Section 4.3.1 pour l'évaluation rapide de fonctions modulaires en utilisant des polynômes modulaires : ici, on sait évaluer les fonctions que l'on manipule (c'est relativement facile pour la fonction $\tau \mapsto j(\ell\tau)$, puisque cela se ramène directement à l'évaluation de j), et l'on s'en sert pour calculer un polynôme modulaire. Dans la méthode de la Section 4.3.1, on utilise un polynôme modulaire que l'on suppose connu, liant entre elles deux fonctions modulaires f et g, et l'on suppose que l'on sait évaluer f rapidement : on en déduit, *via* des itérations de Newton, une méthode d'évaluation de g. Dans un cas donc, on sait évaluer les deux fonctions cela nous permet de calculer le polynôme modulaire, alors que dans l'autre cas on connaît le polynôme modulaire et l'on sait évaluer une fonction, ce qui nous permet d'évaluer l'autre.

4.5 Résultats expérimentaux

4.5.1 Précision nécessaire à l'initialisation des itérations de Newton

Le principal obstacle à la mise en œuvre des Algorithmes 7 et 8 et que l'on ne connaît *a priori* pas les valeurs de h_τ (pour $\tau \in \mathcal{F}$) et de H_2, valeurs qui sont nécessaires pour déterminer la précision à laquelle initialiser les itérations de Newton.

Nous avons pu déterminer que $\left|\frac{f''_\tau(k'(\tau))}{f'_\tau(k'(\tau))}\right|$ est en $\frac{1}{q}$, ce qui montre que h_τ est *au moins* en $\frac{1}{q}$, mais n'avons pas obtenu plus.

Nous avons donc étudié expérimentalement la précision minimale à laquelle il est nécessaire d'initialiser les itérations de Newton sur f_τ pour qu'elles convergent bien vers $k'(\tau)$. Nous avons constaté que cette quantité est quasiment indépendante de $\mathrm{Re}\,(\tau)$, et ne dépend donc que de $\mathrm{Im}\,(\tau)$. La Figure 4.1 montre comment évolue la précision initiale minimale nécessaire (exprimée en bits) en fonction de y, en $\tau = 0.25 + y \cdot i$. Ces données expérimentales montrent que la précision minimale nécessaire augmente en $4.16\,\mathrm{Im}\,(\tau) \simeq (\pi \log_2 e)\,\mathrm{Im}\,(\tau) = \log_2 \frac{1}{|q|}$.

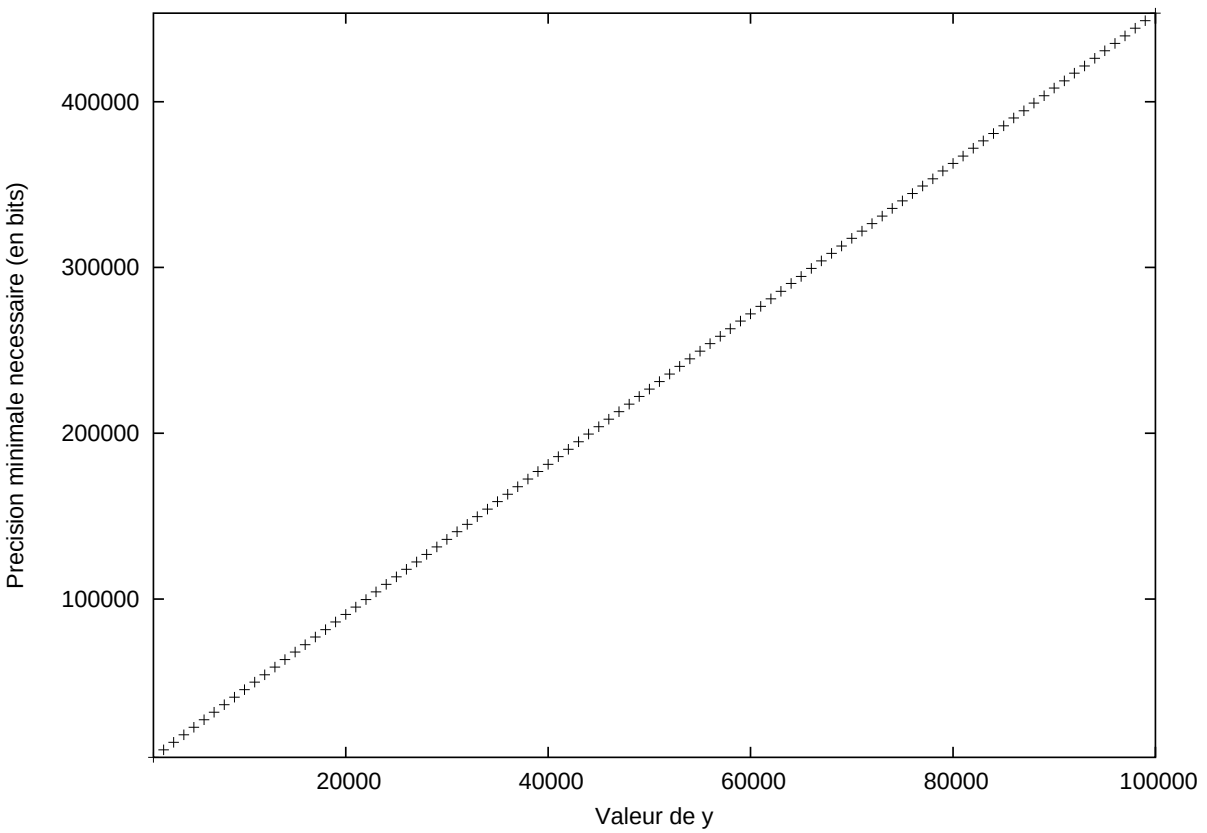

FIG. 4.1 – Précision initiale minimale nécessaire à l'Algorithme 7 en $\tau = 0.25 + y \cdot i$

Nous conjecturons que l'on peut utiliser l'Algorithme 7 en remplaçant h_τ par $100 + 4.6\,\mathrm{Im}\,(\tau)$ sans l'invalider, et de même pour l'Algorithme 8 en remplaçant H_2 par 110.

4.5.2 Temps de calcul

Nous avons implémenté les Algorithmes 6 et 7 en langage C, en utilisant les bibliothèques GMP [Gra02], MPFR [HLPZ04] et MPC [EZ04] pour le calcul multiprécision, ainsi que les routines assembleur pour Athlon 64 de Pierrick Gaudry [Gau05]. Les temps de calcul que nous

donnons ont été mesurés sur un Athlon 64 3400+ (cadencé à 2.4 MHz) disposant de 2 Go de RAM (ce dernier point étant accessoire, puisque les algorithmes implantés sont peu gourmands en mémoire).

La Figure 4.2 donne les temps de calculs des Algorithmes 6 ("Naif") et 7 ("Newton"), pour des précisions allant jusqu'à 20000 bits. On notera que les deux algorithmes ont des temps de calculs identiques pour une précision de l'ordre de 2500 bits, ce qui est relativement faible.

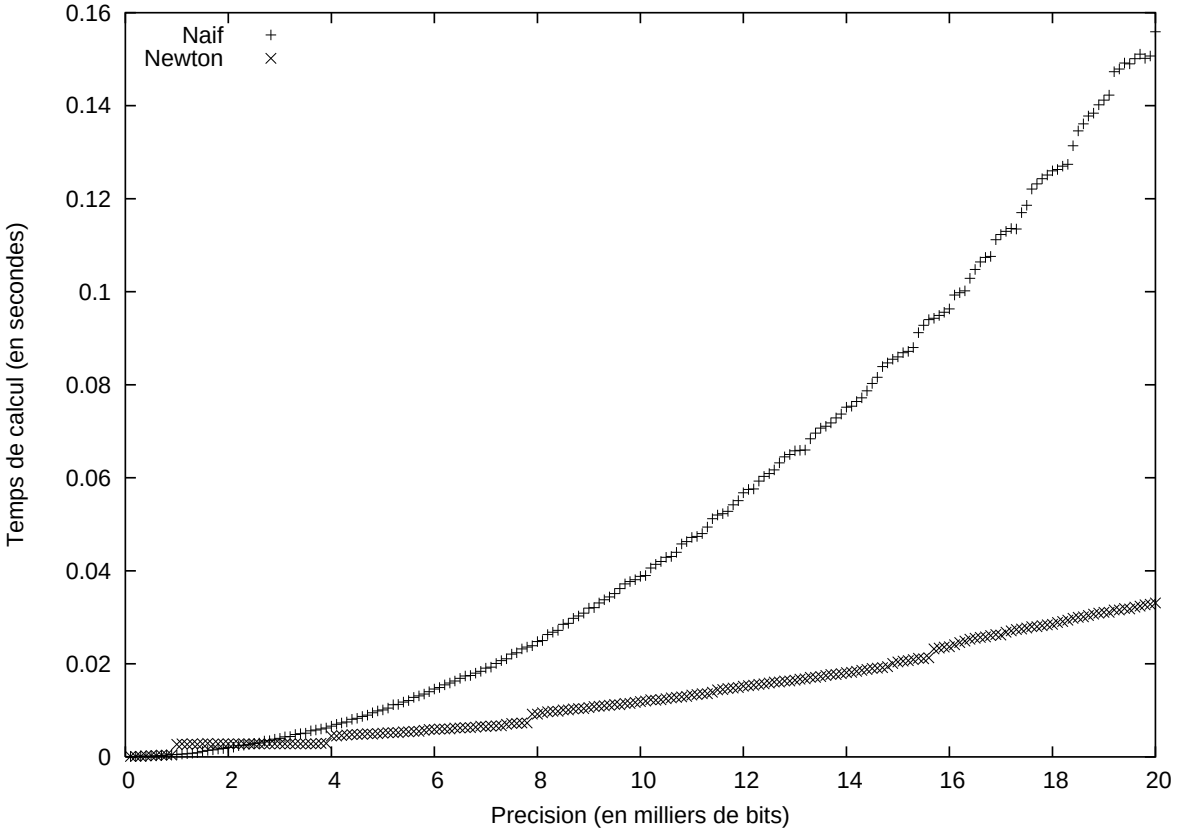

FIG. 4.2 – Temps de calcul pour l'évaluation de $k'(0.123456789+1.23456789\cdot i)$ à faible précision

La Figure 4.3 donne elle les temps de calcul de l'Algorithme 7 pour des précisions bien supérieures.

À titre de comparaison, la Figure 4.4 donne les temps de calcul pour une vingtaine de multiplications (fonction `mpc_mul` de la libraire MPC), sur la même plage de précision que précédemment.

Enfin, la Figure 4.5 donne le ratio entre le temps de calcul de l'Algorithme 7 et la valeur de $20\mathcal{M}(N)\log N$, toujours pour la même plage de précision N. Ces résultats sont en accord avec une complexité en $12\,\mathtt{M}(N)\log N$.

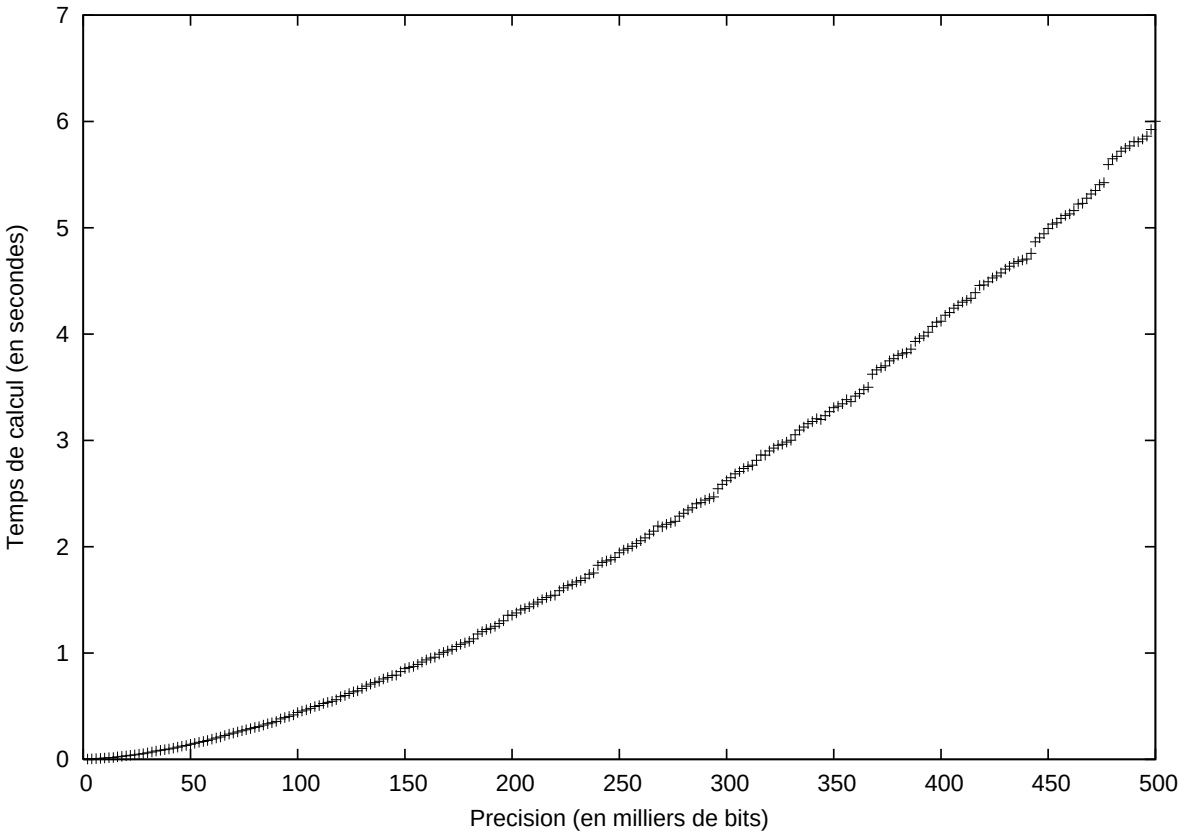

FIG. 4.3 – Temps de calcul pour l'évaluation de $k'(0.123456789+1.23456789\cdot i)$ à haute précision

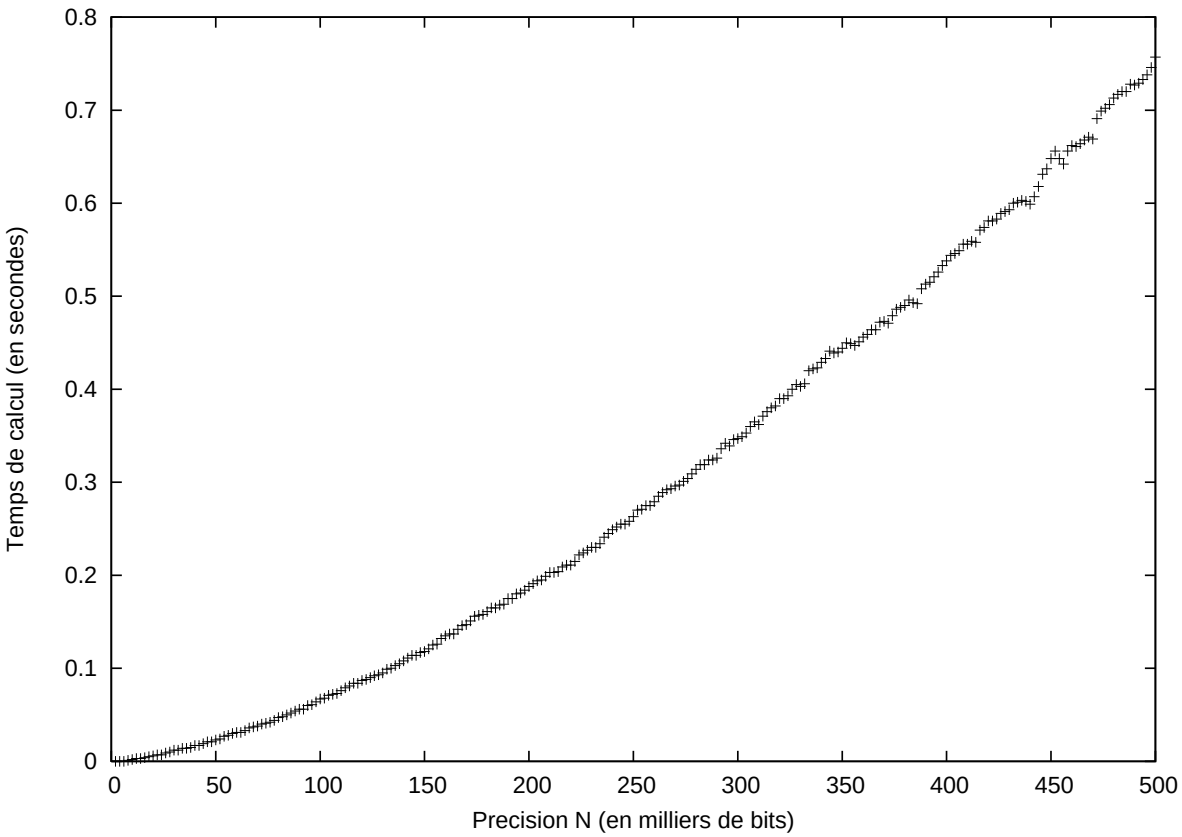

FIG. 4.4 – Temps de calcul pour 20 multiplications (fonction `mpc_mul`)

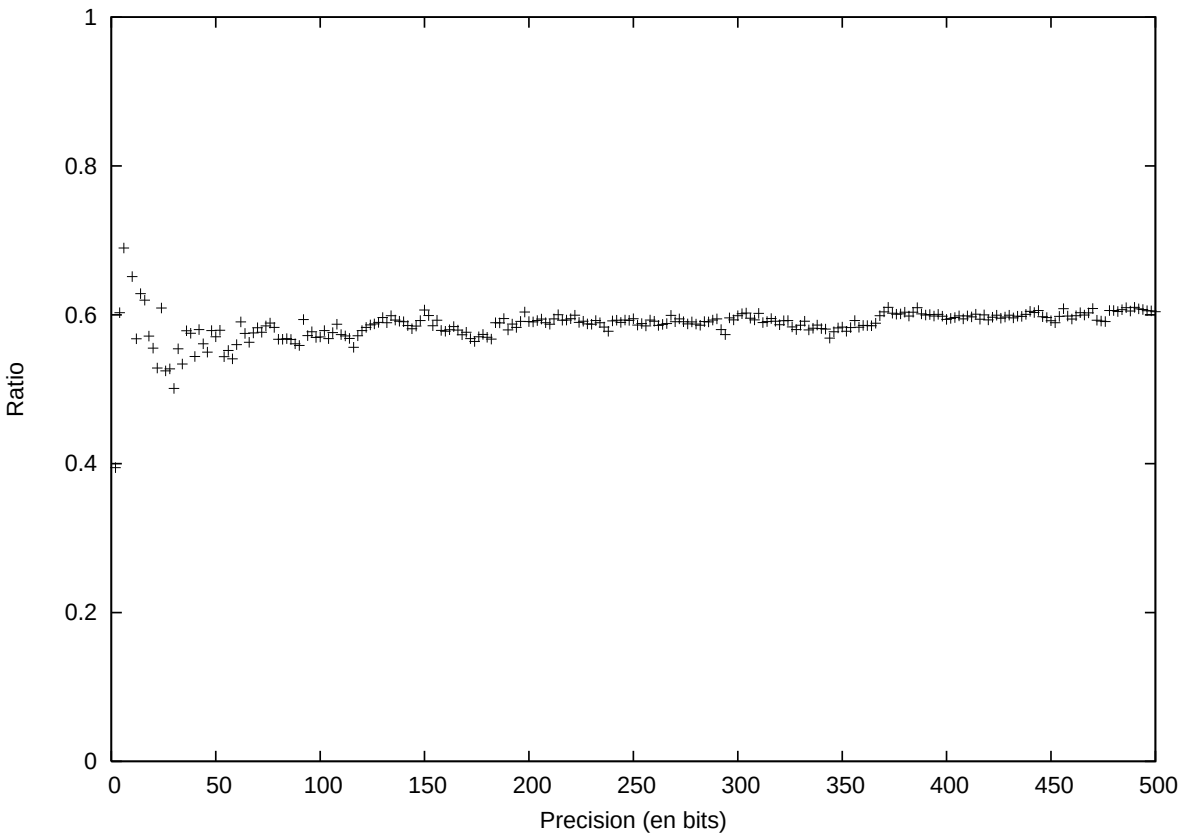

FIG. 4.5 – Ratio entre le temps de calcul de l'Algorithme 7 et $20\,\mathtt{M}(N)\log N$

Deuxième partie

Le genre 2 et au-delà

Chapitre 5

Theta constantes en genre supérieur

L'objectif de ce (court) chapitre est de définir les theta constantes en genre quelconque et de donner quelques unes de leurs propriétés élémentaires. Même si dans les chapitres suivants nous nous intéresserons principalement au cas particulier du genre 2, les démonstrations des propriétés que nous donnons dans le présent chapitre sont —pour la plupart— tout aussi simples à établir en genre quelconque qu'en genre 2.

Dans ce chapitre, on fixe un entier $g \geqslant 1$ correspondant au genre.

5.1 Définitions

Définition 5.1 (demi-espace de Siegel) *On définit le* demi-espace de Siegel $\mathcal{H}_g$ *comme étant l'ensemble des matrices $g \times g$ symétriques à coefficients complexes et dont la partie imaginaire est définie positive.*

Remarquons que $\mathcal{H}_1$ n'est autre que le demi-plan de Poincaré $\mathcal{H}$.

Dans la suite, pour $\tau \in \mathcal{H}_g$, on notera $\lambda(\tau)$ la plus petite valeur propre de la matrice $\mathrm{Im}(\tau)$.

Définition 5.2 (theta constantes avec caractéristique $\frac{1}{2}$) *Les* theta constantes *(avec caractéristique $\frac{1}{2}$) sont les fonctions $\theta_{a,b}$, définies pour tout $a, b \in \{0,1\}^g$ par*

$$\theta_{a,b}(\tau) = \sum_{n \in \mathbb{Z}^g} E\left({}^t\left(n + \frac{a}{2}\right)\tau\left(n + \frac{a}{2}\right) + {}^t\left(n + \frac{a}{2}\right)b\right)$$

pour tout $\tau \in \mathcal{H}_g$. On dit que $\theta_{a,b}$ est la theta constante associée aux caractéristiques $a/2$ et $b/2$.

Tout comme dans le cas du genre 1, il existe une fonction plus générale $\theta : \mathbb{C}^g \times \mathcal{H}_g \to \mathbb{C}$ définie par

$$\theta(z,\tau) = \sum_{n \in \mathbb{Z}^g} E\left({}^t n\tau n + 2{}^t nz\right),$$

et pour $\ell \geqslant 2$, les theta constantes avec caractéristique $\frac{1}{\ell}$ sont alors définies comme étant (à un facteur près) les valeurs de θ à τ fixé en les points de la forme $z = \frac{\tau a + b}{\ell}$, où $a, b \in \mathbb{Z}^g$. Plus précisément, pour $a, b \in \mathbb{Z}^g$, la theta constante associée aux caracteristiques $\frac{a}{\ell}$ et $\frac{b}{\ell}$ est la fonction définie par

$$\theta_{\frac{a}{\ell},\frac{b}{\ell}}(\tau) = E\left(\frac{{}^t a\tau a + 2{}^t ab}{\ell^2}\right)\theta\left(\frac{\tau a + b}{\ell}, \tau\right).$$

Un calcul direct montre que pour tous $a, b, c, d \in \mathbb{Z}^g$ et $\tau \in \mathcal{H}_g$,

$$\theta_{\frac{a}{\ell}+c,\frac{b}{\ell}+d}(\tau) = E\left(\frac{2{}^t ad}{\ell}\right)\theta_{\frac{a}{\ell},\frac{b}{\ell}}(\tau),$$

donc on peut se restreindre à $a, b \in [0, \ell - 1]$.

Notons que pour simplifier les notations, et comme nous ne manipulerons que des theta constantes avec caractéristique $\frac{1}{2}$ par la suite, nous indexons ces theta constantes par $a, b \in \{0,1\}^g$ plutôt que de les indexer par $\frac{a}{2}, \frac{b}{2}$.

Remarquons que si $g, g_1, g_2 \geqslant 1$ sont tels que $g_1 + g_2 = g$, et que $\tau \in \mathcal{H}_g$ est de la forme $\tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}$ avec $\tau_1 \in \mathcal{H}_{g_1}$ et $\tau_2 \in \mathcal{H}_{g_2}$, alors pour tous $a = (a_1, a_2) \in \{0,1\}^2$ et $b = (b_1, b_2) \in \{0,1\}^g$ (avec $a_1, b_1 \in \{0,1\}^{g_1}$ et $a_2, b_2 \in \{0,1\}^{g_2}$), on a

$$\theta_{a,b}(\tau) = \theta_{a_1,b_1}(\tau_1)\theta_{a_2,b_2}(\tau_2).$$

Définition 5.3 (theta constantes paires et impaires) *Soient $a, b \in \{0,1\}^g$, on dit que la theta constante $\theta_{a,b}$ est* paire *(resp.* impaire*) lorsque ${}^t ab \equiv 0 \bmod 2$ (resp. lorsque ${}^t ab \equiv 1 \bmod 2$).*

Une récurrence directe montre qu'il y a $2^{g-1}(2^g + 1)$ theta constantes paires en genre g (donc $2^{g-1}(2^g - 1)$ theta constantes impaires). L'intérêt de distinguer entre ces deux classes de theta constantes vient de la proposition suivante :

Proposition 5.1 *Toute theta constante impaire est identiquement nulle.*

Démonstration : Soient $a, b \in \{0,1\}^g$ tels que ${}^t ab \equiv 1 \bmod 2$, et soit $\tau \in \mathcal{H}_g$. Alors

$$\theta_{a,b}(\tau) = \sum_{n \in \mathbb{Z}^g} E\left({}^t\left(n + \frac{a}{2}\right)\tau\left(n + \frac{a}{2}\right) + {}^t\left(n + \frac{a}{2}\right)b\right),$$

donc en posant $m = -n - a$, on a

$$\begin{aligned} \theta_{a,b}(\tau) &= \sum_{m \in \mathbb{Z}^g} E\left({}^t\left(-m - \frac{a}{2}\right)\tau\left(-m - \frac{a}{2}\right) + {}^t\left(-m - \frac{a}{2}\right)b\right) \\ &= E\left({}^t ab\right) \sum_{m \in \mathbb{Z}^g} E\left({}^t\left(m + \frac{a}{2}\right)\tau\left(m + \frac{a}{2}\right) + {}^t\left(m + \frac{a}{2}\right)b\right), \end{aligned}$$

où l'on a utilisé le fait que si $x \in \mathbb{Z}$, alors $E(x) = (-1)^x = E(-x)$, donc $\theta_{a,b}(\tau) = -\theta_{a,b}(\tau) = 0$. □

Définition 5.4 (theta constantes fondamentales) *Nous appelerons* theta constantes fondamentales *les 2^g theta constantes de la forme $\theta_{0,b}$ pour $b \in \{0,1\}^g$.*

5.2 Le groupe symplectique $\mathrm{Sp}(2g, \mathbb{Z})$ et son action sur $\mathcal{H}_g$

5.2.1 Définition

On note I la matrice identité de taille g, et on introduit la matrice J définie (par blocs) par

$$J = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}.$$

On définit alors le groupe $\mathrm{Sp}(2g, \mathbb{Z})$ par

$$\mathrm{Sp}(2g, \mathbb{Z}) = \left\{\gamma \in \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}) \mid {}^t\gamma J \gamma = J\right\}.$$

De façon équivalente, si $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ (par blocs), alors γ appartient à $\mathrm{Sp}(2g,\mathbb{Z})$ si et seulement si les trois égalités suivantes sont vérifiées :

$$\begin{aligned} {}^tCA &= {}^tAC, && (5.1)\\ {}^tDB &= {}^tBC, && (5.2)\\ {}^tDA - {}^tBC &= I. && (5.3) \end{aligned}$$

Il est clair, d'après la première forme de la définition, que $\mathrm{Sp}(2g,\mathbb{Z})$ est un groupe. On notera que $\mathrm{Sp}(2,\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$. En fait, $\mathrm{Sp}(2g,\mathbb{Z})$ agit sur $\mathcal{H}_g$ de la même façon qu'en genre 1, $\mathrm{Sl}_2(\mathbb{Z})$ agit sur $\mathcal{H}$: pour tous $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g,\mathbb{Z})$ et $\tau \in \mathcal{H}_g$, on pose

$$\gamma \cdot \tau = (A\tau + B)(C\tau + D)^{-1}.$$

Le fait que ceci définit bien une action de groupe n'est pas évident, et nous le montrons maintenant : soient $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g,\mathbb{Z})$ et $\tau \in \mathcal{H}_g$. On pose $\tau_R = \mathrm{Re}\,(\tau)$, $\tau_I = \mathrm{Im}\,(\tau)$, $X = A\tau + B$ et $Y = C\tau + D$. Les égalités (5.1), (5.2) et (5.3) impliquent que

$${}^tX\overline{Y} - {}^tY\overline{X} = 2\tau_I i. \qquad (5.4)$$

On commence par montrer que la matrice Y est inversible : soit $u \in \mathbb{C}^g$ tel que $Yu = 0$. L'égalité (5.4) implique alors que ${}^tu\tau_I\overline{u} = 0$, donc que $u = 0$ puisque τ_I est définie positive. On en déduit l'inversibilité de Y.

Considérons maintenant la matrice XY^{-1} : montrer qu'elle est symétrique revient à montrer que ${}^tYX = {}^tXY$, ce qui est une conséquence directe de la symplecticité de γ et des égalités (5.1), (5.2) et (5.3).

Enfin, en utilisant (5.4) et la symétrie de XY^{-1}, on a

$$\begin{aligned} \mathrm{Im}\left(XY^{-1}\right) &= \frac{1}{2i}\left(XY^{-1} - \overline{XY^{-1}}\right)\\ &= {}^tY^{-1}\tau_I\overline{Y}, \end{aligned}$$

ce qui montre que $\mathrm{Im}\left(XY^{-1}\right)$ est définie positive (puisque τ_I l'est).

On a donc montré que $\gamma \cdot \tau \in \mathcal{H}_g$. Bien sûr, $I_{2g} \cdot \tau = \tau$ pour tout $\tau \in \mathcal{H}_g$, et si $\gamma_1, \gamma_2 \in \mathrm{Sp}(2g,\mathbb{Z})$, on vérifie facilement que

$$\gamma_1 \cdot (\gamma_2 \cdot \tau) = (\gamma_1\gamma_2) \cdot \tau$$

pour tout $\tau \in \mathcal{H}_g$, et l'on a donc bien une action de groupe. Par ailleurs, $-I_{2g}$ agit trivialement, donc on peut considérer l'action de

$$\Gamma_g = \mathrm{Sp}(2g,\mathbb{Z})/\langle -I_{2g}\rangle$$

sur $\mathcal{H}_g$.

Par la suite, on identifiera les éléments de $\mathrm{Sp}(2g,\mathbb{Z})$ avec leur classe dans Γ_g, et on omettra le point dans la notation de l'action de groupe.

Notons que le groupe Γ_g est finiment engendré, et que l'on connaît même explicitement des générateurs :

Proposition 5.2 *Le groupe Γ_g est engendré par J et les $\frac{g(g+1)}{2}$ éléments de la forme*

$$M_{i,j} = \begin{pmatrix} I & m_{i,j} \\ 0 & I \end{pmatrix},$$

où $m_{i,j}$ désigne la matrice $g \times g$ dont toutes les entrées sont nulles sauf les entrées (i,j) et (j,i) valant 1.

DÉMONSTRATION : Il s'agit d'une conséquence directe de [Kli90, Proposition 6, p. 41–42]. □

5.2.2 Le domaine fondamental $\mathcal{F}_g$

On définit l'ensemble $\mathcal{F}_g \subset \mathcal{H}_g$ comme suit : un élément $\tau = (\tau_{u,v})_{u,v\in[1,g]} \in \mathcal{H}_g$ appartient à $\mathcal{F}_g$ si et seulement si τ remplit simultanément les trois conditions suivantes :

1. $|\mathrm{Re}\,(\tau_{u,v})| \leqslant \frac{1}{2}$ pour tous $u, v \in [1,g]$;
2. la matrice $\mathrm{Im}\,(\tau)$ est réduite au sens de Minkowski ;
3. pour tout $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g$,
$$|\mathrm{Det}(C\tau + D)| \geqslant 1.$$

Nous renvoyons à [Sie89, Kli90] pour plus de détails sur la réduction de Minkowski, et rappelons juste qu'une matrice réelle symétrique définie positive $M = (m_{j,k})_{j,k\in[1,n]}$ est dite *réduite au sens de Minkowski* si et seulement si

- pour tous $j \in [1,n]$ et $g = (g_1, \ldots, g_n) \in \mathbb{Z}^n$ tel que $g_j, \ldots, g_n$ soient premiers entre eux dans leur ensemble, ${}^t g m g \geqslant m_{j,j}$; et
- $m_{j,j+1} \geqslant 0$ pour tout $j \in [1, n-1]$.

On notera que dans le cas $g = 1$, on a $\mathcal{F}_1 = \mathcal{F}$.

On a alors la propriété suivante :

Proposition 5.3 *L'ensemble $\mathcal{F}_g$ défini ci-dessus est un domaine fondamental pour l'action de Γ_g sur $\mathcal{H}_g$. Plus précisément, pour tout $\tau \in \mathcal{H}_g$, il existe $\gamma \in \Gamma_g$ tel que $\gamma\tau \in \mathcal{F}_g$, et cet élément γ est unique si $\gamma\tau$ est un point intérieur de $\mathcal{F}_g$.*

DÉMONSTRATION : Ce résultat est dû à Siegel [Sie39], on peut aussi en trouver une démonstration dans [Kli90, Theorem 2, p. 34]. □

On notera que le point (3) dans la définition de $\mathcal{F}_g$ doit être vérifié pour *tous* les éléments de Γ_g. Il est cependant montré dans [Kli90, Proposition 3, p. 33] que pour tout g, il existe un ensemble *fini* $V_g \subset \Gamma_g$ tel que la condition (3) dans la définition de $\mathcal{F}_g$ donnée ci-dessus puisse être remplacée par :

3'. pour tout $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in V_g$,

$$|\mathrm{Det}(C\tau + D)| \geqslant 1.$$

Cependant, à notre connaissance, un tel ensemble V_g n'est explicitement connu qu'en genres $g = 1$ (on peut prendre $V_1 = \{S\}$) et $g = 2$, comme nous le verrons à la Section 6.1.2.

Enfin, le résultat suivant permet d'avoir un peu d'information supplémentaire sur les éléments de $\mathcal{F}_g$.

Lemme 5.1 *Pour tout $\tau \in \mathcal{F}_g$, si l'on note τ_1 le premier élément diagonal de $\mathcal{F}_g$, alors*

$$\mathrm{Im}\,(\tau_1) \geqslant \frac{\sqrt{3}}{2}.$$

Démonstration : Soit $\tau \in \mathcal{F}_g$, on peut alors considérer la matrice $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2$, avec

$$A = \begin{pmatrix} 0 & 0 \\ 0 & I_{g-1} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 \\ 0 & I_{g-1} \end{pmatrix}.$$

On a alors

$$|\mathrm{Det}(C\tau + D)| = |\tau_1|\,,$$

où τ_1 est le premier élément diagonal de τ. Par définition du domaine fondamental $\mathcal{F}_g$, on a donc $|\tau_1| \geqslant 1$, et par ailleurs $|\mathrm{Re}\,(\tau_1)| \leqslant \frac{1}{2}$, d'où l'on déduit finalement que $|\mathrm{Im}\,(\tau_1)| \geqslant \frac{\sqrt{3}}{2}$. □

Nous utiliserons ce lemme au Chapitre 6 pour montrer que pour tout $\tau \in \mathcal{F}_2$, $\lambda\,(\tau) \geqslant \frac{\sqrt{3}}{4}$. En fait, nous pensons que pour tout $n \geqslant 1$, il existe une constante $c(n)$ telle que pour tout matrice $n \times n$ M symétrique, définie positive et réduite au sens de Minkowski, la plus petite valeur propre de M est supérieure à $c(n) \cdot M_1$, où M_1 désigne le premier coefficient diagonal de M. Si ceci était vrai, alors le Lemme 5.1 permettrait de montrer que pour tout $\tau \in \mathcal{F}_g$,

$$\lambda\,(\tau) \geqslant c(g) \cdot \mathrm{Im}\,(\tau_1) \geqslant \frac{\sqrt{3}}{2} c(g).$$

5.3 Les theta constantes comme formes modulaires

La notion de forme modulaire introduite pour le genre 1 au Chapitre 2 peut être généralisée en genre supérieur par la notion de *forme modulaire de Siegel* :

Définition 5.5 (forme modulaire de Siegel) *Soient Γ un sous-groupe d'indice fini de Γ_g et $k \in \mathbb{Z}$. Une fonction $f : \mathcal{H}_g \to \mathbb{C}$ est une* forme modulaire de Siegel *de poids k pour Γ si et seulement si*

1. *elle est holomorphe sur $\mathcal{H}_g$,*
2. *pour tous $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma$ et $\tau \in \mathcal{H}_g$,*

$$f(\gamma\tau) = \mathrm{Det}^k(C\tau + D) f(\tau),$$

   et

3. *dans le cas où $g = 1$, la fonction f est holomorphe aux pointes.*

Définition 5.6 (fonction modulaire de Siegel) *Soit Γ un sous-groupe d'indice fini de Γ_g. Une fonction $f : \mathcal{H}_g \to \mathbb{C}$ est une* fonction modulaire de Siegel *pour Γ si et seulement s'il existe deux formes modulaires de Siegel f_1 et f_2 pour Γ, de même poids, telles que $f = \frac{f_1}{f_2}$ (en particulier, f est invariante sous l'action du groupe Γ).*

On a le résultat (important) suivant :

Théorème 5.1 *En genre g, toute famille de formes modulaires de Siegel (de poids quelconques) algébriquement libre contient au plus* $\frac{g(g+1)}{2}+1$ *éléments, et toute famille de fonctions modulaires de Siegel algébriquement libre contient au plus* $\frac{g(g+1)}{2}$ *éléments.*

Démonstration : Voir [Kli90][Theorem 3, p. 54] pour la première partie. La seconde partie en découle directement. □

Le but de cette section est de montrer que les (puissances huitièmes des) theta constantes sont des formes modulaires de Siegel pour un certain sous-groupe de Γ_g. Pour cela, nous commençons par donner les formules permettant de décrire l'action des éléments de Γ_g sur les carrés des theta constantes.

Proposition 5.4 *Pour tous* $\tau \in \mathcal{H}_g$, $a, b \in \{0,1\}^g$ *et* $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$, *on a*

$$\theta^2_{a,b}(\gamma\tau) = \kappa(\gamma) i^{\varepsilon(\gamma,a,b)} \mathrm{Det}(C\tau + D)\theta^2_{a',b'}(\tau),$$

où, en posant

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = {}^t\gamma \begin{pmatrix} a - (C\,{}^tD)_0 \\ b - (A\,{}^tB)_0 \end{pmatrix},$$

les valeurs de a' *et* $b' \in \{0,1\}^g$ *sont déterminées par*

$$\begin{pmatrix} a' \\ b' \end{pmatrix} \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \bmod 2$$

et

$$\varepsilon(\gamma,a,b) = 2\,{}^t(B\alpha)C\beta - {}^t(D\alpha)B\alpha - {}^t(C\beta)A\beta + 2\,{}^t\left((A\,{}^tB)_0\right)(D\alpha - C\beta).$$

$\kappa(\gamma)$ *est une racine quatrième de l'unité qui ne dépend que de* γ.

Démonstration : Il s'agit d'un cas particulier de [Igu72, Theorem II, p. 175–176].

Nous esquissons ici une autre démonstration : on peut commencer par montrer la proposition dans le cas particulier où γ est l'un des générateurs de Γ_g donnés dans la Proposition 5.2. Pour les éléments de la forme $M_{i,j}$, ceci se fait directement à partir de la définition des theta constantes et est un peu technique, pour J la méthode classique est d'utiliser la formule de Poisson (le calcul est fait par exemple dans [Mum84a, p. 195–197]). Notons que ceci permet de montrer que pour tous $a, b \in \{0,1\}^2$ et $\tau \in \mathcal{H}_g$,

$$\theta^2_{a,b}(J\tau) = (-i)^g \mathrm{Det}(\tau)\theta^2_{b,a}(\tau).$$

Ensuite, on procède par récurrence sur la longueur de la décomposition d'un élément $\gamma \in \Gamma_g$ en produit des générateurs $M_{i,j}$ et J : on suppose que la formule est vraie pour un élément γ, et on montre qu'elle l'est encore pour γJ et les $\gamma M_{i,j}$. Cette phase est elle très technique. □

Cette proposition montre que, pour tout $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g$, il existe

$$\Phi(\gamma,.) : \{0,1\}^{2g} \to [0,3]$$

et $\Psi(\gamma,.)$ une bijection de $\{0,1\}^{2g}$ tels que, pour tous $\tau \in \mathcal{H}_g$ et $a, b \in \{0,1\}^g$,

$$\theta^2_{a,b}(\gamma\tau) = \kappa(\tau)\mathrm{Det}(C\tau + D) i^{\Phi(\gamma,a,b)} \theta^2_{\Psi(\gamma,a,b)}(\tau),$$

avec de plus $\Phi(\gamma,0,0)=0$. Nous utiliserons ces notations par la suite, et plus particulièrement dans les Chapitres 6 et 8.

Introduisons maintenant les groupes

$$\Gamma_{g,2}=\{\gamma\in\Gamma_g : \gamma\equiv I_{2g} \bmod 2\}$$

et

$$\Gamma_{g,2,4}=\left\{\begin{pmatrix} A & B\\ C & D\end{pmatrix}\in\Gamma_{g,2} : B_0\equiv C_0\equiv 0 \bmod 4\right\}.$$

Ce dernier groupe, noté simplement $\Gamma_{2,4}$ par Igusa (nous préférons garder explicitement trace du genre dans la notation), consiste donc simplement en les éléments $\begin{pmatrix} A & B\\ C & D\end{pmatrix}$ de $\Gamma_{g,2}$ tels que les diagonales de B et C soient congrues à zéro modulo 4.

L'importance de ces groupes vis-à-vis des theta constantes vient du corollaire suivant de la Propriété 5.4 :

Corollaire 5.1 *Pour tous* $\gamma=\begin{pmatrix} A & B\\ C & D\end{pmatrix}\in\Gamma_{g,2}$, $a,b\in\{0,1\}^g$ *et* $\tau\in\mathcal{H}_g$,

$$\theta_{a,b}^2(\gamma\tau)=\kappa(\gamma)i^{\varepsilon(\gamma,a,b)}\mathrm{Det}(C\tau+D)\theta_{a,b}^2(\tau).$$

En particulier, si $\gamma\in\Gamma_{g,2,4}$,

$$\theta_{a,b}^2(\gamma\tau)=\kappa(\gamma)\mathrm{Det}(C\tau+D)\theta_{a,b}^2(\tau).$$

Démonstration : La première partie est une conséquence directe de la proposition. Pour montrer la seconde, il suffit de montrer que pour tous $\gamma=\begin{pmatrix} A & B\\ C & D\end{pmatrix}\in\Gamma_{g,2,4}$, $\alpha,\beta\in[0,3]^g$, on a

$$2^t(B\alpha)C\beta-{}^t(D\alpha)B\alpha-{}^t(C\beta)A\beta+2^t\left((A^tB)_0\right)(D\alpha-C\beta)\equiv 0 \bmod 4.$$

Comme les coefficients de B et C sont pairs, il suffit de montrer que

$${}^t\alpha{}^tDB\alpha+{}^t\beta{}^tCA\beta\equiv 0 \bmod 4.$$

Du fait que $\gamma\in\Gamma_{g,2,4}$, on déduit que les matrices $\frac{{}^tCA}{2}$ et $\frac{{}^tDB}{2}$ sont symétriques à coefficients diagonaux pairs, d'où l'on déduit que ${}^t\alpha\frac{{}^tDB}{2}\alpha$ et ${}^t\beta\frac{{}^tCA}{2}\beta$ sont pairs, ce qui termine la démonstration. □

On en déduit que les puissances huitièmes des theta constantes sont des formes modulaires de Siegel de poids 4 pour le groupe $\Gamma_{g,2}$.

5.4 Formules de duplication

Proposition 5.5 *Pour tous* $a,b\in\{0,1\}^g$ *et* $\tau\in\mathcal{H}_g$, *on a*

$$\theta_{a,b}^2(2\tau)=\frac{1}{2^g}\sum_{b_1+b_2\equiv b \bmod 2}(-1)^{{}^tab_1}\theta_{0,b_1}(\tau)\theta_{0,b_2}(\tau).$$

DÉMONSTRATION : Soient $a, b \in \{0,1\}^g$ et soit $\tau \in \mathcal{H}_g$, alors

$$\begin{aligned}
&\sum_{b_1+b_2\equiv b \bmod 2} (-1)^{{}^t a b_1} \theta_{0,b_1}(\tau)\theta_{0,b_2}(\tau) \\
&= \sum_{\substack{b_1+b_2\equiv b \bmod 2 \\ m,n\in\mathbb{Z}^g}} E\left({}^t m\tau m + {}^t n\tau n + {}^t m b_1 + {}^t n b_2 + {}^t b_1\right) \\
&= \sum_{\substack{m,n\in\mathbb{Z}^g \\ b_1\in\{0,1\}^g}} E\left({}^t m\tau m + {}^t n\tau n + {}^t(m+a) b_1 + {}^t n(b+b_1)\right) \\
&= \sum_{m,n\in\mathbb{Z}^g} \left(\sum_{b_1\in\{0,1\}^g} E\left({}^t(m+n+a)b_1\right)\right) E\left({}^t m\tau m + {}^t n\tau n + {}^t nb\right).
\end{aligned}$$

On voit alors facilement que

$$\sum_{b_1\in\{0,1\}^g} E\left({}^t(m+n+a)b_1\right) = \begin{cases} 2^g & \text{si } m+n+a \equiv 0 \bmod 2 \\ 0 & \text{sinon.} \end{cases}$$

En posant $n = m + a + 2c$, on a donc

$$\begin{aligned}
&\sum_{b_1+b_2\equiv b \bmod 2} (-1)^{{}^t a b_1} \theta_{0,b_1}(\tau)\theta_{0,b_2}(\tau) \\
&= 2^g \sum_{m,c\in\mathbb{Z}^g} E\left({}^t m\tau m + {}^t(m+a+2c)\tau(m+a+2c) + {}^t(m+a)b\right),
\end{aligned}$$

et en posant maintenant $m = d - c$, on obtient finalement

$$\begin{aligned}
&\sum_{b_1+b_2\equiv b \bmod 2} (-1)^{{}^t a b_1} \theta_{0,b_1}(\tau)\theta_{0,b_2}(\tau) \\
&= 2^g \sum_{c,d\in\mathbb{Z}^g} E\left({}^t(d-c)\tau(d-c) + {}^t(d+c+a)\tau(d+c+a) + {}^t(d-c+a)b\right) \\
&= 2^g \sum_{c,d\in\mathbb{Z}^g} E\left({}^t\left(c+\tfrac{a}{2}\right) 2\tau \left(c+\tfrac{a}{2}\right) + {}^t\left(d+\tfrac{a}{2}\right) 2\tau \left(d+\tfrac{a}{2}\right) + {}^t\left(c+\tfrac{a}{2}\right) b + {}^t\left(d+\tfrac{a}{2}\right) b\right) \\
&= 2^g \left(\theta_{a,b}(2\tau)\right)^2,
\end{aligned}$$

ce qui conclut la démonstration. □

Proposition 5.6 *Pour tous $a, b \in \{0,1\}^g$ et $\tau \in \mathcal{H}_g$, on a*

$$\theta_{a,b}^2\left(\frac{\tau}{2}\right) = \sum_{a_1+a_2\equiv a \bmod 2} (-1)^{{}^t a_1 b} \theta_{a_1,0}^2(\tau)\theta_{a_2,0}^2(\tau).$$

DÉMONSTRATION : Soient $\tau \in \mathcal{H}_g$, $a, b \in \{0,1\}^g$ et posons $\tau' = -\tau^{-1}$ (*i.e.*, $2\tau = -(\tau'/2)^{-1}$). Le Théorème 2 du Chapitre V de [Igu72] montre qu'il existe alors une racine huitième de l'unité ω telle que, pour tous $t \in \mathcal{H}_g$ et $u, v \in \{0,1\}$,

$$\theta_{u,v}(-t^{-1}) = \omega r \theta_{v,u}(t),$$

où $r^2 = \mathrm{Det}(t)$.

Par ailleurs, la formule de duplication (Proposition 5.5) montre que

$$\theta_{b,a}(2\tau') = \frac{1}{2^g} \sum_{a_1+a_2\equiv a \bmod 2} \theta_{0,a_1}(\tau')\theta_{0,a_2}(\tau'),$$

soit

$$\begin{aligned}
\theta_{b,a}^2(2\tau') &= \theta_{b,a}^2\left(-\left(\frac{\tau}{2}\right)^{-1}\right) \\
&= \omega^2 \mathrm{Det}\left(\frac{\tau}{2}\right) \theta_{a,b}^2\left(\frac{\tau}{2}\right),
\end{aligned}$$

et

$$\begin{aligned}\sum_{a_1+a_2\equiv a \bmod 2} (-1)^{{}^t ba_1}\theta_{0,a_1}(\tau')\theta_{0,a_2}(\tau') &= \sum_{a_1+a_2\equiv a \bmod 2} (-1)^{{}^t a_1 b}\theta_{0,a_1}(-\tau^{-1})\theta_{0,a_2}(-\tau^{-1}) \\ &= \omega^2 \mathrm{Det}(\tau) \sum_{a_1+a_2\equiv a \bmod 2} (-1)^{{}^t ba_1}\theta_{a_1,0}(\tau)\theta_{a_2,0}(\tau),\end{aligned}$$

ce qui termine la démonstration. □

Lemme 5.2 *Pour tous $a, b \in \{0,1\}^g$, si $(\tau_n)_{n\in\mathbb{N}}$ est une suite d'éléments de $\mathcal{H}_g$ telle que $\lim_{n\to+\infty} \lambda(\tau_n) = +\infty$, on a*

$$\lim_{n\to+\infty} \theta_{a,b}(\tau_n) = \begin{cases} 1 & \text{si } a = 0 \\ 0 & \text{si } a \neq 0 \end{cases}$$

Démonstration : Soient $b \in \{0,1\}^g$, $(\tau_n)_{n\in\mathbb{N}} \in \mathcal{H}_g^{\mathbb{N}}$, et notons $q_n = \exp(-\pi\lambda(\tau_n))$, alors la définition des theta constantes montre que pour tout $n \geqslant 0$,

$$\begin{aligned}|\theta_{0,b}(\tau_n) - 1| &\leqslant \sum_{(m_1,\ldots,m_g\in\mathbb{Z}^g\setminus\{0\}} q_n^{m_1^2+\ldots+m_g^2} \\ &\leqslant 2^g \left(\sum_{m\in\mathbb{Z}\setminus\{0\}} q_n^{m^2}\right)\left(\sum_{m\in\mathbb{Z}} q_n^{m^2}\right)^{2^g-1}.\end{aligned}$$

On utilise alors la majoration

$$\sum_{m\geqslant 1} q_n^{m^2} \leqslant \sum_{m\geqslant 1} q_n^m \leq \frac{q_n}{1-q_n},$$

pour obtenir

$$|\theta_{0,b}(\tau_n) - 1| \leqslant 2^g \left(1 + \frac{2q_n}{1-q_n}\right)^{2^g-1} \frac{2q_n}{1-q_n}.$$

Si $\lambda(\tau_n)$ tend vers l'infini, alors bien sûr q_n tend vers zéro, et l'inégalité ci-dessus permet de montrer le résultat puisque le côté droit tend vers zéro.

Si maintenant $a \neq 0$ et que $(\tau_n)_{n\in\mathbb{N}}$ est une suite de $\mathcal{H}_g$ telle que $\lambda(\tau_n)$ tend vers l'infini, alors ce qui précède montre que pour tout $b \in \{0,1\}^g$,

$$\lim_{n\to+\infty} \theta_{0,b}\left(\frac{\tau_n}{2}\right) = 1,$$

et en exprimant les $\theta_{a,b}^2(\tau_n)$ en fonction des $\theta_{0,b}\left(\frac{\tau_n}{2}\right)$ à l'aide de la formule de duplication des theta constantes (Proposition 5.5), on voit facilement que si $a \neq 0$,

$$\lim_{n\to+\infty} \theta_{a,b}^2(\tau_n) = 0,$$

ce qui conclut la démonstration. □

Chapitre 6

Le cas du genre 2

Le but de ce chapitre est d'obtenir quelques résultats particuliers concernant les theta constantes en genre 2. Nous utiliserons la lettre θ pour désigner les theta constantes en genre 2, et la lettre ϑ pour désigner les theta constantes en genre 1.

6.1 Le groupe Γ_2 et le domaine fondamental $\mathcal{F}_2$

6.1.1 Le groupe Γ_2

Dans cette section, on note I la matrice identité de dimension 2. Comme on a utilisé des lettres majuscules pour désigner les éléments de Γ_1, nous utilisons dans cette section des lettres gothiques pour désigner les éléments de Γ_2. On désigne alors par $\mathfrak{I}$ l'identité de Γ_2, et on pose

$$\mathfrak{I} = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}, \qquad \mathfrak{M}_1 = \begin{pmatrix} I & \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & \\ & I \end{matrix} & \end{pmatrix}, \qquad \mathfrak{M}_2 = \begin{pmatrix} I & \begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix} \\ \begin{matrix} 0 & \\ & I \end{matrix} & \end{pmatrix},$$

$$\mathfrak{M}_3 = \begin{pmatrix} I & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \\ \begin{matrix} 0 & \\ & I \end{matrix} & \end{pmatrix}, \qquad \mathfrak{S} = \begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}, \qquad \mathfrak{T} = \begin{pmatrix} T & 0 \\ 0 & {}^tT^{-1} \end{pmatrix},$$

où S et T sont les générateurs de Γ_1 introduits à la Section 2.1.1.

D'après la Proposition 5.2, on a

$$\Gamma_2 = \langle \mathfrak{J}, \mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3 \rangle.$$

Par ailleurs,

$$\mathfrak{M}_2 = \mathfrak{S}\mathfrak{M}_1\mathfrak{S}$$

et

$$\mathfrak{M}_1\mathfrak{M}_2\mathfrak{M}_3 = \mathfrak{J}\mathfrak{T}^{-1}\mathfrak{J}\mathfrak{M}_1\mathfrak{J}\mathfrak{T}\mathfrak{J},$$

d'où l'on déduit que

$$\Gamma_2 = \langle \mathfrak{J}, \mathfrak{M}_1, \mathfrak{S}, \mathfrak{T} \rangle.$$

6.1.2 Le domaine fondamental $\mathcal{F}_2$

Dans le cas particulier du genre 2, on connaît explicitement un nombre fini d'inéquations permettant de définir le domaine fondamental $\mathcal{F}_2$. Plus précisément, on a le théorème suivant, dû à Gottschling [Got59] :

Théorème 6.1 *Le domaine fondamental $\mathcal{F}_2$ est l'ensemble des matrices $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{H}_2$ telles que :*

1. $|\mathrm{Re}\,(\tau_j)| \leqslant \frac{1}{2}$ *pour* $j \in [1,3]$,
2. *la matrice* $\mathrm{Im}\,(\tau)$ *est réduite au sens de Minkowski, et*
3. $|\mathrm{Det}(C\tau + D)| \geqslant 1$ *pour toute matrice symplectique* $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \{\mathfrak{N}_j\}_{j\in[1,19]}$,

avec

$$\mathfrak{N}_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathfrak{N}_2 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathfrak{N}_3 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\mathfrak{N}_4 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad \mathfrak{N}_5 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad \mathfrak{N}_6 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

$$\mathfrak{N}_7 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad \mathfrak{N}_8 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad \mathfrak{N}_9 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix},$$

$$\mathfrak{N}_{10} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \mathfrak{N}_{11} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}, \quad \mathfrak{N}_{12} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

$$\mathfrak{N}_{13} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}, \quad \mathfrak{N}_{14} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad \mathfrak{N}_{15} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & -1 \end{pmatrix},$$

$$\mathfrak{N}_{16} = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathfrak{N}_{17} = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathfrak{N}_{18} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix},$$

$$\mathfrak{N}_{19} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ -1 & 1 & 0 & -1 \end{pmatrix}.$$

Démonstration : Nous renvoyons à l'article original de Gottschling [Got59]. Notons que l'article montre non seulement que ces 19 matrices suffisent à définir $\mathcal{H}_2$, mais aussi qu'elles sont toutes nécessaires en ce sens que pour tout $j \in [1,19]$, il existe $\tau \in \mathcal{H}_2 \setminus \mathcal{F}_2$ qui vérifie les deux premiers points de la définition de $\mathcal{F}_2$ et tel que, pour tout $k \in [1,19] \setminus \{j\}$,

$$|\mathrm{Det}(C_k\tau + D_k)| \geqslant 1.$$

□

Notons qu'une matrice symétrique réelle $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ définie positive est réduite au sens de Minkowski si et seulement si $c \geqslant a$ et $a \geqslant 2b \geqslant 0$. L'Algorithme 9 (dont la validité est démontrée par exemple dans [Kli90]) permet de réduire au sens de Minkowski une matrice symétrique réelle définie positive.

Algorithme : `MinkowskiReduction`

Entrée : $M = \begin{pmatrix} M_1 & M_3 \\ M_3 & M_2 \end{pmatrix}$ une matrice symétrique réelle définie positive

Sortie : une matrice entière unimodulaire U telle que UM^tU soit réduite au sens de Minkowski

$t \leftarrow$ true;
$U \leftarrow I_2$;
while t **do**
  if $2|M_3| \leqslant |M_1|$ **then**
    if $|M_1| \leqslant |M_2|$ **then**
      if $M_3 \leqslant 0$ **then**
        $M \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$;
        $U \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} U$;
      end
      $t \leftarrow$ false;
    else
      $M \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$;
      $U \leftarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} U$;
    end
  end
  $q \leftarrow \lfloor M_3/M_1 \rceil$;
  $M \leftarrow \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} M \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$;
  $U \leftarrow \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} U$;
end
return U;

Algorithme 9: Réduction d'une matrice symétrique réelle au sens de Minkowski

L'Algorithme 10 permet alors de réduire un élément de $\mathcal{H}_2$ dans le domaine fondamental $\mathcal{F}_2$.

Les éléments $\mathfrak{N}_j = \begin{pmatrix} A_j & B_j \\ C_j & D_j \end{pmatrix}$, pour $j \in [1, 19]$, sont ceux introduits dans le Théorème 6.1. La validité de cet algorithme découle du théorème sus-cité, ainsi que du résultat suivant :

Algorithme : `ReduceToF2`
Entrée : $\tau \in \mathcal{H}_2$
Sortie : $(\gamma, \tau') \in \Gamma_2 \times \mathcal{F}_2$ tels que $\tau' = \gamma\tau$

$\gamma \leftarrow \mathfrak{I}$;
$\tau' \leftarrow \tau$;
$t \leftarrow$ true;
while t **do**
  $U \leftarrow$ `MinkowskiReduction`$(\mathrm{Im}\,(\tau'))$;
  $\gamma \leftarrow \begin{pmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{pmatrix} \gamma$;
  $\tau' \leftarrow U\tau'^tU$;
  for $j = 1$ **to** 3 **do**
    $a \leftarrow -\lfloor \mathrm{Re}\left(\tau'_j\right) \rceil$;
    $\tau' \leftarrow \mathfrak{M}_j^a \tau'$;
    $\gamma \leftarrow \mathfrak{M}_j^a \tau'$;
  end
  $t \leftarrow$ false;
  for $j = 1$ **to** 19 **do**
    if $|\mathrm{Det}(C_j\tau' + D_j)| < 1$ **then**
      $t \leftarrow$ true;
      $\tau' \leftarrow \mathfrak{N}_j \tau'$;
      $\gamma \leftarrow \mathfrak{N}_j \gamma$;
    end
  end
end
return (γ, τ');

Algorithme 10: Réduction dans le domaine fondamental $\mathcal{F}_2$

Lemme 6.1 *Pour tout $\tau \in \mathcal{H}_2$ et $\varepsilon > 0$, l'ensemble*

$$\left\{ |\mathrm{Det}(C\tau + D)| \geqslant \varepsilon : \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2 \right\}$$

est fini.

DÉMONSTRATION : Il s'agit d'une conséquence directe de [Kli90, Lemma 1, p.29]. □

Quelques propriétés numériques des éléments de $\mathcal{F}_2$

Soit $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$, le Lemme 5.1 montre qu'alors

$$\mathrm{Im}\,(\tau_1) \geqslant \frac{\sqrt{3}}{2}.$$

Par ailleurs, la matrice $\mathrm{Im}\,(\tau)$ est réduite au sens de Minkowski, *i.e.,*

$$\mathrm{Im}\,(\tau_2) \geqslant \mathrm{Im}\,(\tau_1) \geqslant 2\mathrm{Im}\,(\tau_3) \geqslant 0.$$

Les valeurs propres de $\mathrm{Im}\,(\tau)$ sont les racines de

$$X^2 - (y_1 + y_2)X + (y_1 y_2 - y_3^2) = 0,$$

où $y_j = \mathrm{Im}\,(\tau_j)$. La plus petite de ces valeurs propres est donc

$$\begin{aligned} \lambda\,(\tau) &= \frac{y_1 + y_2 - \sqrt{(y_2 - y_1)^2 + 4y_3^2}}{2} && (6.1) \\ &\geqslant \frac{y_1 + y_2 - 2y_3}{2} && (6.2) \\ &\geqslant \frac{y_2}{2} && (6.3) \\ &\geqslant \frac{y_1}{2} && (6.4) \\ &\geqslant \frac{\sqrt{3}}{4}. && (6.5) \end{aligned}$$

Toutes ces inégalités sont des égalités pour

$$\tau = \frac{\sqrt{3}}{2} i \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \in \mathcal{F}_2.$$

Considérons un élément $\tau \in \mathcal{H}_2$ de la forme $\tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}$. On a alors les égalités suivantes :

$$\mathfrak{M}_1\tau = \begin{pmatrix} T\tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}, \qquad \mathfrak{M}_2\tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & T\tau_2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tau = \begin{pmatrix} S\tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & S\tau_2 \end{pmatrix},$$

et

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tau = \begin{pmatrix} \tau_2 & 0 \\ 0 & \tau_1 \end{pmatrix}$$

(et on vérifie aisément que les matrices que l'on a fait agir sont bien des éléments de Γ_2). On en déduit donc que, si l'on note τ_1' (resp. τ_2') le réduit de τ_1 (resp. de τ_2) dans le domaine fondamental $\mathcal{F}$, alors :

– si $\mathrm{Im}\,(\tau_1') \geqslant \mathrm{Im}\,(\tau_2')$, alors

$$\begin{pmatrix} \tau_1' & 0 \\ 0 & \tau_2' \end{pmatrix} \in \mathcal{F}_2$$

est équivalent à τ modulo l'action de Γ_2 ;

– sinon,

$$\begin{pmatrix} \tau_2' & 0 \\ 0 & \tau_1' \end{pmatrix} \in \mathcal{F}_2$$

est équivalent à τ modulo l'action de Γ_2.

6.2 Theta constantes en genre 2

Afin de simplifier les notations, nous numérotons les theta constantes en genre 2 de 0 à 15 comme suit : pour tous $a = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}, b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \in \{0,1\}^2$ on pose

$$\theta_{b_0+2b_1+4a_0+8a_1} = \theta_{a,b}.$$

Avec cette notation, les 6 theta constantes impaires (donc identiquement nulles) en genre 2 correspondent aux indices $\{5, 7, 10, 11, 13, 14\}$. On note $\mathcal{P}_2 = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$ l'ensemble des indices des theta constantes paires.

6.2.1 Valeurs des theta constantes sur le domaine fondamental $\mathcal{F}_2$

Les méthodes que nous employons dans cette section pour obtenir des résultats sur les valeurs des theta constantes sur $\mathcal{F}_2$ sont sensiblement les mêmes que celles utilisées (dans le même but) par Klingen dans [Kli90, Chapter 9].

Proposition 6.1 *Pour tous $\tau \in \mathcal{F}_2$ et $j \in [0,3]$,*

$$|\theta_j(\tau) - 1| \leqslant 0.405.$$

Démonstration : Soient $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$ et $j \in [0,3]$, alors si l'on note

$$q_u = |E(\tau_u)| = \exp\left(-\pi \mathrm{Im}\,(\tau_u)\right)$$

pour $u \in [1,3]$ et $Q = \exp\left(-\pi\frac{\sqrt{3}}{4}\right)$, on a

$$|\theta_j(\tau) - 1| \leqslant \sum_{(m,n)\in\mathbb{Z}^2} q_1^{m^2} q_3^{2mn} q_2^{n^2}.$$

Le fait que τ soit dans $\mathcal{F}_2$ implique que

$$\mathrm{Im}\,(\tau_2) \geqslant \mathrm{Im}\,(\tau_1) \geqslant 2\mathrm{Im}\,(\tau_3) \geqslant 0,$$

et aussi que $\mathrm{Im}\,(\tau_1) \geqslant \frac{\sqrt{3}}{2}$, d'où l'on déduit que

$$q_1^{m^2} q_3^{2mn} q_2^{n^2} \leqslant \begin{cases} Q^{2(m^2+n^2)} & \text{si} \quad mn \geqslant 0, \\ Q^{2(m^2+n^2+mn} & \text{si} \quad mn < 0. \end{cases}$$

Comme de plus $\lambda(\tau) \geqslant \frac{\mathrm{Im}(\tau_1)}{2}$, on a aussi

$$q_1^{m^2} q_3^{2mn} q_2^{n^2} \leqslant Q^{m^2+n^2}$$

pour tous $m, n \in \mathbb{Z}$.

En utilisant ces majorations, on obtient

$$\sum_{(m,n)\in\{-2,2\}^2\setminus\{(0,0)\}} \leqslant 6Q^2 + 2Q^4 + 4Q^6 + 6Q^8 + 4Q^{10} + 2Q^{16}.$$

Nous donnons maintenant une majoration moins fine du reste de la somme :

$$\begin{aligned} \sum_{(m,n)\in\mathbb{Z}^2, |m|\geqslant 3, |n|\geqslant 3} q_1^{m^2} q_3^{2mn} q_2^{n^2} &\leqslant 4\left(\sum_{m=0}^{2}\sum_{n\geqslant 3} Q^{m^2+n^2} + \sum_{m\geqslant 3}\sum_{n\geqslant 1} Q^{m^2+n^2}\right) \\ &\leqslant 4\frac{1+Q}{(1-Q)^2}Q^9. \end{aligned}$$

Ceci prouve finalement que

$$|\theta_j(\tau) - 1| \leqslant 6Q^2 + 2Q^4 + 4Q^6 + 6Q^8 + 4Q^{10} + 2Q^{16} + 4\frac{1+Q}{(1-Q)^2}Q^9,$$

et une évaluation numérique montre que

$$|\theta_j(\tau) - 1| \leqslant 0.405.$$

□

Proposition 6.2 *Pour tous $\tau \in \mathcal{F}_2$ et $j \in \{4, 6\}$,*

$$\left|\frac{\theta_j(\tau)}{2E\left(\frac{\tau_1}{4}\right)} - 1\right| \leqslant 2\left|E\left(\frac{\tau_1}{2}\right)\right|.$$

Démonstration : Soit $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$ et $j \in \{4, 6\}$, alors si l'on pose $\varepsilon_4 = 0$ et $\varepsilon_6 = 1$, on a

$$\begin{aligned} \theta_j(\tau) &= \sum_{(m,n)\in\mathbb{Z}^2} (-1)^{\varepsilon_j n} E\left(\left(m+\frac{1}{2}\right)^2 \tau_2 + \left(m+\frac{1}{2}\right) n\tau_3 + n^2\tau_2\right) \\ &= E\left(\frac{\tau_1}{4}\right) \sum_{(m,n)\in\mathbb{Z}^2} (-1)^{\varepsilon_j n} E\left((m^2+m)\tau_1 + (2m+1)n\tau_3 + n^2\tau_2\right) \\ &= E\left(\frac{\tau_1}{4}\right)\left(2 + \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(-1,0),(0,0)\}} (-1)^{\varepsilon_j n} E\left((m^2+m)\tau_1 + (2m+1)n\tau_3 + n^2\tau_2\right)\right), \end{aligned}$$

ce qui entraîne

$$\left|\frac{\theta_j(\tau)}{E\left(\frac{\tau_1}{4}\right)}-2\right| \leqslant \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0),(-1,0)\}} q_1^{m^2+m}q_3^{2mn+n}q_2^{n^2}.$$

Si l'on pose $q=\left|E\left(\frac{\tau_1}{2}\right)\right|$, alors en utilisant le même type d'arguments que dans la démonstration de la Proposition 6.1 on obtient

$$\begin{aligned}\sum_{(m,n)\in[-2,2]^2\setminus\{(0,0),(-1,0)\}} q_1^{m^2+m}q_3^{2mn+n}q_2^{n^2} &\leqslant 2q+2q^2+2q^3+2q^4+6q^6+2q^8+q^9+q^{10}+\\ &\quad 3q^{12}+q^{14}+q^{20}\\ &\leqslant 3q,\end{aligned}$$

où l'on a utilisé le fait que comme $\tau\in\mathcal{F}_2$, $q\leqslant\exp\left(-\pi\frac{\sqrt{3}}{4}\right)$, donc

$$2q^2+2q^3+2q^4+6q^6+2q^8+q^9+q^{10}+3q^{12}+q^{14}+q^{20}<q.$$

Majorons maintenant le reste de la somme :

$$\begin{aligned}\sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ |m|>2 \text{ ou } |n|>2}} q_1^{m^2+m}q_3^{2mn+n}q_2^{n^2} &\leqslant \sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ |m|>2 \text{ ou } |n|>2}} q^{m^2+n^2}q_1^m q_3^n\\ &\leqslant \sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ |m|>2 \text{ ou } |n|>2}} q^{m^2+n^2-2|m|-|n|}\\ &\leqslant 4\left(\sum_{\substack{m\geqslant 3,\\ n\in\{1,2\}}} q^{m^2-2|m|+n^2-|n|}+\sum_{\substack{m\geqslant 1,\\ n\geqslant 3}} q^{m^2-2|m|+n^2-|n|}\right)\\ &\quad +2\left(\sum_{m\geqslant 3} q^{m^2-2|m|}+\sum_{n\geqslant 3} q^{n^2-|n|}\right).\end{aligned}$$

En utilisant le Lemme 2.1 ainsi que la borne supérieure que l'on a pour la valeur de q, on obtient finalement

$$\sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ |m|>2 \text{ ou } |n|>2}} q_1^{m^2+m}q_3^{2mn+n}q_2^{n^2}\leqslant q.$$

Les deux majorations obtenues donnent donc

$$\left|\frac{\theta_j(\tau)}{E\left(\frac{\tau_1}{2}\right)}-2\right|\leqslant 4q,$$

ce qui conclut. □

Proposition 6.3 *Pour tous $\tau\in\mathcal{F}_2$ et $j\in\{8,9\}$,*

$$\left|\frac{\theta_j(\tau)}{2E\left(\frac{\tau_2}{4}\right)}-1\right|\leqslant 2\left|E\left(\frac{\tau_1}{2}\right)\right|.$$

DÉMONSTRATION : La démonstration, relativement technique encore une fois, est similaire à celle de la Proposition 6.2, donc non reproduite ici. □

Proposition 6.4 *La fonction θ_{12} ne s'annule pas sur $\mathcal{F}_2$.*

DÉMONSTRATION : Soit $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$, alors (par définition de θ_{12}) :

$$\begin{aligned}
\theta_{12}(\tau) &= \sum_{(m,n)\in\mathbb{Z}^2} E\left(\left(m+\frac{1}{2}\right)^2\tau_1 + 2\left(m+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\tau_3 + \left(n+\frac{1}{2}\right)^2\tau_2\right) \\
&= E\left(\frac{\tau_1+\tau_2+2\tau_3}{4}\right)\sum_{(m,n)\in\mathbb{Z}^2} E\left((m^2+m)\tau_1 + (n^2+n)\tau_2 + (2mn+m+n)\tau_3\right) \\
&= E\left(\frac{\tau_1-3\tau_2+2\tau_3}{4}\right)\sum_{(m,n)\in\mathbb{Z}^2} E\left(f(m,n,\tau)\right),
\end{aligned}$$

où

$$f(m,n,\tau) = (m^2+m)(\tau_1-\tau_3) + (n^2+n)(\tau_2-\tau_3) + (m+n+1)^2\tau_3.$$

En posant $u = -m-1$ et $v = -n-1$, on obtient

$$\sum_{m<0,n<0} E\left(f(m,n,\tau)\right) = \sum_{u\geqslant 0,v\geqslant 0} f(u,v,\tau),$$

et en posant $u = m$ et $v = -n-1$ (resp. $u = -m-1$ et $v = n$), on obtient

$$\sum_{m\geqslant 0,n<0} E\left(f(m,n,\tau)\right) = \sum_{u\geqslant 0,v\geqslant 0} E\left((u^2+u)(\tau_1-\tau_3) + (v^2+v)(\tau_2-\tau_3) + (u-v)^2\tau_3\right)$$

(resp.

$$\sum_{m<0,n\geqslant 0} E\left(f(m,n,\tau)\right) = \sum_{u\geqslant 0,v\geqslant 0} E\left((u^2+u)(\tau_1-\tau_3) + (v^2+v)(\tau_2-\tau_3) + (u-v)^2\tau_3\right)$$

), donc finalement

$$\begin{aligned}
\sum_{(m,n)\in\mathbb{Z}^2} E\left(f(m,n,\tau)\right) &= 2\sum_{u\geqslant 0,v\geqslant 0}\left(E\left((u+v+1)^2\tau_3\right) + E\left((u-v)^2\tau_3\right)\right) \\
&\quad \times E\left((u^2+u)(\tau_1-\tau_3) + (v^2+v)(\tau_2-\tau_3)\right).
\end{aligned}$$

Par ailleurs, on a pour tous $u, v \geqslant 0$

$$E\left((u+v+1)^2\tau_3\right) + E\left((u-v)^2\tau_3\right) = E\left((u-v)^2\tau_3\right)\left(1+E(\tau_3)\right)\sum_{w=0}^{(2u+1)(2v+1)-1} E\left(w(\tau_3+1)\right),$$

donc

$$\sum_{(m,n)\in\mathbb{Z}^2} E\left(f(m,n,\tau)\right) = 2\left(1+E(\tau_3)\right)\sum_{u\geqslant 0,v\geqslant 0} g(u,v,\tau)$$

avec

$$g(u,v,\tau) = E\left((u^2+u)(\tau_1-\tau_3) + (v^2+v)(\tau_2-\tau_3)\right)\sum_{w=0}^{(2u+1)(2v+1)-1} E\left(w(\tau_3+1)\right).$$

Maintenant, on utilise le fait que comme $\tau \in \mathcal{F}_2$, $\mathrm{Im}\,(\tau_j - \tau_3) \geqslant \frac{\sqrt{3}}{4}$ pour $j \in \{1,2\}$, et $\mathrm{Im}\,(\tau_3) \geqslant 0$, donc en posant $Q = \exp\left(-\pi\frac{\sqrt{3}}{4}\right)$, on a

$$\left|\sum_{u\geqslant 0, v\geqslant 0} g(u,v,\tau)\right| \leqslant -1 + \left(\sum_{x\geqslant 0}(2x+1)Q^{x^2+x}\right)^2.$$

On montre facilement que

$$\sum_{x\geqslant 0}(2x+1)Q^{x^2+x} < 1.2$$

donc que

$$\left|\sum_{u\geqslant 0, v\geqslant 0} g(u,v,\tau) - 1\right| \leqslant 0.44.$$

On en déduit directement le résultat. □

Proposition 6.5 *L'ensemble des zéros de θ_{15} sur $\mathcal{F}_2$ est l'ensemble des éléments de $\mathcal{F}_2$ dont les coefficients non diagonaux sont nuls.*

Démonstration : Soit $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$, alors par définition de θ_{15}, on a

$$\begin{aligned}
\theta_{15}(\tau) &= \sum_{(m,n)\in\mathbb{Z}^2} E\left(\left(m+\frac{1}{2}\right)^2\tau_1 + 2\left(m+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\tau_3 + \left(n+\frac{1}{2}\right)^2\tau_2 + (m+n+1)\right) \\
&= -E\left(\frac{\tau_1+\tau_2+2\tau_3}{4}\right)\sum_{(m,n)\in\mathbb{Z}^2} E\left((m^2+m)\tau_1 + (n^2+n)\tau_2 + (2mn+m+n)\tau_3 + m + n\right) \\
&= -E\left(\frac{\tau_1-3\tau_2+2\tau_3}{4}\right)\sum_{(m,n)\in\mathbb{Z}^2} E\left(f(m,n,\tau)\right),
\end{aligned}$$

où

$$f(m,n,\tau) = (m^2+m)(\tau_1-\tau_3) + (n^2+n)(\tau_2-\tau_3) + (m+n+1)^2\tau_3 + m + n.$$

En utilisant les mêmes techniques que dans la démonstration de la Proposition 6.4, on a alors

$$\begin{aligned}
\sum_{(m,n)\in\mathbb{Z}^2} E\left(f(m,n,\tau)\right) &= 2\sum_{u\geqslant 0, v\geqslant 0}\left(E\left((u+v+1)^2\tau_3\right) - E\left((u-v)^2\tau_3\right)\right) \\
&\quad \times E\left((u^2+u)(\tau_1-\tau_3) + (v^2+v)(\tau_2-\tau_3) + m + n\right),
\end{aligned}$$

et par ailleurs on a

$$E\left((u+v+1)^2\tau_3\right) - E\left((u-v)^2\tau_3\right) = E\left((u-v)^2\tau_3\right)\left(1 - E(\tau_3)\right)\sum_{w=0}^{(2u+1)(2v+1)-1} E\left(w\tau_3\right),$$

d'où l'on déduit, en utilisant le fait que $\tau \in \mathcal{F}_2$, que

$$\theta_{15}(\tau) = 2E\left(\frac{\tau_1-3\tau_2+2\tau_3}{4}\right)\left(E(\tau_3)-1\right)\sum_{u\geqslant 0, v\geqslant 0} g(u,v,\tau)$$

avec

$$g(u,v,\tau) = E\left((u^2+u)(\tau_1-\tau_3)+(v^2+v)(\tau_2-\tau_3)+m+n\right)\sum_{w=0}^{(2u+1)(2v+1)-1} E(w\tau_3).$$

Un raisonnement identique à celui utilisé dans la démonstration de la Proposition 6.4 permet alors de montrer que

$$\sum_{u\geqslant 0, v\geqslant 0} g(u,v,\tau) \neq 0,$$

ce qui termine la démonstration. □

On notera qu'il est relativement facile de voir que θ_{15} s'annule sur les matrices diagonales de $\mathcal{H}_2$: en effet, si $\tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} \in \mathcal{H}_2$, alors (d'après une remarque faite à la Section 5.1)

$$\theta_{15}(\tau) = \vartheta_3(\tau_1)\vartheta_3(\tau_2) = 0,$$

puisque ϑ_3 est identiquement nulle.

On définit $\rho : [0,15] \to [0,3]$ par

$$(\rho(j))_{j\in[0,15]} = (0,1,0,1,2,3,2,3,3,3,3,3,3,3,3,3).$$

On a alors le résultat suivant :

Lemme 6.2 *Pour tout $\varepsilon > 0$, il existe $M > 0$ tel que, pour tous $j \in [0,15]$ et $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$ vérifiant $\mathrm{Im}(\tau_2) \geqslant M\mathrm{Im}(\tau_1)$,*

$$\left|\theta_j(\tau) - \vartheta_{\rho(j)}(\tau_1)\right| \leqslant \varepsilon.$$

Démonstration : Soient $M \geqslant 1$ et $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$ tels que $\mathrm{Im}(\tau_2) \geqslant \mathrm{Im}(\tau_1)$.

Soit $b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \in \{0,1\}^2$, alors

$$\begin{aligned}\theta_{0,b}(\tau) - \vartheta_{0,b_0}(\tau_1) &= \sum_{(m,n)\in\mathbb{Z}^2} (-1)^{mb_0+nb_1} E\left(m^2\tau_1+n^2\tau_2+2mn\tau_3\right) - \sum_{m\in\mathbb{Z}} (-1)^{mb_0} E\left(m^2\tau_1\right)\\ &= \sum_{(m,n)\in\mathbb{Z}^2, n\neq 0} (-1)^{mb_0+nb_1} E\left(m^2\tau_1+n^2\tau_2+2mn\tau_3\right).\end{aligned}$$

Si l'on pose $q_j = \exp(-\pi\mathrm{Im}(\tau_j))$ pour $j \in [1,3]$, alors on a

$$\begin{aligned}|\theta_{0,b}(\tau) - \vartheta_{0,b_0}(\tau_1)| &\leqslant \sum_{(m,n)\in\mathbb{Z}^2, n\neq 0} q_1^{m^2} q_2^{n^2} q_3^{2mn}\\ &\leqslant 4\sum_{m\geqslant 0, n>0} q_1^{m^2} q_2^{n^2} q_3^{-2mn}\\ &\leqslant 4\sum_{m\geqslant 0, n>0} q_1^{m^2+Mn^2-mn},\end{aligned}$$

où l'on a utilisé le fait que, comme $\tau \in \mathcal{F}_2$, $\mathrm{Im}(\tau_1) \geqslant 2\mathrm{Im}(\tau_3) \geqslant 0$. On a aussi

$$-mn \leqslant -\frac{m^2+n^2}{2},$$

donc

$$\begin{aligned}|\theta_{0,b}(\tau)-\vartheta_{0,b_0}(\tau_1)| &\leqslant 4\sum_{m\geqslant 0}\left(q_1^{\frac{1}{2}}\right)^{m^2}\sum_{n>0}\left(q_1^{\frac{2M-1}{2}}\right)^{n^2}\\ &\leqslant \frac{4q_1^{\frac{2M-1}{2}}}{\left(1-q_1^{\frac{1}{2}}\right)^2}.\end{aligned}$$

Soient $a=\begin{pmatrix}1\\0\end{pmatrix}$ and $b=\begin{pmatrix}0\\b_1\end{pmatrix}\in\{0,1\}^2$, alors

$$\begin{aligned}\theta_{a,b}(\tau)-\vartheta_{1,0}(\tau_1) &= \sum_{(m,n)\in\mathbb{Z}^2}(-1)^{nb_1}E\left(\left(m+\frac{1}{2}\right)^2\tau_1+n^2\tau_2+2\left(m+\frac{1}{2}\right)n\tau_3\right)\\ &\quad -\sum_{m\in\mathbb{Z}}E\left(\left(m+\frac{1}{2}\right)^2\tau_1\right)\\ &= \sum_{(m,n)\in\mathbb{Z}^2,n\neq 0}(-1)^{nb_1}E\left(\left(m+\frac{1}{2}\right)^2\tau_1+n^2\tau_2+2\left(m+\frac{1}{2}\right)n\tau_3\right)\end{aligned}$$

et

$$\begin{aligned}|\theta_{a,b}(\tau)-\vartheta_{1,0}(\tau_1)| &\leqslant \sum_{(m,n)\in\mathbb{Z}^2,n\neq 0}q_1^{\left(m+\frac{1}{2}\right)^2}q_2^{n^2}q_3^{2\left(m+\frac{1}{2}\right)n}\\ &\leqslant 4\sum_{m\geqslant 0,n>0}q_1^{\left(m+\frac{1}{2}\right)^2}q_2^{n^2}q_3^{-2\left(m+\frac{1}{2}\right)n}.\end{aligned}$$

En utilisant les mêmes techniques que plus haut, il vient

$$\begin{aligned}|\theta_{a,b}(\tau)-\vartheta_{1,0}(\tau_1)| &\leqslant 4\sum_{m\geqslant 0,n>0}q_1^{\frac{\left(m+\frac{1}{2}\right)^2}{2}+\frac{2M-1}{2}n^2}\\ &\leqslant \frac{4q_1^{\frac{2M-1}{2}}}{\left(1-q_1^{\frac{1}{2}}\right)^2}.\end{aligned}$$

Soient $a=\begin{pmatrix}0\\1\end{pmatrix}$ et $b=\begin{pmatrix}b_0\\0\end{pmatrix}\in\{0,1\}^2$, alors

$$\theta_{a,b}(\tau)=\sum_{(m,n)\in\mathbb{Z}^2}(-1)^{mb_0}E\left(m^2\tau_1+\left(n+\frac{1}{2}\right)^2\tau_2+2m\left(n+\frac{1}{2}\right)n\tau_3\right)$$

donc

$$\begin{aligned}|\theta_{a,b}(\tau)| &\leqslant \sum_{(m,n)\in\mathbb{Z}^2}q_1^{m^2}q_2^{\left(n+\frac{1}{2}\right)^2}q_3^{2m\left(n+\frac{1}{2}\right)}\\ &\leqslant 4\sum_{m\geqslant 0,n\geqslant 0}q_1^{\frac{m^2}{2}+\frac{2M-1}{2}\left(n+\frac{1}{2}\right)^2}\\ &\leqslant \frac{4q_1^{\frac{2M-1}{8}}}{\left(1-q_1^{\frac{1}{2}}\right)^2},\end{aligned}$$

où l'on a encore utilisé les mêmes techniques que précédemment.

Soient $a = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \in \{0,1\}^2$, alors

$$\theta_{a,b}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2} E\left(\left(m+\frac{1}{2}\right)^2\tau_1 + \left(n+\frac{1}{2}\right)^2\tau_2 + 2\left(m+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)\tau_3 + \left(m+\frac{1}{2}\right)b_0 + \left(n+\frac{1}{2}\right)b_1\right),$$

donc

$$\begin{aligned} |\theta_{a,b}(\tau)| &\leqslant \sum_{(m,n)\in\mathbb{Z}^2} q_1^{\left(m+\frac{1}{2}\right)^2} q_2^{\left(n+\frac{1}{2}\right)^2} q_3^{2\left(m+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)} \\ &\leqslant 4\sum_{m\geqslant 0, n\geqslant 0} q_1^{\frac{1}{2}\left(m+\frac{1}{2}\right)^2 + \frac{2M-1}{2}\left(n+\frac{1}{2}\right)^2} \\ &\leqslant \frac{4q_1^{\frac{M}{4}}}{\left(1-q_1^{\frac{1}{2}}\right)^2}. \end{aligned}$$

Le résultat découle directement de ces majorations, puisque $q_1 \leqslant \exp\left(-\pi\frac{\sqrt{3}}{2}\right) < 1$ (rappelons que la fonction ϑ_3 est identiquement nulle). □

Ces résultats montrent que la seule theta constante paire pouvant s'annuler sur le domaine fondamental $\mathcal{F}_2$ est θ_{15}. Les formules de transformation des theta constantes sous l'action de Γ_2 (Proposition 5.4) impliquent alors directement le corollaire suivant :

Corollaire 6.1 *Soit $\tau \in \mathcal{H}_2$, et soit $\tau' \in \mathcal{F}_2$ qui lui soit équivalent modulo l'action de Γ_2. Alors soit la matrice τ' est diagonale, auquel cas exactement une des theta constantes paires s'annule en τ, soit τ' n'est pas diagonale, auquel cas aucune des theta constantes paires ne s'annule en τ.*

6.3 Action de Γ_2 sur les carrés des theta constantes

6.3.1 Formules de transformation des theta constantes sous l'action de Γ_2

Le but de cette section est d'expliciter les formules de transformations données par la Proposition 5.4 pour certains éléments de Γ_2. Rappelons qu'avec les notations de la Section 5.3, pour tout $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2$, il existe $\kappa(\gamma) \in [0,3]$, $\Phi(\gamma,.) : [0,15] \to [0,3]$ et $\Psi(\gamma,.)$ une permutation de $[0,15]$ tels que, pour tous $\tau \in \mathcal{H}_2$ et $j \in [0,15]$,

$$\theta_j^2(\gamma\tau) = i^{\kappa(\gamma)}\mathrm{Det}(C\tau+D)i^{\Phi(\gamma,j)}\theta^2_{\Psi(\gamma,j)}(\tau),$$

avec de plus $\Phi(\gamma,0) = 0$

La Proposition 5.4 permet de calculer explicitement Φ et Ψ, mais pas κ. Dans ce qui suit, nous avons déterminé $\kappa(\gamma)$ pour certains éléments de Γ_2 en considérant des valeurs particulières de τ. Par exemple, si l'on souhaite calculer $\kappa(\mathfrak{J})$, on peut fixer $\tau_0 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$. On a alors

$$\theta_0^2(\mathfrak{J}\tau_0) = \theta_0^2(\tau_0) = -i^{\kappa(\mathfrak{J})}\theta_0^2(\tau_0),$$

d'où l'on déduit que $\kappa(\mathfrak{J}) = 2$.

Nous avons procédé de même pour les autres éléments de Γ_2 que nous avons considéré, et comme ils contiennent un ensemble de générateurs du groupe, on peut calculer explicitement $\kappa(\gamma)$ pour tout γ en commençant par décomposer γ en produit de ces générateurs, puis en utilisant les résultats obtenus pour ces derniers, que nous donnons maintenant.

Action de $\mathfrak{J}$

On a $\kappa(\mathfrak{J}) = 2$ et

j	$\Psi(\mathfrak{J}, j)$	$\Phi(\mathfrak{J}, j)$
0	0	0
1	0	4
2	0	8
3	0	12
4	0	1
6	0	9
8	0	2
9	0	6
12	0	3
15	0	15

Action de $\mathfrak{M}_1$

On a $\kappa(\mathfrak{M}_1) = 0$ et

j	$\Psi(\mathfrak{M}_1, j)$	$\Phi(\mathfrak{M}_1, j)$
0	0	1
1	0	0
2	0	3
3	0	2
4	1	4
6	1	6
8	0	9
9	0	8
12	1	12
15	1	15

Action de $\mathfrak{M}_2$

On a $\kappa(\mathfrak{M}_2) = 0$ et

j	$\Psi(\mathfrak{M}_2, j)$	$\Phi(\mathfrak{M}_2, j)$
0	0	2
1	0	3
2	0	0
3	0	1
4	0	6
6	0	4
8	1	8
9	1	9
12	1	12
15	1	15

Action de $\mathfrak{M}_3$

On a $\kappa(\mathfrak{M}_3) = 0$ et

j	$\Psi(\mathfrak{M}_3, j)$	$\Phi(\mathfrak{M}_3, j)$
0	0	0
1	0	1
2	0	2
3	0	3
4	0	6
6	0	4
8	0	9
9	0	8
12	2	15
15	2	12

Action de $\mathfrak{T}$

On a $\kappa(\mathfrak{T}) = 0$ et

j	$\Psi(\mathfrak{T}, j)$	$\Phi(\mathfrak{T}, j)$
0	0	0
1	0	1
2	0	3
3	0	2
4	0	12
6	0	15
8	0	8
9	0	9
12	0	4
15	0	6

Action de $\mathfrak{S}$

On a $\kappa(\mathfrak{S}) = 0$ et

j	$\Psi(\mathfrak{S}, j)$	$\Phi(\mathfrak{S}, j)$
0	0	0
1	0	2
2	0	1
3	0	3
4	0	8
6	0	9
8	0	4
9	0	6
12	0	12
15	0	15

6.3.2 Les quotients de carrés de theta constantes comme fonctions modulaires de Siegel

Introduisons maintenant, pour $j \in [1, 15]$, les fonctions $b_j : \mathcal{H}_2 \to \mathbb{C}$ définies par

$$b_j(\tau) = \frac{\theta_j^2(\tau)}{\theta_0^2(\tau)}.$$

On a alors le résultat suivant :

Proposition 6.6 *La fonction b_1 (resp. b_2, b_3) est une fonction modulaire de Siegel pour le groupe Γ_{b_1} (resp. Γ_{b_2}, Γ_{b_3}), ces groupes étant définis par*

$$\Gamma_{b_1} = \left\{ \gamma \in \Gamma_2 : \gamma \equiv \begin{pmatrix} 1 & a & ab & b \\ 0 & c & c(a+b)+a & 1+c \\ 0 & 0 & 1 & 0 \\ 0 & 1+c & (1+c)(a+b)+a & c \end{pmatrix} \bmod 2, \gamma_{3,1} \equiv 0 \bmod 4 \right\},$$

$$\Gamma_{b_2} = K_{1,2}\Gamma_{b_1}K_{1,2}^{-1}$$

et

$$\Gamma_{b_3} = K_{1,3}\Gamma_{b_2}K_{1,3}^{-1},$$

où

$$K_{1,2} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

et

$$K_{1,3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ces trois groupes ont pour indice 180 *dans* Γ_2.

Démonstration : On commence par vérifier (ceci se fait facilement à la main par exemple) que Γ_{b_1} est bien un sous-groupe de Γ_2. Son indice dans Γ_2 peut alors être calculé par des techniques classiques, puisque l'on connaît des générateurs de Γ_2. L'invariance de b_1 sous l'action de Γ_{b_1} découle de la Proposition 5.4 (et l'on peut par ailleurs prouver qu'il n'existe pas de groupe strictement plus grand que Γ_{b_1} laissant la fonction b_1 invariante).

Un simple calcul (utilisant à nouveau la Proposition 5.4) montre que, pour tout $\tau \in \mathcal{H}_2$,

$$b_2(K_{1,2}\tau) = b_3(K_{1,3}\tau) = b_1(\tau),$$

on en déduit donc le résultat pour Γ_{b_2} et Γ_{b_3}. □

Une conséquence directe de cette proposition est que le triplet (b_1, b_2, b_3) est invariant sous l'action du groupe

$$\Gamma_b = \Gamma_{b_1} \cap \Gamma_{b_2} \cap \Gamma_{b_3},$$

que l'on peut définir par

$$\Gamma_b = \left\{ \gamma \in \Gamma_2 : \gamma \equiv \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \bmod 2, \gamma_{3,1} \equiv \gamma_{4,2} \equiv 0 \bmod 4 \right\},$$

et qui a pour indice 1440 dans Γ_2. De plus, un ensemble de représentants des classes de $\Gamma_b\backslash\Gamma_2$ ainsi qu'un ensemble de générateurs de Γ_b sont effectivement calculables par une généralisation directe au genre 2 de l'Algorithme 2 vu à la Section 2.1.3. Nous avons ainsi calculé un ensemble de générateurs de Γ_b comptant environ 20000 éléments, puis avons montré que ces éléments étaient engendrés à leur tour par les 9 éléments suivants, qui constituent donc à leur tour un système de générateurs de Γ_b :

$$\mathfrak{G}_1 = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathfrak{G}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathfrak{G}_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathfrak{G}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathfrak{G}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{pmatrix}, \quad \mathfrak{G}_6 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathfrak{G}_7 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{G}_8 = \begin{pmatrix} 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 2 \\ 4 & 0 & 3 & 0 \\ 0 & 4 & 0 & 3 \end{pmatrix}, \quad \mathfrak{G}_9 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ -2 & -3 & 0 & 0 \\ 0 & 0 & -3 & 2 \\ 0 & 0 & -2 & 1 \end{pmatrix}.$$

Notons enfin que lorsque $\gamma \in \Gamma_b$, la valeur de $\kappa(\gamma)$ est facile à déterminer, comme le montre le lemme suivant :

Lemme 6.3 *Pour tout*

$$\gamma = \begin{pmatrix} A & & B \\ & d_1 & d_2 \\ C & & \\ & d_3 & d_4 \end{pmatrix} \in \Gamma_b,$$

on a

$$\kappa(\gamma) = (-1)^{\frac{d_1 - d_4}{2}}.$$

Démonstration : Il suffit en fait de le montrer pour les 9 générateurs de Γ_b que nous venons d'exhiber, puisque pour tous $\gamma_1, \gamma_2 \in \Gamma_b$,

$$\kappa(\gamma_1\gamma_2) = \kappa(\gamma_1)\kappa(\gamma_2).$$

On peut maintenant décomposer chacun des $\mathfrak{G}_j$ en produit des générateurs de Γ_2 donnés plus haut comme suit :

$$\begin{array}{lllllllll} \mathfrak{G}_1 & = & \mathfrak{M}_1^2 & \mathfrak{G}_2 & = & \mathfrak{M}_2^2 & \mathfrak{G}_3 & = & \mathfrak{M}_3 \\ \mathfrak{G}_4 & = & \mathfrak{J}\mathfrak{M}_1^{-4}\mathfrak{J} & \mathfrak{G}_5 & = & \mathfrak{J}\mathfrak{M}_2^{-4}\mathfrak{J} & \mathfrak{G}_6 & = & \mathfrak{J}\mathfrak{M}_3^{-2}\mathfrak{J} \\ \mathfrak{G}_7 & = & \mathfrak{M}_3\mathfrak{J}\mathfrak{M}_3\mathfrak{J}\mathfrak{M}_3\mathfrak{S}\mathfrak{J} & \mathfrak{G}_8 & = & \mathfrak{M}_1\mathfrak{M}_2\mathfrak{J}\mathfrak{M}_1^4\mathfrak{M}_2^4\mathfrak{J}\mathfrak{M}_1\mathfrak{M}_2 & \mathfrak{G}_9 & = & \mathfrak{T}^{-1}\mathfrak{S}\mathfrak{T}^{-2}\mathfrak{S}\mathfrak{T}. \end{array}$$

Comme nous avons entièrement décrit l'action des générateurs de Γ_2 sur les carrés des theta constantes (y compris la valeur de κ pour ces générateurs), on peut vérifier que $\kappa(\mathfrak{G}_7) = -1$ et que κ vaut 1 pour les huit autres générateurs de Γ_b, ce qui conclut la démonstration. □

6.3.3 Invariants d'Igusa

Commençons par introduire les fonctions h_4, h_{10}, h_{12} et h_{16} définies par

$$h_4 = \sum_{j\in\mathcal{P}_2} \theta_j^8,$$

$$h_{10} = \prod_{j\in\mathcal{P}_2} \theta_j^2,$$

$$\begin{aligned} h_{12} \;=\; & (\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + (\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4 + (\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4 \\ & + (\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4 + (\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + (\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4 \\ & + (\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + (\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4 + (\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4 \\ & + (\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4 + (\theta_1\theta_2\theta_3\theta_6\theta_9\theta_{15})^4 + (\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4 \\ & + (\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + (\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4 + (\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4, \end{aligned}$$

et

$$\begin{aligned} h_{16} \;=\; & \left(\theta_3^8+\theta_6^8+\theta_9^8+\theta_{12}^8\right)(\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + \left(\theta_3^8+\theta_4^8+\theta_8^8+\theta_{15}^8\right)(\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4 \\ & + \left(\theta_2^8+\theta_6^8+\theta_8^8+\theta_{12}^8\right)(\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4 + \left(\theta_2^8+\theta_4^8+\theta_9^8+\theta_{15}^8\right)(\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4 \\ & + \left(\theta_2^8+\theta_3^8+\theta_8^8+\theta_9^8\right)(\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + \left(\theta_1^8+\theta_6^8+\theta_8^8+\theta_{15}^8\right)(\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4 \\ & + \left(\theta_1^8+\theta_4^8+\theta_9^8+\theta_{12}^8\right)(\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + \left(\theta_1^8+\theta_3^8+\theta_4^8+\theta_6^8\right)(\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4 \\ & + \left(\theta_1^8+\theta_2^8+\theta_{12}^8+\theta_{15}^8\right)(\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4 + \left(\theta_0^8+\theta_6^8+\theta_9^8+\theta_{15}^8\right)(\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4 \\ & + \left(\theta_0^8+\theta_4^8+\theta_8^8+\theta_{12}^8\right)(\theta_1\theta_2\theta_3\theta_6\theta_9\theta_{15})^4 + \left(\theta_0^8+\theta_3^8+\theta_{12}^8+\theta_{15}^8\right)(\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4 \\ & + \left(\theta_0^8+\theta_2^8+\theta_4^8+\theta_6^8\right)(\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + \left(\theta_0^8+\theta_1^8+\theta_8^8+\theta_9^8\right)(\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4 \\ & + \left(\theta_0^8+\theta_1^8+\theta_2^8+\theta_3^8\right)(\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4. \end{aligned}$$

Les formules de transformation des theta constantes sous l'action des générateurs de Γ_2 données à la Section 6.3.1 permettent de montrer que, pour $j \in \{4, 12, 10, 16\}$, h_j est invariante sous l'action de $\mathfrak{M}_1$, $\mathfrak{M}_2$ et $\mathfrak{M}_3$, alors que pour tout $\tau \in \mathcal{H}_2$,

$$h_j(\mathfrak{J}\tau) = \mathrm{Det}(\tau)^j h_j(\tau).$$

Comme $\Gamma_2 = \langle \mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3, \mathfrak{J}\rangle$, on en déduit que h_j est une forme modulaire de Siegel de poids j pour le groupe Γ_2.

Définition 6.1 (invariants d'Igusa, j-invariants en genre 2) *Nous appelerons* invariants d'Igusa *(ou encore* j-invariants en genre 2*) les fonctions j_1, j_2 et j_3 définies par*

$$j_1 = \frac{h_{12}^5}{h_{10}^6}, \quad j_2 = \frac{h_4 h_{12}^3}{h_{10}^4}, \quad j_3 = \frac{h_{16} h_{12}^2}{h_{10}^4}.$$

D'après ce qui précède, ce sont des fonctions modulaires de Siegel pour le groupe Γ_2. Ces fonctions ont été introduites par Igusa [Igu60], qui a montré qu'elles engendrent le corps des fonctions modulaires de Siegel pour Γ_2. En particulier, elles sont algébriquement indépendantes entre elles, et si $\tau, \tau' \in \mathcal{H}_2$ sont tels que $h_{12}(\tau) \neq 0$ et que $j_k(\tau) = j_k(\tau')$ pour tout $k \in [1, 3]$, alors τ et τ' sont équivalents modulo l'action de Γ_2.

On a par ailleurs le résultat suivant, que l'on pourra rapprocher du Théorème 2.1.

Théorème 6.2 *Le corps des fonctions modulaires de Siegel en genre* 2 *est* $\mathbb{C}(j_1, j_2, j_3)$.

Démonstration : Voir les travaux d'Igusa [Igu62], ainsi que la thèse de Weng [Wen01, p. 28–31], qui permet de s'y ramener. □

6.4 Équations modulaires

Proposition 6.7 *Pour tout $\tau \in \mathcal{H}_2$, si l'on définit la matrice $\mathcal{A}(\tau)$ par*

$$\mathcal{A}(\tau) = \frac{1}{\theta_0^2(\tau)} \begin{pmatrix} \theta_8^2(\tau) & \theta_3^2(\tau) & -\theta_6^2(\tau) \\ -\theta_{15}^2(\tau) & \theta_4^2(\tau) & \theta_1^2(\tau) \\ \theta_2^2(\tau) & -\theta_9^2(\tau) & \theta_{12}^2(\tau) \end{pmatrix},$$

alors $\mathcal{A}(\tau)$ est orthogonale : ${}^t\mathcal{A}(\tau).\mathcal{A}(\tau) = I_3$.

Démonstration : Soit $\tau \in \mathcal{H}_2$, alors pour tout $j \in [0, 15]$, $\theta_j^2(\tau)$ peut s'écrire en fonction des $\left(\theta_k\left(\frac{\tau}{2}\right)\right)_{k\in[0,3]}$ en utilisant les formules de duplication (Proposition 5.5). Si l'on réécrit ainsi la matrice $\mathcal{A}(\tau)$ en utilisant ces quatre paramètres, il suffit de vérifier son orthogonalité par un calcul trivial (quoique pénible). □

On notera qu'en remplaçant dans cette dernière proposition τ par $\gamma\tau$ avec $\gamma \in \Gamma_2$, on obtient (en utilisant la formule de transformation donnée à la Propriété 5.4) de nouvelles relations entre theta constantes.

Proposition 6.8 *Pour tout $\tau \in \mathcal{F}_2$, si l'on pose $(a, b, c, d) = \left(\theta_j^2(\tau)\right)_{j\in[0,3]}$, alors*

$$\left(X - \theta_4^4(\tau)\right)\left(X - \theta_6^4(\tau)\right) = X^2 + (b^2 + d^2 - a^2 - c^2)X + (ac - bd)^2,$$

$$\left(X - \theta_8^4(\tau)\right)\left(X - \theta_9^4(\tau)\right) = X^2 + (c^2 + d^2 - a^2 - b^2)X + (ab - cd)^2,$$

et

$$\left(X - \theta_{12}^4(\tau)\right)\left(X - \theta_{15}^4(\tau)\right) = X^2 + (b^2 + c^2 - a^2 - d^2)X + (ad - bc)^2.$$

Démonstration : On procède exactement de la même façon que pour la proposition précédente. □

Notons que cette façon de présenter les relations existant entre les carrés des theta constantes contient moins d'information que la proposition précédente (Proposition 6.8).

Supposons en effet que l'on connaisse le quadruplet $\left(\theta_j^2(\tau)\right)_{j\in[0,3]}$, et supposons par ailleurs pour simplifier qu'aucune theta constante paire ne s'annule en τ. Alors il y a seulement huit possibilités pour le 10-uplet $\left(\theta_j^2(\tau)\right)_{j\in\mathcal{P}_2}$. Ceci peut se voir comme suit : d'après la Proposition 6.8, il y a deux possiblités pour $\theta_4^4(\tau)$, donc quatre possibilités pour $\theta_4^2(\tau)$. On a ensuite, d'après la Proposition 6.7, les égalités suivantes :

$$\theta_6^2(\tau) = \frac{\theta_0^2(\tau)\theta_2^2(\tau) - \theta_1^2(\tau)\theta_3^2(\tau)}{\theta_4^2(\tau)},$$

puis

$$\theta_8^4(\tau) = \theta_0^4(\tau) - \theta_3^4(\tau) - \theta_6^4(\tau),$$

qui laisse deux choix possibles pour $\theta_8^2(\tau)$, et enfin

$$\theta_{15}^2(\tau) = \frac{\theta_1^2(\tau)\theta_6^2(\tau) - \theta_3^2(\tau)\theta_4^2(\tau)}{\theta_8^2(\tau)},$$

$$\theta_{12}^2(\tau) = \frac{\theta_1^2(\tau)\theta_{15}^2(\tau) + \theta_6^2(\tau)\theta_8^2(\tau)}{\theta_2^2(\tau)}$$

et

$$\theta_9^2(\tau) = \frac{\theta_3^2(\tau)\theta_6^2(\tau) - \theta_1^2(\tau)\theta_4^2(\tau)}{\theta_{12}^2(\tau)}.$$

On a donc bien huit différentes possibilités, et il est facile de voir (*via* les résultats de la Section 6.3) que les huit solutions possibles sont les

$$\left\{ \left(\theta_j^2 \left(\tau + \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \right) \right)_{j\in[0,15]} : (a,b,c) \in \{0,1\}^3 \right\}.$$

Les huit solutions (pour (a,b,c) parcourant $\{0,1\}^3$, et en notant $\gamma_{a,b,c} = \mathfrak{M}_1^{2a}\mathfrak{M}_2^b\mathfrak{M}_3^{2c}$) peuvent s'écrire en fonction des $\theta_j^2 = \theta_j^2(\tau)$ comme suit :

(a,b,c)	$\theta_4^2(\gamma_{a,b,c}\tau)$	$\theta_6^2(\gamma_{a,b,c}\tau)$	$\theta_8^2(\gamma_{a,b,c}\tau)$	$\theta_9^2(\gamma_{a,b,c}\tau)$	$\theta_{12}^2(\gamma_{a,b,c}\tau)$	$\theta_{15}^2(\gamma_{a,b,c}\tau)$
$(0,0,0)$	θ_4^2	θ_6^2	θ_8^2	θ_9^2	θ_{12}^2	θ_{15}^2
$(1,0,0)$	$-\theta_4^2$	$-\theta_6^2$	θ_8^2	θ_9^2	$-\theta_{12}^2$	$-\theta_{15}^2$
$(0,1,0)$	θ_6^2	θ_4^2	θ_9^2	θ_8^2	$-\theta_{15}^2$	$-\theta_{12}^2$
$(1,1,0)$	$-\theta_6^2$	$-\theta_4^2$	θ_9^2	θ_8^2	θ_{15}^2	θ_{12}^2
$(0,0,1)$	θ_4^2	θ_6^2	$-\theta_8^2$	$-\theta_9^2$	$-\theta_{12}^2$	$-\theta_{15}^2$
$(1,0,1)$	$-\theta_4^2$	$-\theta_6^2$	$-\theta_8^2$	$-\theta_9^2$	θ_{12}^2	θ_{15}^2
$(0,1,1)$	θ_6^2	θ_4^2	$-\theta_9^2$	$-\theta_8^2$	$-\theta_{15}^2$	$-\theta_{12}^2$
$(1,1,1)$	$-\theta_6^2$	$-\theta_4^2$	$-\theta_9^2$	$-\theta_8^2$	$-\theta_{15}^2$	$-\theta_{12}^2$

Nous terminons cette section par un résultat qui nous sera assez utile au Chapitre 8, et dont la démonstration utilise ce qui précède.

Proposition 6.9 *Pour tous $\tau, \tau' \in \mathcal{H}_2$ tels que*

$$\left[\theta_0^2(\tau) : \theta_1^2(\tau) : \theta_2^2(\tau) : \theta_3^2(\tau)\right] = \left[\theta_0^2(\tau') : \theta_1^2(\tau') : \theta_2^2(\tau') : \theta_3^2(\tau')\right],$$

il existe $\gamma \in \Gamma_b$ tel que $\tau' = \gamma\tau$.

Démonstration : Soient $\tau, \tau' \in \mathcal{H}_2$ tels que

$$\left[\theta_0^2(\tau) : \theta_1^2(\tau) : \theta_2^2(\tau) : \theta_3^2(\tau)\right] = \left[\theta_0^2(\tau') : \theta_1^2(\tau') : \theta_2^2(\tau') : \theta_3^2(\tau')\right].$$

D'après les remarques vues plus haut (et comme $\mathfrak{M}_1^2, \mathfrak{M}_2^2, \mathfrak{M}_3 \in \Gamma_b$), il existe $\gamma_1 \in \Gamma_b$ tel que

$$\left[\theta_j^2(\tau)\right]_{j\in[0,15]} = \left[\theta_j^2(\gamma_1\tau')\right]_{j\in[0,15]}.$$

Introduisons maintenant les éléments de Γ_b suivants :

$$\mathfrak{A}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & -1 & 0 & 0 \\ 0 & 2 & 1 & -2 \\ -2 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{A}_2 = \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 2 & 0 & -2 & -1 \end{pmatrix}, \quad \mathfrak{A}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 0 & 2 & 1 & -4 \\ -2 & 0 & 0 & -1 \end{pmatrix},$$

$$\mathfrak{A}_4 = \begin{pmatrix} 1 & -2 & 0 & -2 \\ 0 & -1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & -1 \end{pmatrix}, \quad \mathfrak{A}_6 = \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & -1 \end{pmatrix}, \quad \mathfrak{A}_8 = \begin{pmatrix} 1 & 0 & 0 & -2 \\ 2 & -1 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$\mathfrak{A}_9 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{A}_{12} = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{A}_{15} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Pour tous $t \in \mathcal{H}_2$ et $\ell \in \{1, 2, 3, 4, 6, 8, 9, 12, 15\}$ on a, d'après [Igu72, Theorem II, p. 175–176]

$$[\theta_j(\mathfrak{A}_\ell t)]_{j\in[0,15]} = \left[(-1)^{\delta_{j,\ell}}\theta_j(t)\right]_{j\in[0,15]}$$

(où δ désigne le symbole de Kronecker).

On en déduit l'existence d'un élément $\gamma_2 \in \Gamma_b$ (élément engendré par les $\mathfrak{A}_\ell$) tel que

$$[\theta_j(\tau)]_{j\in[0,15]} = \left[\theta_j(\gamma_2\gamma_1\tau')\right]_{j\in[0,15]}.$$

Le corollaire de [Igu72, Theorem 4, p. 189] montre qu'alors il existe $\gamma_3 \in \Gamma_b$ tel que $\tau = \gamma_3\gamma_2\gamma_1\tau'$, ce qui termine la démonstration. □

Chapitre 7

Suites de Borchardt : définition et convergence

Le but de ce chapitre est de définir ce que nous appelons les suites de Borchardt, qui peuvent être vues comme une généralisation des suites AGM pour 2^g variables*, et de démontrer leurs propriétés de convergence.

Dans ce chapitre, on fixe un entier $g \geqslant 1$ et on pose $\mathcal{I}_g = (\mathbb{Z}/2\mathbb{Z})^g$.

7.1 Définitions

Soit $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, on dit qu'un 2^g-uplet $(a'_v)_{v\in\mathcal{I}_g}$ est un *itéré de Borchardt* de $(a_v)_{v\in\mathcal{I}_g}$ s'il existe $(\alpha_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ tel que

1. pour tout $v \in \mathcal{I}_g$, $\alpha_v^2 = a_v$, et
2. pour tout $v \in \mathcal{I}_g$,
$$a'_v = \frac{1}{2^g} \sum_{v_1+v_2=v} \alpha_{v_1}\alpha_{v_2}.$$

Le 2^g-uplet $(\alpha_v)_{v\in\mathcal{I}_g}$ est le *choix de racines* correspondant à cette itération de Borchardt. Notons que ce choix n'est pas unique, puisque $(-\alpha_v)_{v\in\mathcal{I}_g}$ est un autre choix correspondant à la même itération.

Remarques :

1. La valeur de a'_0 ne dépend pas du choix de racines fait, mais uniquement de $(a_v)_{v\in\mathcal{I}_g}$, puisque
$$a'_0 = \frac{1}{2^g} \sum_{v\in\mathcal{I}_g} a_v.$$
2. Il y a au plus 2^{g-1} possibilités pour l'itéré $(a'_v)_{v\in\mathcal{I}_g}$ si $(a_v)_{v\in\mathcal{I}_g}$ est fixé. En effet, il y a au plus 2^g choix possibles de racines, et deux choix opposés conduisent au même itéré. Bien évidemment, il peut y avoir moins de possibilités (si certains des a_v sont nuls par exemple).

Si $(\alpha_v)_{v\in\mathcal{I}_g}$ est un choix de racines, on dira que c'est un *bon choix* si, pour tous $v_1, v_2 \in \mathcal{I}_g$,

$$|\alpha_{v_1} - \alpha_{v_2}| < |\alpha_{v_1} + \alpha_{v_2}|.$$

Dans le cas contraire, on parlera de *mauvais choix*.

*En ce sens qu'en genre g, les suites de Borchardt de 2^g éléments sont liées aux theta constantes de la même façon que les suites AGM en genre 1.

Une suite $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est une *suite de Borchardt* (associée à $(a_v^{(0)})_{v\in\mathcal{I}_g}$) si, pour tout $n\in\mathbb{N}$, $(a_v^{(n+1)})_{v\in\mathcal{I}_g}$ est un itéré de Borchardt de $(a_v^{(n)})_{v\in\mathcal{I}_g}$.

7.1.1 Historique

Nous avons baptisé ainsi les suites de Borchardt du fait qu'elles ont été introduites par Carl-Wilhelm Borchardt pour généraliser l'AGM. Dans [Bor76], Borchardt explique que dès 1858 (soit 18 ans avant publication), il avait eu l'idée de considérer des itérations de la forme

$$a_{n+1}=\frac{a_n+b_n+c_n+d_n}{4},$$

$$b_{n+1}=\frac{\sqrt{a_n}\sqrt{b_n}+\sqrt{c_n}\sqrt{d_n}}{2},$$

$$c_{n+1}=\frac{\sqrt{a_n}\sqrt{c_n}+\sqrt{b_n}\sqrt{d_n}}{2},$$

$$d_{n+1}=\frac{\sqrt{a_n}\sqrt{d_n}+\sqrt{b_n}\sqrt{c_n}}{2},$$

associées à des nombre réels positifs a_0,b_0,c_0,d_0 vérifiant

$$a_0-b_0-c_0+d_0>0.$$

Il montrait alors que pour tout $n\geqslant 0$, on a

$$a_n-b_n-c_n+d_n>0,$$

et

$$a_n-d_n<\frac{1}{2^n}(a_0-d_0),$$

ce qui permet de montrer la convergence des quatre suites (a_n), (b_n), (c_n) et (d_n) vers une même limite commune.

Pour lui, il s'agissait d'une généralisation intéressante de l'AGM car
- la limite ne dépend pas de l'ordre des quatre éléments de départ ;
- la fonction qui, à (a_0,b_0,c_0,d_0), associe la limite de la suite de Borchardt (réelle positive) qui leur est associée, satisfait à une équation différentielle généralisant celle que satisfait l'AGM [Bor61, Bor79] (ce qui est à rapprocher du calcul d'intégrales hyperelliptiques, comme l'AGM l'est du calcul d'intégrales elliptiques).

Il annonçait aussi que l'on peut considérer des moyennes du même type entre 2^g éléments, pour $g\geqslant 3$, mais qu'alors même si le procédé converge encore (sur les réels positifs), la limite dépend de l'ordre des 2^g éléments de départ.

Dans [Bor78], Borchardt complète l'étude (du point de vue algébrique) des séquences de Borchardt de quatre éléments amorcée dans l'article suscité.

Borchardt semble ne pas s'être intéressé à la convergence de ce type de séquences sur les complexes.

7.2 Convergence

Le but principal de cette section est de montrer le théorème suivant :

Théorème 7.1 *Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de Borchardt, et soit $(\alpha_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de choix de racines associée. Alors il existe un unique $A\in\mathbb{C}$ tel que, pour tout $v\in\mathcal{I}_g$,*

$$\lim_{n\to+\infty} a_v^{(n)} = A.$$

De plus, $A=0$ si et seulement si la suite $(\alpha_v^{(n)})$ contient une infinité de mauvais choix de racines.

Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de Borchardt, et soit $(\alpha_v^{(n)})$ une suite de choix de racines associée. On définit la suite $(M_n)_{n\in\mathbb{N}}$ par

$$M_n = \mathrm{Max}_{v\in\mathcal{I}_g}\left(\left|a_v^{(n)}\right|\right)$$

pour tout $n\geqslant 0$. Il est facile de voir, à partir de la définition d'une suite de Borchardt, que la suite (M_n) est décroissante.

On commence par montrer que si la suite $(\alpha_v^{(n)})$ comporte une infinité de mauvais choix, alors la suite (M_n) converge vers zéro. Ceci est une conséquence directe du résultat suivant :

Lemme 7.1 *Avec les notations ci-dessus, si $n\geqslant 0$ est tel que $(\alpha_v^{(n)})_{v\in\mathcal{I}_g}$ est un mauvais choix de racines, alors*

$$M_{n+3}\leqslant (1-r_g)M_n,$$

où

$$r_g = \frac{1}{2^g}\left(1-\sqrt{1-\frac{2-\sqrt{2}}{2^{2g}}}\right) > 0.$$

Démonstration : Soit $n\in\mathbb{N}$ tel que $(\alpha_v^{(n)})_{v\in\mathcal{I}_g}$ soit un mauvais choix de racines, alors il existe $v_1,v_2\in\mathcal{I}_g$ tels que

$$\left|\alpha_{v_1}^{(n)}+\alpha_{v_2}^{(n)}\right|\leqslant\left|\alpha_{v_1}^{(n)}-\alpha_{v_2}^{(n)}\right|.$$

On a donc :

$$\begin{aligned}\left|\alpha_{v_1}^{(n)}+\alpha_{v_2}^{(n)}\right|^2 &\leqslant \left|\alpha_{v_1}^{(n)}+\alpha_{v_2}^{(n)}\right|\cdot\left|\alpha_{v_1}^{(n)}-\alpha_{v_2}^{(n)}\right| \\ &\leqslant \left|\alpha_{v_1}^{(n)}\right|^2+\left|\alpha_{v_2}^{(n)}\right|^2.\end{aligned}$$

En multipliant les deux côtés par $\left|\alpha_{v_1}^{(n)}\right|^2$, on obtient

$$\begin{aligned}\left|a_{v_1}^{(n)}+\alpha_{v_1}^{(n)}\alpha_{v_2}^{(n)}\right|^2 &\leqslant \left|a_{v_1}^{(n)}\right|^2+\left|\alpha_{v_1}^{(n)}\alpha_{v_2}^{(n)}\right|^2 \\ &\leqslant 2M_n^2,\end{aligned}$$

et finalement

$$\left|a_{v_1}^{(n)}+\alpha_{v_1}^{(n)}\alpha_{v_2}^{(n)}\right|\leqslant\sqrt{2}M_n. \tag{7.1}$$

En utilisant la définition d'un itéré de Borchardt, on a alors

$$\begin{aligned}a_0^{(n+2)} &= \frac{1}{2^g}\sum_{v\in\mathcal{I}_g} a_v^{(n+1)} \\ &= \frac{1}{2^g}\left(a_0^{(n+1)}+a_{v_1+v_2}^{(n+1)}+\sum_{v\in\mathcal{I}_g\setminus\{0,v_1+v_2\}} a_v^{(n+1)}\right),\end{aligned}$$

donc

$$\left|a_0^{(n+2)}\right| \leqslant \left(1 - \frac{1}{2^{g-1}}\right) M_{n+1} + \frac{1}{2^g}\left|a_0^{(n+1)} + a_{v_1+v_2}^{(n+1)}\right|.$$

En utilisant à nouveau la définition d'un itéré de Borchardt, on a

$$\begin{aligned} a_0^{(n+1)} + a_{v_1+v_2}^{(n+1)} &= \frac{1}{2^g}\left(\sum_{v\in\mathcal{I}_g} a_v^{(n)} + \sum_{w\in\mathcal{I}_g} \alpha_w^{(n)}\alpha_{v_1+v_2+w}^{(n)}\right) \\ &= \frac{1}{2^g}\left(a_{v_1}^{(n)} + \alpha_{v_1}^{(n)}\alpha_{v_2}^{(n)} + \sum_{v\in\mathcal{I}_g\setminus\{v_1\}} a_v^{(n)} + \sum_{w\in\mathcal{I}_g\setminus\{v_1\}} \alpha_w^{(n)}\alpha_{v_1+v_2+w}^{(n)}\right). \end{aligned}$$

En considérant les modules et en utilisant l'inégalité (7.1), on obtient

$$\left|a_0^{(n+1)} + a_{v_1+v_2}^{(n+1)}\right| \leqslant \frac{\sqrt{2} + 2(2^g - 1)}{2^g} M_n,$$

donc

$$\begin{aligned} \left|a_0^{(n+2)}\right| &\leqslant \left(1 - \frac{1}{2^{g-1}}\right) M_{n+1} + \frac{\sqrt{2} + 2(2^g - 1)}{2^{2g}} M_n \\ &\leqslant \left(1 - \frac{1}{2^{g-1}}\right) M_n + \frac{\sqrt{2} + 2(2^g - 1)}{2^{2g}} M_n \\ &\leqslant \left(1 - \frac{2 - \sqrt{2}}{2^{2g}}\right) M_n. \end{aligned}$$

Pour tout $v \in \mathcal{I}_g$, on a alors

$$\begin{aligned} a_v^{(n+3)} &= \frac{1}{2^g}\sum_{w\in\mathcal{I}_g} \alpha_w^{(n+2)}\alpha_{w+v}^{(n+2)} \\ &= \frac{1}{2^g}\left(\alpha_0^{(n+2)}\alpha_v^{(n+2)} + \sum_{w\in\mathcal{I}_g\setminus\{0\}} \alpha_w^{(n+2)}\alpha_{w+v}^{(n+2)}\right), \end{aligned}$$

et

$$\begin{aligned} \left|a_v^{(n+3)}\right| &\leqslant \frac{1}{2^g}\left(\sqrt{M_n}\sqrt{\left|a_0^{(n+2)}\right|} + (2^g - 1)M_{n+2}\right) \\ &\leqslant \frac{1}{2^g}\left(\sqrt{M_n}\sqrt{\left|a_0^{(n+2)}\right|} + (2^g - 1)M_n\right). \end{aligned}$$

En utilisant notre borne sur $\left|a_0^{(n+2)}\right|$, on obtient finalement

$$\left|a_v^{(n+3)}\right| \leqslant \left(1 - \frac{1}{2^g}\left(1 - \sqrt{1 - \frac{2 - \sqrt{2}}{2^{2g}}}\right)\right) M_n,$$

ce qui termine la démonstration. □

On suppose maintenant que $(\alpha_v^{(n)})$ ne contient qu'un nombre fini de mauvais choix de racines. Quitte à opérer une translation d'indice, on peut même supposer que tous les choix de racines sont bons. Pour montrer la convergence de $(a_v^{(n)})$, on commence par montrer le lemme suivant :

Lemme 7.2 *Soient $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, $(a'_v)_{v\in\mathcal{I}_g}$ un itéré de Borchardt de $(a_v)_{v\in\mathcal{I}_g}$ et $(\alpha_v)_{v\in\mathcal{I}_g}$ un choix de racines associé à cette itération. Si $(\alpha_v)_{v\in\mathcal{I}_g}$ est un bon choix, alors*

$$\sum_{(v_1,v_2)\in\mathcal{I}_g^2} \left|a'_{v_1} - a'_{v_2}\right| \leqslant \left(1 - \frac{1}{2^g}\right) \sum_{(v_1,v_2)\in\mathcal{I}_g^2} \left|a_{v_1} - a_{v_2}\right|.$$

Démonstration : Soit $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, $(\alpha_v)_{v\in\mathcal{I}_g}$ un bon choix de racines associé et $(a'_v)_{v\in\mathcal{I}_g}$ l'itéré de Borchardt correspondant. Pour tous $v_1, v_2 \in \mathcal{I}_g$, comme le choix de racines est bon, on a

$$\begin{aligned}\left|\frac{a_{v_1}+a_{v_2}}{2} - \alpha_{v_1}\alpha_{v_2}\right| &= \frac{1}{2}\left|\alpha_{v_1} - \alpha_{v_2}\right|^2 \\ &\leqslant \frac{1}{2}\left|\alpha_{v_1} - \alpha_{v_2}\right| \cdot \left|\alpha_{v_1} + \alpha_{v_2}\right| \\ &\leqslant \frac{1}{2}\left|a_{v_1} - a_{v_2}\right|,\end{aligned}$$

donc pour tout $v \in \mathcal{I}_g$,

$$\begin{aligned}\left|a'_0 - a'_v\right| &= \frac{1}{2^g}\left|\sum_{v_1\in\mathcal{I}_g} (a_{v_1} - \alpha_{v_1}\alpha_{v+v_1})\right| \\ &= \frac{1}{2^g}\left|\sum_{v_1\in\mathcal{I}_g} \left(\frac{a_{v_1}+a_{v+v_1}}{2} - \alpha_{v_1}\alpha_{v+v_1}\right)\right| \\ &\leqslant \frac{1}{2^g}\sum_{v_1\in\mathcal{I}_g} \left|\frac{a_{v_1}+a_{v+v_1}}{2} - \alpha_{v_1}\alpha_{v+v_1}\right| \\ &\leqslant \frac{1}{2^{g+1}}\sum_{v_1\in\mathcal{I}_g} \left|a_{v_1} - a_{v+v_1}\right|.\end{aligned}$$

On en déduit donc que

$$\sum_{v\in\mathcal{I}_g} \left|a'_0 - a'_v\right| \leqslant \frac{1}{2^{g+1}} \sum_{(v_1,v_2)\in\mathcal{I}_g^2} \left|a_{v_1} - a_{v_2}\right|.$$

On peut alors conclure en utilisant l'inégalité triangulaire comme suit :

$$\begin{aligned}
\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a'_{v_1}-a'_{v_2}\right| &= 2\sum_{v_1\in\mathcal{I}_g}\left|a'_0-a'_{v_1}\right|+\sum_{(v_1,v_2)\in(\mathcal{I}_g\setminus\{0\})^2}\left|a'_{v_1}-a'_{v_2}\right| \\
&\leqslant \frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}|+\sum_{\substack{(v_1,v_2)\in(\mathcal{I}_g\setminus\{0\})^2\\ v_1\neq v_2}}\left|a'_{v_1}-a'_{v_2}\right| \\
&\leqslant \frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}|+\sum_{\substack{(v_1,v_2)\in(\mathcal{I}_g\setminus\{0\})^2\\ v_1\neq v_2}}\left(\left|a'_0-a'_{v_1}\right|+\left|a'_0-a'_{v_2}\right|\right) \\
&\leqslant \frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}|+2(2^g-2)\sum_{v\in\mathcal{I}_g}\left|a'_0-a'_v\right| \\
&\leqslant \frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}|+\left(1-\frac{1}{2^{g-1}}\right)\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}| \\
&\leqslant \left(1-\frac{1}{2^g}\right)\sum_{(v_1,v_2)\in\mathcal{I}_g^2}|a_{v_1}-a_{v_2}|\,.
\end{aligned}$$

□

Une récurrence directe utilisant ce lemme montre que, pour tout $n\in\mathbb{N}$,

$$\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(n)}-a_{v_2}^{(n)}\right|\leqslant\left(1-\frac{1}{2^g}\right)^n\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(0)}-a_{v_2}^{(0)}\right|. \tag{7.2}$$

Soit alors $n\geqslant 0$, on a

$$\begin{aligned}
\left|a_0^{(n+1)}-a_0^{(n)}\right| &= \frac{1}{2^g}\left|\sum_{v\in\mathcal{I}_g}\left(a_v^{(n)}-a_0^{(n)}\right)\right| \\
&\leqslant \frac{1}{2^g}\sum_{v\in\mathcal{I}_g}\left|a_v^{(n)}-a_0^{(n)}\right| \\
&\leqslant \frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(n)}-a_{v_2}^{(n)}\right| \\
&\leqslant \left(1-\frac{1}{2^g}\right)^n\frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(0)}-a_{v_2}^{(0)}\right|,
\end{aligned}$$

et si l'on fixe $N\geqslant 0$, on a donc, pour tout $m>N$,

$$\begin{aligned}
\left|a_0^{(m)}-a_0^{(N)}\right| &\leqslant \sum_{n=N}^{m-1}\left|a_0^{(n+1)}-a_0^{(n)}\right| \\
&\leqslant \sum_{n=N}^{m-1}\left(1-\frac{1}{2^g}\right)^n\frac{1}{2^g}\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(0)}-a_{v_2}^{(0)}\right| \\
&\leqslant \left(1-\frac{1}{2^g}\right)^N\sum_{(v_1,v_2)\in\mathcal{I}_g^2}\left|a_{v_1}^{(0)}-a_{v_2}^{(0)}\right|,
\end{aligned}$$

ce qui prouve que la suite $(a_0^{(n)})_{n\in\mathbb{N}}$ est de Cauchy, donc converge. Si on note A sa limite, alors l'inégalité (7.2) montre que, pour tout $v \in \mathcal{I}_g$,

$$\lim_{n\to+\infty} a_v^{(n)} = A.$$

Reste à montrer que $A \neq 0$. Pour cela, on commence par remarquer que le fait que tous les choix de racines soient bons implique qu'il existe une droite Δ du plan complexe, passant par l'origine, telle que tous les $a_v^{(n)}$ soient situés du même côté de Δ (la droite Δ exclue). Quitte à multiplier tous les $a_v^{(n)}$ par une même constante non nulle, on peut donc supposer que, pour tout $v \in \mathcal{I}_g$ et $n \geqslant 0$, $\mathrm{Re}\left(a_v^{(n)}\right) > 0$ et quitte à multiplier tous les $\alpha_v^{(n)}$ par -1, on peut aussi supposer que $\mathrm{Im}\left(\alpha_v^{(n)}\right) > 0$ (du fait que tous les choix de racines sont bons).

On considère alors la suite $(m_n)_{n\in\mathbb{N}}$ définie par

$$m_n = \mathrm{Min}_{v\in\mathcal{I}_g} \mathrm{Re}\left(a_v^{(n)}\right),$$

pour tout $n \in \mathbb{N}$. Le fait que $A \neq 0$ est alors une conséquence directe du résultat suivant :

Lemme 7.3 *Avec les notations et suppositions faites ci-dessus, la suite $(m_n)_{n\in\mathbb{N}}$ est croissante.*

Démonstration : Nous allons utiliser le fait suivant : pour tous $x, y \in \mathbb{C}$ tels que $\mathrm{Re}(x) > 0$ et $\mathrm{Re}(y) > 0$, si l'on note z la racine carrée de xy ayant partie réelle positive, alors

$$\mathrm{Re}(z) \geqslant \mathrm{Min}\left(\mathrm{Re}(x), \mathrm{Re}(y)\right).$$

Pour voir pourquoi cela est vrai, on pose $x = Xe^{ir}$ et $y = Ye^{is}$ avec $r, x \in]-\pi/2, \pi/2[$. Alors $\mathrm{Re}(x) = X\cos r$ et $\mathrm{Re}(y) = Y\cos s$, et $\mathrm{Re}(z) = \sqrt{XY}\cos\left(\frac{r+s}{2}\right)$, donc

$$\begin{aligned}\log\left(\mathrm{Re}(z)\right) &= \log\left(\sqrt{XY}\cos\left(\frac{r+s}{2}\right)\right)\\ &= \frac{\log X + \log Y}{2} + \log\left(\cos\left(\frac{r+s}{2}\right)\right),\end{aligned}$$

et en utilisant la concavité de la fonction $\log\circ\cos$[†], on obtient

$$\begin{aligned}\log\left(\mathrm{Re}(z)\right) &\geqslant \frac{\log X + \log Y}{2} + \frac{\log(\cos r) + \log(\cos s)}{2}\\ &\geqslant \frac{\log\left(\mathrm{Re}(x)\right) + \log\left(\mathrm{Re}(y)\right)}{2},\end{aligned}$$

ce qui implique directement

$$\mathrm{Re}(z) \geqslant \mathrm{Min}\left(\mathrm{Re}(x), \mathrm{Re}(y)\right)$$

comme annoncé.

En utilisant la définition d'une itération de Borchardt, ceci montre que $m_1 \geqslant m_0$, et une récurrence directe montre que la suite (m_n) est croissante. □

Nous allons maintenant montrer le caractère quadratique de la convergence des suites de Borchardt. Pour cela, nous commençons par le résultat auxilliaire suivant :

[†]Cette idée est due à T. Houtmann.

Lemme 7.4 *Soit* $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ *tels que* $\mathrm{Re}\,(a_v) > 0$ *pour tout* v*, et soit* $(a'_v)_{v\in\mathcal{I}_g}$ *l'itéré de Borchardt associé correspondant au choix de racines* (α_v) *où* $\mathrm{Re}\,(\alpha_v) > 0$ *pour tout* v*. Soit de plus* $\varepsilon \leqslant \sqrt{\frac{3}{2}} - 1$ *tel que pour tout* v*,*

$$|a_v - a_0| \leqslant |a_0|\,\varepsilon,$$

alors pour tout v*,*

$$\left|a'_v - a'_0\right| \leqslant \frac{5}{2}\,|a_0|\,\varepsilon^2 \leqslant \frac{7}{2}\,\left|a'_0\right|\,\varepsilon^2.$$

Démonstration : Soient (a_v), (α_v) et (a'_v) comme ci-dessus, et soit $\varepsilon \leqslant \sqrt{\frac{3}{2}} - 1$ tel que pour tout $v \in \mathcal{I}_g$,

$$|a_v - a_0| \leqslant |a_0|\,\varepsilon.$$

Pour tout v, on pose $a_v = a_0(1+\varepsilon_v)$, de sorte que $|\varepsilon_v| \leqslant \varepsilon$.

Pour $z \in \mathbb{C}$ tel que $\mathrm{Re}\,(z) > 0$, notons $\sqrt{z}$ la racine carrée de z ayant partie réelle positive. Alors, en considérant le développement de Taylor de la fonction $z \mapsto \sqrt{1+z}$ au voisinage de zéro, on montre que pour tout $z \in \mathbb{C}$ tel que $|z| \leqslant \frac{1}{2}$,

$$\left|\sqrt{1+z} - 1 - \frac{z}{2}\right| \leqslant \frac{|z|}{2}.$$

Soient maintenant $v_1, v_2 \in \mathcal{I}_g$, on a

$$\left|\alpha_{v_1}\cdot\alpha_{v_2} - \frac{a_{v_1}+a_{v_2}}{2}\right| = |a_0|\cdot\left|\sqrt{1+\varepsilon_{v_1}+\varepsilon_{v_2}+\varepsilon_{v_1}\cdot\varepsilon_{v_2}} - 1 - \frac{\varepsilon_{v_1}+\varepsilon_{v_2}}{2}\right|.$$

La condition $\varepsilon \leqslant \sqrt{\frac{3}{2}} - 1$ implique que

$$|\varepsilon_{v_1}+\varepsilon_{v_2}+\varepsilon_{v_1}\cdot\varepsilon_{v_2}| \leqslant |\varepsilon_{v_1}| + |\varepsilon_{v_2}| + |\varepsilon_{v_1}\cdot\varepsilon_{v_2}| \leqslant 2\varepsilon + \varepsilon^2 \leqslant \frac{1}{2},$$

d'où l'on déduit que

$$\begin{aligned}\left|\alpha_{v_1}\cdot\alpha_{v_2} - \frac{a_{v_1}+a_{v_2}}{2}\right| &\leqslant |a_0|\left(\frac{|\varepsilon_{v_1}+\varepsilon_{v_2}+\varepsilon_{v_1}\cdot\varepsilon_{v_2}|^2}{4} + |\varepsilon_{v_1}\cdot\varepsilon_{v_2}|\right)\\ &\leqslant |a_0|\left(1+\frac{(2+\varepsilon)^2}{4}\right)\varepsilon^2\\ &\leqslant \frac{5\,|a_0|}{2}\varepsilon^2.\end{aligned}$$

Comme, par définition,

$$a'_v = \frac{1}{2^g}\sum_{v_1+v_2=v}\alpha_{v_1}\alpha_{v_2}$$

pour tout v, et qu'en particulier

$$a'_0 = \frac{1}{2^g}\sum_{v\in\mathcal{I}_g} a_v,$$

l'identité triangulaire permet d'en déduire que pour tout $v \in \mathcal{I}_g$,

$$\left|a'_v - a'_0\right| \leqslant \frac{5\,|a_0|}{2}\varepsilon^2.$$

Pour conclure, il suffit de remarquer que, d'après la définition de a'_0 et l'inégalité triangulaire, on a

$$\left|a'_0 - a_0\right| \leqslant |a_0|\,\varepsilon,$$

d'òu l'on déduit que $|a_0| \leqslant \frac{1}{1-\varepsilon}\,|a'_0|$. Une application numérique permet finalement d'en déduire la dernière inégalité.

□

Nous sommes maintenant en mesure de démontrer le résultat suivant :

Proposition 7.1 *Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de Borchardt telle que pour tous $v \in \mathcal{I}_g, n \in \mathbb{N}$, $\mathrm{Re}\left(a_v^{(n)}\right) > 0$. Notons A sa limite et $(M_n)_{n\in\mathbb{N}}$ la suite (décroissante) des maxima des modules des a_v^n, et supposons qu'il existe un indice $N \geqslant 0$ tel que pour tout v,*

$$\left|a_v^{(N)} - a_0^{(N)}\right| \leqslant \left|a_0^{(N)}\right|\varepsilon,$$

avec $\varepsilon < \sqrt{\frac{3}{2}} - 1$. Alors pour tout $k \geqslant 0$, on a

$$\left|A - a_0^{(N+k)}\right| \leqslant \frac{10}{2}\left(\frac{7\varepsilon}{2}\right)^{2^k} M_N.$$

Démonstration : Reprenons les notations introduites dans l'énoncé de la proposition.

Comme $\frac{7}{2}\left(\sqrt{\frac{3}{2}} - 1\right) < 1$, on en déduit que $\frac{7}{2}\varepsilon^2 < \varepsilon$, et l'on peut alors procéder par récurrence pour montrer à partir du Lemme 7.4 que pour tout $k \geqslant 0$,

$$\left|a_v^{(N+k)} - a_0^{(N+k)}\right| \leqslant \frac{2}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k}\left|a_0^{(N+k)}\right|$$

pour tout v.

Pour tout $k \geqslant 0$, comme $a_0^{(N+k+1)}$ est la moyenne arithmétique des $a_v^{(N+k)}$, on a

$$\left|a_0^{(N+k+1)} - a_0^{(N+k)}\right| \leqslant \frac{2}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k}\left|a_0^{(N+k)}\right| \leqslant \frac{2}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k} M_N.$$

On en déduit que, pour tout $\ell \geqslant 1$,

$$\begin{aligned}\left|a_0^{(N+k+\ell)} - a_0^{(N+k)}\right| &\leqslant \sum_{j=0}^{\ell-1}\left|a_0^{(N+k+j+1)} - a_0^{(N+k+j)}\right| \\ &\leqslant \frac{2}{7}M_N\sum_{j=0}^{\ell-1}\left(\frac{7\varepsilon}{2}\right)^{2^{k+j}} \\ &\leqslant \frac{10}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k} M_N.\end{aligned}$$

En faisant tendre ℓ vers l'infini, on en déduit le résultat annoncé. □

Cette proposition se restreint aux suites de Borchardt dont tous les éléments ont partie réelle strictement positive. Notons qu'il est toujours possible de se ramener à ce cas : si $(a_v^{(n)})$ est une suite de Borchardt convergeant vers une limite $A \neq 0$, alors la suite $(a_v^{(n)}/A)$ est une

suite de Borchardt convergeant vers 1. En particulier, à partir d'un certain indice N, tous les éléments $(a_v^{(n)}/A)_{v\in\mathcal{I}_g,n\geqslant N}$ ont partie réelle strictement positive, donc quitte à translater les indices, on peut se ramener dans les conditions d'application de la Proposition 7.1.

Le Lemme 7.2 et le fait que la suite $\left|a_0^{(n)}\right|$ est bornée (elle est dans l'intervalle $[m_0, M_0]$ par exemple) permettent de montrer qu'il existe nécessairement un indice N tel que pour tout $v \in \mathcal{I}_g$,

$$\left|a_v^{(N)} - a_0^{(N)}\right| \leqslant \left|a_0^{(N)}\right| \varepsilon,$$

avec $\varepsilon \leqslant \sqrt{\frac{3}{2}} - 1$. La Proposition 7.1 et sa démonstration montrent alors que pour tout $k \geqslant 0$,

$$\left|A - a_0^{(N+k)}\right| \leqslant \frac{10}{2}\left(\frac{7\varepsilon}{2}\right)^{2^k} M_N$$

et

$$\left|a_v^{(N+k)} - a_0^{(N+k)}\right| \leqslant \frac{2}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k} \left|a_0^{(N+k)}\right|$$

pour tout v, ce qui permet de montrer que pour tout v,

$$\left|A - a_v^{(N+k)}\right| \leqslant \frac{12}{7}\left(\frac{7\varepsilon}{2}\right)^{2^k} M_N,$$

donc chacune des suites $(a_v^{(n)})_{n\in\mathbb{N}}$ converge quadratiquement vers la limite A.

7.3 Quelques remarques

– Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de Borchardt, et soit $\lambda \in \mathbb{C}\backslash\{0\}$, alors la suite $(\lambda a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est elle aussi de Borchardt, ce qui montre que pour tous $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^g$ et $\lambda \in \mathbb{C} \setminus \{0\}$,

$$\mathcal{B}_g(\lambda a_v)_{v\in\mathcal{I}_g} = \left\{\lambda x : x \in \mathcal{B}_g(a_v)_{v\in\mathcal{I}_g}\right\}.$$

– Dans le cas où $g \in \{1, 2\}$, si $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ et $(a'_v)_{v\in\mathcal{I}_g}$ est un itéré de Borchardt de (a_v), et si $(\alpha_v)_{v\in\mathcal{I}_g}$ est un choix de racines associé à cette itération, alors (par définition d'une itération de Borchardt) :

$$\left\{a'_v : v \in \mathcal{I}_g\right\} = \left\{\frac{1}{2^g}\sum_{v\in\mathcal{I}_g} \alpha_v\alpha_{\sigma(v)} : \sigma \in \mathrm{Perm}(\mathcal{I}_g)\right\}.$$

Ceci est bien sûr faux dès que $g \geqslant 3$.
Une conséquence directe de ce fait est que, si $g \in \{1, 2\}$ et que l'on fixe $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, alors pour tout $\sigma \in \mathrm{Perm}(\mathcal{I}_g)$,

$$\mathcal{B}_g(a_v)_{v\in\mathcal{I}_g} = \mathcal{B}_g(a_{\sigma(v)})_{v\in\mathcal{I}_g}.$$

– Un autre point important, toujours dans le cas où $g \in \{0, 1\}$, est que si $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est une suite de Borchardt et que $N \geqslant 0$ est tel qu'au moins 2^{g-1} (*i.e.*, la moitié) des $(a_v^{(N)})_{v\in\mathcal{I}_g}$ sont nuls, alors cela est encore vrai pour tout $n \geqslant N$, donc la limite d'une telle séquence est nécessairement nulle.

– Supposons que $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ soit une suite de Borchardt, alors si l'on définit $(A_w^{(n)})_{w\in\mathcal{I}_{g+1},n\in\mathbb{N}}$ par

$$A_{(v,e)}^{(n)} = a_v^{(n)}$$

pour tous $v \in \mathcal{I}_g$, $e \in \mathbb{Z}/2\mathbb{Z}$ et $n \in \mathbb{N}$, alors il est aisé de vérifier que $(A_w^{(n)})$ est encore une suite de Borchardt.

– Si $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est une suite de Borchardt, que $(\alpha_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ est une suite de choix de racines associée et que l'on suppose de plus que tous les éléments de ces deux suites ont partie réelle strictement positive, alors la limite $A \neq 0$ de la suite $(a_v^{(n)})$ n'est pas nécessairement contenue dans l'enveloppe convexe des $(a_v^{(0)})_{v\in\mathcal{I}_g}$. Ceci se voit facilement en considérant l'AGM (cas où $g = 1$), qui est un cas particulier de suite de Borchardt pour g quelconque d'après la remarque précédente. On a toutefois quelques renseignements sur la position de A par rapport aux $(a_v^{(n)})_{v\in\mathcal{I}_g}$, pour un n fixé : on sait que

$$|A| \leqslant \mathrm{Max}_{v\in\mathcal{I}_g}\left(a_v^{(n)}\right),$$

$$\mathrm{Re}\,(A) \geqslant \mathrm{Min}_{v\in\mathcal{I}_g}\left(\mathrm{Re}\left(a_v^{(n)}\right)\right)$$

et

$$\mathrm{Min}_{v\in\mathcal{I}_g}\left(\mathrm{Arg}\left(a_v^{(n)}\right)\right) \leqslant \mathrm{Arg}(A) \leqslant \mathrm{Max}_{v\in\mathcal{I}_g}\left(\mathrm{Arg}\left(a_v^{(n)}\right)\right).$$

– Soit $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ une suite de Borchardt, alors si cette suite converge vers zéro, la convergence est en général linéaire et non quadratique. L'archétype de ce type de suite est l'AGM associée à $a_0 = 1$ et $b_0 = 0$: on a alors $b_n = 0$ et $|a_n| = \frac{1}{2^n}$ pour tout n.

– Le lien entre les theta constantes et les suites de Borchardt est le suivant : si l'on fixe $\tau \in \mathcal{H}_g$, alors la Proposition 5.5 montre que la suite

$$(\theta_{0,b}(2^n\tau))_{b\in\{0,1\}^g,n\in\mathbb{N}}$$

est une suite de Borchardt (modulo un léger abus de notation : on a identifié $\{0,1\}^g$ à $\mathcal{I}_g$) qui, d'après le Lemme 5.2, converge vers 1.
Dans le cas où $g = 1$, nous avons même vu au Chapitre 3 que toutes les suites AGM sont, à une constante près, de ce type (sauf cas dégénérés). Nous allons voir au Chapitre 8 que c'est encore le cas lorsque $g = 2$ (quoique les cas dégénérés soient plus difficiles à caractériser).

7.4 Une fonction associée à la moyenne de Borchardt

7.4.1 Définition

Soit $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$, on lui associe la suite de Borchardt $(a_v^{(n)})_{v\in\mathcal{I}_g,n\in\mathbb{N}}$ définie par $a_0^{(0)} = 1$, $a_v^{(0)} = z_v$ pour $v \in \mathcal{I}_g \setminus \{0\}$, et où l'on définit $(a_v^{(n)})_{v\in\mathcal{I}_g}$ par récurrence sur n en posant

$$a_0^{(n+1)} = \frac{1}{2^g}\sum_{v\in\mathcal{I}_g} a_v^{(n)},$$

et

$$a_v^{(n+1)} = \frac{1}{2^g}\sum_{v_1+v_2=v} b_{v_1}^{(n)} b_{v_2}^{(n)},$$

où $b_0^{(n)}$ est une racine carrée *quelconque* de $a_0^{(n)}$, et, pour $v \neq 0$, $b_v^{(n)} = 0$ dans le cas où $b_0^{(n)} = 0$, sinon $b_v^{(n)}$ est une racine carrée de $a_v^{(n)}$ telle que

$$\left|b_0^{(n)} - b_v^{(n)}\right| \leqslant \left|b_0^{(n)} + b_v^{(n)}\right|, \tag{7.3}$$

avec $\mathrm{Im}\left(\frac{b_v^{(n)}}{b_0^{(n)}}\right) > 0$ en cas d'égalité dans (7.3) (dans le cas où $a_v^{(n)} = 0$, on prend $b_v^{(n)} = 0$).

D'après le Théorème 7.1, cette suite $(a_v^{(n)})$ converge vers une unique valeur complexe, que l'on définit comme étant $B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$.

Notons que dans le cas où $g \leqslant 2$, la valeur de $B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$ ne dépend que de l'ensemble $\{z_v\}_{v\in\mathcal{I}_g\setminus\{0\}}$, ce qui n'est plus le cas lorsque $g > 2$ (Borchardt avait déjà remarqué ce fait dans le cas où l'on se restreint aux suites de réels positifs).

On peut par ailleurs facilement montrer (nous ne le détaillons pas ici car le calcul est un peu technique) que pour tout $z \in \mathbb{C}$,

$$M(z) = B_1(z),$$

c'est-à-dire que dans le cas particulier où $g = 1$, la manière de définir la suite de Borchardt (en fait, une suite AGM) décrite ci-dessus correspond bien à ne prendre que des bons choix de racines, au sens défini à la Section 3.2.

7.4.2 Évaluation

Soit $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$ tels que $\mathrm{Re}\,(z_v) > 0$ pour tout $v \in \mathcal{I}_g \setminus \{0\}$ (dans la plupart des cas que nous considérerons par la suite, cette condition sera vérifiée). On note alors $(a_v^{(n)})_{v\in\mathcal{I}_g, n\in\mathbb{N}}$ la suite de Borchardt associée au calcul de $A = B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$, et l'on reprend les notations introduites à la Section 7.2. On note de plus, pour $n \geqslant 0$,

$$\Delta_n = \sum_{v_1,v_2\in\mathcal{I}_g} \left|a_{v_1}^{(n)} - a_{v_2}^{(n)}\right|.$$

Posons

$$n_1 = \left\lceil \frac{\log\left(1 - \frac{1}{2^g}\right)}{\log \frac{m_0}{7\Delta_0}} \right\rceil,$$

on a alors (d'après le Lemme 7.2)

$$\Delta_{n_1} \leqslant \left(1 - \frac{1}{2^g}\right)^{n_1} \Delta_0 \leqslant \frac{m_0}{7} \leqslant \frac{\left|a_0^{(n_1)}\right|}{7}.$$

La Proposition 7.1 montre alors que pour tout $k \geqslant 0$,

$$\left|A - a_0^{(n_1+k)}\right| \leqslant \frac{1}{7\times 2^{2^k-1}} \left|a_0^{(n_1+k)}\right| \leqslant \frac{1}{7\times 2^{2^k-1}} M_0.$$

Comme $|A| \geqslant m_0$, on en déduit que

$$\left|\frac{A - a_0^{(n_1+k)}}{A}\right| \leqslant \frac{1}{7\times 2^{k-1}} \frac{M_0}{m_0}$$

pour tout $k \geqslant 0$.

Ceci démontre le résultat suivant :

Proposition 7.2 *Avec les notations introduites ci-dessus, pour tout $N \geqslant 1$, si l'on pose*

$$B\left(N,(z_v)\right) = \left\lceil \frac{\log\left(1-\frac{1}{2^g}\right)}{\log \frac{m_0}{7\Delta_0}} \right\rceil + N + 1 + \left\lceil \log_2 \frac{M_0}{7m_0} \right\rceil,$$

alors $a_0^{(B(N,(z_v)))}$ est une approximation de $B_g\left((z_v)\right)$ avec une précision relative de N bits.

En particulier, si le (2^g-1)-uplet $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}}$ est fixé, alors

$$B\left(N,(z_v)\right) = O(\log N),$$

ce qui reste vrai si l'on fait varier (z_v) en supposant m_0 minoré et M_0 majoré (ce qui permet de majorer Δ_0).

On en déduit la validité de l'Algorithme 11 pour l'évaluation de B_g.

Algorithme : `EvaluateBg`
Entrée : $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$ tels que $\mathrm{Re}\,(z_v) > 0$ pour tout v, $N \in \mathbb{N}$
Sortie : A tel que $\left|\frac{A}{B_g((z_v))} - 1\right| \leqslant 2^{-N}$

$B \leftarrow B\left(N+1,(z_v)\right)$;
$a_0 \leftarrow 1$;
for $v \in \mathcal{I}_g \setminus \{0\}$ **do**
  $a_v \leftarrow z_v$;
end
for $n = 1$ **to** B **do**
  for $v \in \mathcal{I}_g$ **do**
    $r_v \leftarrow \sqrt{a_v}$ (tel que $\mathrm{Re}\,(r_v) > 0$);
    $b_v \leftarrow 0$;
  end
  for $v \in \mathcal{I}_g$ **do**
    $b_0 \leftarrow b_0 + a_v$;
    for $v_1 \in \mathcal{I}_g$ **do**
      $b_v \leftarrow b_v + r_{v_1} r_{v+v_1}$;
    end
  end
  for $v \in \mathcal{I}_g$ **do**
    $a_v \leftarrow b_v / 2^g$;
  end
end
return a_0;

Algorithme 11: Évaluation de la moyenne de Borchardt B_g

En procédant comme à la Section 3.4.2 pour la complexité de l'évaluation de l'AGM, on montre qu'il est suffisant de travailler toujours à précision $N + g\log_2(3)B\left(N+1,(z_v)\right)$, ce qui montre que la complexité en temps de l'Algorithme 11 est en

$$O\left(\mathcal{M}\left(N + B\left(N,(z_v)\right)\right) B\left(N,(z_v)\right)\right)$$

dans le cas général (g étant fixé), donc en

$$O\left(\mathcal{M}(N)\log N\right)$$

dans le cas où (z_v) est fixé ou bien dans le cas où m_0 est minoré et M_0 majoré.

Chapitre 8

Limites des suites de Borchardt de quatre éléments

Dans ce chapitre, nous reprenons les notations utilisées pour les theta constantes au Chapitre 6 : les theta constantes en genre 2 sont représentées par la lettre θ, alors que les theta constantes en genre 1 sont représentées par la lettre ϑ.

Le but de ce chapitre est de démontrer le résultat suivant, qui peut être vu comme une généralisation du Théorème 3.1 :

Théorème 8.1 *Pour tout $\tau \in \mathcal{H}_2$, on a*

$$\mathcal{B}_2\left(\theta_j^2(\tau)\right)_{j\in[0,3]} = \left\{ \frac{1}{\kappa(\gamma)\mathrm{Det}(C\tau+D)} : \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_b \right\} \cup \{0\},$$

où l'ensemble noté $\mathcal{B}_2$ est celui défini à la Section 7.3.

Notons que pour tous $\tau \in \mathcal{H}_2$ et $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_b$, on a

$$\frac{1}{\kappa(\gamma)\mathrm{Det}(C\tau+D)} = \frac{\theta_j^2(\tau)}{\theta_j^2(\gamma\tau)},$$

pour tout $j \in [0,3]$ tel que $\theta_j(\tau) \neq 0$ (c'est une conséquence directe de la définition de $\kappa(\gamma)$ et de celle du groupe Γ_b). Cette forme du résultat est celle qui se rapproche le plus de l'énoncé du Théorème 3.1.

Le Lemme 6.3 permet de déterminer facilement la valeur de $\kappa(\gamma)$ lorsque $\gamma = \begin{pmatrix} A & & B \\ & d_1 & d_2 \\ C & & \\ & d_3 & d_4 \end{pmatrix} \in \Gamma_b$: on a alors

$$\kappa(\gamma) = (-1)^{\frac{d_1-d_4}{2}}.$$

Par ailleurs, ce théorème permet de paramétrer les limites de toutes les suites de Borchardt de quatre éléments complexes. Soit en effet $(a,b,c,d) \in \mathbb{C}^4$, alors :

– si au moins deux éléments parmi a, b, c et d sont nuls, alors pour toute suite de Borchardt $(a_{j,n})_{j\in[0,3],n\in\mathbb{N}}$ associée à (a,b,c,d) et pour tout $n \geqslant 0$, une récurrence directe permet de montrer qu'au moins deux éléments parmi les $a_{j,n}$ ($j \in [0,3]$) sont nuls, donc toute suite de Borchardt associée à (a,b,c,d) a une limite nulle ;

– si (à permutation près) on a

$$(a, b, c, d) = (\alpha, -\alpha, \beta, -\beta),$$

alors si (a', b', c', d') est un itéré de Borchardt de (a, b, c, d), un simple calcul permet de vérifier qu'au moins deux éléments parmi a', b', c' et d' sont nuls, et d'après ce qui précède, on en déduit que toute suite de Borchardt associée à (a, b, c, d) a une limite nulle ;

– si (à permutation près) on a

$$(a, b, c, d) = (\alpha, \alpha, \beta, \beta),$$

alors si (a', b', c', d') est un itéré de Borchardt de (a, b, c, d), soit (a', b', c', d') est de l'une des deux formes précédentes, soit (à permutation près)

$$(a', b', c', d') = \left(\frac{\alpha+\beta}{2}, \frac{\alpha+\beta}{2}, \pm\sqrt{\alpha\beta}, \pm\sqrt{\alpha\beta} \right),$$

dans tous les cas une récurrence directe permet de montrer que $\mathcal{B}_2(a, b, c, d) = \mathcal{B}_1(\alpha, \beta)$;

– enfin, si l'on n'est dans aucun des trois cas précédents, alors on peut montrer (en partant de [Run97] et en considérant encore l'action de Γ_2 sur les carrés de theta constantes) qu'il existe $\tau \in \mathcal{H}_2$ tel que

$$[a : b : c : d] = \left[\theta_0^2(\tau) : \theta_1^2(\tau) : \theta_2^2(\tau) : \theta_3^2(\tau)\right],$$

et alors le Théorème 8.1 permet de déterminer $\mathcal{B}_2(a, b, c, d)$ (qui est entièrement paramétré par τ). Notons qu'alors τ peut être déterminé explicitement par les méthodes exposées au Chapitre 9 ; toutefois il serait plus agréable d'avoir une méthode plus directe (similaire à celle existant en genre 1, voir le Théorème 3.2).

La démonstration, dans son principe, est relativement similaire à celle que nous avons donnée du Théorème 3.1, mais les détails sont toutefois beaucoup plus techniques.

Tout comme dans la Section 3.3, nous commençons par décrire les principales étapes de la démonstration, avant d'entrer dans les détails. Ceci met en évidence les similitudes avec la démonstration que nous avons donnée du Théorème 3.1.

Dans la suite de cette section, nous fixons $\tau_0 \in \mathcal{H}_2$ et posons

$$A_0 = (a_{j,0})_{j\in[0,3]} = \left(\theta_j^2(\tau_0)\right)_{j\in[0,3]}$$

et

$$\mathcal{L}(\tau_0) = \left\{ \frac{1}{\kappa(\gamma)\mathrm{Det}(C\tau_0 + D)} : \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_b \right\}.$$

8.1 Schéma de la démonstration

Tout comme dans le cas du genre 1, il est relativement facile de montrer l'inclusion

$$(\mathcal{L}(\tau_0) \cup \{0\}) \subset \mathcal{B}_2(A_0). \tag{8.1}$$

Étant donnée la définition d'un mauvais choix, il est toujours possible de construire une suite de Borchardt associée à A_0 ayant un nombre infini de mauvais choix. D'après le Théorème 7.1, une telle suite converge vers zéro, donc $\mathcal{B}_2(A_0)$ contient zéro.

Par ailleurs, les formules de duplication des theta constantes (Proposition 5.5) montrent que pour tout $\tau \in \mathcal{H}_2$, la suite $\left(\theta_j^2(2^n\tau)\right)_{j\in[0,3],n\in\mathbb{N}}$ est une suite de Borchardt qui, d'après

le Lemme 5.2, converge vers 1. On en déduit bien sûr que $\mathcal{B}_2(A_0)$ contient 1. Par ailleurs, si $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_b$, alors

$$\left[\theta_j^2(\gamma\tau_0)\right]_{j\in[0,3]} = \left[\theta_j^2(\tau_0)\right]_{j\in[0,3]},$$

donc (d'après la première remarque de la Section 7.3)

$$\mathcal{B}_2\left(\theta_j^2(\tau_0)\right)_{j\in[0,3]} = \frac{\theta_\ell^2(\tau_0)}{\theta_\ell^2(\gamma\tau_0)}\mathcal{B}_2\left(\theta_j^2(\gamma\tau_0)\right)_{j\in[0,3]},$$

où $\ell \in [0,3]$ est tel que $\theta_\ell(\tau_0) \neq 0$ (l'existence d'un tel ℓ est assurée par le Corollaire 6.1). D'après ce qui précède,

$$1 \in \mathcal{B}_2\left(\left(\theta_j^2(\gamma\tau_0)\right)_{j\in[0,3]}\right),$$

d'où

$$\frac{1}{\kappa(\gamma)\mathrm{Det}(C\tau_0+D)} = \frac{\theta_\ell^2(\tau_0)}{\theta_\ell^2(\gamma\tau_0)} \in \mathcal{B}_2(A_0),$$

ce qui termine la démonstration de la première inclusion.

Pour montrer la seconde inclusion, fixons une suite de Borchardt $(a_{j,n})_{j\in[0,3],n\in\mathbb{N}}$ associée à $(a_{j,0})_{j\in[0,3]}$ convergeant vers une limite $\mathcal{A} \neq 0$. Définissons alors, pour tout $n \geqslant 0$, l'ensemble

$$T_n = \left\{\tau \in \mathcal{H}_2 : \left[\theta_j^2(\tau)\right]_{j\in[0,3]} = [a_{j,n}]_{j\in[0,3]}\right\}.$$

Cet ensemble va jouer le même rôle que son homonyme dans la démonstration du Théorème 3.1, mais comme, contrairement à ce qui se passe en genre 1, les theta constantes peuvent s'annuler en genre 2, nous ne considérons pas ici les quotients de carrés des theta constantes mais nous plaçons dans l'espace projectif pour contourner le problème.

Nous montrerons qu'aucun des ces ensembles T_n ne peut être vide, donc qu'il existe une suite $(\tau_n)_{n\in\mathbb{N}}$ telle que pour tout $n \geqslant 1$, $\tau_n \in T_n \cap \mathcal{F}_b$, où $\mathcal{F}_b$ est un domaine fondamental bien choisi pour l'action du groupe Γ_b sur $\mathcal{F}_2$.

En utilisant le fait que les quatre suites $(a_{j,n})_{n\in\mathbb{N}}$ convergent vers la même limite non-nulle $\mathcal{A}$ ainsi que des propriétés particulières du domaine fondamental $\mathcal{F}_2$, nous montrerons que $(\lambda(\tau_n))_{n\in\mathbb{N}}$ tend vers l'infini.

Nous en déduirons alors l'existence d'un indice $N \geqslant 0$ tel que, pour tout $n \geqslant 0$,

$$(a_{j,N+n})_{j\in[0,3]} = \left(\mathcal{A}\theta_j^2(2^n\tau_N)\right)_{j\in[0,3]},$$

puis l'existence d'un élément $\tau_0' \in \mathcal{H}_2$ tel que

$$(a_{j,0})_{j\in[0,3]} = \left(\mathcal{A}\theta_j^2(\tau_0')\right)_{j\in[0,3]}.$$

Si $\ell \in [0,3]$ est tel que $\theta_\ell(\tau_0) \neq 0$,

$$\mathcal{A} = \frac{\theta_\ell^2(\tau_0)}{\theta_\ell^2(\tau_0')}$$

avec

$$\left[\theta_j^2(\tau_0)\right]_{j\in[0,3]} = \left[\theta_j^2(\tau_0')\right]_{j\in[0,3]},$$

et la Proposition 6.9 montre qu'il existe $\gamma \in \Gamma_b$ tel que $\tau_0' = \gamma\tau_0$, donc que

$$\mathcal{A} = \frac{\theta_\ell^2(\tau_0)}{\theta_\ell^2(\gamma\tau_0)} \in \mathcal{L}(\tau_0).$$

8.2 Preuve détaillée

L'inclusion (8.1) a déjà été entièrement démontrée dans la section précédente, nous ne décrivons donc ici que la démonstration de la seconde inclusion.

Nous fixons dans cette section une suite de Borchardt $(a_{j,n})_{j\in[0,3],n\in\mathbb{N}}$ associée à $(a_{j,0})_{j\in[0,3]}$, convergeant vers une limite $\mathcal{A}\neq 0$.

8.2.1 Non-vacuité des ensembles T_n

Définissons les ensembles T_n par

$$T_n=\left\{\tau\in\mathcal{H}_2:\left[\theta_j^2(\tau)\right]_{j\in[0,3]}=\left[a_{j,n}\right]_{j\in[0,3]}\right\}$$

pour tout $n\geqslant 0$.

Pour prouver qu'aucun de ces ensembles ne peut être vide, nous allons utiliser le lemme suivant :

Lemme 8.1 *Pour tout $\tau\in\mathcal{H}_2$, si $(a,b,c,d)\in\mathbb{C}^4$ est un itéré de Borchardt du quadruplet $\left(\theta_j^2(\tau)\right)_{j\in[0,3]}$, alors*

$$[a:b:c:d]\in\left\{\left[\theta_j^2(2\gamma\tau)\right]_{j\in[0,3]}:\gamma\in\{\mathfrak{C}_k:k\in[0,7]\}\right\},$$

où

$$\mathfrak{C}_k=\begin{pmatrix} I & 0\\ C_k & I\end{pmatrix}$$

pour $k\in[0,7]$, avec

$$C_0=\begin{pmatrix}0&0\\0&0\end{pmatrix},\quad C_1=\begin{pmatrix}2&0\\0&0\end{pmatrix},\quad C_2=\begin{pmatrix}0&0\\0&2\end{pmatrix},\quad C_3=\begin{pmatrix}2&0\\0&2\end{pmatrix},$$
$$C_4=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad C_5=\begin{pmatrix}2&1\\1&0\end{pmatrix},\quad C_6=\begin{pmatrix}0&1\\1&2\end{pmatrix},\quad C_7=\begin{pmatrix}2&1\\1&2\end{pmatrix}.$$

Démonstration : Soit $\tau\in\mathcal{H}_2$. Il est facile, en utilisant les formules de duplication des theta constantes (Proposition 5.5), de voir que les huit itérés de Borchardt possibles à partir de $\left(\theta_j^2(\tau)\right)_{j\in[0,3]}$ sont

- $(A_0,B_0,C_0,D_0)=\left(+\theta_0^2(2\tau),+\theta_1^2(2\tau),+\theta_2^2(2\tau),+\theta_3^2(2\tau)\right)$;
- $(A_1,B_1,C_1,D_1)=\left(+\quad,-\quad,+\quad,-\quad\right)$;
- $(A_2,B_2,C_2,D_2)=\left(+\quad,+\quad,-\quad,-\quad\right)$;
- $(A_3,B_3,C_3,D_3)=\left(+\quad,-\quad,-\quad,+\quad\right)$;
- $(A_4,B_4,C_4,D_4)=\left(+\theta_0^2(2\tau),+\theta_9^2(2\tau),+\theta_6^2(2\tau),-\theta_{15}^2(2\tau)\right)$;
- $(A_5,B_5,C_5,D_5)=\left(+\quad,-\quad,+\quad,+\quad\right)$;
- $(A_6,B_6,C_6,D_6)=\left(+\quad,+\quad,-\quad,+\quad\right)$;
- $(A_7,B_7,C_7,D_7)=\left(+\quad,-\quad,-\quad,-\quad\right)$.

Les formules de transformation des theta constantes (Proposition 5.4) montrent alors que pour tout $j\in[0,7]$,

$$[A_k:B_k:C_k:D_k]=\left[\theta_0^2(2\mathfrak{G}_k\tau):\theta_1^2(2\mathfrak{G}_k\tau):\theta_2^2(2\mathfrak{G}_k\tau):\theta_3^2(2\mathfrak{G}_k\tau)\right],$$

d'où le résultat. □

Un récurrence directe utilisant ce résultat (et le fait que par hypothèse T_0 est non vide puisque $\tau_0\in T_0$) permet de montrer que pour tout $n\geqslant 0$, T_n est non vide.

8.2.2 Le domaine fondamental $\mathcal{F}_b$

Commençons par introduire l'ensemble $\mathcal{G}_1$ défini par

$$\begin{aligned}\mathcal{G}_1 \;=\; \{&\mathfrak{I},\mathfrak{T},\mathfrak{S},\mathfrak{TS},\mathfrak{ST},\mathfrak{TST},\mathfrak{M}_1\mathfrak{T},\mathfrak{M}_1,\mathfrak{M}_2\mathfrak{ST},\mathfrak{TM}_2\mathfrak{ST},\mathfrak{M}_2\mathfrak{S},\mathfrak{TM}_2\mathfrak{S},\mathfrak{M}_1\mathfrak{TS},\mathfrak{M}_1\mathfrak{S}\\ &\mathfrak{M}_2\mathfrak{TST},\mathfrak{M}_1\mathfrak{M}_2\mathfrak{ST},\mathfrak{M}_2,\mathfrak{TM}_2,\mathfrak{M}_1\mathfrak{TST},\mathfrak{M}_1\mathfrak{ST},\mathfrak{M}_2\mathfrak{TS},\mathfrak{M}_1\mathfrak{M}_2\mathfrak{S},\mathfrak{M}_2\mathfrak{T},\mathfrak{M}_1\mathfrak{M}_2\}\,.\end{aligned}$$

L'intérêt de cet ensemble est le suivant : pour toute permutation σ de l'ensemble $[0,3]$, il existe un unique élément $\gamma \in \mathcal{G}_1$ tel que

$$\left(\Phi\left(\gamma,j\right)\right)_{j\in[0,3]} = \left(\sigma(j)\right)_{j\in[0,3]}.$$

On peut vérifier ceci directement en utilisant les formules de transformation des theta constantes sous l'action de $\mathfrak{T}$, $\mathfrak{S}$, $\mathfrak{M}_1$ et $\mathfrak{M}_2$.

La correspondance entre les éléments de $\mathcal{G}_1$ et les permutations de $[0,3]$ est la suivante :

Permutation σ	$\gamma \in \mathcal{G}_1$	Permutation σ	$\gamma \in \mathcal{G}_1$
$(0,1,2,3)$	$\mathfrak{I}$	$(2,0,1,3)$	$\mathfrak{M}_1\mathfrak{TS}$
$(0,1,3,2)$	$\mathfrak{T}$	$(2,0,3,1)$	$\mathfrak{M}_1\mathfrak{S}$
$(0,2,1,3)$	$\mathfrak{S}$	$(2,1,0,3)$	$\mathfrak{M}_2\mathfrak{TST}$
$(0,2,3,1)$	$\mathfrak{TS}$	$(2,1,3,0)$	$\mathfrak{M}_1\mathfrak{M}_2\mathfrak{ST}$
$(0,3,1,2)$	$\mathfrak{ST}$	$(2,3,0,1)$	$\mathfrak{M}_2$
$(0,3,2,1)$	$\mathfrak{TST}$	$(2,3,1,0)$	$\mathfrak{TM}_2$
$(1,0,2,3)$	$\mathfrak{M}_1\mathfrak{T}$	$(3,0,1,2)$	$\mathfrak{M}_1\mathfrak{TST}$
$(1,0,3,2)$	$\mathfrak{M}_1$	$(3,0,2,1)$	$\mathfrak{M}_1\mathfrak{ST}$
$(1,2,0,3)$	$\mathfrak{M}_2\mathfrak{ST}$	$(3,1,0,2)$	$\mathfrak{M}_2\mathfrak{TS}$
$(1,2,3,0)$	$\mathfrak{TM}_2\mathfrak{ST}$	$(3,1,2,0)$	$\mathfrak{M}_1\mathfrak{M}_2\mathfrak{S}$
$(1,3,0,2)$	$\mathfrak{M}_2\mathfrak{S}$	$(3,2,0,1)$	$\mathfrak{M}_2\mathfrak{T}$
$(1,3,2,0)$	$\mathfrak{TM}_2\mathfrak{S}$	$(3,2,1,0)$	$\mathfrak{M}_1\mathfrak{M}_2$

Notons que, bien évidemment, deux éléments distincts de $\mathcal{G}_1$ ne peuvent être équivalents modulo Γ_b. L'ensemble $\mathcal{G}_1$ peut donc être complété en un ensemble de représentants des classes de Γ_2 sous l'action de Γ_b. Il est possible d'expliciter un tel ensemble, mais sa taille (rappelons qu'il a $[\Gamma_2 : \Gamma_b] = 1440$ éléments) nous en a dissuadé. Nous fixons donc $\mathcal{G}$ un tel ensemble, sans lui imposer de condition à part qu'il doit contenir $\mathcal{G}_1$.

Si l'on pose

$$\mathcal{F}_b = \bigcup_{\gamma\in\mathcal{G}} \gamma\mathcal{F}_2,$$

alors $\mathcal{F}_b$ est un domaine fondamental pour l'action de Γ_b sur $\mathcal{H}_2$.

Nous allons maintenant prouver deux lemmes qui nous donneront des informations concernant l'action de Γ_2 sur les theta constantes fondamentales.

Lemme 8.2 *Pour tout $\gamma \in \Gamma_2$, il existe $j \in [0,3]$ tel que $\Phi\left(\gamma,j\right) \in [0,3]$.*

Dit autrement, les quatre theta constantes fondamentales ne peuvent s'envoyer sur quatre theta constantes non fondamentales sous l'action de Γ_2.

Démonstration : Soit $\gamma \in \Gamma_2$, et supposons que pour tout $j \in [0,3]$, $\Phi\left(\gamma,j\right) \geqslant 4$. Alors soit $\{\Phi\left(\gamma,4\right),\Phi\left(\gamma,6\right)\}$, soit $\{\Phi\left(\gamma,8\right),\Phi\left(\gamma,9\right)\}$, soit $\{\Phi\left(\gamma,12\right),\Phi\left(\gamma,15\right)\}$ est inclus dans $[0,3]$. Nous supposons dans ce qui suit qu'il s'agit de $\{\Phi\left(\gamma,4\right),\Phi\left(\gamma,6\right)\}$, mais les autres cas peuvent être traités de façon similaire.

La Proposition 6.8 montre que, pour tout $\tau \in \mathcal{H}_2$, $\Psi(\gamma,4)^2\,\theta^4_{\Phi(\gamma,4)}(\tau)$ et $\Psi(\gamma,6)^2\,\theta^4_{\Phi(\gamma,6)}(\tau)$ sont les deux racines de

$$X^2-(a^2+c^2-b^2-d^2)X+(ac-bd)^2=0,$$

avec $(a,b,c,d)=\left(\Psi(\gamma,j)\,\theta^2_{\Phi(\gamma,j)}(\tau)\right)_{j\in[0,3]}$.

Si nous faisons tendre τ vers $\begin{pmatrix} i\infty & 0\\ 0 & i\infty\end{pmatrix}$, alors le Lemme 5.2 montre que a, b, c et d vont tendre vers zéro alors que les modules des racines du polynôme tendront vers 1, ce qui est une contradiction. □

Lemme 8.3 *Pour tout $\gamma\in\Gamma_2$ tel que*

$$\{\Phi(\gamma,j)\}_{j\in[0,3]}=\{1,3,4,6\},$$

il existe un indice $j\in[1,3]$ tel que

$$\Psi(\gamma,j)\neq\Psi(\gamma,0).$$

Démonstration : Soit $\gamma\in\Gamma_2$ tel que

$$\{\Phi(\gamma,j)\}_{j\in[0,3]}=\{1,3,4,6\},$$

et supposons de plus que pour tout $j\in[0,3]$,

$$\Psi(\gamma,j)=0.$$

Supposons maintenant que $0\in\{\Phi(\gamma,4),\Phi(\gamma,6)\}$. La Proposition 6.8 montre alors que pour tout $\tau\in\mathcal{H}_2$, $\Psi(\gamma,4)^2\,\theta^4_{\Phi(\gamma,4)}(\tau)$ et $\Psi(\gamma,6)^2\,\theta^4_{\Phi(\gamma,6)}(\tau)$ sont les deux racines de

$$X^2-(a^2+c^2-b^2-d^2)X+(ac-bd)^2=0,$$

avec

$$(a,b,c,d)=\left(\Psi(\gamma,j)\,\theta^2_{\Phi(\gamma,j)}(\tau)\right)_{j\in[0,3]}=\left(\theta^2_{\Phi(\gamma,j)}(\tau)\right)_{j\in[0,3]}.$$

Si l'on fait tendre τ vers $\begin{pmatrix} i & 0\\ 0 & i\infty\end{pmatrix}$, alors pour tout $j\in\{1,3,4,6\}$, $\theta_j(\tau)$ tend vers $\vartheta_1(i)=\vartheta_2(i)\neq 0$, ce qui implique que les deux coefficients du polynôme ci-dessus tendent vers zéro, alors que le module de l'une des racines tend vers $|\vartheta_0(i)|^4=2\,|\vartheta_1(i)|^4\neq 0$, ce qui ne peut être.

Les cas $0\in\{\Phi(\gamma,8),\Phi(\gamma,9)\}$ et $0\in\{\Phi(\gamma,12),\Phi(\gamma,15)\}$ se traitent de manière similaire. □

Le Lemme 8.3 montre que si l'on écrit*

$$\mathcal{G}=\mathcal{G}_1\sqcup\mathcal{G}_2\sqcup\mathcal{G}_3$$

avec

$$\mathcal{G}_3=\{\gamma\in\mathcal{G}:\exists j\in[0,3]:\Phi(\gamma,j)>3\} \tag{8.2}$$

*Le symbole $\sqcup$ désignant l'union disjointe.

et $\mathcal{G}_2 = \mathcal{G} \setminus (\mathcal{G}_1 \cup \mathcal{G}_3)$, alors

$$\mathcal{G}_2 = \left\{\gamma \in \mathcal{G} : \Phi(\gamma, j) \leq 3 \text{ pour tout } j \in [0,3] \text{ et } \exists (k,\ell) \in [0,3]^2 \text{ t.q. } \Psi(\gamma,k) \neq \Psi(\gamma,\ell)\right\}. \tag{8.3}$$

Revenons maintenant aux ensembles T_n introduits dans la section précédente : par définition de Γ_b, pour tous $\gamma \in \Gamma_b$ et $\tau \in T_n$, on a $\gamma\tau \in T_n$, donc les ensembles $T_n \cap \mathcal{F}_b$ sont tous non-vides.

Pour la suite de la démonstration, nous fixons une suite $(\tau_n)_{n\in\mathbb{N}}$ telle que, pour tout $n \geqslant 1$, $\tau_n \in T_n \cap \mathcal{F}_b$.

8.2.3 Limite de la suite $(\lambda(\tau_n))_{n\in\mathbb{N}}$

Le but de cette section, la plus longue et la plus technique de la démonstration, est de montrer que

$$\lim_{n\to+\infty} \lambda(\tau_n) = +\infty.$$

Pour cela, nous commençons par introduire la fonction $D : \mathcal{H}_2 \to \mathbb{R}^+$ définie par

$$D(\tau) = \mathrm{Max}_{(j,k)\in[0,3]^2, j\neq k} \left(d\left(\theta_j^2(\tau), \theta_k^2(\tau)\right)\right)$$

pour tout $\tau \in \mathcal{H}_2$, avec

$$d(x,y) = \begin{cases} \mathrm{Arctan}\left(\left|\frac{y}{x} - 1\right|\right) & \text{si } x \neq 0 \\ \frac{\pi}{2} & \text{si } x = 0 \end{cases}.$$

Notons que la fonction D est continue sur $\mathcal{H}_2$, et que $D(\tau) = 0$ si et seulement si

$$\left[\theta_j^2(\tau)\right]_{j\in[0,3]} = [1:1:1:1].$$

En particulier, comme les quatre suites $(a_{j,n})_{n\in\mathbb{N}}$ convergent toutes vers la même limite $\mathcal{A}$ non nulle, on a

$$\lim_{n\to+\infty} D(\tau_n) = 0. \tag{8.4}$$

Les propriétés de convergence des theta constantes (Lemme 5.2) montrent qu'il existe une constante $B > 0$ telle que, pour tout $\tau \in \mathcal{F}_2$ vérifiant $\lambda(\tau) \geqslant B$, on ait

$$\left|\theta_j^2(\tau) - 1\right| \leqslant \frac{1}{10} \tag{8.5}$$

pour $j \in [0,3]$, et

$$\left|\theta_j^2(\tau)\right| \leqslant \frac{1}{10} \tag{8.6}$$

pour $j \geqslant 4$.

Nous introduisons maintenant les régions $\mathcal{F}_{2,B^+}$, $\mathcal{F}_{2,B^-}$ et $\mathcal{F}_{1,B^-}$ définies par

$$\mathcal{F}_{2,B^+} = \{\tau \in \mathcal{F}_2 : \lambda(\tau) > B\},$$

$$\mathcal{F}_{2,B^-} = \{\tau \in \mathcal{F}_2 : \lambda(\tau) \leqslant B\}$$

et

$$\mathcal{F}_{1,B^-} = \left\{\tau_1 \in \mathbb{C} : \exists(\tau_2,\tau_3) \in \mathbb{C}^2 \text{ t.q. } \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_{2,B^-}\right\}.$$

Notons dès à présent que $\mathcal{F}_{1,B^-}$ est inclus dans un compact lui-même inclus dans $\mathcal{F}$: le fait qu'il est inclus dans $\mathcal{F}$ est évident, et si $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_{2,B^-}$, alors $\lambda(\tau) \leqslant B$, donc (du fait que $\mathrm{Im}(\tau)$ est réduite au sens de Minkowski) $\mathrm{Im}(\tau_1) \leqslant 2B$.

Pour montrer que la suite $(\lambda(\tau_n))_{n\in\mathbb{N}}$ tend vers l'infini, nous allons commencer par montrer l'existence d'un indice $N_B \geqslant 0$ tel que, pour tout $n \geqslant N_B$,

$$\tau_n \in \bigcup_{\gamma\in\mathcal{G}_1} \gamma\mathcal{F}_{2,B^+}.$$

Nous en déduirons ensuite que nécessairement, pour $n \geqslant N_B$,

$$\lambda(\tau_n) \geqslant \left(\frac{3-\sqrt{5}}{2}\right)^2 B,$$

ce qui, quitte à augmenter B, montre que $(\lambda(\tau_n))_{n\in\mathbb{N}}$ tend bien vers l'infini.

Le Lemme 2.3 montre qu'il existe $\varepsilon_B > 0$ tel que, pour tous $t \in \mathcal{F}_{1,B^-}$, $(\omega,u,v) \in \{\pm i,\pm 1\}\times[0,3]\times[0,3]$ différent de $(1,1,2)$ et tel que $u<v$, l'inégalité suivante est vérifiée :

$$\left|\vartheta_u^2(t) - \omega\vartheta_v^2(t)\right| \geqslant \varepsilon_B. \tag{8.7}$$

Nous pouvons supposer que $\varepsilon_B \leqslant 1$ (le contraire serait en fait impossible), et appliquer le Lemme 6.2 pour montrer l'existence d'une constante $M>0$ (dépendant de ε_B) telle que pour tous $j\in[0,15]$ et $\tau = \begin{pmatrix}\tau_1 & \tau_3\\ \tau_3 & \tau_2\end{pmatrix} \in \mathcal{F}_{2,B^-}$ vérifiant $\mathrm{Im}(\tau_2) \geqslant M\mathrm{Im}(\tau_1)$,

$$\left|\theta_j^2(\tau) - \vartheta_{\rho(j)}^2(\tau_1)\right| \leqslant \frac{\varepsilon_B}{100}. \tag{8.8}$$

Nous fixons pour la suite un tel M, et définissons les régions

$$\mathcal{F}_{2,B^-,M^-} = \left\{\tau = \begin{pmatrix}\tau_1 & \tau_3\\ \tau_3 & \tau_2\end{pmatrix} \in \mathcal{F}_{2,B^-} : \mathrm{Im}(\tau_2) \leqslant M\mathrm{Im}(\tau_1)\right\} \tag{8.9}$$

et

$$\mathcal{F}_{2,B^-,M^+} = \left\{\tau = \begin{pmatrix}\tau_1 & \tau_3\\ \tau_3 & \tau_2\end{pmatrix} \in \mathcal{F}_{2,B^-} : \mathrm{Im}(\tau_2) > M\mathrm{Im}(\tau_1)\right\}. \tag{8.10}$$

Nous allons montrer l'existence d'une constante $\varepsilon>0$ (dépendant de B) telle que, pour tout $\tau \in \mathcal{F}_b \setminus \left(\bigcup_{\gamma\in\mathcal{G}_1}\gamma\mathcal{F}_{2,B^+}\right)$, $D(\tau)\geqslant\varepsilon$. Pour cela, nous distinguons les différents cas possibles.

Cas de $\bigcup_{\gamma\in\mathcal{G}}\gamma\mathcal{F}_{2,B^-,M^-}$

D'après sa définition, la région $\mathcal{F}_{2,B^-,M^-}$ est un compact de $\mathcal{F}_2$ donc, $\bigcup_{\gamma\in\mathcal{G}}\gamma\mathcal{F}_{2,B^-,M^-}$ est un compact de $\mathcal{H}_2$, et comme la fonction D est continue sur $\mathcal{H}_2$ et ne s'y annule pas, on en déduit l'existence d'une constante $\varepsilon_1>0$ telle que, pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}}\gamma\mathcal{F}_{2,B^-,M^-}$, $D(\tau)\geqslant\varepsilon_1$.

Cas de $\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^+}$

Soient $\tau\in\mathcal{F}_{2,B^+}$ et $\gamma\in\mathcal{G}_2$. Par définition de $\mathcal{G}_2$ (8.3), il existe $j\in[1,3]$ tel que $\Psi(\gamma,j)\in\{\pm i,-1\}$, et on a donc

$$\begin{aligned}
\left|\frac{\theta_j^2(\gamma\tau)}{\theta_0^2(\gamma\tau)}-1\right| &= \left|\Psi(\gamma,j)\,\frac{\theta^2_{\Phi(\gamma,j)}(\tau)}{\theta^2_{\Phi(\gamma,0)}(\tau)}-1\right| \\
&= \frac{1}{\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|}\left|\Psi(\gamma,j)\,\theta^2_{\Phi(\gamma,j)}(\tau)-\theta^2_{\Phi(\gamma,0)}(\tau)\right| \\
&\geqslant \frac{1}{\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|}\left(\left|\theta^2_{\Phi(\gamma,j)}(\tau)\right|\cdot|\Psi(\gamma,j)-1|-\left|\theta^2_{\Phi(\gamma,j)}(\tau)-\theta^2_{\Phi(\gamma,0)}(\tau)\right|\right) \\
&\geqslant \frac{1}{\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|}\left(\sqrt{2}\left|\theta^2_{\Phi(\gamma,j)}(\tau)\right|-\left|\theta^2_{\Phi(\gamma,j)}(\tau)-\theta^2_{\Phi(\gamma,0)}(\tau)\right|\right) \\
&\geqslant \frac{1}{\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|}\left(\sqrt{2}\left|\theta^2_{\Phi(\gamma,j)}(\tau)\right|-\left|\theta^2_{\Phi(\gamma,j)}(\tau)-1\right|-\left|\theta^2_{\Phi(\gamma,0)}(\tau)-1\right|\right)
\end{aligned}$$

et en utilisant (8.5), on obtient

$$\begin{aligned}
\left|\frac{\theta_j^2(\gamma\tau)}{\theta_0^2(\gamma\tau)}-1\right| &\geqslant \frac{10}{11}\left(\frac{9\sqrt{2}}{10}-\frac{2}{10}\right) \\
&\geqslant \frac{9\sqrt{2}-2}{11}.
\end{aligned}$$

En posant $\varepsilon_2=\operatorname{Arctan}\left(\frac{9\sqrt{2}-2}{11}\right)>0$, on a donc $D(\tau)\geqslant\varepsilon_2$ pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^+}$.

Cas de $\bigcup_{\gamma\in\mathcal{G}_3}\gamma\mathcal{F}_{2,B^+}$

Soient $\tau\in\mathcal{F}_{2,B^+}$ et $\gamma\in\mathcal{G}_3$. Par définition de $\mathcal{G}_3$ (8.2), il existe deux indices $j,k\in[0,3]$ tels que $\Phi(\gamma,j)\in[0,3]$ et $\Phi(\gamma,k)\geqslant 4$, et alors

$$\begin{aligned}
\left|\frac{\theta_k^2(\gamma\tau)}{\theta_j^2(\gamma\tau)}-1\right| &= \left|\frac{\theta^2_{\Phi(\gamma,k)}(\tau)}{\theta^2_{\Phi(\gamma,j)}(\tau)}-1\right| \\
&\geqslant 1-\left|\frac{\theta^2_{\Phi(\gamma,k)}(\tau)}{\theta^2_{\Phi(\gamma,j)}(\tau)}\right|,
\end{aligned}$$

et en utilisant (8.5) and (8.6), il vient

$$\left|\frac{\theta_k^2(\gamma\tau)}{\theta_j^2(\gamma\tau)}-1\right|\geqslant\frac{8}{9}.$$

En posant $\varepsilon_3=\operatorname{Arctan}\left(\frac{8}{9}\right)>0$, on a donc $D(\tau)\geqslant\varepsilon_3$ pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}_3}\gamma\mathcal{B}_{2,B^+}$.

Cas de $\bigcup_{\gamma\in\mathcal{G}_1}\gamma\mathcal{F}_{2,B^-,M^+}$

Soient $\tau\in\mathcal{F}_{2,B^-,M^+}$ et $\gamma\in\mathcal{G}_1$. D'après la définition de $\mathcal{G}_1$ (voir la Section 8.2.2), il existe $j,k\in[0,3]$ tels que $\Phi(\gamma,j)=0$ et $\Phi(\gamma,k)=1$, donc

$$\begin{aligned}\left|\frac{\theta_j^2(\gamma\tau)}{\theta_k^2(\gamma\tau)}-1\right| &= \left|\frac{\theta_0^2(\tau)}{\theta_1^2(\tau)}-1\right|\\ &= \frac{1}{\left|\theta_1^2(\tau)\right|}\left|\theta_0^2(\tau)-\vartheta_0^2(\tau_1)+\vartheta_0^2(\tau_1)-\vartheta_1^2(\tau_1)+\vartheta_1^2(\tau_1)-\theta_1^2(\tau)\right|\\ &\geqslant \frac{1}{\left|\theta_1^2(\tau)\right|}\left(\left|\vartheta_0^2(\tau_1)-\vartheta_1^2(\tau_1)\right|-\left|\theta_0^2(\tau)-\vartheta_0^2(\tau_1)\right|-\left|\theta_1^2(\tau)-\vartheta_1^2(\tau_1)\right|\right),\end{aligned}$$

et en utilisant (8.7) et (8.8), il vient

$$\left|\frac{\theta_j^2(\gamma\tau)}{\theta_k^2(\gamma\tau)}-1\right|\geqslant\frac{1}{\left|\theta_1^2(\tau)\right|}\frac{49\varepsilon_B}{50}.$$

La Proposition 6.1 implique par ailleurs que

$$\left|\theta_1^2(\tau)\right|\leqslant(1.405)^2\leqslant 2,$$

d'où

$$\left|\frac{\theta_j^2(\tau)}{\theta_k^2(\tau)}-1\right|\geqslant\frac{49\varepsilon_B}{100}.$$

Si l'on pose $\varepsilon_4=\operatorname{Arctan}\left(\frac{49\varepsilon_B}{100}\right)>0$, on a donc, pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}_1}\gamma\mathcal{F}_{2,B^-,M^+}$, $D(\tau)\geqslant\varepsilon_4$.

Cas de $\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^-,M^+}$

Soient $\tau\in\mathcal{F}_{2,B^-,M^+}$ et $\gamma\in\mathcal{G}_2$. D'après la définition de $\mathcal{G}_2$ (8.3), il existe un indice $j\in[1,3]$ tel que $\Psi(\gamma,j)\in\{\pm i,-1\}$, et d'après (8.8) et la définition de $\mathcal{F}_{2,B^-,M^+}$ (8.10), il existe $u,v\in\{0,1\}$ tels que

$$\left|\theta_{\Phi(\gamma,0)}^2(\tau)-\vartheta_u^2(\tau_1)\right|\leqslant\frac{\varepsilon_B}{100}\tag{8.11}$$

et

$$\left|\theta_{\Phi(\gamma,j)}^2(\tau)-\vartheta_v^2(\tau_1)\right|\leqslant\frac{\varepsilon_B}{100}.\tag{8.12}$$

On peut alors écrire

$$\begin{aligned}\left|\frac{\theta_j^2(\gamma\tau)}{\theta_0^2(\gamma\tau)}-1\right| &= \left|\Psi(\gamma,j)\frac{\theta_{\Phi(\gamma,j)}^2(\tau)}{\theta_{\Phi(\gamma,0)}^2(\tau)}-1\right|\\ &= \frac{1}{\left|\theta_{\Phi(\gamma,0)}^2(\tau)\right|}\left|\Psi(\gamma,j)\,\theta_{\Phi(\gamma,j)}^2(\tau)-\theta_{\Phi(\gamma,0)}^2(\tau)\right|\\ &= \frac{1}{\left|\theta_{\Phi(\gamma,0)}^2(\tau)\right|}\left|\Psi(\gamma,j)\left(\theta_{\Phi(\gamma,j)}^2(\tau)-\vartheta_v^2(\tau_1)\right)+\Psi(\gamma,j)\,\vartheta_v^2(\tau_1)-\vartheta_u^2(\tau_1)+\vartheta_u^2(\tau_1)-\theta_{\Phi(\gamma,0)}^2(\tau)\right|\\ &\geqslant \frac{1}{\left|\theta_{\Phi(\gamma,0)}^2(\tau)\right|}\left(\left|\Psi(\gamma,j)\,\vartheta_v^2(\tau_1)-\vartheta_u^2(\tau_1)\right|-\left|\theta_{\Phi(\gamma,j)}^2(\tau)-\vartheta_v^2(\tau_1)\right|-\left|\theta_{\Phi(\gamma,0)}^2(\tau)-\vartheta_u^2(\tau_1)\right|\right)\\ &\geqslant \frac{1}{\left|\theta_{\Phi(\gamma,0)}^2(\tau)\right|}\left(\left|\Psi(\gamma,j)\,\vartheta_v^2(\tau_1)-\vartheta_u^2(\tau_1)\right|-\frac{2\varepsilon_B}{100}\right),\end{aligned}$$

où l'on a utilisé (8.11) et (8.12) pour obtenir la dernière minoration. Par définition de ε_B (8.7), on a alors

$$\left|\Psi(\gamma,j)\,\vartheta_v^2(\tau_1)-\vartheta_u^2(\tau_1)\right|\geqslant\varepsilon_B$$

donc

$$\left|\frac{\theta_j^2(\gamma\tau)}{\theta_0^2(\gamma\tau)}-1\right|\geqslant\frac{1}{\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|}\frac{49\varepsilon_B}{50},$$

d'où, en utilisant la Proposition 6.1 comme plus haut :

$$\left|\theta^2_{\Phi(\gamma,0)}(\tau)\right|\leqslant(1.405)^2\leqslant 2,$$

et finalement

$$\left|\frac{\theta_j^2(\gamma\tau)}{\theta_0^2(\gamma\tau)}-1\right|\geqslant\frac{49\varepsilon_B}{100}.$$

Ceci prouve que pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^-,M^+}$, $D(\tau)\geqslant\varepsilon_4$.

Cas de $\bigcup_{\gamma\in\mathcal{G}_3}\gamma\mathcal{F}_{2,B^-,M^+}$

Soit $\gamma\in\mathcal{G}_3$, le Lemme 8.2 montre que l'on est nécessairement dans l'un des quatre cas suivants :

1. il existe $j,k\in[0,3]$ tels que $\Phi(\gamma,j)\in[0,3]$ et $\Phi(\gamma,k)\geqslant 8$;
2. il existe $j,k\in[0,3]$ tels que $(\Phi(\gamma,j),\Phi(\gamma,k))\in\{(0,1),(0,3),(1,2),(2,3)\}$;
3. $\{\Phi(\gamma,j)\}_{j\in[0,3]}=\{0,2,4,6\}$;
4. $\{\Phi(\gamma,j)\}_{j\in[0,3]}=\{1,3,4,6\}$.

Dans les cas 1 à 3, il existe $j,k\in[0,3]$ tels que

$$\rho(\Phi(\gamma,j))<\rho(\Phi(\gamma,k))$$

et

$$(\rho(\Phi(\gamma,j)),\rho(\Phi(\gamma,k)))\neq(1,2).$$

Dans le cas 4, on définit $j,\ell\in[0,3]$ par $\Phi(\gamma,j)=1$ et $\Phi(\gamma,\ell)=3$. Dans le cas où $\Psi(\gamma,j)=\Psi(\gamma,\ell)$, le Lemme 8.3 montre qu'il existe $k\in[0,3]$ tel que $\Phi(\gamma,k)\in\{4,6\}$ et $\Psi(\gamma,j)\neq\Psi(\gamma,k)$. En particulier, dans ce dernier cas, on a $\rho(\Phi(\gamma,j))=1$ et $\rho(\Phi(\gamma,k))=2$.

Soit maintenant $\tau\in\mathcal{F}_{2,B^-,M^+}$. D'après ce qui précède, soit on est dans le cas 4 et il existe $j,\ell\in[0,3]$ tels que $\Phi(\gamma,j)=1$, $\Phi(\gamma,\ell)=3$ et $\Psi(\gamma,j)\neq\Psi(\gamma,\ell)$, auquel cas le raisonnement utilisé plus haut pour traiter le cas de $\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^-,M^+}$ montre que $D(\gamma\tau)\geqslant\varepsilon_4$, soit il existe $j,k\in[0,3]$ tels que

$$\left(\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)},\rho(\Phi(\gamma,j)),\rho(\Phi(\gamma,k))\right)\in\{(x,y,z)\in\{\pm i,\pm 1\}\times[0,3]\times[0,3],y<z\}\setminus\{(1,1,2)\}.$$

D'après (8.11), (8.12) et la définition de $\mathcal{F}_{2,B^-,M^+}$ (8.10), on a

$$\left|\theta^2_{\Phi(\gamma,u)}(\tau)-\vartheta^2_{\rho(\Phi(\gamma,u))}(\tau_1)\right|\leqslant\frac{\varepsilon_B}{100}\tag{8.13}$$

pour $u\in\{j,k\}$.

Alors

$$\begin{aligned}
\left|\frac{\theta_j^2(\gamma\tau)}{\theta_k^2(\gamma\tau)}-1\right| &= \left|\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)}\frac{\theta^2_{\Phi(\gamma,j)}(\tau)}{\theta^2_{\Phi(\gamma,k)}(\tau)}-1\right| \\
&= \frac{1}{\left|\theta^2_{\Phi(\gamma,k)}(\tau)\right|}\left|\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)}\theta^2_{\Phi(\gamma,j)}(\tau)-\theta^2_{\Phi(\gamma,k)}(\tau)\right| \\
&= \frac{1}{\left|\theta^2_{\Phi(\gamma,k)}(\tau)\right|}\left|\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)}\left(\theta^2_{\Phi(\gamma,j)}(\tau)-\vartheta^2_{\rho(\Phi(\gamma,j))}(\tau_1)\right)+\right. \\
&\quad \left.\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)}\vartheta^2_{\rho(\Phi(\gamma,j))}(\tau_1)-\vartheta^2_{\rho(\Phi(\gamma,k))}(\tau_1)+\vartheta^2_{\rho(\Phi(\gamma,k))}(\tau_1)-\theta^2_{\Phi(\gamma,k)}(\tau)\right| \\
&\geqslant \frac{1}{\left|\theta^2_{\Phi(\gamma,k)}(\tau)\right|}\left(\left|\frac{\Psi(\gamma,j)}{\Psi(\gamma,k)}\vartheta^2_{\rho(\Phi(\gamma,j))}(\tau_1)-\vartheta^2_{\rho(\Phi(\gamma,k))}(\tau_1)\right|-\frac{\varepsilon_B}{50}\right),
\end{aligned}$$

où l'on a utilisé (8.13) pour obtenir la dernière minoration.

Nous avons déjà vu que

$$\left|\theta^2_{\Phi(\gamma,j)}(\tau)\right|\leqslant 2,$$

et par définition de ε_B (8.7) on a

$$\left|\frac{\Psi(\gamma,k)}{\Psi(\gamma,j)}\vartheta^2_{\rho(\Phi(\gamma,j))}(\tau_1)-\vartheta^2_{\rho(\Phi(\gamma,k))}(\tau_1)\right|\geqslant\varepsilon_B,$$

d'où

$$\left|\frac{\theta_k^2(\gamma\tau)}{\theta_j^2(\gamma\tau)}-1\right|\geqslant\frac{49\varepsilon_B}{100},$$

ce qui montre que là aussi $D(\gamma\tau)\geqslant\varepsilon_4$.

On a donc montré que pour tout $\tau\in\bigcup_{\gamma\in\mathcal{G}_2}\gamma\mathcal{F}_{2,B^-,M^+}$, $D(\tau)\geqslant\varepsilon_4$.

Si l'on pose finalement $\varepsilon=\mathrm{Min}_{u\in[1,4]}(\varepsilon_u)>0$, alors dans tous les cas on a montré que pour tout $\tau\in\left(\bigcup_{\gamma\in\mathcal{G}}\gamma\mathcal{F}_2\right)\setminus\left(\bigcup_{\gamma\in\mathcal{G}_1}\gamma\mathcal{F}_{2,B^+}\right)$, $D(\tau)\geqslant\varepsilon$.

En particulier, comme $\lim_{n\to+\infty}D(\tau_n)=0$, ceci montre bien que pour tout $B>0$, il existe $N_B\geqslant 0$ tel que

$$(n\geqslant N_B)\Rightarrow\left(\tau_n\in\bigcup_{\gamma\in\mathcal{G}_1}\gamma\mathcal{F}_{2,B^+}\right).$$

Pour en déduire la limite de $(\lambda(\tau_n))_{n\in\mathbb{N}}$, nous allons utiliser le résultat suivant :

Lemme 8.4 *Pour tout $\tau\in\mathcal{H}_2$,*

$$\lambda(\mathfrak{T}\tau)\geqslant\frac{3-\sqrt{5}}{2}\lambda(\tau).$$

Démonstration : Soit $\tau\in\mathcal{H}_2$, alors par définition de $\lambda(\tau)$, on a

$$\lambda(\tau)=\mathrm{Min}_{v\in\mathbb{R}^2\setminus\{0\}}\frac{{}^tv\mathrm{Im}(\tau)v}{\|v\|_2^2}.$$

Comme $\mathfrak{T}\tau = {}^tT\tau T$, on a aussi

$$\begin{aligned}
\lambda(\mathfrak{T}\tau) &= \mathrm{Min}_{v\in\mathbb{R}^2\setminus\{0\}} \frac{{}^t(Tv)\mathrm{Im}(\tau)(Tv)}{\|v\|_2^2} \\
&\geqslant \left(\mathrm{Min}_{v\in\mathbb{R}^2\setminus\{0\}} \frac{{}^t(Tv)\mathrm{Im}(\tau)(Tv)}{\|Tv\|_2^2}\right)\left(\mathrm{Min}_{v\in\mathbb{R}^2\setminus\{0\}} \frac{\|Tv\|_2^2}{\|v\|_2^2}\right) \\
&\geqslant \lambda(\tau)\mathrm{Min}_{v\in\mathbb{R}^2,\|v\|^2=1}\|Tv\|_2^2 \\
&\geqslant \lambda(\tau)\mathrm{Min}_{\alpha\in\mathbb{R}}\left((\sin\alpha+\cos\alpha)^2+\sin^2\alpha\right) \\
&\geqslant \lambda(\tau)\mathrm{Min}_{\alpha\in\mathbb{R}}\left(1+\sin\alpha(\sin\alpha+2\cos\alpha)\right).
\end{aligned}$$

On peut alors étudier la fonction $f(\alpha) = \sin\alpha(\sin\alpha + 2\cos\alpha)$: elle est 2-périodique, et sa dérivée est

$$\begin{aligned}
f'(\alpha) &= 2(\cos\alpha\sin\alpha + \cos^2\alpha - \sin^2\alpha) \\
&= \sin 2\alpha + 2\cos 2\alpha.
\end{aligned}$$

La fonction f est donc minimale en $\alpha = -\frac{\mathrm{Arctan}(2)}{2}$, et $f(\alpha) = \frac{3-\sqrt{5}}{2}$, d'où le résultat. □

Il est facile de voir que pour tout $\tau \in \mathcal{H}_2$, $\lambda(\mathfrak{S}\tau) = \lambda(\tau)$, $\lambda(\mathfrak{M}_1\tau) = \lambda(\tau)$ et $\lambda(\mathfrak{M}_2\tau) = \lambda(\tau)$, donc, en utilisant le Lemme 8.4 ainsi que la définition de $\mathcal{G}_1$ (voir la Section 8.2.2), on montre que pour tous $\tau \in \mathcal{H}_2$ et $\gamma \in \mathcal{G}_1$, $\lambda(\gamma\tau) \geqslant \left(\frac{3-\sqrt{5}}{2}\right)^2 \lambda(\tau)$.

On en déduit que pour tout $B > 0$, si $N_B \geqslant 0$ est défini comme précédemment, alors

$$(n \geqslant N_B) \Rightarrow \left(\lambda(\tau_n) \geqslant \left(\frac{3-\sqrt{5}}{2}\right)^2 B\right),$$

ce qui montre bien finalement que

$$\lim_{n\to+\infty} \lambda(\tau_n) = +\infty.$$

8.2.4 Conclusion de la démonstration

D'après le Lemme 5.2, il existe $C > 0$ tel que pour tout $\tau \in \mathcal{H}_2$ vérifiant $\lambda(\tau) \geqslant C$ et pour tout $j \in [0,3]$,

$$|\theta_j(\tau) - 1| \leqslant \frac{1}{10}. \tag{8.14}$$

D'après la section précédente et la convergence des quatre suites $(a_{j,n})_{n\in\mathbb{N}}$ vers $\mathcal{A}$, il existe $N_C \geqslant 0$ tel que pour tout $n \geqslant N_C$,

$$|a_{j,n} - \mathcal{A}| \leqslant \frac{|\mathcal{A}|}{10}$$

et $\lambda(\tau_{N_C}) \geqslant C$.

On a alors

$$\begin{aligned}\left|\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}-\mathcal{A}\right| &= \frac{1}{\left|\theta_0^2(\tau_{N_C})\right|}\left|a_{0,N_C}-\mathcal{A}+\mathcal{A}\left(1-\theta_0^2(\tau_{N_C})\right)\right| \\ &\leqslant \frac{1}{\left|\theta_0^2(\tau_{N_C})\right|}\left(\left|a_{0,N_C}-\mathcal{A}\right|+\left|\mathcal{A}\right|\cdot\left|1-\theta_0^2(\tau_{N_C})\right|\right) \\ &\leqslant \frac{1}{1-\frac{1}{10}}\left(\frac{|\mathcal{A}|}{10}+\frac{|\mathcal{A}|}{10}\right) \\ &\leqslant \frac{2}{9}\left|\mathcal{A}\right|,\end{aligned}$$

donc en particulier

$$\left|\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right|\leqslant\frac{11}{9}\left|\mathcal{A}\right|. \tag{8.15}$$

D'après la démonstration du Lemme 8.1, on sait qu'il existe *a priori* huit possibilités pour le triplet $(a_{1,N_C+1},a_{2,N_C+1},a_{3,N_C+1})$: on a

$$\begin{aligned}a_{1,N_C+1} &= \frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\frac{\varepsilon_{1,1}\theta_0(\tau_{N_C})\theta_1(\tau_{N_C})+\varepsilon_{1,2}\theta_2(\tau_{N_C})\theta_3(\tau_{N_C})}{2}, \\ a_{2,N_C+1} &= \frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\frac{\varepsilon_{2,1}\theta_0(\tau_{N_C})\theta_2(\tau_{N_C})+\varepsilon_{2,2}\theta_1(\tau_{N_C})\theta_3(\tau_{N_C})}{2}, \\ a_{3,N_C+1} &= \frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\frac{\varepsilon_{3,1}\theta_0(\tau_{N_C})\theta_3(\tau_{N_C})+\varepsilon_{3,2}\theta_1(\tau_{N_C})\theta_2(\tau_{N_C})}{2},\end{aligned}$$

les huit valeurs possibles du 6-uplet $(\varepsilon_{1,1},\varepsilon_{1,2},\varepsilon_{2,1},\varepsilon_{2,2},\varepsilon_{3,1},\varepsilon_{3,2})$ étant

1. $(-1,+1,-1,+1,-1,+1)$;
2. $(-1,+1,+1,-1,+1,-1)$;
3. $(+1,-1,-1,+1,+1,-1)$;
4. $(+1,-1,+1,-1,-1,+1)$;
5. $(+1,+1,-1,-1,-1,-1)$;
6. $(-1,-1,+1,+1,-1,-1)$;
7. $(-1,-1,-1,-1,+1,+1)$;
8. $(+1,+1,+1,+1,+1,+1)$.

Dans les cas 1 à 4, (8.14) montre directement que

$$|a_{1,N_C+1}|\leqslant\frac{3}{10}\left|\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right|,$$

et d'après (8.15) on a

$$|a_{1,N_C+1}|\leqslant\frac{11}{30}\left|\mathcal{A}\right|,$$

ce qui est en contradiction avec le fait que, par hypothèse,

$$|a_{1,N_C+1}-\mathcal{A}|\leqslant\frac{1}{10}.$$

Dans le cas 5, (8.14) implique que

$$\left|a_{2,N_C+1}+\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right|\leqslant\frac{3}{10}\left|\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right|,$$

et d'après (8.15) on a

$$\begin{aligned} |a_{2,N_C+1}+\mathcal{A}| &\leqslant \left|a_{2,N_C+1}+\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right|+\left|\mathcal{A}-\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\right| \\ &\leqslant \left(\frac{11}{30}+\frac{1}{10}\right)|\mathcal{A}| \\ &\leqslant \frac{7}{15}\,|\mathcal{A}|\,, \end{aligned}$$

ce qui est en contradiction avec le fait que, par hypothèse,

$$|a_{2,N_C+1}-\mathcal{A}| \leqslant \frac{1}{10}.$$

Les cas 6 et 7 se traitent de façon similaire au cas 5, en considérant (par exemple) la valeur de a_{1,N_C+1} qui, dans les deux cas, sera trop proche de $-\mathcal{A}$ pour vérifier

$$|a_{1,N_C+1}-\mathcal{A}| \leqslant \frac{|\mathcal{A}|}{10}.$$

Ceci montre que le cas 8 est le seul possible, donc que

$$(a_{j,N_C+n})_{j\in[0,3]} = \left(\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\theta_j^2(2\tau_{N_C})\right)_{j\in[0,3]}.$$

Bien sûr, on a $\lambda(2\tau_{N_C}) = 2\lambda(\tau_{N_C}) \geqslant C$, et donc par une récurrence directe on montre que pour tout $n \geqslant 0$,

$$(a_{j,N_C+n})_{j\in[0,3]} = \left(\frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}\theta_j^2(2^n\tau_{N_C})\right)_{j\in[0,3]},$$

et le Lemme 5.2 permet d'en déduire que

$$\mathcal{A} = \frac{a_{0,N_C}}{\theta_0^2(\tau_{N_C})}.$$

La conclusion de la démonstration repose entièrement sur le résultat suivant :

Lemme 8.5 *Soient $\tau \in \mathcal{H}_2$ et $(a,b,c,d) \in \mathbb{C}^4$ tels qu'il existe une itération de Borchardt allant de (a,b,c,d) à $\left(\theta_j^2(\tau)\right)_{j\in[0,3]}$. Alors*

$$(a,b,c,d) \in \left\{\left(\theta_j^2\left(\frac{\tau+C_k}{2}\right)\right)_{j\in[0,3]} : k\in[0,7]\right\},$$

où les matrices C_k sont définies dans le Lemme 8.1.

Démonstration : Soient $\tau \in \mathcal{H}_2$ et $(x,y,z,t) \in \mathbb{C}^4$ tels que

$$\begin{aligned} x^2+y^2+z^2+t^2 &= 4\theta_0^2(\tau), \\ xy+zt &= 2\theta_1^2(\tau), \\ xz+yt &= 2\theta_2^2(\tau), \\ xt+yz &= 2\theta_3^2(\tau). \end{aligned}$$

La formule de duplication des theta constantes (Proposition 5.5) montre que

$$\begin{aligned}(x+y+z+t)^2 &= 16\theta_0^2(2\tau),\\ (x-y+z-t)^2 &= 16\theta_4^2(2\tau),\\ (x+y-z-t)^2 &= 16\theta_8^2(2\tau),\\ (x-y-z+t)^2 &= 16\theta_{12}^2(2\tau),\end{aligned}$$

donc qu'il existe $(\varepsilon_{4j})_{j\in[0,3]} \in \{\pm 1\}^4$ tel que

$$\begin{aligned}x+y+z+t &= 4\varepsilon_0\theta_0(2\tau),\\ x-y+z-t &= 4\varepsilon_4\theta_4(2\tau),\\ x+y-z-t &= 4\varepsilon_8\theta_8(2\tau),\\ x-y-z+t &= 4\varepsilon_{12}\theta_{12}(2\tau),\end{aligned}$$

et

$$\begin{aligned}x &= \varepsilon_0\theta_0(2\tau)+\varepsilon_4\theta_4(2\tau)+\varepsilon_8\theta_8(2\tau)+\varepsilon_{12}\theta_{12}(2\tau),\\ y &= \varepsilon_0\theta_0(2\tau)-\varepsilon_4\theta_4(2\tau)+\varepsilon_8\theta_8(2\tau)-\varepsilon_{12}\theta_{12}(2\tau),\\ z &= \varepsilon_0\theta_0(2\tau)+\varepsilon_4\theta_4(2\tau)-\varepsilon_8\theta_8(2\tau)-\varepsilon_{12}\theta_{12}(2\tau),\\ t &= \varepsilon_0\theta_0(2\tau)-\varepsilon_4\theta_4(2\tau)-\varepsilon_8\theta_8(2\tau)+\varepsilon_{12}\theta_{12}(2\tau).\end{aligned}$$

Supposons maintenant que $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,1,-1,1)$ par exemple, alors la Proposition 5.6 montre que

$$\begin{aligned}x^2 &= (\theta_0(2\tau)+\theta_4(2\tau)-\theta_8(2\tau)+\theta_{12}(2\tau))^2\\ &= \theta_0^2(\tau)+\theta_6^2(\tau)-\theta_9^2(\tau)+\theta_{15}^2(\tau),\end{aligned}$$

et la formule de transformation des theta constantes sous l'action de Γ_2 (Proposition 5.4) montre que

$$\begin{aligned}x^2 &= \theta_0^2(\mathfrak{M}_2^2\mathfrak{M}_1\tau)+\theta_4^2(\mathfrak{M}_2^2\mathfrak{M}_1\tau)+\theta_8^2(\mathfrak{M}_2^2\mathfrak{M}_1\tau)+\theta_{12}^2(\mathfrak{M}_2^2\mathfrak{M}_1\tau)\\ &= \theta_0^2(\tau+C_6)+\theta_4^2(\tau+C_6)+\theta_8^2(\tau+C_6)+\theta_{12}^2(\tau+C_6).\end{aligned}$$

Une seconde application de la Proposition 5.6 implique

$$x^2 = \theta_0^2\left(\frac{\tau+C_6}{2}\right),$$

et la même méthode permet aussi de montrer que

$$\begin{aligned}y^2 &= \theta_1^2\left(\frac{\tau+C_6}{2}\right),\\ z^2 &= \theta_2^2\left(\frac{\tau+C_6}{2}\right),\\ t^2 &= \theta_3^2\left(\frac{\tau+C_6}{2}\right).\end{aligned}$$

En utilisant cette technique, on vérifie facilement que
– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,1,1,1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_0}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,-1,1,-1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_1}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,1,-1,-1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_2}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,-1,-1,1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_3}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,1,1,-1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_4}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,-1,1,1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_5}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,1,-1,1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_6}{2}\right)\right)_{j\in[0,3]};$$

– si $(\varepsilon_{4j})_{j\in[0,3]} = \pm(1,-1,-1,-1)$, alors

$$(x^2,y^2,z^2,t^2) = \left(\theta_j^2\left(\frac{\tau+C_7}{2}\right)\right)_{j\in[0,3]};$$

ce qui termine la démonstration. □

Une récurrence directe utilisant ce lemme permet de montrer l'existence d'un élément $\tau_0' \in \mathcal{H}_2$ tel que

$$(a_{j,0})_{j\in[0,3]} = \left(\mathcal{A}\theta_j^2(\tau_0')\right)_{j\in[0,3]}.$$

Si $\ell \in [0,3]$ est tel que $\theta_\ell(\tau_0) \neq 0$, on a alors

$$\mathcal{A} = \frac{\theta_\ell^2(\tau_0')}{\theta_\ell^2(\tau_0)}$$

avec

$$\left[\theta_j^2(\tau_0)\right]_{j\in[0,3]} = \left[\theta_0^2(\tau_0')\right]_{j\in[0,3]}.$$

La Proposition 6.9 montre alors qu'il existe $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_b$ tel que $\tau_0' = \gamma\tau_0$, et la Proposition 5.4 permet finalement d'obtenir

$$\mathcal{A} = \frac{\theta_\ell^2(\tau_0)}{\theta_\ell^2(\gamma\tau_0)} = \frac{1}{\kappa(\gamma)\mathrm{Det}(C\tau_0+D)} \in \mathcal{L}(\tau_0),$$

ce qui conclut la démonstration du Théorème 8.1.

8.3 Quelques remarques

8.3.1 Généralisation au genre supérieur

Nous avons présenté le Théorème 8.1 comme une généralisation du Théorème 3.1 au genre 2. On peut alors se demander dans quelle mesure ce résultat peut être généraliser au genre supérieur. Le Théorème 5.1 apporte une première réponse : en genre $g \geqslant 3$, les $2^g - 1$ fonctions $\frac{\theta_{0,b}^2}{\theta_{0,0}^2}$ ne sont pas algébriquement indépendantes, donc si l'on se donne un 2^g-uplet $(a_b)_{b\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, il n'existe en général aucun $\tau \in \mathcal{H}_g$ tel que

$$[a_b]_{b\in\mathcal{I}_g} = \left[\theta_{0,b}^2(\tau)\right]_{b\in\mathcal{I}_g}.$$

Même si l'on fixe un élément $\tau \in \mathcal{H}_g$ et que l'on pose

$$a_b^{(0)} = \theta_{0,b}^2(\tau)$$

pour $b \in \mathcal{I}_g$, étudier les limites des suites de Borchardt associées à $\left(a_b^{(0)}\right)_{b\in\mathcal{I}_g}$ ne peut se faire avec les techniques utilisées dans ce chapitre : en particulier, les Lemmes 8.1 et 8.5 ne peuvent être généralisés.

Une généralisation possible consisterait à considérer des itérations de Borchardt modifiées. En effet, nous avons vu plus haut que pour $\tau \in \mathcal{H}_g$, les quantités $\left(\theta_{0,b}^2(\tau)\right)_{b\in\mathcal{I}_g}$ sont liées algébriquement. En particulier, il existe un nombre fini de relations algébriques $(R_j)_{j\in J_g}$ engendrant l'idéal des relations algébriques vérifiées par les $\theta_{0,b}^2$. On peut alors poser $\left(a_v^{(0)}\right)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ vérifiant les relations R_j, et définir récursivement les itérés de Borchardt modifiées comme étant ceux parmi les itérés de Borchardt qui vérifient ces relations R_j. On peut alors penser que si l'on considère ces itérations modifiées, le Théorème 8.1 peut se généraliser au genre supérieur. Le principal problème pratique est que l'on ne connaît pas explicitement ces relations R_j : une méthode pour les calculer consisterait à évaluer numériquement les valeurs des $\theta_{0,b}^2(\tau)$ pour un $\tau \in \mathcal{H}_g$ fixé, puis d'utiliser l'algorithme LLL pour en déduire les relations algébriques (il faudrait ensuite démontrer que ces relations sont bien exactes, par un autre moyen).

8.3.2 Domaine fondamental adapté à la fonction B_2

Notons que dans ce chapitre, nous n'avons pas généralisé au genre 2 tous les résultats connus concernant l'AGM, et en particulier la Propriété 3.2. Il est possible de définir l'ensemble[†]

$$\left\{\tau \in \mathcal{H}_2 : B_2\left(b_1(\tau), b_2(\tau), b_3(\tau)\right) = \frac{1}{\theta_0^2(\tau)}\right\}.$$

Le Théorème 8.1 montre que cet ensemble contient nécessairement un domaine fondamental pour l'action de Γ_b sur $\mathcal{H}_2$. Il serait intéressant de savoir déterminer cet ensemble par un nombre *fini* de conditions sur ses éléments (de la même façon qu'en genre 1 on sait déterminer $\mathcal{F}_{k'}$).

[†]Sous cette forme, cet ensemble est mal défini car θ_0 s'annule en certains points de $\mathcal{H}_2$; il serait plus correct de considérer une fonction B_2 de quatre variables (et de travailler en coordonnées projectives), mais la différence est cosmétique.

Chapitre 9

Matrices de Riemann de courbes hyperelliptiques

Le but de ce chapitre est de donner des algorithmes pour calculer, étant donnée une courbe hyperelliptique, la *matrice de Riemann* qui lui est associée. Ceci peut être utilisé pour calculer explicitement des isogénies entre courbes de genre 2 [vW00], pour démontrer qu'une courbe de genre 2 a multiplication complexe par un corps CM donné [vW99a, vW99b], et nous verrons dans le Chapitre 10 une application au calcul de polynômes modulaires en genre 2.

Nous commençons, dans la Section 9.1, par donner quelques définitions et propriétés concernant les courbes hyperelliptiques sur les complexes et leurs matrices de Riemann associées. Ensuite, dans la Section 9.2, nous donnons différents algorithmes permettant de calculer ces matrices, dont des algorithmes quasi-optimaux utilisant la moyenne de Borchardt. Nous nous concentrons plus particulièrement sur le cas du genre 2, en décrivant rapidement dans quelle mesure les algorithmes que nous présentons peuvent être généralisés au genre supérieur.

9.1 Courbes hyperelliptiques sur $\mathbb{C}$

Nous avons choisi, dans ce mémoire, de ne pas (ou très peu) parler de *courbes*. Le présent chapitre fait exception, puisqu'il présente un certain nombre d'algorithmes permettant de calculer des objets associés à des courbes de genre 2.

Dans cette section, nous donnons quelques résultats sur les courbes hyperelliptiques de genre g quelconque définies sur $\mathbb{C}$. En particulier, nous montrons comment à une telle courbe peut être associée un élément de $\mathcal{H}_g$ que l'on appelle la matrice de Riemann associée à la courbe. Nous définissons aussi un certain nombre d'invariants qui peuvent être associés à des (classes de) courbes (en genre 2 cette fois-ci).

Dans le reste de cette section, nous fixons un entier $g \geqslant 1$ et nous nous intéressons aux courbes hyperelliptiques de genre g.

9.1.1 Matrice de Riemann associée à une courbe hyperelliptique

La construction que nous résumons dans cette section est décrite en détail dans [Mum84a, pages 135–145] et dans [Mum84b, pages 75–94]. Nous n'en rappelons ici que les grands traits, en omettant toutes les démonstrations.

Soit $\mathcal{C}$ une courbe hyperelliptique de genre g définie sur $\mathbb{C}$. Une telle courbe admet une

équation de la forme

$$\mathcal{C} : y^2 = f(x) = \prod_{j=0}^{2g+1} (x - e_j),$$

où les racines $(e_j)_{j\in[0,2g+1]}$ du polynôme f sont deux à deux distinctes, et où les segments $[e_{2j}, e_{2j+1}]$ (pour $j \in [0, g]$) ne se coupent pas.

Si l'on considère l'ouvert

$$U = \mathbb{C} \setminus \left(\bigcup_{j\in[0,g]} [e_{2j}, e_{2j+1}] \right)$$

de $\mathbb{P}^1(\mathbb{C})$, alors il existe une fonction $z \mapsto g(z)$, holomorphe sur U, telle que pour tout $z \in U$, $g^2(z) = f(z)$. Cette fonction g peut être vue comme *une* détermination possible de la racine carrée de f. La courbe $\mathcal{C}$ peut alors être considérée comme une surface de Riemann (à g trous), en procédant comme suit :

- on part de deux copies U_1 et U_2 de U (chacune vue comme une sphère dans laquelle on a découpé $g + 1$ "fentes" suivant les segments $[e_{2j}, e_{2j+1}]$), correspondant l'une à la partie $y = g(x)$ et l'autre à la partie $y = -g(x)$ de la courbe ;
- chaque bord d'une fente $[e_{2j}, e_{2j+1}]$ de U_1 est alors "recollé" au bord correspondant (en termes de détermination de racine) de la fente correspondante de U_2 : on obtient deux sphères reliées entre elles par $g + 1$ "tubes", soit en fait un tore à g trous.

Cette construction est illustrée par les Figures 9.1 et 9.2.

On peut alors définir des chemins $(A_j)_{j\in[1,g]}$ et $(B_j)_{j\in[1,g]}$ comme illustré dans le cas où $g = 2$ par la Figure 9.2, ces chemins formant une base du groupe d'homologie de la surface de Riemann de la courbe, puisque A_j n'intersecte B_k que si $j = k$, les A_j (resp. les B_k) ne s'intersectant pas entre eux.

La Figure 9.3 permet sans doute de mieux visualiser le tore à deux trous et la base d'homologie associée (toujours dans le cas où $g = 2$).

Par ailleurs, l'ensemble

$$\left\{ \frac{x^j dx}{y} : j \in [0, g-1] \right\}$$

forme une base des formes différentielles de première espèce sur $\mathcal{C}$, et les matrices

$$\Omega_0 = \left(\int_{A_j} \frac{x^{k-1} dx}{y} \right)_{j,k\in[1,g]}$$

et

$$\Omega_1 = \left(\int_{B_j} \frac{x^{k-1} dx}{y} \right)_{j,k\in[1,g]}$$

sont appelées *matrices des périodes* de $\mathcal{C}$. Ces matrices ne sont qu'un choix possible, puisqu'elles dépendent des choix fait d'une part pour les (A_j) et (B_k), d'autre part du choix de la base pour les formes différentielles de première espèce. Les intégrales apparaissant dans ces matrices des périodes sont des *intégrales hyperelliptiques*.

Si l'on pose $\tau = \Omega_0^{-1}.\Omega_1$, alors $\tau \in \mathcal{H}_g$, et on dit que τ est une *matrice de Riemann* associée à $\mathcal{C}$. On notera que cette matrice de Riemann dépend encore du choix des (A_j) et (B_k), mais plus de la base des formes différentielles.

On note L_τ le réseau $L_\tau = \mathbb{Z}^g \oplus \tau\mathbb{Z}^g$. Ce réseau L_τ est lié à la jacobienne $\mathrm{Jac}(\mathcal{C})$ de $\mathcal{C}$ par le résultat suivant :

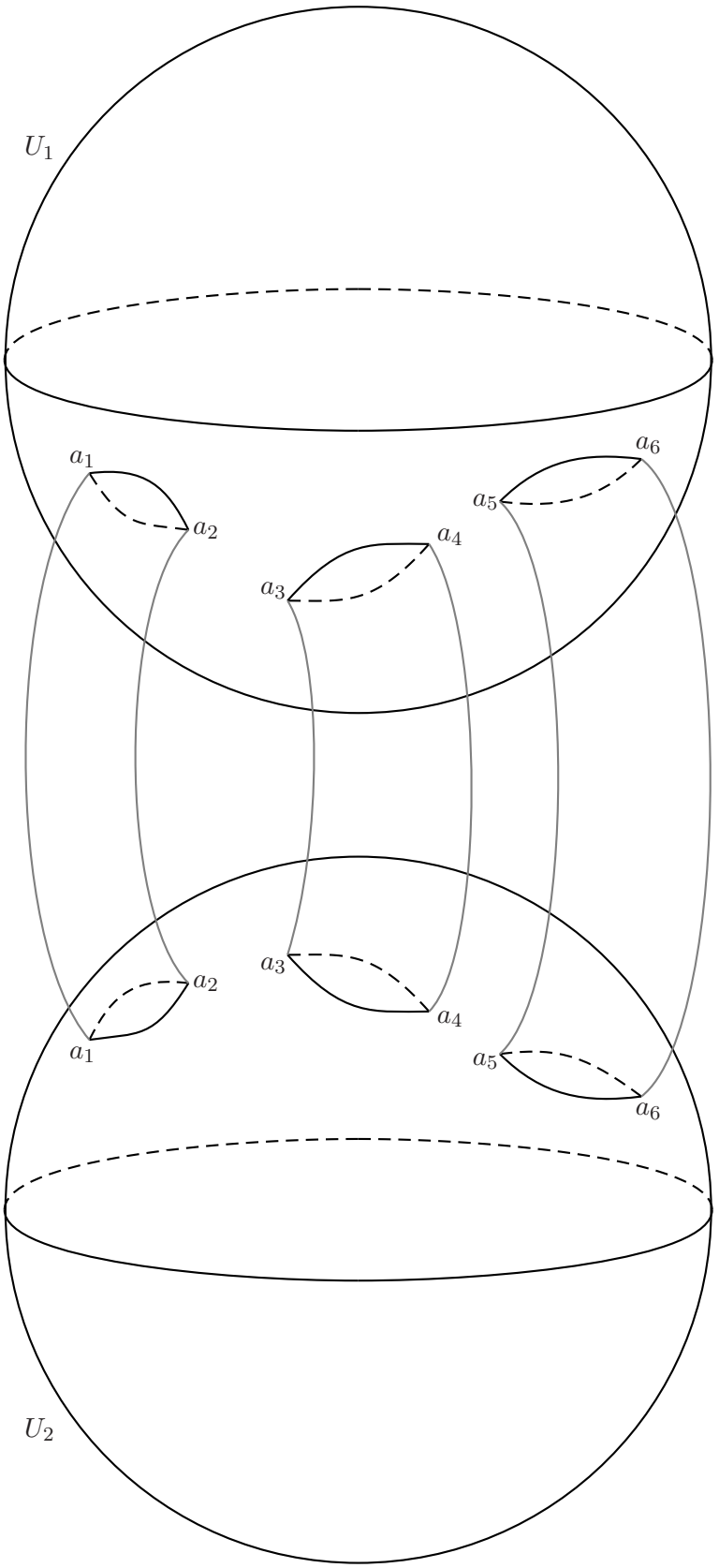

FIG. 9.1 – Construction de la surface de Riemann associée à $\mathcal{C} : y^2 = \prod_{j=1}^{6}(x - a_j)$

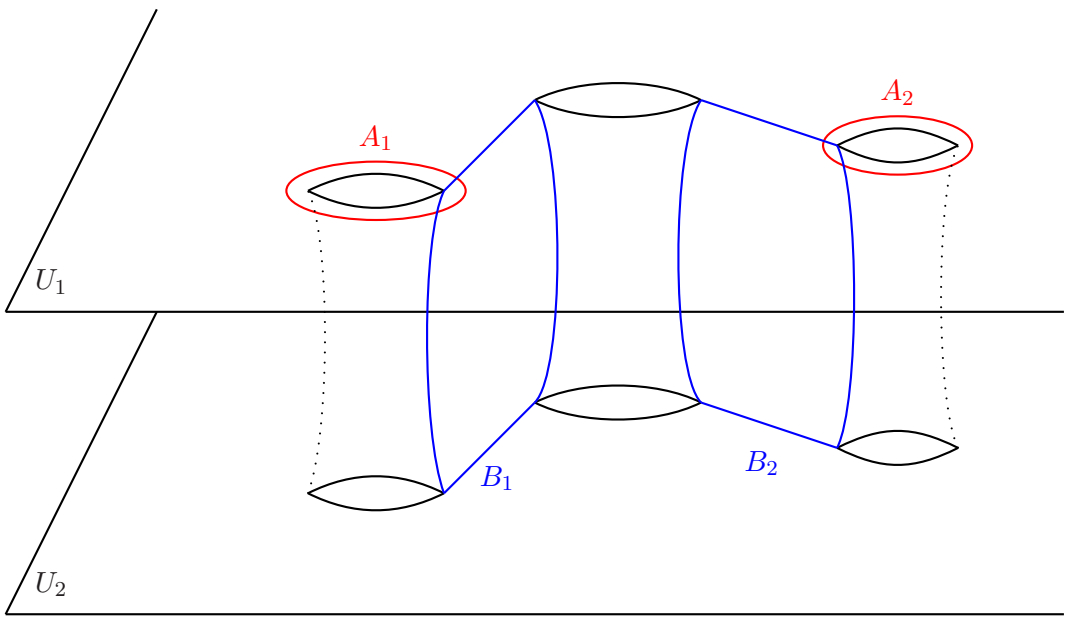

FIG. 9.2 – Surface de Riemann associée à la courbe $y^2 = f(x)$: un tore à $g = 2$ trous

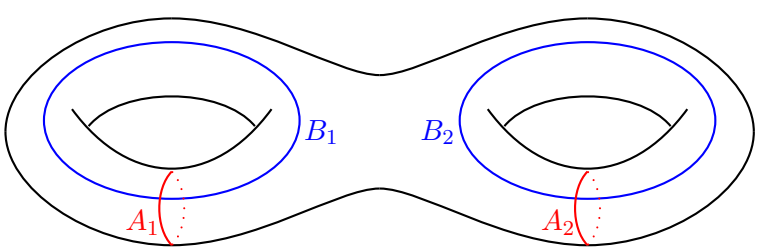

FIG. 9.3 – Une base du premier groupe d'homologie sur un tore à deux trous

Théorème 9.1 (Abel–Jacobi) *Le tore $\mathbb{C}^g/L_\tau$ est isomorphe à $\mathrm{Jac}(\mathcal{C})$, l'isomorphisme correspondant étant donné par*

$$\begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) & \to & \mathbb{C}^g/L_\tau \\ P_1+...+P_j-jP_{e_0} & \mapsto & \left(\sum_{k=1}^{j}\int_{e_0}^{P_k}\omega\right) \bmod L_\tau, \end{array}$$

où l'on a noté P_{e_0} le point de $\mathcal{C}$ de coordonnées affines $(e_0,0)$, et

$$\omega = \begin{pmatrix} \frac{dx}{y} \\ \vdots \\ \frac{x^{g-1}dx}{y} \end{pmatrix}.$$

Le tore (à g trous) $\mathbb{C}^g/L_\tau$ est souvent appelé *jacobienne analytique* de la courbe $\mathcal{C}$.

Le théorème ci-dessus montre que si deux courbes $\mathcal{C}_1$ et $\mathcal{C}_2$ ont leurs jacobiennes isomorphes, et que l'on désigne par τ_1 (resp. par τ_2) une matrice de Riemann associée à $\mathcal{C}_1$ (resp. à $\mathcal{C}_2$), alors les réseaux L_{τ_1} et L_{τ_2} sont isomorphes, et les matrices τ_1 et τ_2 sont équivalentes modulo l'action du groupe Γ_g.

Dans le cas du genre 2, si toutes les racines e_j sont réelles et si de plus

$$e_0 < e_1 < e_2 < e_3 < e_4 < e_5,$$

alors on peut prendre

$$\Omega_0 = 2i \begin{pmatrix} -\int_{e_2}^{e_3}\frac{dx}{\sqrt{-f(x)}} & \int_{e_4}^{e_5}\frac{dx}{\sqrt{-f(x)}} \\ -\int_{e_2}^{e_3}\frac{xdx}{\sqrt{-f(x)}} & \int_{e_4}^{e_5}\frac{xdx}{\sqrt{-f(x)}} \end{pmatrix}$$

et

$$\Omega_1 = 2 \begin{pmatrix} \int_{e_1}^{e_2}\frac{dx}{\sqrt{f(x)}} & \left(\int_{e_1}^{e_2}\frac{dx}{\sqrt{f(x)}} - \int_{e_3}^{e_4}\frac{dx}{\sqrt{f(x)}}\right) \\ \int_{e_1}^{e_2}\frac{xdx}{\sqrt{f(x)}} & \left(\int_{e_1}^{e_2}\frac{xdx}{\sqrt{f(x)}} - \int_{e_3}^{e_4}\frac{xdx}{\sqrt{f(x)}}\right) \end{pmatrix}.$$

9.1.2 Les formules de Thomae

Soit, comme plus haut, $\mathcal{C}$ une courbe hyperelliptique de genre $g \geqslant 1$, donnée par une équation de la forme

$$y^2 = \prod_{j\in[0,2g+1]}(x-e_j).$$

Choisissons maintenant une base du groupe d'homologie de la surface de Riemann associé à la courbe comme sur la Figure 9.4. On peut alors construire la matrice de Riemann τ associée à la courbe *via* ce choix des (A_j) et (B_k) comme vu plus haut.

On note $S = \{e_j\}_{j\in[0,2g+1]}$, et pour $j \in [1, 2g+2]$, on note

- a_j l'élément de $\{0,1\}^g$ dont la seule coordonnée non nulle est la i-ème ;
- b'_j l'élément de $\{0,1\}^g$ dont les $(i-1)$ premières coordonnées valent 1 et les $g+1-i$ dernières sont nulles ; et
- b''_j l'élément de $\{0,1\}^g$ dont les i premières coordonnées valent 1 et les $g-i$ dernières sont nulles.

Pour $j \in [1, 2g+2]$, on pose alors $\eta_{2j-1} = (a_j, b'_j)$ et $\eta_{2j} = (a_j, b''_j)$, et pour tout ensemble $S \subset E$, on définit η_S comme étant l'élément de $\{0,1\}^{2g}$ qui est congru modulo 2 à

$$\sum_{e_j\in S}\eta_j.$$

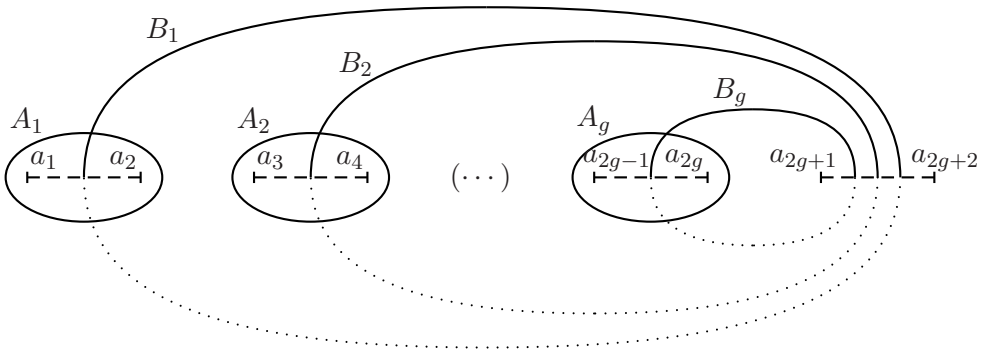

FIG. 9.4 – Base canonique d'homologie associée aux formules de Thomae

Enfin, on fixe un ensemble $B \subset E$ contenant $g+1$ éléments, et l'on note, pour tous $S, T \subset E$,

$$S \circ T = (S \cup T) \setminus (S \cap T)\,.$$

On a alors le résultat suivant, connu sous le nom de *formules de Thomae*, qui nous permet de relier les valeurs des theta constantes en τ aux racines de f :

Théorème 9.2 *Avec les notations définies ci-dessus, il existe une constante $c \in \mathbb{C} \setminus \{0\}$ telle que, pour tout $S \subset E$ de cardinal pair, on ait*

$$\theta^4_{\eta_S}(\tau) = \begin{cases} 0 & \text{si} \quad \#S \circ U \neq g+1; \\ (-1)^{\#S\cap U} c \prod_{\substack{x \in S\circ U \\ y \notin S\circ U}} \frac{1}{x-y} & \text{si} \quad \#S \circ U = g+1. \end{cases}$$

DÉMONSTRATION : Nous renvoyons à l'article original de Thomae [Tho70], ou bien à une preuve sans doute plus accessible de Fay [Fay73]. Notons que Thomae donnait aussi la valeur de la constante c, dont nous n'aurons pas besoin par la suite. □

En particulier, ce théorème permet, à partir de l'équation d'une courbe, de calculer directement (aux signes près) les valeurs des quotients des carrés des theta constantes en une matrice de Riemann τ associée à la courbe.

9.2 Calcul de matrices de Riemann

Dans cette section, nous nous intéressons au problème du calcul numérique d'une matrice de Riemann associée à une courbe (hyperelliptique) donnée soit par une équation de la forme $y^2 = f(x)$ comme dans la section précédente, soit par certains de ses invariants (nous verrons lesquels).

Notre principale motivation pour ce travail était d'essayer de généraliser au genre 2 les algorithmes d'évaluation rapide des theta constantes et de fonctions modulaires introduits au Chapitre 4. En particulier, notre objectif était de déterminer une fonction "analogue" à la fonction f_τ du chapitre sus-cité. La Section 9.2.3 présente les résultats qui seront utilisés au Chapitre 10 pour construire cet analogue.

Notons que l'évaluation (rapide) de matrices de Riemann a aussi un intérêt intrinsèque. Van Wamelen par exemple l'utilise pour montrer qu'une courbe hyperelliptique donnée par son équation sur $\mathbb{Q}$ a multiplication complexe (en donnant le corps CM correspondant) [vW99a, vW99b], ou bien pour expliciter une isogénie entre deux courbes hyperelliptiques définies sur les rationnels [vW00].

9.2.1 Méthodes utilisant l'intégration numérique

Nous avons vu plus haut que les matrices de Riemann associées aux courbes hyperelliptiques peuvent être définies *via* les matrices des périodes à partir d'intégrales hyperelliptiques. On peut donc, pour évaluer numériquement une matrice de Riemann associée à une courbe hyperelliptique, choisir explicitement une base du groupe d'homologie de la courbe, et se ramener à l'évaluation numérique de $2g^2$ intégrales hyperelliptiques. Nous comparons donc maintenant les complexités de différentes méthodes pour ce faire.

Quadrature de Gauss

Nous ne donnons ici qu'un bref aperçu de cette méthode. Pour (beaucoup) plus de détails, nous renvoyons à [DR84, Chapter 2, Section 7].

Le principe consiste, après s'être ramené à l'intervalle d'intégration $[-1, 1]$ par changement de variable, à approcher une intégrale de la forme

$$\int_{-1}^{1} \frac{x^j dx}{\sqrt{f(x)}}$$

par une somme de la forme

$$\sum_{k=1}^{n} \frac{w_{k,n} x_{k,n}^j}{\sqrt{f(x_{k,n})}},$$

pour un entier n fixé, où

- les $(x_{k,n})_{k\in[1,n]}$ sont les racines du polynôme de Legendre P_n ;
- les $(w_{k,n})_{k\in[1,n]}$ sont les poids associés, définis par

$$w_{k,n} = \frac{2(1 - x_{k,n}^2)}{(n+1)^2 P_{n+1}(x_{k,n})^2}.$$

Rappelons que les polynômes de Legendre sont définis par $P_0(X) = 1$, $P_1(X) = X$ et

$$(n+1)P_{n+1}(X) = (2n+1)XP_n(X) - nP_{n-1}(X)$$

pour tout $n \geqslant 1$.

Dans le cas qui nous intéresse, pour obtenir une approximation de l'intégrale avec une précision de N bits, il est nécessaire d'utiliser un nombre de points $n = O(N)$, ce qui entraîne une complexité en $O\left(\mathcal{M}(N)N\right) = O\left(N^{2+\varepsilon}\right)$.

Cette méthode a été implémentée par Paul van Wamelen* dans le package `AnalyticJacobian` du logiciel Magma [BCP97, Com05].

Évaluation rapide de fonctions holonomes

Pour $\alpha \in \mathbb{C}$, on pose

$$h_{\alpha,j}(z) = \int_{\alpha}^{z} \frac{x^j dx}{\sqrt{f(x)}}.$$

L'évaluation d'une matrice de Riemann peut se ramener à l'évaluation de telles fonctions $h_{\alpha,j}(z)$ (on évaluera en des racines du polynôme f). On note que pour tout $j \geqslant 0$ (et pour tout α), la fonction $h_{\alpha,j}$ vérifie

$$2zf(z)h''_{\alpha,j}(z) + \left(zf'(z) - 2jf(z)\right) h'_{\alpha,j}(z) = 0$$

*Cette implémentation est toutefois limitée à une précision maximale de 2000 chiffres décimaux.

pour tout z (par ailleurs, $h_{\alpha,j}$ est holomorphe). Une telle fonction (vérifiant une équation différentielle linéaire à coefficients polynomiaux) est dite *holonome*, et cette propriété peut être utilisée pour évaluer rapidement $h_{\alpha,j}$ par *continuation analytique*. Nous renvoyons à [CC87, vdH99] pour une description des algorithmes à mettre en œuvre, permettant d'évaluer $h_{\alpha,j}$ avec une précision relative de N bits en temps $O\left(\mathcal{M}(N\log N)\log N\right)$. On notera toutefois que ces algorithmes sont relativement compliqués à implanter (nous n'en avons d'ailleurs pas trouvé d'implantation ayant la complexité annoncée[†]).

9.2.2 L'algorithme de Richelot

Dans le cas d'une courbe hyperelliptique de genre 2 donnée par une équation de la forme

$$\mathcal{C} : y^2 = f(x),$$

le polynôme f étant de degré 5 ou 6 avec *toutes ses racines réelles*, Richelot [Ric36] a donné dès 1836 un algorithme convergeant quadratiquement permettant d'évaluer les intégrales hyperelliptiques associées à la courbe $\mathcal{C}$. Nous renvoyons au très complet article de Bost et Mestre [BM88] pour un exposé détaillé de cet algorithme et sa mise en parallèle avec l'AGM réelle.

L'algorithme de Richelot a une complexité en $O\left(\mathcal{M}(N)\log N\right)$.

Notons que Königsberger [Kön65] a donné une interprétation de l'algorithme de Richelot en termes de theta constantes.

9.2.3 Méthode utilisant la moyenne de Borchardt

Le but de cette section est de démontrer (de façon constructive !) le théorème suivant :

Théorème 9.3 *Soit $\mathcal{C}$ une courbe hyperelliptique de genre $g \geqslant 1$, que l'on se donne par les racines $(e_j)_{j\in[1,2g+2]}$ d'une équation de la forme $\mathcal{C} : y^2 = \prod_{j\in[1,2g+2]}(x-e_j)$. Alors on peut évaluer une matrice de Riemann associée à $\mathcal{C}$ avec une précision N en temps*

$$O\left(\mathcal{M}(N)\log N\right).$$

Notons tout de suite que ce résultat de complexité est valable lorsque la courbe $\mathcal{C}$ est fixée et que la précision N requise augmente. Il n'est alors plus nécessaire de distinguer entre précision relative et précision absolue : asymptotiquement, les deux notions coïncident.

Le cas du genre 1

Dans le cas du genre 1, nous avons en fait déjà vu un algorithme permettant le calcul de τ : en effet, nous avons montré à la Section 4.2.1 que pour tout $\tau \in \mathcal{F}$,

$$\tau = i\frac{M\left(k'(\tau)\right)}{M\left(\sqrt{1-k'^2(\tau)}\right)}. \tag{9.1}$$

De plus, l'équation d'une courbe elliptique peut toujours être mise sous la forme

$$y^2 = x(x-1)\left(x-k'^2(\tau')\right)$$

[†]Le package `algcurves` du logiciel Maple [Gar02], codé par Bernard Deconinck et Mark van Hoeij, implémente le calcul de matrices de Riemann par continuation analytique pour l'évaluation de fonctions holonomes, mais sans utiliser la technique de *binary splitting* (aussi appelée scindage binaire), qui permet d'atteindre la complexité annoncée. Ce package, utilisant les idées de [DvH01], permet par ailleurs de calculer une matrice de Riemann associée à une courbe *quelconque*, et pas seulement hyperelliptique.

où τ' est une "matrice de Riemann" (en fait, un élément de $\mathcal{H}$) associée à la courbe. On peut donc toujours, à partir d'une équation de la courbe, calculer une valeur de $k'^2(\tau')$, mais cette valeur ne correspond pas nécessairement à une valeur de τ' dans le domaine fondamental $\mathcal{F}$. On notera cependant que l'ensemble

$$\left\{k'^2(\gamma\tau) : \gamma \in \Gamma_1\right\}$$

est fini (en général, il est de cardinal $[\Gamma_1 : \Gamma_{k'^2}] = 6$). De plus, une fois que $k'^2(\tau')$ est connu, alors $k^2(\tau')$ l'est lui aussi puisque $k^2 + k'^2 = 1$, et l'on peut alors déterminer l'ensemble ci-dessus. L'une des valeurs de cet ensemble correspond alors à $k'^2(\tau)$, pour τ dans le domaine fondamental $\mathcal{F}$, et l'on veut déterminer laquelle. Pour ce faire, on peut procéder comme suit :

1. utiliser une méthode d'intégration numérique pour évaluer (à faible précision) un élément $\tau_1 \in \mathcal{H}$ associé à la courbe elliptique ;
2. réduire cet élément en un $\tau_2 \in \mathcal{F}$;
3. évaluer $k'^2(\tau_2)$, toujours à faible précision (en utilisant l'Algorithme 6 par exemple).

Parmi les 6 possibilités pour $k'^2(\tau)$, on retient celle qui est la plus proche de la valeur de $k'^2(\tau_2)$ que l'on a calculée[‡], correspondant donc à $\tau \in \mathcal{F}$. La valeur de $k'(\tau)$ est alors uniquement déterminée (on sait que $\mathrm{Re}\,(k'(\tau)) > 0$), et l'on peut utiliser l'égalité (9.1) pour évaluer τ à grande précision.

Nous allons montrer comment cet algorithme peut être généralisé au genre supérieur, en commençant par traiter en détail le cas du genre 2, avant d'aborder le cas d'un genre g quelconque.

Le cas du genre 2

Les formules de Thomae (Théorème 9.2) permettent, à partir d'une équation de la forme

$$y^2 = \prod_{j\in[0,5]} (x - e_j)$$

(donnée sous forme factorisée, *i.e.*, on suppose que l'on connaît les e_j), de déterminer les $b_j^2(\tau') = \frac{\theta_j^4}{\theta_0^4}(\tau')$ ($j \in [0, 15]$), pour une matrice de Riemann $\tau' \in \mathcal{H}_2$ associée à la courbe. Notons maintenant Γ_{b^2} le sous-groupe de Γ_2 pour lequel les fonctions b_1^2, b_2^2 et b_3^2 sont modulaires (ce groupe a pour indice 720 dans Γ_2, et l'on peut bien sûr calculer un ensemble de représentants de ses classes). L'ensemble

$$\mathfrak{B}(\tau') = \left\{\left(b_j^2(\gamma\tau')\right)_{j\in[1,15]} : \gamma \in \Gamma_{b^2}\right\}$$

est alors effectivement calculable (on peut précalculer l'action d'une famille de représentants des classes de $\Gamma_{b^2}\backslash\Gamma_2$ sur les b_j^2), et contient en général 720 éléments.

On note maintenant τ l'élément de $\mathcal{F}_2$ qui est équivalent à τ', et l'on veut déterminer les $b_j^2(\tau)$. Pour cela, une méthode possible (similaire à ce que nous avons fait ci-dessus dans le cas du genre 1) est la suivante :

1. calculer τ' à faible précision (par intégration numérique) ;
2. réduire τ' dans le domaine fondamental $\mathcal{F}_2$ pour obtenir une approximation de τ à faible précision ;
3. évaluer les $b_j^2(\tau)$ ($j \in [0, 15]$), toujours à faible précision, en utilisant un algorithme du type de l'Algorithme 15 par exemple.

[‡]La connaissance de τ_2 à faible précision permet de minorer la distance entre les différentes possibilités pour $k'^2(\tau)$.

Dans l'ensemble $\mathfrak{B}(\tau')$ introduit plus haut, on repère alors l'élément le plus proche de ces valeurs calculées à faible précision. Ceci permet de calculer les $b_j^2(\tau)$ (*via* les calculs à faible précision, on détermine une matrice $\gamma \in \Gamma_2$ telle que $b_j^2(\gamma\tau') = b_j^2(\tau)$, et l'on peut alors déterminer les $b_j^2(\tau)$ à la précision souhaitée en utilisant les formules de transformation des theta constantes sous l'action de γ données par la Proposition 5.4).

On peut alors aussi déterminer les $b_j(\tau)$ (en utilisant par exemple encore des valeurs à faible précision pour déterminer les signes des racines à prendre, encore que l'on puisse aussi utiliser les Propositions 6.1, 6.2 et 6.3, permettant de montrer par exemple que pour $j \in [1,3]$, $\mathrm{Re}\,(b_j(\tau)) > 0$, donc de déterminer directement certains signes de racines). Tout ceci montre la validité de l'Algorithme 12.

Algorithme : `Eval_bj_FromCurveEq`
Entrée : $(e_1, \ldots, e_6) \in \mathbb{C}^6$ décrivant la courbe hyperelliptique $\mathcal{C} : y^2 = \prod_{j\in[1,6]}(x - e_j)$, $N \in \mathbb{N}$
Sortie : $(b_j(\tau))_{j\in[0,15]}$, où $\tau \in \mathcal{F}_2$ est une matrice de Riemann associée à $\mathcal{C}$, à précision N

1. calculer la matrice de Riemann τ' associée à $\mathcal{C}$ par un choix particulier de base du groupe d'homologie, par intégration numérique, à faible précision;
2. $(\gamma, \tau) \leftarrow$`ReduceToF2`$(\tau')$;
3. calculer les $b_j^2(\tau')$ par les formules de Thomae, à précision N;
4. calculer les $b_j^2(\tau) = b_j^2(\gamma\tau')$ à précision N, en utilisant les formules de transformation (Proposition 5.4) pour les exprimer en fonction des $b_j^2(\tau')$;
5. calculer les $b_j(\tau)$ à faible précision à partir de la valeur de τ obtenue plus haut, en utilisant les définitions des theta constantes comme des séries;
6. en déduire les $b_j(\tau)$ à précision N, en utilisant leurs approximations pour choisir parmi les racines carrées possible des $b_j^2(\tau)$;
7. **return** $(b_j(\tau))_{j\in[0,15]}$;

Algorithme 12: Évaluation des $b_j(\tau)$ associés à une courbe

Dans cet algorithme, seulement un nombre constant d'opérations se font à précision N, toutes les autres (en nombre constant aussi d'ailleurs) se font à faible précision, d'où une complexité en $O\left(\mathcal{M}(N)\right)$.

Maintenant intervient la moyenne de Borchardt, qui va nous permettre, *via* le résultat suivant, de calculer les $\theta_j^2(\tau)$ (nous rappelons que la fonction B_2 est définie à la Section 7.4.1, et que la valeur de $B_2(x, y, z)$ est inchangée par permutation des variables x, y et z).

Proposition 9.1 *Pour tout $\tau \in \mathcal{F}_2$,*

$$B_2\left(b_1(\tau), b_2(\tau), b_3(\tau)\right) = \frac{1}{\theta_0^2(\tau)}.$$

Démonstration : Fixons un élément $\tau \in \mathcal{F}_2$ et notons, pour $n \in \mathbb{N}$,

$$(a_n, b_n, c_n, d_n) = \left(\frac{\theta_j^2(2^n\tau)}{\theta_0^2(\tau)}\right)_{j\in[0,3]}.$$

Cette suite est une suite de Borchardt associée à $(1, b_1(\tau), b_2(\tau), b_3(\tau))$, qui converge vers $\frac{1}{\theta_0^2(\tau)}$. Pour montrer le résultat annoncé, il suffit de montrer que tous les choix de racines de cette

suite sont bons. Ceci découle directement du fait que comme $\tau \in \mathcal{F}_2$, alors pour tout $n \geqslant 0$, $\lambda(2^n\tau) \geqslant \frac{\sqrt{3}}{2}$ donc (en vertu de la Proposition 6.1) $\mathrm{Re}\,(\theta_j(2^n\tau)) > 0$ (pour $j \in [0,3]$). □

Cette proposition nous montre que l'on peut calculer $\theta_0^2(\tau)$ *via* une moyenne de Borchardt. On a ensuite, pour tout $j \in [1,15]$, $\theta_j^2(\tau) = b_j(\tau)\theta_0^2(\tau)$.

Pour calculer τ, nous allons dans un premier temps supposer que la conjecture suivante est vraie.

Conjecture 9.1 *Pour tout $\tau \in \mathcal{F}_2$ et pour tout $\gamma \in \{(\mathfrak{JM}_1)^2, (\mathfrak{JM}_2)^2, (\mathfrak{JM}_3)^2\}$,*

$$B_2\left(b_1(\gamma\tau), b_2(\gamma\tau), b_3(\gamma\tau)\right) = \frac{1}{\theta_0^2(\gamma\tau)}.$$

En posant $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix}$ et en utilisant les formules de transformation des carrés des theta constantes sous l'action de $\mathfrak{J}$, $\mathfrak{M}_1$, $\mathfrak{M}_2$ et $\mathfrak{M}_3$ données à la Section 6.3, on montre que

$$\left(b_1\left((\mathfrak{JM}_1)^2\tau\right), b_2\left((\mathfrak{JM}_1)^2\tau\right), b_3\left((\mathfrak{JM}_1)^2\tau\right)\right) = \left(\frac{\theta_0^2(\tau)}{\theta_4^2(\tau)}, \frac{\theta_6^2(\tau)}{\theta_4^2(\tau)}, \frac{\theta_2^2(\tau)}{\theta_4^2(\tau)}\right),$$

$$\left(b_1\left((\mathfrak{JM}_2)^2\tau\right), b_2\left((\mathfrak{JM}_2)^2\tau\right), b_3\left((\mathfrak{JM}_2)^2\tau\right)\right) = \left(\frac{\theta_9^2(\tau)}{\theta_8^2(\tau)}, \frac{\theta_0^2(\tau)}{\theta_8^2(\tau)}, \frac{\theta_1^2(\tau)}{\theta_8^2(\tau)}\right),$$

$$\left(b_1\left((\mathfrak{JM}_3)^2\tau\right), b_2\left((\mathfrak{JM}_3)^2\tau\right), b_3\left((\mathfrak{JM}_3)^2\tau\right)\right) = \left(\frac{\theta_8^2(\tau)}{\theta_0^2(\tau)}, \frac{\theta_4^2(\tau)}{\theta_0^2(\tau)}, \frac{\theta_{12}^2(\tau)}{\theta_0^2(\tau)}\right),$$

et de plus

$$\theta_0^2\left((\mathfrak{JM}_1)^2\tau\right) = -i\tau_1\theta_4^2(\tau),$$
$$\theta_0^2\left((\mathfrak{JM}_2)^2\tau\right) = -i\tau_2\theta_8^2(\tau),$$

et enfin

$$\theta_0^2\left((\mathfrak{JM}_3)^2\tau\right) = (\tau_3^2 - \tau_1\tau_2)\theta_0^2(\tau).$$

Si la Conjecture 9.1 est vraie, on peut alors calculer τ à partir des $\theta_j^2(\tau)$ comme suit :

$$\tau_1 = \frac{i}{\theta_4^2(\tau) B_2\left(\frac{\theta_0^2(\tau)}{\theta_4^2(\tau)}, \frac{\theta_6^2(\tau)}{\theta_4^2(\tau)}, \frac{\theta_2^2(\tau)}{\theta_4^2(\tau)}\right)},$$

$$\tau_2 = \frac{i}{\theta_8^2(\tau) B_2\left(\frac{\theta_9^2(\tau)}{\theta_8^2(\tau)}, \frac{\theta_0^2(\tau)}{\theta_8^2(\tau)}, \frac{\theta_1^2(\tau)}{\theta_8^2(\tau)}\right)},$$

et

$$\tau_3^2 - \tau_1\tau_2 = \frac{1}{\theta_0^2(\tau) B_2\left(\frac{\theta_8^2(\tau)}{\theta_0^2(\tau)}, \frac{\theta_4^2(\tau)}{\theta_0^2(\tau)}, \frac{\theta_{12}^2(\tau)}{\theta_0^2(\tau)}\right)}.$$

Notons que ceci permet de déterminer τ au signe de τ_3 près. Cette indétermination peut être levée par le fait que comme $\tau \in \mathcal{F}_2$, alors $\mathrm{Im}\,(\tau_3) \geqslant 0$. On notera toutefois que τ et $\begin{pmatrix} \tau_1 & -\tau_3 \\ -\tau_3 & \tau_2 \end{pmatrix}$ sont équivalents modulo l'action de

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Algorithme : `Eval_tau_From_bj`
Entrée : $(b_j)_{j\in[0,15]} \in \mathbb{C}^{16}$
Sortie : $\tau \in \mathcal{F}_2$ tel que $b_j = b_j(\tau)$ pour tout j (en supposant qu'un tel τ existe)

$T_0 \leftarrow (B_2(b_1, b_2, b_3))^{-1}$;
for $j = 1$ **to** 15 **do**
  $T_j \leftarrow T_0 b_j$;
end
$\tau_1 \leftarrow \left(-iT_4 B_2\left(\frac{T_0}{T_4}, \frac{T_6}{T_4}, \frac{T_2}{T_4}\right)\right)^{-1}$;
$\tau_2 \leftarrow \left(-iT_8 B_2\left(\frac{T_9}{T_8}, \frac{T_0}{T_8}, \frac{T_1}{T_8}\right)\right)^{-1}$;
$a \leftarrow \left(T_0 B_2\left(\frac{T_8}{T_0}, \frac{T_4}{T_0}, \frac{T_{12}}{T_0}\right)\right)^{-1}$;
$\tau_3 = \sqrt{a + \tau_1\tau_2}$ (tel que $\mathrm{Im}(\tau_3) \geqslant 0$);
return $\begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix}$;

Algorithme 13: Calcul de $\tau \in \mathcal{F}_2$ à partir des $b_j(\tau)$

On en déduit donc l'Algorithme 13, dont la validité repose sur le fait que la Conjecture 9.1 est vérifiée.

Notons qu'en fait, la seule connaissance du triplet $(b_j(\tau))_{j\in[1,3]}$ est suffisante pour le calcul de $\tau \in \mathcal{F}_2$. En effet, on peut alors calculer comme précédemment les $\theta_j^2(\tau)$ (pour $j \in [0,3]$) *via* une moyenne de Borchardt. On peut alors en déduire les $\theta_j(\tau)$ ($j \in [0,3]$) par extraction de racines carrées (l'indétermination dans le signe étant levée par la Proposition 6.1 : on sait que $\mathrm{Re}(\theta_j(\tau)) > 0$ pour $j \in [0,3]$). En utilisant les formules de duplication (Proposition 5.5), on peut alors calculer les carrés de *toutes* les theta constantes en 2τ, puis procéder de manière similaire à précédemment. On en déduit l'Algorithme 14, dont la validité repose encore sur la véracité de la Conjecture 9.1.

On notera que si $\tau \in \mathcal{F}_2$, on n'a pas nécessairement $2\tau \in \mathcal{F}_2$, ce qui explique pourquoi il est nécessaire d'effectuer la dernière étape, qui permet de s'assurer que le résultat que l'on va renvoyer est bien réduit.

La complexité de ces deux algorithmes se ramène à la complexité de quatre évaluations de la fonction B_2 (moyenne de Borchardt) : elle est donc en $O(\mathcal{M}(N)\log N)$. On notera par ailleurs la simplicité de ces algorithmes (en particulier, on n'utilise que des opérations élémentaires : additions/soustractions, multiplications, inversions et racines carrées).

Les Algorithmes 12, 13 et 14 décrits ci-dessus montrent que, si la Conjecture 9.1 est vérifiée, alors on peut évaluer une matrice de Riemann associée à une courbe hyperelliptique avec N bits de précision en temps $O(\mathcal{M}(N)\log N)$. Ceci vaut lorsque la courbe est fixée et que l'on augmente N.

Notons que la Proposition 9.1 et la Conjecture 9.1 peuvent être vues comme une généralisation partielle (et non démontrée) au genre 2 de la Proposition 3.2. Il serait d'ailleurs intéressant de déterminer l'ensemble

$$\left\{\tau \in \mathcal{H}_2 : B(b_1(\tau), b_2(\tau), b_3(\tau)) = \frac{1}{\theta_0^2(\tau)}\right\}.$$

Il est facile de voir que cet ensemble contient nécessairement un domaine fondamental pour l'action de Γ_b sur $\mathcal{H}_2$, ainsi que les images de cet ensemble sous l'action du groupe engendré par

Algorithme : `Eval_tau_From_b123`
Entrée : $(b_1, b_2, b_3) \in \mathbb{C}^3$
Sortie : $\tau \in \mathcal{F}_2$ tel que $b_j = b_j(\tau)$ pour $j \in [1,3]$ (en supposant qu'un tel τ existe)

$T_0 \leftarrow (B_2(b_1, b_2, b_3))^{-1}$;
for $j = 1$ **to** 15 **do**
  $T_j \leftarrow T_0 b_j$;
end
for $j = 0$ **to** 3 **do**
  $R_j \leftarrow \sqrt{T_j}$ (tel que $\mathrm{Re}(R_j) > 0$);
end
$V_0 \leftarrow \frac{T_0+T_1+T_2+T_3}{4}$;
$V_1 \leftarrow \frac{R_0 \cdot R_1+R_2 \cdot R_3}{2}$;
$V_2 \leftarrow \frac{R_0 \cdot R_2+R_1 \cdot R_3}{2}$;
$V_3 \leftarrow \frac{R_0 \cdot R_3+R_1 \cdot R_2}{2}$;
$V_4 \leftarrow \frac{T_0-T_1+T_2-T_3}{4}$;
$V_6 \leftarrow \frac{R_0 \cdot R_2-R_1 \cdot R_3}{2}$;
$V_8 \leftarrow \frac{T_0+T_1-T_2-T_3}{4}$;
$V_1 \leftarrow \frac{R_0 \cdot R_1-R_2 \cdot R_3}{2}$;
$V_{12} \leftarrow \frac{T_0-T_1-T_2+T_3}{4}$;
$\tau_1 \leftarrow \left(-2iV_4 B_2\left(\frac{V_0}{V_4}, \frac{V_6}{V_4}, \frac{V_2}{V_4}\right)\right)^{-1}$;
$\tau_2 \leftarrow \left(-2iV_8 B_2\left(\frac{V_9}{V_8}, \frac{V_0}{V_8}, \frac{V_1}{V_8}\right)\right)^{-1}$;
$a \leftarrow \left(2V_0 B_2\left(\frac{V_8}{V_0}, \frac{V_4}{V_0}, \frac{V_{12}}{V_0}\right)\right)^{-1}$;
$\tau_3 \leftarrow \sqrt{a + \tau_1\tau_2}$ (tel que $\mathrm{Im}(\tau_3) \geqslant 0$);
$\tau_3 \leftarrow \tau_3 - \lfloor \mathrm{Re}(\tau_3) \rceil$;
return $\begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix}$;

Algorithme 14: Calcul de $\tau \in \mathcal{F}_2$ à partir de $(b_1(\tau), b_2(\tau), b_3(\tau))$

les translations entières (*i.e.*, le groupe engendré par $\mathfrak{M}_1$, $\mathfrak{M}_2$ et $\mathfrak{M}_3$), mais nous n'avons guère obtenu que des résultats conjecturaux pour ce problème.

La Conjecture 9.1 a été testée (et vérifiée) numériquement pour plusieurs millions de matrices $\tau \in \mathcal{F}_2$ aléatoires.

Variantes

La première variante permet de s'affranchir de la Conjecture 9.1 dans l'Algorithme 13. Fixons $\gamma \in \{(\mathfrak{JM}_1)^2, (\mathfrak{JM}_2)^2, (\mathfrak{JM}_3)^2\}$, $\tau \in \mathcal{F}_2$ et supposons que l'on connaisse les valeurs des $b_j(\gamma\tau)$ ($j \in [1,3]$), *ainsi qu'un approximation de τ à faible précision* (qui peut être obtenue comme un sous-produit de l'Algorithme 12). On sait que la suite

$$\left(\frac{\theta_j^2(2^n\gamma\tau)}{\theta_0^2(\gamma\tau)}\right)_{j\in[0,3],n\in\mathbb{N}}$$

est une suite de Borchardt associée à $(1, b_1(\gamma\tau), b_2(\gamma\tau), b_3(\gamma\tau))$ qui converge vers $\frac{1}{\theta_0^2(\gamma\tau)}$. On cherche à déterminer les choix de racines de cette suite, qui correspondent (par exemple) aux

$$\left(\frac{\theta_j(2^n\gamma\tau)}{\theta_0(\gamma\tau)}\right)_{j\in[0,3],n\in\mathbb{N}}.$$

À l'aide de l'approximation de τ dont on dispose, on peut calculer (à faible précision) les premiers termes de cette suite de choix de racines par un analogue de l'Algorithme 15, qui nous permettront de choisir les racines lors de calculs à grande précision. Bien sûr, il n'est nécessaire de calculer qu'un nombre fini (qui dépendra en fait de la valeur de τ) des premiers choix de racines, puisque l'on sait que les quatre suites vont converger vers une même limite (donc à partir d'un moment, les racines à prendre sont toutes situées dans un même quart de plan, ce qui lève les ambiguïtés). Lorsque τ est fixé, il s'agit de précalculs dont le coût ne modifiera pas le coût asymptotique du calcul de τ. On en déduit donc une preuve du Théorème 9.3 dans le cas du genre 2.

La seconde variante permet de s'affranchir du calcul numérique d'intégrales hyperelliptiques (même à faible précision) dans l'Algorithme 12. Supposons en effet que l'on dispose des valeurs des $b_j^2(\tau')$, où τ' est une matrice de Riemann associée à une courbe $\mathcal{C}$. Alors, d'après ce que l'on a vu plus haut, l'ensemble

$$\mathfrak{B}(\tau') = \left\{ \left(b_j^2(\gamma\tau')\right)_{j\in[1,15]} : \gamma \in \Gamma_{b^2} \right\}$$

est effectivement calculable, et est de cardinal au plus 720. Si $\tau \in \mathcal{F}_2$ est équivalent à τ', alors on sait que $(b_j(\tau))_{j\in[1,15]}$ est dans l'ensemble

$$\mathfrak{B}'(\tau') = \left\{ \left(\varepsilon_j b_j(\gamma\tau')\right)_{j\in[1,15]} : (\varepsilon_j)_{j\in[1,15]} \in \{\pm 1\}^{15}, \gamma \in \Gamma_{b^2} \right\},$$

qui est fini et explicitement calculable.

Pour déterminer $(b_j(\tau))$ dans cet ensemble $\mathfrak{B}'(\tau')$, on peut (en travaillant à faible précision)

1. poser $S = \mathfrak{B}'(\tau')$;
2. choisir un élément $(\beta_j)_{j\in[1,15]} \in S$;
3. calculer un élément $t = \texttt{Eval_tau_From_bj}(\beta_j)$;
4. si $t \notin \mathcal{F}_2$, enlever (β_j) de S et retourner en 2 ;

5. évaluer les $b_j(t)$ par un analogue de l'Algorithme 15 ;
6. vérifier si les $b_j(t)$ correspondent avec les β_j : si c'est le cas, alors on a bien $(\beta_j) = (b_j(\tau))$, sinon on enlève (β_j) de S et on retourne en 2.

On notera que l'on peut en fait utiliser les Proposition 6.1, 6.2 et 6.3 pour réduire la taille de l'ensemble S au préalable (par exemple, on sait que pour $j \in [0,4]$, $\mathrm{Re}\,(b_j(\tau) > 0)\dots$).

Cette seconde variante ne peut être utilisée que si l'on suppose que la Conjecture 9.1 est vérifiée, et ne change pas la complexité asymptotique du calcul de τ (ni même du calcul des $b_j(\tau)$, puisqu'elle ne fait intervenir qu'un nombre fini de calculs à faible précision).

En genre g quelconque

Dans cette section, nous fixons un entier $g \geqslant 3$ et supposons (comme ci-dessus dans le cas du genre 2) que l'on se donne une courbe hyperelliptique de genre g par les racines $(e_j)_{j\in[1,2g+2]}$ d'un équation de la forme $\mathcal{C} : y^2 = \prod_{j\in[1,2g+2]}(x - e_j)$.

Pour simplifier les notations, on note $b_v = \frac{\theta^2_{0,v}}{\theta^2_{0,0}}$ pour $v \in \{0,1\}^g$ (et l'on identifie naturellement $\{0,1\}^g$ avec $\mathcal{I}_g$).

On peut alors, par un algorithme tout à fait similaire à l'Algorithme 12, déterminer les valeurs des $b_j(\tau')$ pour une matrice de Riemann τ' associée à la courbe $\mathcal{C}$, ainsi qu'une approximation à faible précision de la matrice τ' (on ne passe pas par un élément de $\mathcal{F}_g$, pour la bonne raison que l'on ne connaît pas d'algorithme de réduction dans $\mathcal{F}_g$).

On peut alors, en procédant de façon similaire à ce que nous avons décrit dans la première variante ci-dessus, calculer à faible précision les premiers termes de la suite de Borchardt

$$\left(\frac{\theta^2_{0,v}(2^n\tau')}{\theta^2_{0,0}(\tau')}\right)_{v\in\mathcal{I}_g, n\in\mathbb{N}}$$

associée à $\big(1, b_{v_1}(\tau'), \dots, b_{v_{2^g-1}}(\tau')\big)$, puis s'en servir pour déterminer les choix de racines de cette suite et évaluer sa limite à la précision souhaitée. Cette limite vaut $\frac{1}{\theta^2_{0,0}(\tau')}$, et comme dans le cas du genre 2, on en déduit les $\theta^2_{0,v}(\tau') = \theta^2_{0,0}(\tau')b_v(\tau')$.

Posons maintenant, pour $j,k \in [1,g]^2$, m_j la matrice $g\times g$ dont tous les coefficients diagonaux sont nuls sauf le j-ème qui vaut 1, et $m_{j,k}$ la matrice $g \times g$ dont tous les coefficients sont nuls sauf ceux de coordonnées (j,k) et (k,j) qui valent 1. On définit alors

$$M_j = \begin{pmatrix} I & m_j \\ 0 & I \end{pmatrix} \in \Gamma_g$$

et

$$M_{j,k} = \begin{pmatrix} I & m_{j,k} \\ 0 & I \end{pmatrix} \in \Gamma_g.$$

On pose enfin $\gamma_j = (JM_j)^2$ et $\gamma_{j,k} = (JM_{j,k})^2$.

En procédant comme ci-dessus (*i.e.*, en utilisant des calculs à faible précision pour déterminer les choix de racines), on peut alors déterminer, pour tout $j \in [1,g]$, $\theta^2_{0,0}(\gamma_j\tau')$ (comme limite de la suite de Borchardt

$$\left(\frac{\theta^2_{0,v}(2^n\gamma_j\tau')}{\theta^2_{0,0}(\tau')}\right)_{v\in\mathcal{I}_g, n\in\mathbb{N}}$$

associée à $\big(1, b_{v_1}(\gamma_j\tau'), \dots, b_{v_{2^g-1}}(\gamma_j(\tau')\big)$, ce quadruplet pouvant s'exprimer à partir des $\theta^2_{0,v}(\tau')$ en utilisant les formules de transformation de la Proposition 5.4). De la même façon, on peut déterminer les $\theta^2_{0,v}(\gamma_{j,k}\tau')$.

Si l'on note $\tau' = (\tau'_{j,k})_{j,k\in[1,g]}$, alors les éléments diagonaux de τ' peuvent être calculés *via*

$$\theta^2_{0,0}(\gamma_j\tau') = \kappa(\gamma_j)\tau'_{j,j}\theta^2_{\Psi((,\gamma)_j,0)}(\tau'),$$

et les carrés des éléments non diagonaux de τ' *via*

$$\theta^2_{0,0}(\gamma_{j,k}\tau') = \kappa(\gamma_{j,k})(\tau^2_{j,k} - \tau_{j,j}\tau_{k,k})\theta^2_{\Psi((,\gamma)_{j,k},0)}(\tau')$$

(cette égalité découle, encore une fois, de la Proposition 5.4).

On peut utiliser l'approximation de τ' à faible précision que l'on a calculée pour déterminer le bon choix de racines pour le calcul des éléments non diagonaux de τ'.

Ceci termine la démonstration du Théorème 9.3 dans le cas général.

Notons enfin que ce genre de technique peut aussi être utilisé pour déterminer une matrice de Riemann associée à une courbe de genre 3 non hyperelliptique, en utilisant les travaux de Ritzenthaler [Rit03, Rit04] pour déterminer les quotients des theta constantes à partir d'une équation de la courbe (puisque dans ce cas, on ne peut utiliser les formules de Thomae).

9.2.4 Méthode de Mestre

Nous décrivons dans cette section un algorithme alternatif, relativement similaire à l'Algorithme 14, et dont le principe est dû à Mestre [Mes04]. Nous exposons le principe de l'algorithme dans le cas du genre 2, mais il peut se généraliser au genre supérieur.

Comme précédemment, on se donne un triplet $(b_1, b_2, b_3) \in \mathbb{C}^3$, et l'on cherche à déterminer $\tau \in \mathcal{F}_2$ tel que $b_j = b_j(\tau)$ pour $j \in [1, 3]$ (on suppose qu'un tel τ existe).

Comme précédemment, on calcule

$$\theta^2_0(\tau) = \frac{1}{B_2\left(b_1, b_2, b_3\right)},$$

puis on en déduit les $\theta^2_j(\tau) = b_j\theta^2_0(\tau)$ pour $j \in [1, 3]$.

D'après la Proposition 6.1, on sait que pour tous $n \in \mathbb{N}$ et $j \in [0, 3]$, $\mathrm{Re}\left(\theta_j(2^n\tau)\right) > 0$ (puisque $\tau \in \mathcal{F}_2$). Si l'on fixe un entier $n \in \mathbb{N}$, on peut donc (en effectuant n itérations de Borchardt correspondant à des bons choix de racines en partant de $\left(\theta^2_j(\tau)\right)_{j\in[0,3]}$) calculer les $\theta^2_j(2^n\tau)$, et même les $\theta_j(2^n\tau)$ pour $j \in [0, 3]$.

En considérant les développements en série des theta constantes on montre que si l'on pose $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix}$ on a

$$|\theta_0(2^n\tau) - \theta_1(2^n\tau) - 4E(2^n\tau_1)| = O(2^{-2n}),$$

et

$$|\theta_0(2^n\tau) - \theta_2(2^n\tau) - 4E(2^n\tau_2)| = O(2^{-2n}).$$

Si l'on souhait calculer τ à précision N, on peut alors poser $n = N$, et alors

$$\left|\tau_1 - \frac{1}{2^n\pi i}\log\frac{\theta_0(2^n\tau) - \theta_1(2^n\tau)}{4}\right| = O(2^{-N}),$$

et

$$\left|\tau_2 - \frac{1}{2^n\pi i}\log\frac{\theta_0(2^n\tau) - \theta_2(2^n\tau)}{4}\right| = O(2^{-N}).$$

Reste à déterminer τ_3. Pour cela, on utilise à nouveau les développements en séries des theta constantes pour montrer que

$$\left| \frac{\theta_0(2^n\tau) - \theta_1(2^n\tau) - \theta_2(2^n\tau) + \theta_3(2^n\tau)}{16E\left(2^n(\tau_1+\tau_2)\right)} - \cos(2\tau_3) \right| = O(2^{-N}),$$

ce qui permet enfin de déterminer τ_3 (au signe près, mais les deux choix possibles, nous l'avons vu plus haut, sont équivalents modulo l'action de Γ_2). On notera qu'en utilisant l'évaluation rapide du logarithme complexe (et des itérations de Newton), on peut inverser la fonction cos en temps $O\left(\mathcal{M}(N)\log N\right)$. Si l'on veut calculer τ à précision N, il est nécessaire de calculer les $\theta_j(2^n\tau)$ avec une précision de l'ordre de $4N$. On en déduit que la complexité de cette méthode est encore en $O\left(\mathcal{M}(N)\log N\right)$. Les mêmes idées peuvent encore être utilisées en genre supérieur, et (si le genre est fixé) la complexité est encore en $O\left(\mathcal{M}(N)\log N\right)$.

Une analyse un peu plus détaillée des constantes en jeu permet de montrer que l'algorithme présenté à la section précédente est théoriquement un peu plus rapide que celui-ci, mais surtout il est *a priori* plus simple à implémenter, puisqu'ici il faut aussi ici disposer d'une implémentation du logarithme complexe rapide, ainsi que de la fonction Arccos.

9.3 Résultats expérimentaux

Nous avons implémenté les Algorithmes 12 et 14 en langage C, en utilisant les bibliothèques GMP [Gra02], MPFR [HLPZ04] et MPC [EZ04] pour le calcul multiprécision, ainsi que les routines assembleur pour Athlon 64 de Pierrick Gaudry [Gau05]. Les temps de calcul que nous donnons ont été mesurés sur un Athlon 64 3400+ (cadencé à 2.4 MHz) disposant de 2 Go de RAM (ce dernier point étant accessoire, puisque les algorithmes implantés sont peu gourmands en mémoire).

La Figure 9.5 donne les temps de calcul cumulés des Algorithmes 12 et 14, pour l'évaluation d'une matrice de Riemann associée à la courbe $\mathcal{C}$ d'équation

$$y^2 = \prod_{j=1}^{6} \left(x - j(1+2i)\right),$$

pour des précisions allant de 2000 à 500000 bits. Une approximation d'une matrice de Riemann pour cette courbe est

$$\tau = \begin{pmatrix} 1.276714171333\,i & 0.422129728054\,i \\ 0.422129728054\,i & 1.276714171333\,i \end{pmatrix} \in \mathcal{F}_2,$$

et les invariants d'Igusa correspondants valent

$$\begin{aligned} j_1 &= \frac{363673752818875}{1492992}, \\ j_2 &= \frac{389990194915}{93312}, \\ j_3 &= \frac{120187932625}{93312}. \end{aligned}$$

Comme précédemment, nous notons $\mathtt{M}(N)$ le temps de calcul pour la multiplication de deux nombres complexes à précision N bits, par la fonction `mpc_mul` de MPC (voir la Figure 4.4).

La Figure 9.6 donne elle le ratio entre le temps d'évaluation de la matrice de Riemann associée à $\mathcal{C}$ et $10\,\mathcal{M}(N)\log N$, toujours sur la même plage de précision N. Ceci valide bien

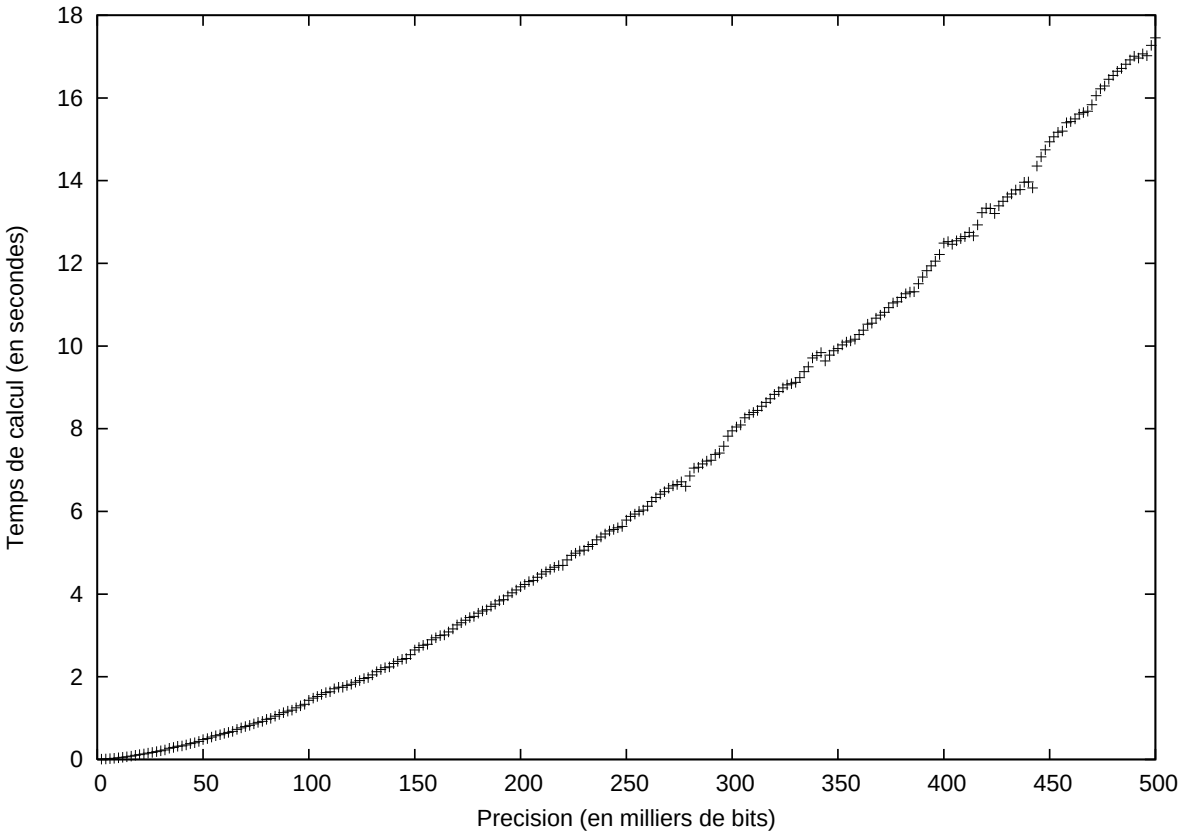

FIG. 9.5 – Temps de calcul l'évaluation d'une matrice de Riemann associée à la courbe $\mathcal{C}$

notre étude de complexité, et permet même de déterminer la constante de la notation $O(.)$: le temps de calcul semble majoré par $40\,\mathtt{M}(N)\log N$.

La Figure 9.7 donne le temps de calcul (sur la même machine que plus haut) de la fonction `AnalyticJacobian` de MAGMA, sur la même courbe $\mathcal{C}$ (cette fonction est celle qui permet d'avoir accès à une matrice de Riemann associée en MAGMA, elle utilise —comme nous l'avons vu plus haut— la méthode de quadrature de Gauss-Legendre pour évaluer numériquement des intégrales hyperelliptiques). À titre de comparaison, pour une précision de 1200 bits, le temps de calcul de la matrice de Riemann associée à $\mathcal{C}$ en MAGMA est de l'ordre de 97 secondes, alors que notre implémentation prend moins de 5 millisecondes.

Enfin, la Figure 9.8 donne le ratio entre le temps de calcul de la fonction `AnalyticJacobian` de MAGMA et $N\mathcal{M}(N)$ (pour la multiplication de MAGMA), sur la même plage de précision que précédemment. Cette courbe est en accord avec le fait que la complexité de `AnalyticJacobian` soit en $O\left(\mathcal{M}(N)N\right)$.

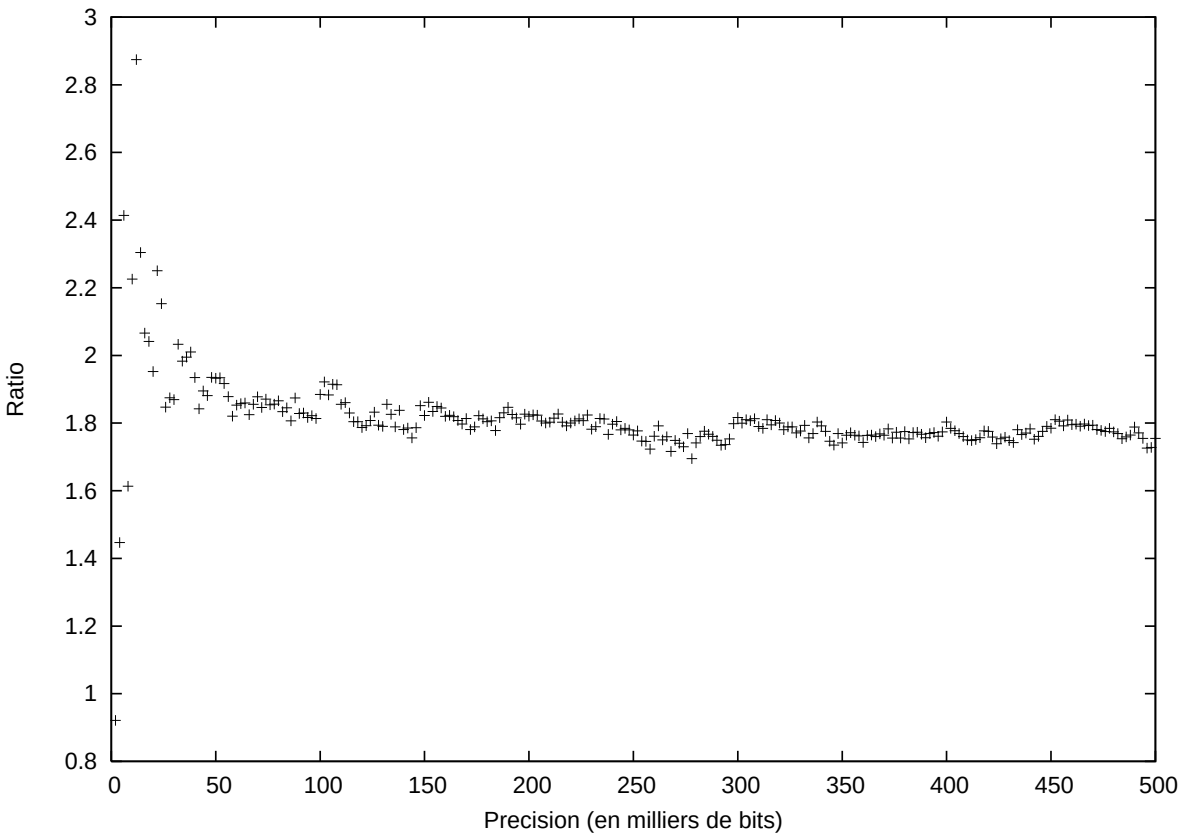

FIG. 9.6 – Ratio entre le temps de calcul des Algorithmes 12 et 14 et $(20\,\mathtt{M}(N)\log N)$

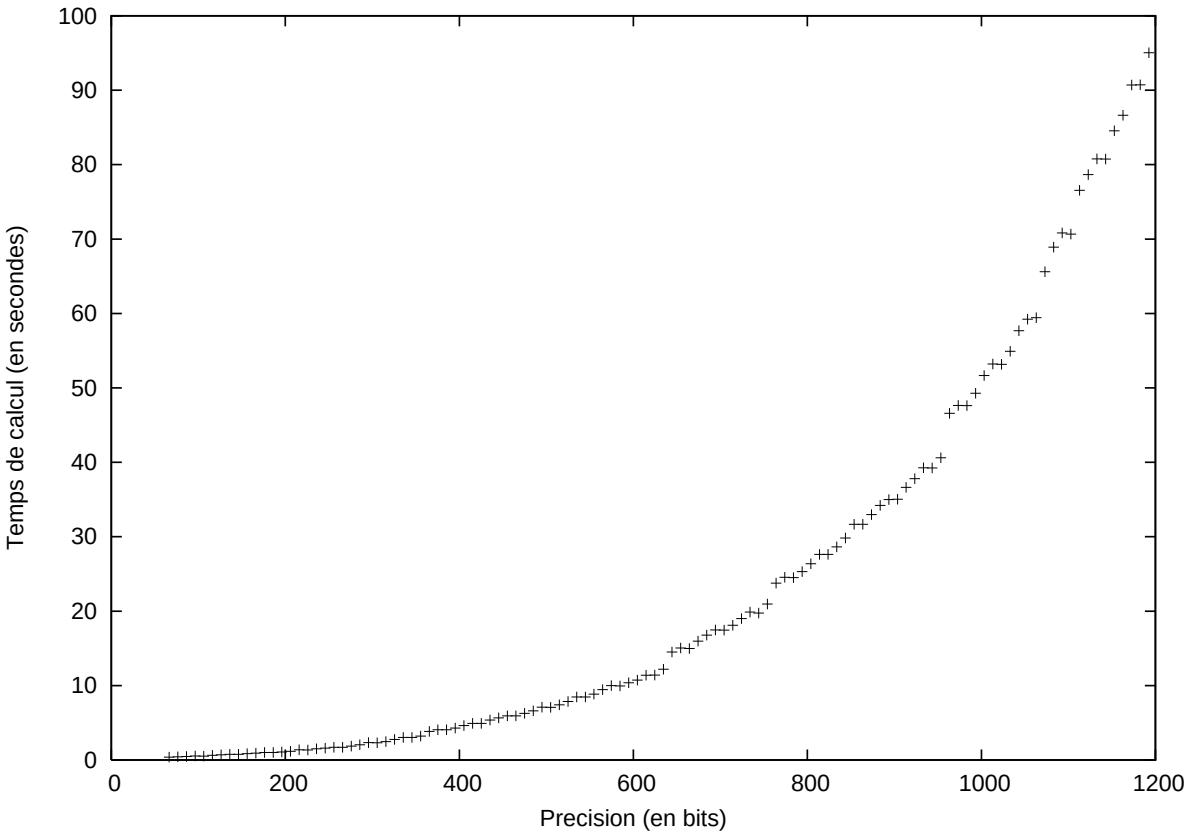

FIG. 9.7 – Temps de calcul de la fonction `AnalyticJacobian` de MAGMA pour la courbe $\mathcal{C}$

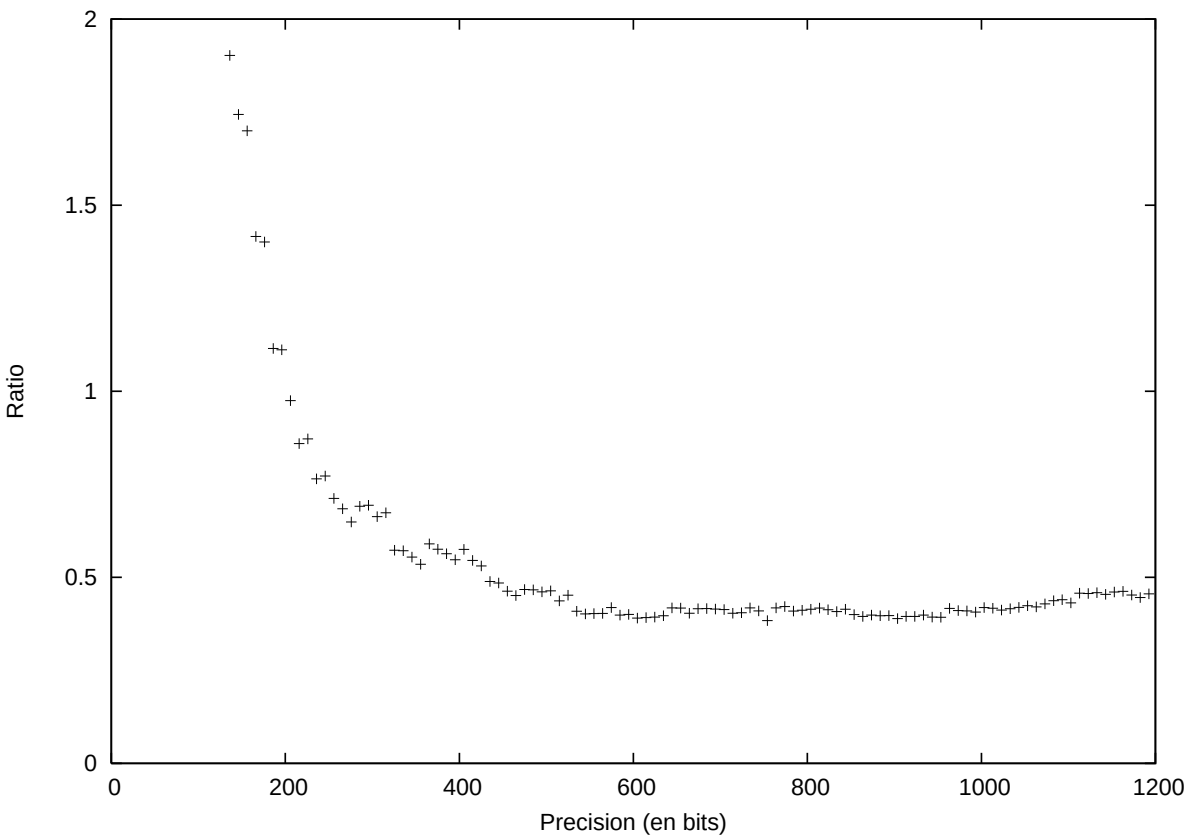

FIG. 9.8 – Ratio entre le temps de calcul de `AnalyticJacobian` et $20\,\mathcal{M}(N)N$

Chapitre 10

Évaluation des theta constantes en genre 2

Nous nous intéressons dans ce chapitre au problème suivant : étant donnée une matrice de Riemann $\tau \in \mathcal{H}_2$, évaluer numériquement (et, si possible, rapidement) les theta constantes en τ.

Nous allons tout de suite restreindre le cadre dans lequel nous nous plaçons : tout d'abord, nous allons dans la suite de ce chapitre supposer que τ est dans le domaine fondamental $\mathcal{F}_2$. Ceci est justifié par le fait que l'on connaît les formules de transformations des (carrés des) theta constantes sous l'action du groupe Γ_2 (voir la Proposition 5.4, ainsi que la Section 6.3). Par ailleurs, nous avons vu à la Section 6.4 que la donnée des seules theta constantes fondamentales (*i.e.*, les quatre premières) suffit, à quelques déterminations de signes de racines près, à déterminer toutes les autres. Nous nous limiterons donc à l'évaluation des quatre theta constantes fondamentales, tout en notant qu'il suffit de connaître des approximations à faible précision des autres theta constantes (que l'on peut calculer par leur définitions comme séries, avec des algorithmes proches de celui exposé à la Section 10.1 pour lever les indéterminations précitées.

10.1 Méthode naïve

La définition des theta constantes nous suggère une première façon de procéder : pour tous $b \in \{0,1\}^2$ et $\tau \in \mathcal{H}_2$, on a

$$\theta_{0,b}(\tau) = \sum_{n \in \mathbb{Z}^2} (-1)^{{}^t bn} E\left({}^t n \tau n\right),$$

donc une manière de faire est d'approcher cette somme. Pour ceci, nous introduisons les sommes partielles $S_{b,N}$ définies, pour tous $b = (b_0, b_1) \in \{0,1\}^2$ et $B \geqslant 0$, par

$$S_{b,B}(\tau) = \sum_{(m,n) \in [-B,B]^2} (-1)^{b_0 m + b_1 n} E\left(m^2 \tau_1 + n^2 \tau_2 + 2mn\tau_3\right),$$

pour tout $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{H}_2$.

On a alors le résultat suivant :

Lemme 10.1 *Pour tous $b \in \{0,1\}^2$, $B \geqslant 0$ et $\tau \in \mathcal{F}_2$,*

$$|\theta_{0,b}(\tau) - S_{b,B}(\tau)| \leqslant 16 \exp\left(-\pi\lambda(\tau)\right)^{B+1}.$$

Démonstration : Soit $b \in \{0,1\}^2$, $B \geqslant 0$ et $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$. Si l'on pose $Q = \exp(-\pi\lambda(\tau))$, alors on a

$$\left|E(m^2\tau_1 + n^2\tau_2 + 2mn\tau_3)\right| \leqslant Q^{m^2+n^2}$$

pour tous $m, n \in \mathbb{Z}$, donc

$$\begin{aligned} |\theta_{0,b}(\tau) - S_{b,B}(\tau)| &\leqslant \sum_{(m,n)\in\mathbb{Z}^2\setminus[-B,B]^2} Q^{m^2+n^2} \\ &\leqslant 4\left(\sum_{m\geqslant B+1, n\in[0,B]} Q^{m^2+n^2} + \sum_{m>0, n\geqslant B+1} Q^{m^2+n^2}\right) \\ &\leqslant 4\left(\frac{Q^{(B+1)^2}}{(1-Q)^2} + \frac{Q^{(B+1)^2+1}}{(1-Q)^2}\right) \\ &\leqslant 8\frac{Q^{(B+1)^2}}{(1-Q)^2}. \end{aligned}$$

Comme $\tau \in \mathcal{F}_2$, on a de plus $\lambda(\tau) \geqslant \frac{\sqrt{3}}{4}$ donc

$$|\theta_{0,b}(\tau) - S_{b,B}(\tau)| \leqslant 16Q^{(B+1)^2},$$

ce qui termine la démonstration. □

En utilisant la Proposition 6.1, on obtient alors la majoration suivante :

$$\left|\frac{S_{b,B}(\tau)}{\theta_{0,b}(\tau)} - 1\right| \leqslant 40\exp\left(-\pi\lambda(\tau)\right)^{(B+1)^2}$$

pour tous $B \geqslant 0$, $b \in \{0,1\}^2$ et $\tau \in \mathcal{F}_2$.

On en déduit que pour tout $N \geqslant 1$, si $B \geqslant 0$ vérifie

$$B \geqslant \sqrt{\frac{N - \log_2(40)}{\pi\log_2(e)\lambda(\tau)}} - 1 \geqslant \sqrt{\frac{4\left(N - \log_2(40)\right)}{\pi\log_2(e)\sqrt{3}}} - 1,$$

alors $S_{b,B}(\tau)$ est une approximation de $\theta_b(\tau)$ à précision relative N.

Par ailleurs, si $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{H}_2$ et que l'on note $q_1 = \exp(\pi i\tau_1)$, $q_2 = \exp(\pi i\tau_2)$ et $q_3 = \exp(2\pi i\tau_3)$ (notez le facteur 2 ajouté ici dans la définition de q_3), alors pour tous $b = (b_0, b_1) \in \{0,1\}^2$ et $B \geqslant 1$, en utilisant les symétries apparaissant dans la définition de $S_{b,B}$, on obtient :

$$S_{b,B}(\tau) = 1 + 2\sum_{n=1}^{B}\left((-1)^{nb_0}q_1^{n^2} + q_2^{n^2}\left((-1)^{nb_1} + \sum_{m=1}^{B}(-1)^{mb_0+nb_1}q_1^{m^2}\left(q_3^{mn} + q_3^{-mn}\right)\right)\right). \tag{10.1}$$

Notons que pour $b \in \{0,1\}^2$, les quatre fonctions $S_{b,B}$ font intervenir les mêmes termes *au signe près*, donc la complexité de l'évaluation simultanée des quatre fonctions est sensiblement la même que celle de l'évaluation d'une seule de ces fonctions.

L'Algorithme 15 utilise (10.1) pour évaluer des approximations des theta constantes. Pour accélérer les calculs, les $q_1^{m^2}$ sont précalculés (pour $m \in [1, B]$) en utilisant une chaîne d'addition adaptée (on utilise d'ailleurs aussi des chaînes adaptées pour calculer les $q_2^{n^2}$ ainsi que les $q_3^{\pm mn}$).

Algorithme : `EvaluateThetas_g2`

Entrée : $\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{F}_2$, $N \geqslant 1$

Sortie : $(T_j)_{j\in[0,3]}$ tel que pour tout $j \in [0,3]$, $|T_j/\theta_j(\tau) - 1| \leqslant 2^{-N}$

$B \leftarrow \left\lfloor \sqrt{\frac{4(N-\log_2(40))}{\pi \log_2(e)\sqrt{3}}} \right\rfloor$;
$q_j \leftarrow \exp(\pi i \tau_j)$ pour $j \in [1,2]$, $q_3 \leftarrow \exp(2\pi i \tau)$;
$q_4 \leftarrow 1/q_3$;
// Partie de précalcul des puissances de q_1
$a \leftarrow q_1$, $b \leftarrow q_1^2$, $Q_{1,s}[1] \leftarrow q_1$;
for $m = 2$ **to** B **do**
  $a \leftarrow ab$;
  $Q_{1,s}[m] \leftarrow aQ_{1,s}[m-1]$;
end
// Partie de calcul effectif des sommes
$S_j \leftarrow 0$ pour $j \in [0,3]$;
$Q_2 \leftarrow 1$, $a_3 \leftarrow 1$, $a_4 \leftarrow 1$, $b_2 \leftarrow q_2$, $c_2 \leftarrow q_2^2$;
for $n = 1$ **to** B **do**
  $a_3 \leftarrow a_3 q_3$, $a_4 \leftarrow a_4 q_4$;
  $Q_2 \leftarrow Q_2 b_2$, $b_2 \leftarrow b_2 c_2$;
  // On a $Q_2 = q_2^{n^2}$, $a_3 = q_3^n$ et $a_4 = q_3^{-n}$
  $S_0 \leftarrow S_0 + Q_{1,s}[n]$;
  $S_1 \leftarrow S_1 + (-1)^n Q_{1,s}[n]$;
  $S_2 \leftarrow S_2 + Q_{1,s}[n]$;
  $S_3 \leftarrow S_3 + (-1)^n Q_{1,s}[n]$;
  $Q_3 \leftarrow 1$, $Q_4 \leftarrow 1$;
  $A_0 \leftarrow 1$, $A_1 \leftarrow 1$, $A_2 \leftarrow (-1)^n$, $A_3 \leftarrow (-1)^n$;
  for $m = 1$ **to** B **do**
    $Q_3 \leftarrow Q_3 a_3$, $Q_4 \leftarrow Q_4 a_4$;
    // On a $Q_3 = q_3^{mn}$ et $Q_4 = q_4^{mn}$
    $s \leftarrow Q_{1,s}[m](Q_3 + Q_4)$;
    $A_0 \leftarrow A_0 + s$, $A_1 \leftarrow A_1 + (-1)^m s$, $A_2 \leftarrow A_2 + (-1)^n s$, $A_3 \leftarrow A_3 + (-1)^{m+n} s$;
  end
  $S_j \leftarrow S_j + Q_2 A_j$ pour $j \in [0,3]$;
end
return $(1 + 2S_j)_{j\in[0,3]}$;

Algorithme 15: Évaluation "naïve" des theta constantes θ_j ($j \in [0,3]$)

Analysons maintenant rapidement la complexité de cet algorithme : le nombre d'opérations arithmétiques est clairement en B^2, donc (vu la formule donnant B) il est linéaire en la précision relative N demandée. Par ailleurs, si l'on veut le résultat à une précision relative N (et comme les theta constantes que l'on calcule sont, d'après la Proposition 6.1, proches de 1), il faudra effectuer tous les calculs à une précision absolue de $N+k\log N$ bits (où k est une petite constante indépendante de la valeur de N), donc la complexité en temps de cet algorithme est en

$$O\left(N\mathcal{M}(N)\right) = O\left(N^{2+\varepsilon}\right).$$

Notons que nous avons ici choisi, par souci de simplification, de définir les sommes partielles comme des sommes sur un carré $[-B,B]\times[-B,B]$. Si l'on veut minimiser le nombre de points de $\mathbb{Z}^2$ utilisés pour définir les sommes partielles, il est plus naturel de considérer les points de $\mathbb{Z}^2$ situés dans des ellipses centrées en l'origine, dont le grand axe et le petit axe sont donnés par les deux vecteurs propres de la matrice $\mathrm{Im}\,(\tau)$ (les valeurs propres associées permettant de définir exactement ces ellipses). Pour plus de détails, nous renvoyons à [DHB+04], qui s'intéresse au problème plus général de l'évaluation des *fonctions theta* (par opposition aux theta constantes).

10.2 Méthode utilisant la moyenne de Borchardt et des itérations de Newton

Le but de cette section est d'introduire une généralisation au genre 2 de la technique d'évaluation de la fonction k' (et des theta constantes en genre 1) introduite au Chapitre 4.

Dans cette section, nous reprenons la notation $\mathbb{C}^{r+}$ du chapitre précité pour désigner l'ensemble des nombres complexes à partie réelle strictement positive, et l'on définit, pour $z\in\mathbb{C}^{r+}$, $\sqrt{z}$ comme étant l'unique racine carrée de z appartenant à $\mathbb{C}^{r+}$.

La première étape est d'obtenir un analogue en genre 2 de la fonction f_τ introduite à la Section 4.2.1 : nous fixons donc un élément $\tau\in\mathcal{F}_2$, et allons construire une fonction

$$F_\tau : \left(\mathbb{C}^{r+}\right)^3 \to \mathbb{C}^3$$

telle que

$$F_\tau\left(b_1(\tau), b_2(\tau), b_3(\tau)\right) = 0.$$

Pour cela, nous allons utiliser les idées introduites à la Section 9.2.3, en supposant pour l'instant que la Conjecture 9.1 est vraie.

Soit $(x,y,z)\in\mathbb{R}^3$, on pose

$$a_0 = \frac{1}{B_2(x,y,z)},$$

puis $a_1 = a_0x$, $a_2 = a_0y$ et $a_3 = a_0z$. On note alors (b_0,b_1,b_2,b_3) le *bon choix de racines* associé à (a_0,a_1,a_2,a_3), et l'on définit

$$c_0 = \frac{a_0+a_1+a_2+a_3}{4},$$
$$c_1 = \frac{b_0b_1+b_2b_3}{2},$$
$$c_2 = \frac{b_0b_2+b_1b_3}{2},$$
$$c_3 = \frac{b_0b_3+b_1b_2}{2},$$
$$c_4 = \frac{a_0-a_1+a_2-a_3}{4},$$

$$c_6 = \frac{b_0 b_2 - b_1 b_3}{2},$$
$$c_8 = \frac{a_0 + a_1 - a_2 - a_3}{4},$$
$$c_9 = \frac{b_0 b_1 - b_2 b_3}{2},$$

et

$$c_{12} = \frac{a_0 - a_1 - a_2 + a_3}{4}.$$

Si l'on désigne par γ l'élément de Γ_2 tel que $\gamma(2\tau) \in \mathcal{F}_2$, on pose alors, pour tout $j \in \{0,1,2,3,4,6,8,9,12\}$,

$$d_j = \Phi(\gamma, j)\, c_{\Psi(\gamma,j)}.$$

Enfin, on définit F_τ par

$$F_\tau(x,y,z) = (F_{\tau,1}, F_{\tau,2}, F_{\tau_3})(x,y,z) = \left(t_1 - T_1, t_2 - T_2, u - T_1 T_2 + T_3^2\right)$$

où

$$t_1 = \frac{i}{\kappa(\gamma) d_4 B_2\left(\frac{d_0}{d_4}, \frac{d_6}{d_4}, \frac{d_2}{d_4}\right)},$$
$$t_2 = \frac{i}{\kappa(\gamma) d_8 B_2\left(\frac{d_9}{d_8}, \frac{d_0}{d_8}, \frac{d_1}{d_8}\right)},$$
$$u = \frac{-1}{d_0 B_2\left(\frac{d_8}{d_0}, \frac{d_4}{d_0}, \frac{d_{12}}{d_0}\right)}$$

et

$$\begin{pmatrix} T_1 & T_3 \\ T_3 & T_2 \end{pmatrix} = \gamma \begin{pmatrix} 2\tau_1 & 2\tau_3 \\ 2\tau_3 & 2\tau_2 \end{pmatrix}.$$

Pour montrer que $F_\tau(b_1(\tau), b_2(\tau), b_3(\tau)) = 0$, il suffit de suivre le raisonnement de la Section 9.2.3 : avec les notations auxilliaires introduites ci-dessus, on a alors $a_j = \theta_j^2(\tau)$ pour $j \in [0,3]$, puis $c_j = \theta_j^2(2\tau)$ pour $j \in \{0,1,2,3,4,6,8,9,12\}$. On se ramène à $\gamma(2\tau)$ parce que ce que l'on a exposé à la Section 9.2.3 était valable sur $\mathcal{F}_2$ seulement, et alors on a bien $t_1 = T_1$, $t_2 = T_3$ et $u = T_1 T_2 - T_3^2$, d'où le fait que F_τ s'annule.

Nous conjecturons en fait que pour tout $\tau \in \mathcal{F}_2$, l'élément $\gamma \in \Gamma_2$ apparaissant dans la définition de F_τ, défini de façon à ce que $\gamma(2\tau) \in \mathcal{F}_2$, est toujours de la forme

$$\gamma = \mathfrak{M}_1^{e_1} \mathfrak{M}_2^{e_2} \mathfrak{M}_3^{e_3},$$

avec $(e_1, e_2, e_3) \in \{-1, 0, 1\}^3$, ce qui simplifie quelque peu les choses.

On peut précalculer $\kappa(\gamma)$ ainsi que les $\Phi(\gamma, j)$ et $\Psi(\gamma, j)$.

Nous ne détaillons pas ici formellement d'algorithme pour l'évaluation de F_τ, mais il est clair que la complexité de l'évaluation de F_τ est en $O(\mathcal{M}(N) \log N)$ (puisque cette évaluation se ramène à quatre calculs de moyennes de Borchardt).

Nous supposons dans la suite que la fonction F_τ est analytique autour de $(b_1(\tau), b_2(\tau), b_3(\tau))$, et que la matrice jacobienne

$$J_\tau(b_1(\tau), b_2(\tau), b_3(\tau)) = \begin{pmatrix} \frac{\partial F_{\tau,1}}{\partial x} & \frac{\partial F_{\tau,1}}{\partial y} & \frac{\partial F_{\tau,1}}{\partial z} \\ \frac{\partial F_{\tau,2}}{\partial x} & \frac{\partial F_{\tau,2}}{\partial y} & \frac{\partial F_{\tau,2}}{\partial z} \\ \frac{\partial F_{\tau,3}}{\partial x} & \frac{\partial F_{\tau,3}}{\partial y} & \frac{\partial F_{\tau,3}}{\partial z} \end{pmatrix} (b_1(\tau), b_2(\tau), b_3(\tau))$$

est inversible.

Sous ces conditions, la fonction $\tau \mapsto (b_1(\tau), b_2(\tau), b_3(\tau))$ peut être évaluée par des itérations de Newton sur la fonction F_τ (notez la similarité entre la fonction F_τ que nous considérons ici et la fonction f_τ considérée au Chapitre 4).

Si $(x_0, y_0, z_0) \in (\mathbb{C}^{r+})^3$ est "suffisamment proche" de $(b_1(\tau), b_2(\tau), b_3(\tau))$, alors la suite $(x_n, y_n, z_n)_{n\in\mathbb{N}}$, définie par récurrence par

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} - \left(J_\tau(x_n, y_n, z_n)\right)^{-1} \begin{pmatrix} F_{\tau,1}(x_n, y_n, z_n) \\ F_{\tau,2}(x_n, y_n, z_n) \\ F_{\tau,3}(x_n, y_n, z_n) \end{pmatrix}$$

converge *quadratiquement* vers $(b_1(\tau), b_2(\tau), b_3(\tau))$ (voir [BCSS97, Chapter 8] par exemple pour plus de détails sur les itérations de Newton multivariées).

Comparativement aux résultats que nous avons réussi à obtenir au Chapitre 4 dans le cas du genre 1, nous avons malheureusement beaucoup moins de résultats ici sur la convergence des itérations de Newton. L'algorithme que nous décrivons maintenant est donc seulement heuristique, mais son efficacité est validée par les résultats expérimentaux donnés à la Section 10.3.

Le principal problème qui reste à résoudre pour faire des itérations de Newton sur F_τ est l'évaluation de la matrice jacobienne $J_\tau(x, y, z)$ des dérivées partielles.

Une première voie est de calculer, pour $\varepsilon \in \mathbb{C}$ "petit", les valeurs $F_\tau(x, y, z)$, $F_\tau(x+\varepsilon, y, z)$, $F_\tau(x, y+\varepsilon, z)$ et $F_\tau(x, y, z+\varepsilon)$. Si l'on souhaite calculer $J_\tau(x, y, z)$ avec une précision de N bits, il est suffisant de prendre ε tel que $|\varepsilon| = O(2^{-N})$ et de calculer les quatre valeurs ci-dessus avec une précision de l'ordre de $2N$ bits, l'approximation de $J_\tau(x, y, z)$ étant alors donnée par

$$\frac{1}{\varepsilon}\left(\begin{pmatrix} F_{\tau,1}(x+\varepsilon, y, z) & F_{\tau,1}(x, y+\varepsilon, z) & F_{\tau,1}(x, y, z+\varepsilon) \\ F_{\tau,2}(x+\varepsilon, y, z) & F_{\tau,2}(x, y+\varepsilon, z) & F_{\tau,2}(x, y, z+\varepsilon) \\ F_{\tau,3}(x+\varepsilon, y, z) & F_{\tau,3}(x, y+\varepsilon, z) & F_{\tau,3}(x, y, z+\varepsilon) \end{pmatrix} - \begin{pmatrix} F_{\tau,1} & F_{\tau,1} & F_{\tau,1} \\ F_{\tau,2} & F_{\tau,2} & F_{\tau,2} \\ F_{\tau,3} & F_{\tau,3} & F_{\tau,3} \end{pmatrix}(x, y, z)\right).$$

La seconde voie est celle que nous employons en pratique. D'après la définition de la fonction F_τ, le calcul de la matrice jacobienne de cette dernière fonction peut se ramener au calcul du gradient de la fonction $(x, y, z) \mapsto B_2(x, y, z)$ définie *via* la moyenne de Borchardt. Notons $(a_n, b_n, c_n, d_n)_{n\in\mathbb{N}}$ la suite de Borchardt associée au calcul de $B_2(x, y, z)$. Pour tout n, a_n, b_n, c_n et d_n sont des fonctions de (x, y, z). On peut donc calculer leurs dérivées partielles par récurrence, puisque

$$a_{n+1} = \frac{a_n + b_n + c_n + d_n}{4},$$

$$b_{n+1} = \frac{\sqrt{a_n}\sqrt{b_n} + \sqrt{c_n}\sqrt{d_n}}{2},$$

$$c_{n+1} = \frac{\sqrt{a_n}\sqrt{c_n} + \sqrt{b_n}\sqrt{d_n}}{2}$$

et

$$d_{n+1} = \frac{\sqrt{a_n}\sqrt{d_n} + \sqrt{b_n}\sqrt{c_n}}{2}.$$

On a donc $\frac{\partial a_0}{\partial \alpha} = 0$ et

$$\frac{\partial b_0}{\partial \alpha} = \delta_{x,\alpha}, \quad \frac{\partial c_0}{\partial \alpha} = \delta_{y,\alpha}, \quad \frac{\partial d_0}{\partial \alpha} = \delta_{z,\alpha}$$

pour tout $\alpha \in \{x, y, z\}$, où $\delta_{\beta,\alpha}$ est le symbole de Kronecker (qui vaut 1 si et seulement si $\alpha = \beta$, et est nul sinon). Par récurrence, on a alors

$$\frac{\partial a_{n+1}}{\partial \alpha} = \frac{1}{4}\left(\frac{\partial a_n}{\partial \alpha} + \frac{\partial b_n}{\partial \alpha} + \frac{\partial c_n}{\partial \alpha} + \frac{\partial d_n}{\partial \alpha}\right),$$

$$\frac{\partial b_{n+1}}{\partial \alpha} = \frac{1}{4}\left(\frac{\sqrt{b_n}}{\sqrt{a_n}}\frac{\partial a_n}{\partial \alpha} + \frac{\sqrt{a_n}}{\sqrt{b_n}}\frac{\partial b_n}{\partial \alpha} + \frac{\sqrt{d_n}}{\sqrt{c_n}}\frac{\partial c_n}{\partial \alpha} + \frac{\sqrt{c_n}}{\sqrt{d_n}}\frac{\partial d_n}{\partial \alpha}\right),$$

$$\frac{\partial c_{n+1}}{\partial \alpha} = \frac{1}{4}\left(\frac{\sqrt{c_n}}{\sqrt{a_n}}\frac{\partial a_n}{\partial \alpha} + \frac{\sqrt{a_n}}{\sqrt{c_n}}\frac{\partial c_n}{\partial \alpha} + \frac{\sqrt{d_n}}{\sqrt{b_n}}\frac{\partial b_n}{\partial \alpha} + \frac{\sqrt{b_n}}{\sqrt{d_n}}\frac{\partial d_n}{\partial \alpha}\right)$$

et

$$\frac{\partial d_{n+1}}{\partial \alpha} = \frac{1}{4}\left(\frac{\sqrt{d_n}}{\sqrt{a_n}}\frac{\partial a_n}{\partial \alpha} + \frac{\sqrt{a_n}}{\sqrt{d_n}}\frac{\partial d_n}{\partial \alpha} + \frac{\sqrt{b_n}}{\sqrt{c_n}}\frac{\partial c_n}{\partial \alpha} + \frac{\sqrt{c_n}}{\sqrt{b_n}}\frac{\partial b_n}{\partial \alpha}\right)$$

pour tout $\alpha \in \{x, y, z\}$. Nous conjecturons alors que la suite

$$\left(\frac{\partial a_n}{\partial x}, \frac{\partial a_n}{\partial y}, \frac{\partial a_n}{\partial z}\right)_{n\in\mathbb{N}}$$

converge *quadratiquement* vers le gradient

$$\left(\frac{\partial B_2(x,y,z)}{\partial x}, \frac{\partial B_2(x,y,z)}{\partial y}, \frac{\partial B_2(x,y,z)}{\partial z}\right).$$

Dans le cas de B_1, ce résultat est démontré par exemple dans [BB87]. Dans le cas de B_2, nous avons seulement pu vérifier cette conjecture numériquement. Pour évaluer le gradient de B_2, nous utilisons donc une variante de l'Algorithme 11 qui, en plus de renvoyer un élément a_k approximant $B_2(x, y, z)$ renvoie aussi les trois dérivées partielles de a_k.

L'Algorithme 16 permet donc d'évaluer les fonctions b_1, b_2 et b_3.

Algorithme : `Evaluate_b123_Newton`
Entrée : $\tau \in \mathcal{F}_2$, $N \in \mathbb{N}$
Sortie : $(b_j)_{j\in[1,3]}$ approximant les $b_j(\tau)$ avec une précision relative de N bits

$(t_0, t_1, t_2, t_3) \leftarrow$`EvaluateThetas_g2`$(\tau, N_1)$;
$(x_0, y_0, z_0) \leftarrow \left(\frac{t_1^2}{t_0^2}, \frac{t_2^2}{t_0^2}, \frac{t_3^2}{t_0^2}\right)$;
$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \leftarrow \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} - \left(J_\tau(x_0, y_0, z_0)\right)^{-1} \begin{pmatrix} F_{\tau,1}(x_0, y_0, z_0) \\ F_{\tau,2}(x_0, y_0, z_0) \\ F_{\tau,3}(x_0, y_0, z_0) \end{pmatrix};$$
$j \leftarrow 1$;
while $\left|\frac{\alpha_{n+1}-\alpha_n}{\alpha_n}\right| > 2^{-N}$ *pour un* $\alpha \in \{x, y, z\}$ **do**
$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} \leftarrow \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} - \left(J_\tau(x_n, y_n, z_n)\right)^{-1} \begin{pmatrix} F_{\tau,1}(x_n, y_n, z_n) \\ F_{\tau,2}(x_n, y_n, z_n) \\ F_{\tau,3}(x_n, y_n, z_n) \end{pmatrix};$$
$j \leftarrow j + 1$;
end
return (x_j, y_j, z_j);

Algorithme 16: Évaluation des $(b_j)_{j\in[1,3]}$ par itérations de Newton

Deux importants détails sont à signaler concernant cet algorithme :
– la constante N_1 doit être telle que les itérations de Newton que l'on va effectuer ensuite convergent. En pratique, nous partons de $N_1 = 200$ bits, et nous détectons ensuite si les itérations de Newton convergent. Si ce n'est pas le cas, nous recommençons en doublant N_1, et ainsi de suite ;

– la condition d'arrêt ne suffit en théorie pas à garantir l'exactitude du résultat... mais nous n'avons pas été capable d'obtenir mieux !

Comme toujours avec les itérations de Newton, la précision de calcul est augmentée au fur et à mesure (on la double à chaque itération). La convergence de ces itérations étant supposée quadratique, on en déduit que la complexité heuristique de cet algorithme est en $O(\mathcal{M}(N)\log N)$. Cette analyse semble confirmée par les résultats expérimentaux que nous avons obtenus (voir la Section 10.3).

Notons que l'on peut évaluer les theta constantes avec la même complexité asymptotique, puisque

$$\theta_0^2(\tau) = \frac{1}{B_2\left(b_1(\tau), b_2(\tau), b_3(\tau)\right)}$$

permet de déterminer $\theta_0^2(\tau)$, puis on calcule

$$\theta_j^2(\tau) = \theta_0^2(\tau) b_j(\tau)$$

pour $j \in [1,3]$. Les $(\theta_j(\tau))_{j\in[0,4]}$ sont alors uniquement déterminés (on sait qu'ils ont partie réelle strictement positive), et les autres theta constantes peuvent s'en déduire *via* les équations modulaires données aux Propositions 6.7 et 6.8 par exemple (les bons choix de racines pouvant être déterminés en évaluant les theta constantes à faible précision par un algorithme analogue à l'Algorithme 15).

On peut aussi évaluer les invariants d'Igusa avec la même complexité (en passant par les theta constantes et la définition que nous avons donnée des invariants d'Igusa à la Section 6.3.3).

10.3 Résultats expérimentaux

Nous avons implémenté les Algorithmes 15 et 16 en langage C, en utilisant les bibliothèques GMP [Gra02], MPFR [HLPZ04] et MPC [EZ04] pour le calcul multiprécision, ainsi que les routines assembleur pour Athlon 64 de Pierrick Gaudry [Gau05]. Les temps de calcul que nous donnons ont été mesurés sur un Athlon 64 3400+ (cadencé à 2.4 MHz) disposant de 2 Go de RAM (ce dernier point étant accessoire, puisque les algorithmes implantés sont peu gourmands en mémoire).

La Figure 10.1 donne les temps de calcul des Algorithmes 15 (noté "Naïve") et 16 (noté "Newton"), pour des précisions allant jusqu'à 30000 bits, en

$$\tau = \begin{pmatrix} \frac{3+10\cdot i}{10} & \frac{-2+3\cdot i}{10} \\ \frac{-2+3\cdot i}{10} & \frac{4+12\cdot i}{10} \end{pmatrix} \in \mathcal{F}_2,$$

Les temps de calculs des deux algorithmes sont sensiblement égaux pour une précision de 3700 bits.

Comme précédemment, nous notons $\mathtt{M}(N)$ le temps de calcul pour la multiplication de deux nombres complexes à précision N bits, par la fonction `mpc_mul` de MPC (voir la Figure 4.4).

La Figure 10.2 donne le ratio entre le temps de calcul de l'Algorithme 15 et $\frac{N}{100}\mathtt{M}(N)$, dans la même plage de précision que ci-dessus. Ces données correspondent bien avec une complexité en $19\,N\mathtt{M}(N)$.

La Figure 10.3 donne le temps de calcul de l'Algorithme 16, pour des précisions allant jusqu'à 200000 bits (et en la même matrice $\tau \in \mathcal{F}_2$ que ci-dessus).

La Figure 10.4 donne le ratio entre le temps de calcul de l'Algorithme 16 et $100\,\mathtt{M}(N)\log N$, dans la même plage de précision que ci-dessus. Ces données correspondent bien avec une complexité en $800\,\mathtt{M}(N)\log N$.

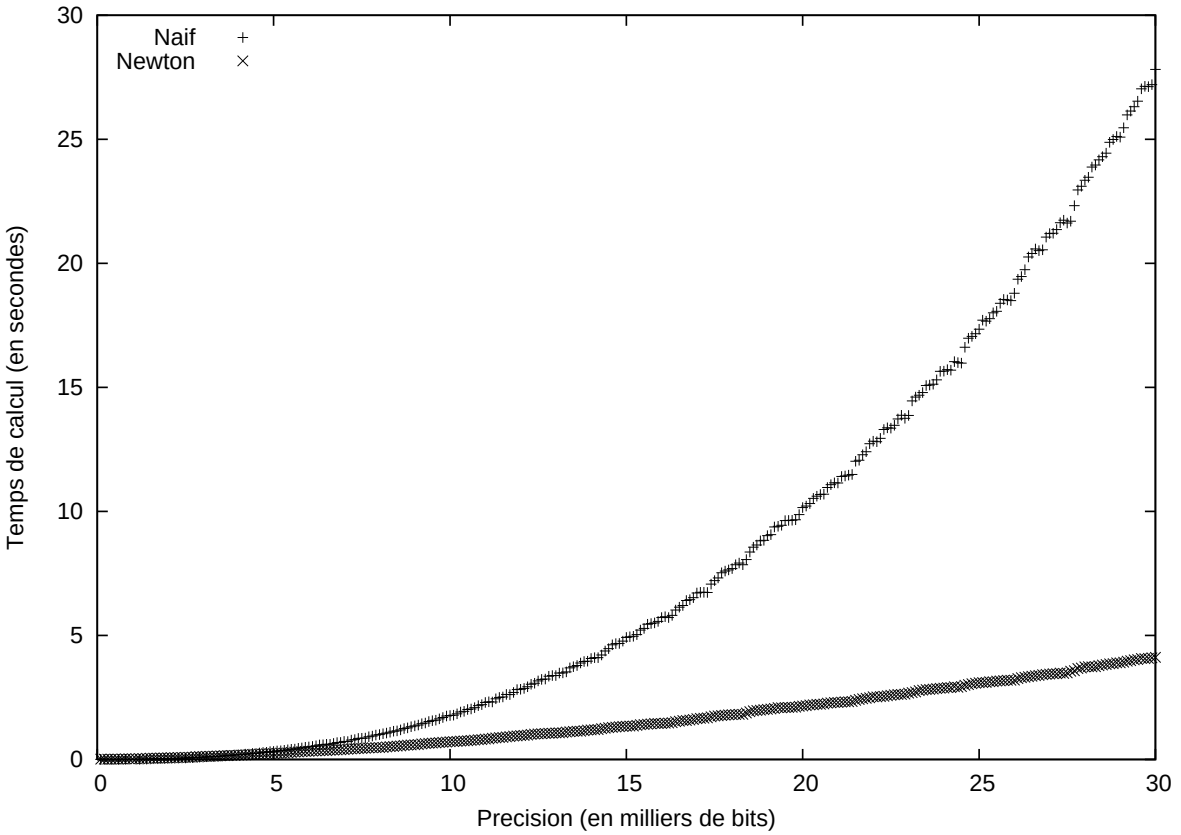

FIG. 10.1 – Temps de calcul pour l'évaluation de $(b_j(\tau))$ par les Algorithmes 15 et 16

10.4 Applications

10.4.1 Calcul de polynômes de classes

La théorie de la multiplication complexe, que nous avons rapidement évoquée dans le cas du genre 1 à la Section 4.4.1, peut encore être utilisée en genre 2 pour construire des courbes hyperelliptiques ayant des propriétés particulières (comme dans le cas du genre 1, on utilise pour cela les liens existants entre la structure de l'anneau d'endomorphisme et le cardinal de la jacobienne sur un corps fini). Nous ne décrivons pas ici cette méthode, mais renvoyons aux travaux de Weng [Wen01, Wen03].

En genre 2, la multiplication complexe effective passe par le calcul de polynômes de classe, analogues de ceux existant en genre 1. À un corps CM K correspond un ensemble fini S_K de matrices de Riemann de variétés abéliennes principalement polarisées ayant multiplication complexe par l'ordre maximal $\mathcal{O}_K$. On définit alors les polynômes de classe

$$H_{K,1}(X) = \prod_{\tau \in S_K} \left(X - j_1(\tau)\right),$$

$$H_{K,2}(X) = \sum_{\tau \in S_K} j_2(\tau) \prod_{\tau' \in S_K \setminus \{\tau\}} \left(X - j_1(\tau')\right)$$

et

$$H_{K,3}(X) = \sum_{\tau \in S_K} j_3(\tau) \prod_{\tau' \in S_K \setminus \{\tau\}} \left(X - j_1(\tau')\right)$$

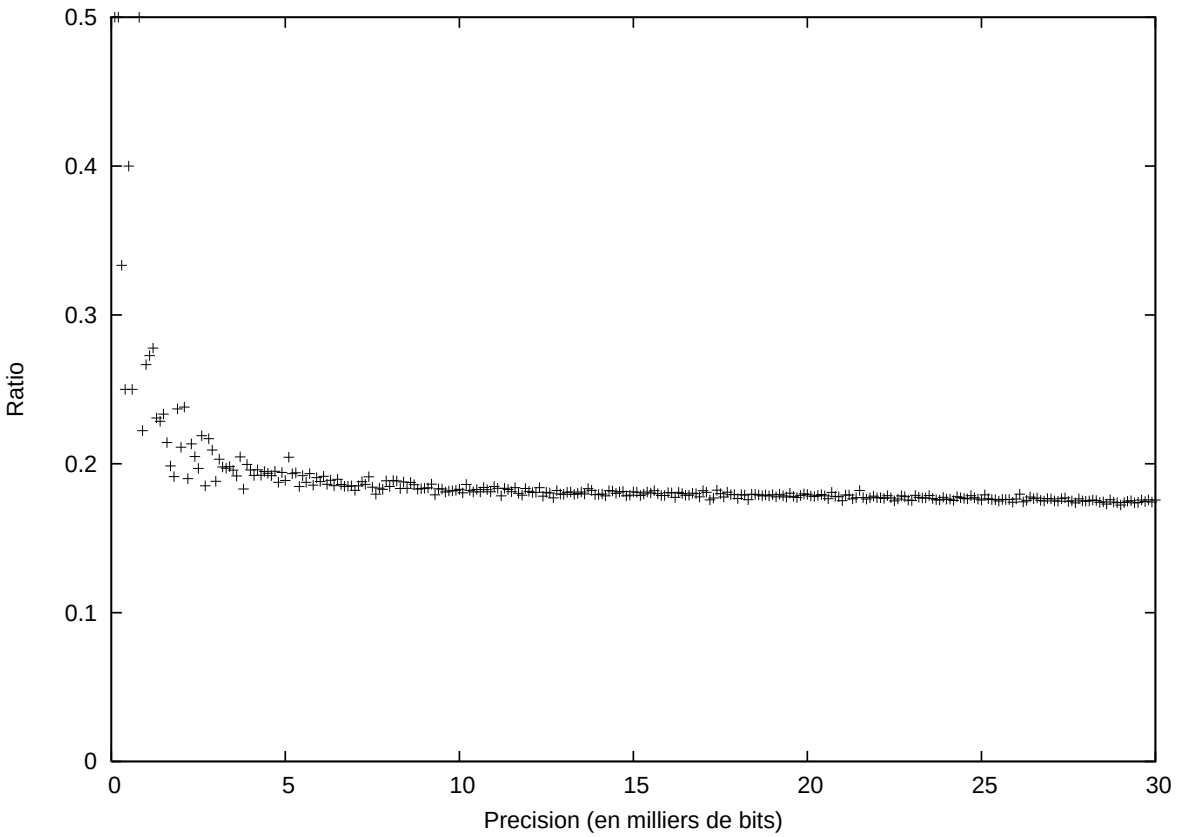

FIG. 10.2 – Ratio entre le temps de calcul de l' Algorithme 15 et $\frac{N}{100}\mathtt{M}(N)$

(où les fonctions j_1, j_2 et j_3 sont les invariants d'Igusa, introduits à la Section 6.3.3). Ces polynômes sont à coefficients rationnels. On peut donc les construire par évaluation des invariants d'Igusa en les éléments de S_K (les coefficients des éléments de S_K sont des nombres algébriques), puis par interpolation et reconstruction des coefficients rationnels (cette dernière étape se faisant facilement, par exemple en utilisant des développements en fractions continues). C'est la méthode qu'utilise Weng dans [Wen01, Wen03], et c'est alors l'évaluation numérique des invariants d'Igusa (qui se ramène directement à l'évaluation des theta constantes, vu la définition que nous avons donnée des invariants d'Igusa) en les matrices de S_K qui est l'étape la plus coûteuse. On peut utiliser l'Algorithme 16 (ou plus précisément sa variante permettant l'évaluation des invariants d'Igusa) pour accélérer le calcul des polynômes de classe.

Notons qu'une méthode utilisant un *lift p-adique* a récemment été introduite par Gaudry, Houtmann, Kohel, Ritzenthaler et Weng [GHK+05], qui permet le calcul des polynômes de classes associés à un corps CM K à partir d'*une* courbe ayant multiplication complexe par $\mathcal{O}_K$ (cette courbe pouvant être déterminée par exemple par recherche exhaustive). L'idée est de calculer à une certaine précision le relevé p-adique canonique de cette courbe : ses j-invariants sont algébriques, et l'on peut retrouver leurs polynômes minimaux par exemple en utilisant l'algorithme LLL.

Une fois les polynômes de classe calculés, la construction d'une courbe ayant multiplication complexe par $\mathcal{O}_K$ sur un corps fini premier $\mathbb{F}_p$ se fait comme suit :

- on réduit $H_{K,1}$, $H_{K,2}$ et $H_{K,3}$ modulo p pour obtenir $\overline{H}_{K,1}$, $\overline{H}_{K,2}$ et $\overline{H}_{K,3}$;
- on détermine une racine $\overline{j}_1 \in \mathbb{F}_p$ de $\overline{H}_{K,1}$;

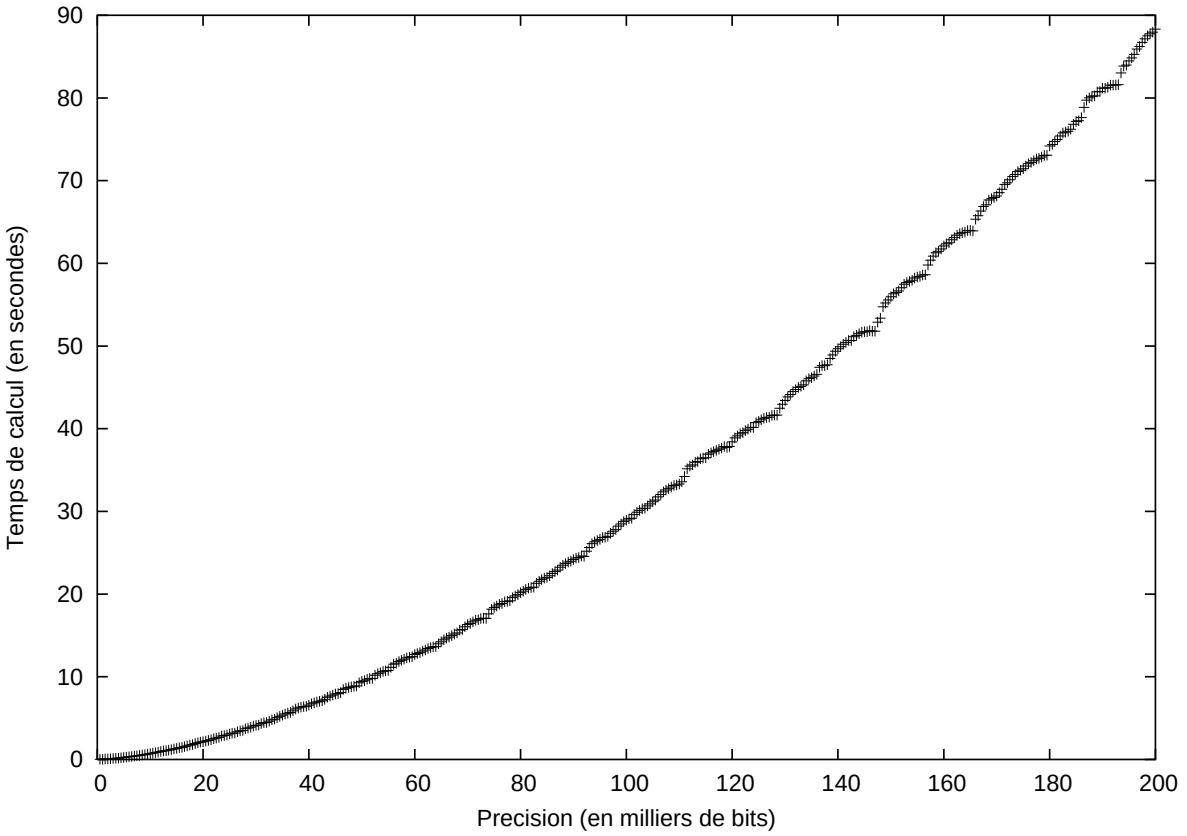

FIG. 10.3 – Temps de calcul pour l'évaluation de $(b_j(\tau))$ par l'Algorithme 16 à haute précision

– on calcule

$$\overline{j}_k = \frac{\overline{H}_{K,k}(\overline{j}_1)}{\overline{H}'_{K,k}(\overline{j}_1)}$$

pour $k \in [2,3]$;
– on utilise l'algorithme de Mestre [Mes91] pour construire une courbe hyperelliptique sur $\mathbb{F}_p$ ayant pour j-invariants $(\overline{j}_1, \overline{j}_2, \overline{j}_3)$.

10.4.2 Calcul de polynômes modulaires

Les polynômes modulaires auxquels nous nous intéressons dans cette section sont liés à des groupes modulaires de forme $\Gamma_0(p)$ (définis ci-dessous) généralisant en genre 2 les groupes homonymes existant en genre 1. Ils lient algébriquement les invariants associés à une jacobienne de courbe avec les invariants des jacobiennes qui lui sont (p,p)-isogènes.

De tels polynômes pourraient peut-être être utilisés pour généraliser les améliorations d'Elkies et Atkin à l'algorithme de Schoof au genre 2 (on calculerait modulo le noyau d'une (p,p)-isogénie plutôt que modulo la p-torsion). Cette piste est envisagée par Pierrick Gaudry*, mais il faut noter que (comme nous le verrons à la fin de cette section) ces polynômes modulaires sont "gros", et difficiles à calculer (pour l'instant). Cette section n'est donc qu'exploratoire !

*Qui s'était déjà, dans sa thèse [Gau00, pages 55–69], intéressé au calcul explicite de polynômes modulaires en genre 2.

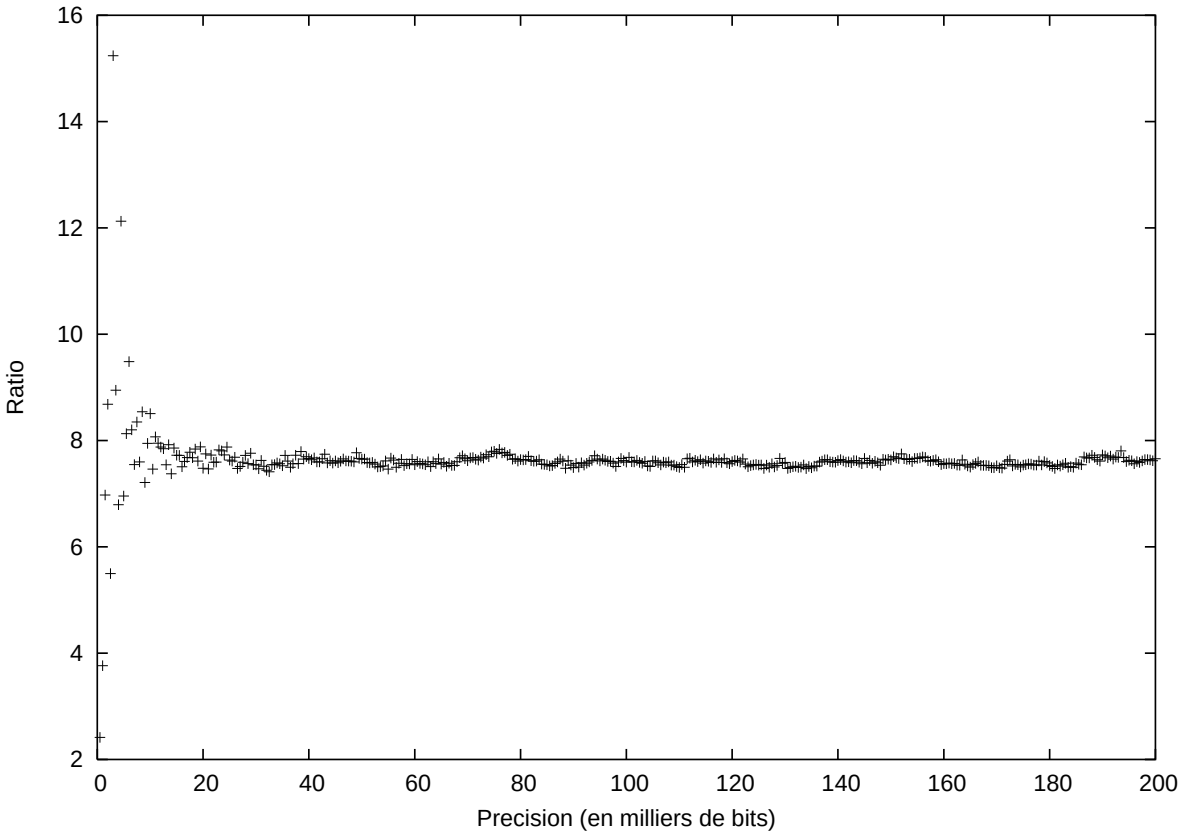

FIG. 10.4 – Ratio entre le temps de calcul de l' Algorithme 16 et $100\,\mathtt{M}(N)\log N$

Le groupe $\Gamma_0(p)$

Définition 10.1 (groupe $\Gamma_0(p)$) *Pour tout entier $p \geqslant 0$, on note $\Gamma_0(p)$ le sous-groupe de Γ_2 défini par*

$$\Gamma_0(p) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_2 : C \equiv 0 \bmod p \right\}.$$

Dans la suite de cette section, nous nous restreindrons au cas où p est premier.
Pour tous $a, b, c \in [0, p-1]$, on pose :

$$T_1(a,b,c) = \begin{pmatrix} I & & 0 \\ a & b & \\ b & c & I \end{pmatrix},$$

$$T_2(a,b,c) = \begin{pmatrix} 0 & & -I \\ & a & b \\ I & b & c \end{pmatrix},$$

$$T_3(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & a \\ -a & 1 & 0 & 0 \end{pmatrix},$$

et

$$T_4 = \begin{pmatrix} -1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

On a alors le résultat suivant :

Proposition 10.1 *Pour tout nombre premier p,*

$$[\Gamma_2 : \Gamma_0(p)] = p^3 + p^2 + p + 1,$$

et l'ensemble $\mathcal{C}_p$ défini par

$$\begin{aligned} \mathcal{C}_p &= \left\{T_1(a,b,c), (a,b,c) \in [0,p-1]^3\right\} \\ &\cup \left\{T_2(a,b,c), (a,b,c) \in [0,p-1]^3 \text{ tels que } ac \equiv b^2 \bmod p\right\} \\ &\cup \left\{T_3(a), a \in [0,p-1]\right\} \\ &\cup \left\{T_4\right\} \end{aligned}$$

est un ensemble de représentants pour les classes de Γ_2 sous l'action (à gauche) de $\Gamma_0(p)$.

Démonstration : Soit p un nombre premier. On vérifie facilement (à la main ou, mieux encore, en utilisant un logiciel de calcul formel) que si $X, Y \in \mathcal{C}_p$, alors $XY^{-1} \in \Gamma_0(p)$ si et seulement si $X = Y$.

Dénombrons maintenant les triplets $(a,b,c) \in \mathbb{F}_p^3$ tels que $ac = b^2$: il y a
- $(p-1)^2$ triplets de la forme $(a, b, b^2/a)$ pour $(a,b) \in (\mathbb{F}_p \setminus \{0\})^2$;
- $p-1$ triplets de la forme $(a,0,0)$ pour $a \in \mathbb{F}_p \setminus \{0\}$;
- $p-1$ triplets de la forme $(0,0,c)$ pour $c \in \mathbb{F}_p \setminus \{0\}$; et
- le triplet $(0,0,0)$;

soit au total p^2 triplets. On en déduit directement que $\mathrm{card}(\mathcal{C}_p) = p^3 + p^2 + p + 1$.

Pour conclure la démonstration, il reste à montrer que l'on a bien des représentants de toutes les classes. Comme $I \in \mathcal{C}_p$ et que l'ensemble $\mathcal{G} = \{J, S_2, T_2, M_1\}$ engendre Γ_2, il suffit de montrer que pour tous $X \in \mathcal{C}_p$ et $Y \in \mathcal{G}$, il existe $Z \in \mathcal{C}_p$ tel que $XYZ^{-1} \in \Gamma_0(p)$, calcul peu instructif que l'on ne reproduit pas ici.

□

Polynômes modulaires pour $\Gamma_0(p)$

Fixons un entier premier p, et définissons, pour $\ell \in [1,3]$, la fonction

$$\begin{aligned} j_{\ell,p} : \ \mathcal{H}_2 &\to \mathbb{C} \\ \tau &\mapsto j_\ell(p\tau), \end{aligned}$$

où j_1, j_2 et j_3 sont les invariants d'Igusa (introduits à la Section 6.3.3). Ces fonctions sont des fonctions modulaires de Siegel pour le groupe $\Gamma_0(p)$. Pour le voir, il suffit de remarquer que pour tous $\gamma = \begin{pmatrix} A & B \\ pC & D \end{pmatrix} \in \Gamma_0(p)$, $\ell \in [1,3]$ et $\tau \in \Gamma_2$, on a

$$\begin{aligned} j_{\ell,p}(\gamma\tau) &= j_\ell\left((pA\tau + pB)(pC\tau + D)^{-1}\right) \\ &= j_\ell\left(\gamma'(p\tau)\right) \\ &= j_\ell(p\tau) \\ &= j_{\ell,p}(\tau), \end{aligned}$$

où l'on a posé $\gamma' = \begin{pmatrix} A & pB \\ C & D \end{pmatrix} \in \Gamma_2$, et utilisé le fait que j_ℓ est modulaire pour Γ_2.

Le Théorème 5.1 montre alors que chacune des fonctions $j_{\ell,p}$ est liée algébriquement aux fonctions j_1, j_2 et j_3. Si l'on note $\mathcal{C}_p$ un ensemble de représentants des classes de $\Gamma_0(p)\backslash\Gamma_2$, on définit alors les polynômes

$$\Phi_{1,p}(X) = \prod_{\gamma\in\mathcal{C}_p} (X - j_{1,p}(\gamma\tau)),$$

$$\Psi_{2,p}(X) = \sum_{\gamma\in\mathcal{C}_p} j_{2,p}(\gamma\tau) \prod_{\gamma'\in\mathcal{C}_p\backslash\{\gamma\}} (X - j_{1,p}(\gamma\tau))$$

et

$$\Psi_{3,p}(X) = \sum_{\gamma\in\mathcal{C}_p} j_{3,p}(\gamma\tau) \prod_{\gamma'\in\mathcal{C}_p\backslash\{\gamma\}} (X - j_{1,p}(\gamma\tau)).$$

Par un raisonnement analogue à celui utilisé pour la démonstration de la Proposition 2.17 dans le cas du genre 1, on montre que les coefficients de ces polynômes, vus comme des fonctions de τ, sont des fonctions modulaires de Siegel pour le groupe Γ_2. D'après le Théorème 6.2, ces coefficients sont donc des fractions rationnelles en $j_1(\tau)$, $j_2(\tau)$ et $j_3(\tau)$, et nous supposerons dans la suite (sans le démontrer) que ces coefficients vivent dans $\mathbb{Q}(j_1, j_2, j_3)$ (une méthode possible pour le démontrer est de considérer les développements en séries en q des coefficients, comme suggéré par exemple par Gaudry dans [Gau00, p. 60–70]).

Notre but dans le reste de cette section est de donner un algorithme permettant de déterminer les polynômes modulaires $\Phi_{1,p}(X)$, $\Psi_{2,p}(X)$ et $\Psi_{3,p}(X)$ comme éléments de $\mathbb{Q}(j_1, j_2, j_3)[X]$ (c'est-à-dire de déterminer l'expression de chacun des coefficients des polynômes modulaires comme une fraction rationnelle en j_1, j_2 et j_3 à coefficients rationnels —ou entiers, puisque l'on pourra toujours s'y ramener—). Pour cela, nous allons utiliser une technique d'évaluation/interpolation, similaire dans l'idée avec celle proposée dans le cadre du genre 1 à la Section 4.4.2.

Principe du calcul des polynômes modulaires

Fixons un élément $\tau \in \mathcal{H}_2$. Alors, en utilisant les définitions des invariants d'Igusa à partir des theta constantes (voir la Section 6.3.3) et les Algorithmes 15 ou 16, on peut évaluer rapidement $j_1(\tau)$, $j_2(\tau)$ et $j_3(\tau)$ (en temps $O(\mathcal{M}(N)\log N)$ *a priori* si l'on utilise l'algorithme "rapide").

De la même façon, on peut évaluer les coefficients des polynômes $\Phi_{1,p}$, $\Psi_{2,p}$ et $\Psi_{3,p}$ (en évaluant les invariants d'Igusa en les $\gamma\tau$, pour γ parcourant l'ensemble de représentants des classes de $\Gamma_0(p)\backslash\Gamma_2$ donné par la Proposition 10.1 par exemple).

Supposons que $c = c(\tau)$ soit un coefficient d'un des polynômes modulaires d'indice p. On sait qu'il existe $N, D \in \mathbb{Z}[X, Y, Z]$ tels que, pour tout $\tau \in \mathcal{H}_2$,

$$c(\tau) = \frac{N(j_1(\tau), j_2(\tau), j_3(\tau))}{D(j_1(\tau), j_2(\tau), j_3(\tau))}.$$

Pour déterminer N et D, on peut calculer les valeurs de $c(\tau)$ et des $j_\ell(\tau)$ pour un certain nombre de valeurs distinctes de τ, puis interpoler N et D. Nous ne savons malheureusement pas effectuer cette étape d'interpolation dans ce cadre[†]. Pour résoudre le problème, nous allons commencer par montrer que l'on peut, au lieu de commencer par fixer τ, se donner un triplet de valeurs $(x, y, z) \in (\mathbb{C}\setminus\{0\})^3$, et déterminer $\tau \in \mathcal{H}_2$ tel que

$$(j_1(\tau), j_2(\tau), j_3(\tau)) = (x, y, z).$$

[†]Si $c(\tau)$ était une fraction rationnelle en *une seule* des fonctions $j_\ell(\tau)$, le problème serait plus simple, comme nous le verrons plus loin.

Pour cela, nous allons utiliser les résultats du Chapitre 9. Si l'on se donne un triplet de valeurs (x, y, z), on peut commencer par utiliser l'algorithme introduit par Mestre dans [Mes91] pour déterminer l'équation d'une courbe hyperelliptique ayant pour j-invariants x, y et z. La sortie de cet algorithme est un polynôme $P(X)$ de degré 6 décrivant la courbe d'équation $y^2 = P(x)$. On détermine alors des approximations des six racines complexes de ce polynôme (dans notre cas, en utilisant l'algorithme dit de Weierstrass–Durand–Kerner, décrit dans [Dur68, p. 277–280] et dans [Ker66]), puis on utilise les Algorithmes 12 et 13 pour déterminer un élément $\tau \in \mathcal{F}_2$ en lequel les invariants d'Igusa s'évaluent approximativement en x, y et z. La détermination de τ avec une précision de N bits se fait en temps $O(\mathcal{M}(N) \log N)$, et le temps pour évaluer $c(\tau)$ (toujours à précision N) est heuristiquement en $O\left(p^3 \mathcal{M}(N) \log N\right)$ (le facteur p^3 vient du nombre d'évaluation d'invariants d'Igusa nécessaires pour déterminer $c(\tau)$, qui est proportionnel à l'indice de $\Gamma_0(p)$ dans Γ_2, valant $p^3 + p^2 + p + 1$).

Ceci permet de se ramener au problème suivant : étant donné un "oracle" qui, étant donné des valeurs (x, y, z) *choisies*, donne la valeur de $\frac{N(x,y,z)}{D(x,y,z)}$, déterminer les polynômes $N(X, Y, Z)$ et $D(X, Y, Z)$ (qui vivent, on le rappelle, dans $\mathbb{Z}[X, Y, Z]$). Nous appelons ce problème l'*interpolation d'une fraction rationnelle*.

Interpolation d'une fraction rationnelle univariée

Supposons que l'on veuille *interpoler* (au sens défini ci-dessus) une fraction rationnelle $f(X) = \frac{A(X)}{B(X)}$, avec $A(X), B(X) \in \mathbb{Z}[X]$. Si l'on note α (resp. β) le degré de A (resp. de B), et que l'on dispose des valeurs de f en $x_1, \ldots, x_{\alpha+\beta+1}$ ($\alpha + \beta + 2$ nombres complexes distincts), alors on peut déterminer $(A_0, \ldots, A_\alpha, B_0, \ldots, B_\beta) \in \mathbb{Z}^{\alpha+\beta+2}$ tels que

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^\alpha & -f(x_1) & -f(x_1)x_1 & \ldots & -f(x_1)x_1^\beta \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^\alpha & -f(x_n) & -f(x_n)x_n & \ldots & -f(x_n)x_n^\beta \end{pmatrix} \cdot \begin{pmatrix} A_0 \\ \vdots \\ A_\alpha \\ B_0 \\ \vdots \\ B_\beta \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

et alors

$$f(X) = \frac{\sum_{n=0}^{\alpha} A_n X^n}{\sum_{n=0}^{\beta} B_n X^n}.$$

On notera que cette solution est définie à une constante (multiplicative) près.

En pratique, cette méthode nécessite la connaissance préalable des degrés α et β. On peut cependant les déterminer facilement, en considérant les matrices

$$M(m, n) = \begin{pmatrix} 1 & \ldots & x_1^m & -f(x_1) & \ldots & -f(x_1)x_1^n \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \ldots & x_{m+n+2}^m & -f(x_{m+n+2}) & \ldots & -f(x_{m+n+2})x_{m+n+2}^n \end{pmatrix}.$$

L'idée est de déterminer la plus petite valeur de n telle que l'espace des solutions du système associé à $M(2^n, 2^n)$ soit non-nul. Une base de l'espace des solutions permettra alors de déterminer les valeurs de α et β, ainsi qu'une solution $(A_0, \ldots, A_\alpha, B_0, \ldots, B_\beta)$.

Pour vérifier un tant soit peu les calculs et pouvoir mieux appréhender la complexité de cette méthode, il est possible de choisir des valeurs $x_j \in \mathbb{Q}[i]$ (si possible de petite hauteur). On évalue alors (*via* l'oracle) la valeur de $f(x_j)$ à une précision suffisante pour déterminer sa valeur exacte dans $\mathbb{Q}[i]$ (cette précision sera en $O(h(\alpha + \beta))$, où h est la hauteur de x_j, la valeur exacte

étant ensuite déterminée en considérant classiquement les développements en fraction continue des parties réelle et imaginaire de $f(x_j)$). Si l'on procède ainsi pour toutes les valeurs de x_j, on peut ensuite choisir un entier premier p congru à 1 modulo 4 (de sorte que -1 soit un résidu quadratique pour simplifier les choses), et réduire modulo p les x_j et $f(x_j)$ (ce qui permet de réduire i en un élément $i_p \in \mathbb{F}_p$ tel que $i_p^2 = -1$) afin de déterminer des solutions pour A et B modulo p (on évite les nombres p qui ne sont pas premiers avec l'un des dénominateurs des x_j ou $f(x_j)$). Le plus simple est sans doute de déterminer les coefficients de A et B modulo p en forçant le monôme de plus bas degré de B à avoir pour coefficient 1. Si l'on répète ce processus pour un nombre suffisant de nombres premiers p distincts, on peut alors reconstruire les coefficients de A et B par le théorème des restes chinois. Notons que comme l'on a forcé le monôme de plus bas degré de B à être unitaire, les coefficients de A et B que l'on recherche ne sont pas entiers mais rationnels : il suffit de les calculer (*via* les restes chinois) modulo le produit des premiers p, puis d'utiliser l'algorithme d'Euclide étendu pour reconstruire les rationnels correspondants, et finalement déterminer une solution $A(X), B(X) \in \mathbb{Z}[X]$ au problème de départ.

Une variante un peu moins naïve (permettant en particulier de s'affranchir de l'étape d'algèbre linéaire), présentée dans [BP94, p. 45–48] ou dans [GG99, p. 110–112], consiste à calculer deux polynômes $P(X), V(X) \in \mathbb{Z}[X]$ tels que, pour tout j, $P(x_j) = f(x_j)$ et $V(x_j) = 0$. Les polynômes $A(X)$ et $B(X)$ peuvent ensuite être calculés par l'algorithme d'Euclide (étendu) entre $P(X)$ et $V(X)$. Bien sûr, en pratique il est là encore préférable d'utiliser le théorème des restes chinois pour se ramener à travailler modulo de (petits) nombres premiers.

Nous n'analysons pas en détail la complexité de la reconstruction de fractions rationnelles. Dans le cas qui nous intéresse, même si nous avons utilisé la méthode "naïve" à base d'algèbre linéaire, l'étape limitante en pratique est l'évaluation de f en les x_j. Notons que quelle que soit la méthode utilisée, il faut disposer des valeurs de f en $O(\alpha + \beta)$ points distincts.

Interpolation d'une fraction rationnelle multivariée

Nous revenons ici au problème de départ. Nous limitons en fait notre présentation au cas d'une fraction rationnelle en deux variables $f(X, Y) = \frac{A(X,Y)}{B(X,Y)} \in \mathbb{Q}(X, Y)$, les autres cas s'en déduisant directement.

Une première idée est de déterminer, pour une valeur $y \in \mathbb{Q}[i]$ fixée, la fraction rationnelle *univariée* $f(X, y)$ (par la méthode décrite plus haut). Si l'on procède ainsi pour plusieurs valeurs distinctes $y_1, \ldots, y_n$ de y, on obtient des décompositions sous la forme

$$f(X, y_j) = \frac{\sum_{k=0} \alpha_X A_k(y_j) X^k}{\sum_{k=0}^{\beta_X} B_k(y_j) X^k},$$

où les coefficients $A_k(y_j)$ et $B_k(y_j)$ sont des polynômes en y_j (ceci revient à considérer $f(X, Y)$ comme vivant dans $\mathbb{Z}[Y](X)$). Le problème est que l'*on ne peut pas interpoler les polynômes $A_k(Y)$ et $B_k(Y)$, car ils ne sont déterminés qu'à une constante multiplicative près !*

Nous décrivons maintenant la méthode que nous avons utilisée[‡]. Écrivons la fraction rationnelle f sous la forme

$$f(X, Y) = \frac{\sum_{k=0}^{d_A} A_k(X, Y)}{\sum_{k=0}^{d_B} B_k(X, Y)},$$

où $A_k(X, Y)$ (resp. $B_k(X, Y)$) est un polynôme *homogène* de degré k (à coefficients rationnels). On suppose ici que $B_0 = 1$ (on peut toujours s'y ramener en considérant $f(X + r_x, Y + r_y)$ avec r_x, r_y aléatoires).

[‡]Cette méthode nous a été suggérée par Éric Schost, nous l'en remercions ici.

k	$n_{1,k}$	$d_{1,k}$	$n_{2,k}$	$d_{2,k}$	$n_{3,k}$	$d_{3,k}$
0	60	51	75	42	50	30
1	58	49	72	42	48	30
2	58	49	72	42	48	30
3	57	48	70	42	46	30
4	57	48	70	42	46	30
5	55	46	67	42	45	30
6	55	46	67	42	45	30
7	53	45	65	42	43	30
8	52	45	65	42	43	30
9	49	43	62	42	41	30
10	48	43	62	42	41	30
11	46	42	60	42	40	30
12	45	42	60	42	40	30
13	41	39	55	42	36	30
14	37	36	50	42	33	30

TAB. 10.1 – Degrés des numérateurs et dénominateurs des $c_{2,k}$ en j_1, j_2 et j_3

On peut alors, pour différentes valeurs y_j, reconstruire la fraction rationnelle univariée $f(X, Xy_j)$ (en utilisant les méthodes décrites plus haut), sous la forme

$$f(X, Xy_j) = \frac{\sum_{k=0}^{d_A} A_{k,j} X^k}{\sum_{k=0}^{d_B} B_{k,j} X^k},$$

avec $B_{0,j} = 1$ pour tout j. Les $A_k(X, Y)$ et $B_k(X, Y)$ peuvent alors être calculés par simple interpolation.

Nous ne détaillons pas la complexité de cette méthode, mais notons qu'elle nécessite la connaissance de $O\left(d_Y(f)d_t(f)\right)$ valeurs de f, où $d_Y(f)$ désigne le degré maximal en Y du numérateur et du dénominateur de f, et $d_t(f)$ le degré "total" de f, c'est-à-dire la somme des degrés totaux du numérateur et du dénominateur.

Résultats expérimentaux

Nous avons commencé par essayer de calculer $\Phi_{1,2}$, $\Psi_{2,2}$ et $\Psi_{3,2}$. En pratique, nous avons écrit $\Phi_{1,2}$ sous la forme

$$\Phi_{1,2}(X) = X^{15} + \sum_{k=0}^{14} c_{2,k}(j_1, j_2, j_3) X^k,$$

avec $c_{2,k}(j_1, j_2, j_3) \in \mathbb{Q}(j_1, j_2, j_3)$, et utilisé les méthodes décrites plus haut pour obtenir l'expression des fractions rationnelles $c_{2,k}$. Avant toute chose, nous avons déterminé les degrés en j_1, j_2 et j_3 des numérateurs et dénominateurs de chacun des $c_{2,k}$. Ces données sont rassemblées dans la Table 10.1, où $n_{k,\ell}$ (resp. $d_{k,\ell}$) désigne le degré du numérateur (resp. du dénominateur) de $c_{2,k}$ en j_ℓ.

En expérimentant, nous avons remarqué que si, pour $j_1, j_2, j_3 \in \mathbb{Z}[i]$, on calcule $c_{2,k}(j_1, j_2, j_3) = \frac{x+yi}{z}$ avec $x, y, z \in \mathbb{Z}$, alors en considérant la factorization de z, on constate que z est "presque" une puissance sixième. Toujours en expérimentant, nous en sommes venu à supposer que pour tout k, le dénominateur de $1458\, j_1^{d_{1,k}-36} c_{2,k}(j_1, j_2, j_3)$ est toujours une même puissance sixième (ne dépendant pas de k).

Nous avons donc cherché à déterminer $D_2(j_1,j_2,j_3) \in \mathbb{Z}[j_1,j_2,j_3]$ tel que, pour tout $k \in [0,14]$,

$$c_{2,k}(j_1,j_2,j_3) = \frac{N_{2,k}(j_1,j_2,j_3)}{1458\, j_1^{d_{1,k}-36} D_2(j_1,j_2,j_3)^6},$$

avec $N_{2,k}(j_1,j_2,j_3) \in \mathbb{Z}[j_1,j_2,j_3]$.

Pour cela, nous nous sommes concentré sur le cas $k=14$, pour lequel le degré du numérateur est le plus bas. Nous avons commencé par fixer deux valeurs $y,z \in \mathbb{Z}[i]$ (ayant de petites hauteurs), et nous avons évalué $c_{2,14}(x,xy,xz)$ pour différentes valeurs de $x \in \mathbb{Z}[i]$ (elles aussi de petites hauteurs), jusqu'à avoir assez de valeurs pour reconstruire la fraction rationnelle $c_{2,14}(X,Xy,Xz)$. Le tableau ci-dessus montre qu'il est *a priori* suffisant d'utiliser

$$37+36+50+42+33+30+2 = 230$$

valeurs distinctes de x. En pratique, seulement 40 valeurs distinctes ont été nécessaires. Ceci s'explique comme suit : *a fortiori* on a pu vérifier que $c_{2,14}$ est de la forme

$$c_{2,14}(j_1,j_2,j_3) = \frac{\sum_{k=30}^{50} N_{2,14,k}(j_1,j_2,j_3)}{1458\, \left(j_1 \sum_{k=4}^{7} D_{2,k}(j_1,j_2,j_3)\right)^6},$$

où les $N_{2,14,k}$ et $D_{2,k}$ sont des polynômes homogènes de degré k. Si l'on s'intéresse à $c_{2,14}(X,Xy,Xz)$, il y a donc simplification de X^{30} entre numérateur et dénominateur, et cette fraction rationnelle en X peut finalement être représentée comme le quotient d'un polynôme de degré 20 en X sur un autre de degré 18. La reconstruction de ces polynômes nécessite alors $20+18+2 = 40$ valeurs distinctes, ce qui correspond bien.

En utilisant par ailleurs 8 valeurs distinctes pour y et 6 valeurs distinctes pour z, nous avons pu déterminer entièrement le dénominateur de $c_{2,14}(j_1,j_2,j_3)$, qui est de la forme

$$1458\,(j_1 D_2(j_1,j_2,j_3))^6$$

avec

$$\begin{aligned}
D_2(j_1,j_2,j_3) &= 236196 j_1^5 - 972 j_1^4 j_2^2 + 5832 j_1^4 j_2 j_3 + 19245600 j_1^4 j_2 - 8748 j_1^4 j_3^2 - 104976000 j_1^4 j_3 \\
&+ 125971200000 j_1^4 + j_1^3 j_2^4 - 12 j_1^3 j_2^3 j_3 - 77436 j_1^3 j_2^3 + 54 j_1^3 j_2^2 j_3^2 + 870912 j_1^3 j_2^2 j_3 - 507384000 j_1^3 j_2^2 \\
&- 108 j_1^3 j_2 j_3^3 - 3090960 j_1^3 j_2 j_3^2 + 2099520000 j_1^3 j_2 j_3 + 81 j_1^3 j_3^4 + 3499200 j_1^3 j_3^3 + 78 j_1^2 j_2^5 - 1332 j_1^2 j_2^4 j_3 \\
&+ 592272 j_1^2 j_2^4 + 8910 j_1^2 j_2^3 j_3^2 - 4743360 j_1^2 j_2^3 j_3 - 29376 j_1^2 j_2^2 j_3^3 + 9331200 j_1^2 j_2^2 j_3^2 + 47952 j_1^2 j_2 j_3^4 \\
&- 31104 j_1^2 j_3^5 - 159 j_1 j_2^6 + 1728 j_1 j_2^5 j_3 - 41472 j_1 j_2^5 - 6048 j_1 j_2^4 j_3^2 + 6912 j_1 j_2^3 j_3^3 + 80 j_2^7 - 384 j_2^6 j_3.
\end{aligned}$$

Ce calcul a nécessité $40 \times 8 \times 6 = 1920$ évaluations de $c_{2,14}(x,xy,xz)$, la précision nécessaire pour reconstruire la valeur exacte dans $\mathbb{Q}[i]$ étant (compte tenu des hauteurs des valeurs de $x,y,z \in \mathbb{Z}[i]$ utilisées) de 3000 bits.

En utilisant notre implémentation en langage C des Algorithmes 12, 13 et 16, le temps d'une évaluation de c_{14} était de l'ordre de 2.15 secondes (ce temps correspond au calcul de $\tau \in \mathcal{F}_2$ tel que $(x,xy,xz) = (j_1(\tau), j_2(\tau), j_3(\tau))$ d'une part, et à l'évaluation de $j_1(2\gamma_k\tau)$ pour les 15 représentants γ_k de $\Gamma_0(2)\backslash\Gamma_2$ d'autre part), sur un AMD Athlon 64 3400+ (avec 2 Go de RAM, mais ces calculs sont peu gourmands en mémoire). Le temps total consacré aux évaluations de c_{14} pour le calcul de D_2 a donc été d'environ 70 minutes. La phase d'interpolation a été programmée de façon relativement naïve en Magma, et le temps de calcul a été négligeable.

L'avantage de commencer par le calcul de D_2 est que nous avons pu nous en servir ensuite pour réduire les calculs nécessaires à la détermination des numérateurs des $c_{2,k}(j_1,j_2,j_3)$, en se

k	$n_{1,k}$	$d_{1,k}$	$n_{2,k}$	$d_{2,k}$	$n_{3,k}$	$d_{3,k}$	k	$n_{1,k}$	$d_{1,k}$	$n_{2,k}$	$d_{2,k}$	$n_{3,k}$	$d_{3,k}$
0	304	288	420	360	278	234	20	293	277	402	360	266	234
1	302	286	417	360	276	234	21	293	277	402	360	266	234
2	302	286	417	360	276	234	22	292	276	400	360	264	234
3	302	286	417	360	276	234	23	292	276	400	360	264	234
4	301	285	415	360	274	234	24	292	276	400	360	264	234
5	301	285	415	360	274	234	25	289	274	397	360	263	234
6	301	285	415	360	274	234	26	288	274	397	360	263	234
7	299	283	412	360	273	234	27	287	274	397	360	263	234
8	299	283	412	360	273	234	28	285	273	395	360	261	234
9	299	283	412	360	273	234	29	284	273	395	360	261	234
10	298	282	410	360	271	234	30	283	273	395	360	261	234
11	298	282	410	360	271	234	31	280	271	392	360	259	234
12	298	282	410	360	271	234	32	279	271	392	360	259	234
13	296	280	407	360	269	234	33	278	271	392	360	259	234
14	296	280	407	360	269	234	34	276	270	390	360	258	234
15	296	280	407	360	269	234	35	275	270	390	360	258	234
16	295	279	405	360	268	234	36	274	270	390	360	258	234
17	295	279	405	360	268	234	37	268	265	382	360	253	234
18	295	279	405	360	268	234	38	263	261	375	360	248	234
19	293	277	402	360	266	234	39	257	256	367	360	243	234

TAB. 10.2 – Degrés des numérateurs et dénominateurs des $c_{3,k}$ en j_1, j_2 et j_3

ramenant à l'évaluation/interpolation des *polynômes* trivariés $N_{2,k}(j_1, j_2, j_3)$ (ce qui permettait aussi de réduire la précision nécessaire dans les évaluations). La détermination des $N_{2,k}(j_1, j_2, j_3)$ a nécessité (d'après la Table 10.1) 61 valeurs de j_1, 76 valeurs de j_2 et 51 valeurs de j_3, soit $61 \times 76 \times 51 = 236436$ évaluations, mais la précision nécessaire n'était plus que de 1500 bits, et chaque évaluation prenait alors (sur la même machine que précédemment) de l'ordre de 0.92 seconde, soit un temps total pour les évaluations d'environ 3600 minutes (soit 60 heures). Là encore, la phase d'interpolation a été programmée en MAGMA, et le temps de calcul a été négligeable.

Nous ne donnons pas ici explicitement les expressions des polynômes $N_{2,k}(j_1, j_2, j_3)$ (une fois compressés, les fichiers contenant leurs coefficients occupent environ 26.8 Mo d'espace disque !). Ces polynômes sont toutefois disponibles (ainsi que les polynômes définissant $\Psi_{2,2}$ et $\Psi_{2,3}$) à l'adresse `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/MODPOL_2.tar.gz`. On notera que les dénominateurs de tous les coefficients de $\Psi_{2,2}$ et de $\Psi_{2,3}$ sont de la même forme que ceux des $c_{2,k}$, à savoir

$$\mathrm{Cste}\, j_1^{\cdot\cdot} D_2(j_1, j_2, j_3)^6.$$

Nous nous sommes ensuite attaqué au calcul de $\Phi_{3,1}$ (que nous n'avons pas terminé). Les résultats que nous avons obtenus sont les suivants : si l'on pose

$$\Phi_{3,1}(X) = X^{40} + \sum_{k=0}^{39} c_{3,k}(j_1, j_2, j_3) X^k,$$

alors nous avons commencé par déterminer les degrés $d_{\ell,k}$ (resp. $n_{\ell,k}$) des numérateurs (resp. dénominateurs) des $c_{3,k}$ en les j_ℓ, qui sont donnés dans la Table 10.2.

En procédant comme pour $\Phi_{2,1}$, nous avons remarqué que pour tout k, $c_{3,k}$ s'écrivait sous

la forme

$$c_{3,k}(j_1,j_2,j_3) = \frac{N_{3,k}(j_1,j_2,j_3)}{2^4 \times 3^{41} \times 5^5 \times 19^{10} \times 29^5\, j_1^{d_{1,k}-252} D_3(j_1,j_3,j_3)^{18}},$$

avec $N_{3,k}(j_1,j_2,j_3) \in \mathbb{Z}[j_1,j_2,j_3]$ et $D_3(j_1,j_2,j_3) \in \mathbb{Z}[j_1,j_2,j_3]$, D_3 étant de degré 14 en j_1, 20 en j_2 et 13 en j_3 (les degrés des $N_{3,k}$ se déduisant quant à eux directement du tableau donné ci-dessus).

En nous intéressant à $c_{3,39}$, nous avons pu entièrement déterminer D_3, que nous donnons p. 227. Ce calcul a nécessité l'évaluation de $c_{3,39}$ en $197 \times 21 \times 14 = 57918$ valeurs distinctes de (j_1,j_2,j_3), à une précision de 11000 bits. Chaque évaluation nécessitant de l'ordre de 36.5 secondes, le temps total de calcul nécessaire (pour les évaluations) est de l'ordre de 587 heures (les calculs ont été parallélisés sur 6 processeurs identiques, ce qui a permis de se ramener à un temps de calcul réel d'environ 4 jours). Comme précédemment, l'interpolation a été programmée en Magma, et le temps de calcul a été négligeable comparé à la phase d'évaluation.

Nous n'avons pas déterminé les $N_{3,k}(j_1,j_2,j_3)$, mais il semblerait qu'ils soient factorisables (des puissances cinquièmes et sixièmes apparaissant dans leurs factorisations), ce qui pourrait être utilisé pour réduire le temps de calcul nécessaire à leur détermination. Leur calcul complet parait envisageable, mais sera coûteux en temps de calcul (si l'on s'en tient à l'utilisation des techniques évoquées ci-dessus).

Plusieurs pistes sont intéressantes si l'on souhaite poursuivre dans le calcul et l'étude de polynômes modulaires en genre 2 pour les groupes $\Gamma_0(p)$:

- essayer de démontrer certaines de leurs propriétés (par exemple, trouver une signification au dénominateur commun qui a l'air d'apparaître, et une formule pour la puissance à laquelle il apparaît) ;
- utiliser des séries trivariées (comme proposé par exemple dans la thèse de Pierrick Gaudry [Gau00]) pour *démontrer* que les résultats que nous avons obtenus sont corrects, et/ou améliorer l'algorithme de calcul que nous avons utilisé ;
- essayer de trouver d'autres invariants que ceux d'Igusa, tels que les polynômes modulaires associés aient de meilleures propriétés (plus petites hauteurs par exemple), comme on le fait en genre 1.

$$
\begin{aligned}
D_3(j_1,j_2,j_3) = {} & 2^4\times 3^{31}\times 5^5\times 19^{10}\times 29^5 j_1^{12} - 2^4\times 3^{32}\times 19^5\times 47\times 17064586291\, j_1^{13} + 2^6\times 3^{31}\times 5^3\times 13\times 19^7\times 29^2\times 131\times 1949\, j_1^{12} j_3 \\
& - 2^4\times 3^{30}\times 5^2\times 7\times 19^6\times 29\times 4701082031\, j_1^{12} j_2 + 2^{11}\times 3^{28}\times 5^4\times 19^8\times 29^3\times 5557\, j_1^{11} j_2 j_3 - 2^9\times 3^{27}\times 5^3\times 19^9\times 23\times 29^2\times 37\times 149\, j_1^{11} j_2^2 \\
& - 2^2\times 3^{30}\times 11^{12} j_1^{14} + 2^{12}\times 3^{29}\times 5\times 11^5\times 19^2\times 41\times 1399\, j_1^{13} j_3 - 2^5\times 3^{27}\times 19^4\times 59\times 109\times 6570848059\, j_1^{12} j_3^2 \\
& + 2^9\times 3^{24}\times 5^2\times 19^6\times 29\times 449\times 160827643\, j_1^{11} j_3^3 - 2^3\times 3^{28}\times 7\times 11^5\times 19\times 305677787\, j_1^{13} j_2 + 2^8\times 3^{26}\times 11\times 19^3\times 12997844123599\, j_1^{12} j_2 j_3 \\
& - 2^5\times 3^{24}\times 5\times 11\times 19^5\times 3517\times 53807008819\, j_1^{11} j_2 j_3^2 - 2^2\times 3^{25}\times 19^2\times 163\times 368477994090277\, j_1^{12} j_2^2 \\
& + 2^7\times 3^{23}\times 19^4\times 64634951\times 486375839\, j_1^{11} j_2^2 j_3 + 2^9\times 3^{24}\times 5^2\times 7\times 11\times 19^6\times 29\times 61\times 241\times 59051\, j_1^{10} j_2^2 j_3^2 \\
& - 2^3\times 3^{21}\times 19^3\times 225900161\times 27135844457\, j_1^{11} j_2^3 - 2^9\times 3^{23}\times 5\times 11\times 19^5\times 23413242718669\, j_1^{10} j_2^3 j_3 \\
& + 2^5\times 3^{22}\times 19^4\times 83\times 349813\times 4414606477\, j_1^{10} j_2^4 - 2^9\times 3^{24}\times 13\times 19^5\times 41\times 7849496341\, j_1^9 j_2^5 - 2^4\times 3^{28}\times 11^{10} j_1^{13} j_3^2 \\
& + 2^7\times 3^{26}\times 5^2\times 11^3\times 19\times 239\times 592133\, j_1^{12} j_3^3 - 2^6\times 3^{24}\times 13\times 19^3\times 53\times 953\times 289296559\, j_1^{11} j_3^4 - 2^{12}\times 3^{27}\times 19^5\times 7943431\, j_1^{10} j_3^5 \\
& + 2^5\times 3^{27}\times 11^{10} j_1^{13} j_2 j_3 - 2^6\times 3^{26}\times 11^3\times 30977\times 3469639\, j_1^{12} j_2 j_3^2 + 2^9\times 3^{23}\times 13\times 19^2\times 557\times 62927\times 2729633\, j_1^{11} j_2 j_3^3 \\
& + 2^{11}\times 3^{23}\times 19^4\times 36533154133859\, j_1^{10} j_2 j_3^4 - 2^4\times 3^{26}\times 11^{10} j_1^{13} j_2^2 + 2^4\times 3^{25}\times 11^3\times 149\times 263\times 277\times 32099\, j_1^{12} j_2^2 j_3 \\
& - 2^4\times 3^{23}\times 19\times 251\times 433\times 2039\times 1155491891\, j_1^{11} j_2^2 j_3^2 - 2^{10}\times 3^{22}\times 19^3\times 73\times 518831\times 107124221\, j_1^{10} j_2^2 j_3^3 \\
& - 2^2\times 3^{23}\times 5\times 11^3\times 23\times 59\times 71\times 2390879\, j_1^{12} j_2^3 + 2^8\times 3^{21}\times 5\times 7\times 19\times 607819187655293\, j_1^{11} j_2^3 j_3 \\
& + 2^7\times 3^{23}\times 11\times 19^2\times 2909\times 2301281960303\, j_1^{10} j_2^3 j_3^2 + 2^{13}\times 3^{23}\times 19^4\times 858883\times 6258697\, j_1^9 j_2^3 j_3^3 - 2^2\times 3^{20}\times 11\times 29221\times 13097683362521\, j_1^{11} j_2^4 \\
& - 2^{12}\times 3^{20}\times 13\times 19\times 853\times 49417\times 334911601\, j_1^{10} j_2^4 j_3 - 2^{12}\times 3^{21}\times 19^3\times 1136567\times 1232464019\, j_1^9 j_2^4 j_3^2 \\
& + 2^4\times 3^{19}\times 5\times 7^2\times 17\times 103\times 353583879893971\, j_1^{10} j_2^5 + 2^{10}\times 3^{20}\times 5^3\times 19^2\times 2879\times 10457\times 21317083\, j_1^9 j_2^5 j_3 \\
& - 2^6\times 3^{19}\times 19\times 29\times 449\times 51131\times 9269294087\, j_1^9 j_2^6 - 2^{12}\times 3^{21}\times 19^3\times 157\times 193077561767\, j_1^8 j_2^6 j_3 + 2^{11}\times 3^{21}\times 5\times 7\times 13\times 19^2\times 47\times 9019003787\, j_1^8 j_2^7 \\
& - 2^4\times 3^{25}\times 5\times 11^8 j_1^{12} j_3^4 - 2^8\times 3^{24}\times 11\times 23\times 359\times 5363887\, j_1^{11} j_3^5 + 2^7\times 3^{21}\times 5\times 7\times 19^2\times 5241332618339\, j_1^{10} j_3^6 \\
& + 2^6\times 3^{24}\times 5\times 11^8 j_1^{12} j_2 j_3^3 + 2^6\times 3^{23}\times 11\times 13^2\times 4084495637\, j_1^{11} j_2 j_3^4 - 2^{14}\times 3^{21}\times 19\times 46021575357193\, j_1^{10} j_2 j_3^5 \\
& - 2^{11}\times 3^{26}\times 5\times 19^3\times 2251\times 22807\, j_1^9 j_2 j_3^6 - 2^5\times 3^{24}\times 5\times 11^8 j_1^{12} j_2^2 j_3^2 - 2^6\times 3^{22}\times 7\times 11\times 145580724439\, j_1^{11} j_2^2 j_3^3 \\
& + 2^4\times 3^{20}\times 7\times 233\times 81899\times 13955891671\, j_1^{10} j_2^2 j_3^4 + 2^{13}\times 3^{20}\times 7\times 19^2\times 51787\times 163788913\, j_1^9 j_2^2 j_3^5 + 2^6\times 3^{22}\times 5\times 11^8 j_1^{12} j_2^3 j_3 \\
& + 2^3\times 3^{21}\times 11\times 23\times 59\times 24749\times 164011\, j_1^{11} j_2^3 j_3^2 - 2^6\times 3^{18}\times 1527894629629140391\, j_1^{10} j_2^3 j_3^3 - 2^7\times 3^{19}\times 19\times 289629349486378333\, j_1^9 j_2^3 j_3^4 \\
& - 2^4\times 3^{21}\times 5\times 11^8 j_1^{12} j_2^4 - 2^4\times 3^{20}\times 5^2\times 7\times 11\times 24509\times 182029\, j_1^{11} j_2^4 j_3 + 2^3\times 3^{18}\times 110246267\times 22315765057\, j_1^{10} j_2^4 j_3^2 \\
& + 2^{11}\times 3^{19}\times 367\times 501746471342317\, j_1^9 j_2^4 j_3^3 + 2^{11}\times 3^{20}\times 19^2\times 331691\times 332432941\, j_1^8 j_2^4 j_3^4 + 2^3\times 3^{19}\times 5^2\times 7\times 11\times 13^2\times 317\times 10753\, j_1^{11} j_2^5 \\
& - 2^9\times 3^{17}\times 104067191\times 116556229\, j_1^{10} j_2^5 j_3 - 2^5\times 3^{17}\times 281\times 701\times 143110201279489\, j_1^9 j_2^5 j_3^2 - 2^{18}\times 3^{18}\times 19^2\times 71\times 1373\times 87398407\, j_1^8 j_2^5 j_3^3 \\
& + 3^{15}\times 13\times 104543\times 1759532749063\, j_1^{10} j_2^6 + 2^6\times 3^{16}\times 3785393\times 1469365755259\, j_1^9 j_2^6 j_3 + 2^7\times 3^{17}\times 11\times 1279\times 530730870516383\, j_1^8 j_2^6 j_3^2 \\
& - 2^3\times 3^{16}\times 67\times 251\times 541\times 254161305991\, j_1^9 j_2^7 - 2^{11}\times 3^{16}\times 5^2\times 17\times 109\times 28909\times 176172169\, j_1^8 j_2^7 j_3 \\
& - 2^{11}\times 3^{18}\times 5^2\times 19\times 179\times 4003\times 14631839\, j_1^7 j_2^7 j_3^2 + 2^4\times 3^{16}\times 1829155862631992107\, j_1^8 j_2^8 + 2^{13}\times 3^{16}\times 11\times 127\times 47387\times 24532093\, j_1^7 j_2^8 j_3 \\
& + 2^7\times 3^{15}\times 7\times 127\times 683\times 17981\times 1014557\, j_1^7 j_2^9 + 2^{11}\times 3^{16}\times 5\times 15121\times 24071\times 39419\, j_1^6 j_2^{10} - 2^7\times 3^{21}\times 5\times 11^6 j_1^{11} j_3^6 \\
& + 2^9\times 3^{20}\times 139\times 9439\times 23357\, j_1^{10} j_3^7 - 2^{15}\times 3^{20}\times 5\times 7\times 19\times 739425329\, j_1^9 j_3^8 + 2^8\times 3^{21}\times 5\times 11^6 j_1^{11} j_2 j_3^5 - 2^8\times 3^{19}\times 5\times 31\times 2837900633\, j_1^{10} j_2 j_3^6 \\
& + 2^{12}\times 3^{21}\times 11549\times 309353347\, j_1^9 j_2 j_3^7 - 2^7\times 3^{20}\times 5^2\times 11^6 j_1^{11} j_2^2 j_3^4 + 2^6\times 3^{19}\times 5\times 29501\times 12118591\, j_1^{10} j_2^2 j_3^5 \\
& - 2^{10}\times 3^{18}\times 23\times 2549\times 3359\times 2306753\, j_1^9 j_2^2 j_3^6 - 2^{16}\times 3^{20}\times 7\times 19\times 955597939\, j_1^8 j_2^2 j_3^7 + 2^9\times 3^{18}\times 5^2\times 11^6 j_1^{11} j_2^3 j_3^3 \\
& - 2^4\times 3^{17}\times 5^2\times 17\times 23563\times 3595639\, j_1^{10} j_2^3 j_3^4 + 2^9\times 3^{17}\times 7\times 11\times 13\times 80077\times 22613431\, j_1^9 j_2^3 j_3^5 + 2^{14}\times 3^{20}\times 19\times 128219302819\, j_1^8 j_2^3 j_3^6 \\
& - 2^7\times 3^{18}\times 5^2\times 11^6 j_1^{11} j_2^4 j_3^2 + 2^6\times 3^{16}\times 5\times 19\times 94637239717\, j_1^{10} j_2^4 j_3^3 - 2^8\times 3^{17}\times 1051\times 2099\times 675639527\, j_1^9 j_2^4 j_3^4 \\
& - 2^{12}\times 3^{18}\times 7\times 17892676054037\, j_1^8 j_2^4 j_3^5 + 2^8\times 3^{17}\times 5\times 11^6 j_1^{11} j_2^5 j_3 - 2^5\times 3^{16}\times 17\times 1553\times 7177\times 18797\, j_1^{10} j_2^5 j_3^2 \\
& + 2^7\times 3^{15}\times 7\times 229\times 25919\times 168130307\, j_1^9 j_2^5 j_3^3 + 2^{10}\times 3^{19}\times 23^2\times 217454967241\, j_1^8 j_2^5 j_3^4 + 2^{16}\times 3^{19}\times 7\times 65032448497\, j_1^7 j_2^5 j_3^5 \\
& - 2^7\times 3^{15}\times 5\times 11^6 j_1^{11} j_2^6 + 2^7\times 3^{14}\times 5\times 29\times 47\times 2777\times 46199\, j_1^{10} j_2^6 j_3 - 2^5\times 3^{14}\times 613\times 217319\times 101345213\, j_1^9 j_2^6 j_3^2 \\
& - 2^9\times 3^{16}\times 2372756188260637\, j_1^8 j_2^6 j_3^3 - 2^{14}\times 3^{17}\times 6311\times 5256671467\, j_1^7 j_2^6 j_3^4 - 2^4\times 3^{13}\times 5\times 47\times 61091\times 67733\, j_1^{10} j_2^7 \\
& + 2^6\times 3^{14}\times 19\times 877\times 36902721601\, j_1^9 j_2^7 j_3 + 2^8\times 3^{15}\times 29\times 457\times 174799\times 1336561\, j_1^8 j_2^7 j_3^2 + 2^{12}\times 3^{16}\times 17\times 41\times 409599151231\, j_1^7 j_2^7 j_3^3 \\
& - 2^5\times 3^{12}\times 507349\times 860517659\, j_1^9 j_2^8 - 2^6\times 3^{14}\times 11\times 19\times 31\times 379\times 1758651787\, j_1^8 j_2^8 j_3 - 2^{10}\times 3^{16}\times 19\times 181\times 12923\times 8578123\, j_1^7 j_2^8 j_3^2 \\
& - 2^{16}\times 3^{17}\times 130729\times 7167367\, j_1^6 j_2^8 j_3^3 + 2^4\times 3^{13}\times 2502264181899431\, j_1^8 j_2^9 + 2^9\times 3^{14}\times 499\times 2185411087481\, j_1^7 j_2^9 j_3 \\
& + 2^{14}\times 3^{14}\times 13\times 171233\times 29973487\, j_1^6 j_2^9 j_3^2 - 2^8\times 3^{14}\times 5^2\times 7\times 23593\times 32337101\, j_1^7 j_2^{10} - 2^{12}\times 3^{14}\times 7\times 29\times 43\times 6319982881\, j_1^6 j_2^{10} j_3 \\
& + 2^{10}\times 3^{12}\times 373\times 4789\times 69109921\, j_1^6 j_2^{11} - 2^{16}\times 3^{14}\times 4969\times 300359489\, j_1^5 j_2^{11} j_3 + 2^{14}\times 3^{13}\times 5\times 73\times 139\times 163\times 520963\, j_1^5 j_2^{12} \\
& - 2^6\times 3^{19}\times 5\times 11^4 j_1^{10} j_3^8 + 2^{10}\times 3^{17}\times 63092123\, j_1^9 j_3^9 + 2^{17}\times 3^{20}\times 5\, j_1^8 j_3^{10} + 2^9\times 3^{18}\times 5\times 11^4 j_1^{10} j_2 j_3^7 \\
& - 2^7\times 3^{18}\times 7\times 17\times 71\times 97\times 509\, j_1^9 j_2 j_3^8 - 2^{14}\times 3^{17}\times 5\times 269\times 2061691\, j_1^8 j_2 j_3^9 - 2^8\times 3^{17}\times 5\times 7\times 11^4 j_1^{10} j_2^2 j_3^6 + 2^9\times 3^{18}\times 108716203\, j_1^9 j_2^2 j_3^7 \\
& + 2^{15}\times 3^{16}\times 9767\times 1276579\, j_1^8 j_2^2 j_3^8 + 2^9\times 3^{16}\times 5\times 7\times 11^4 j_1^{10} j_2^3 j_3^5 - 2^5\times 3^{15}\times 5\times 43\times 79\times 1528937\, j_1^9 j_2^3 j_3^6 - 2^{12}\times 3^{15}\times 71\times 691\times 8114567\, j_1^8 j_2^3 j_3^7 \\
& - 2^{15}\times 3^{17}\times 697542973\, j_1^7 j_2^3 j_3^8 - 2^7\times 3^{15}\times 5^2\times 7\times 11^4 j_1^{10} j_2^4 j_3^4 + 2^6\times 3^{15}\times 5\times 2083\times 361447\, j_1^9 j_2^4 j_3^5 + 2^{10}\times 3^{15}\times 449\times 2748159773\, j_1^8 j_2^4 j_3^6 \\
& + 2^{16}\times 3^{15}\times 5^2\times 11\times 50130251\, j_1^7 j_2^4 j_3^7 + 2^9\times 3^{14}\times 5\times 7\times 11^4 j_1^{10} j_2^5 j_3^3 - 2^5\times 3^{15}\times 23\times 27616361\, j_1^9 j_2^5 j_3^4 - 2^9\times 3^{13}\times 13\times 4091\times 207679247\, j_1^8 j_2^5 j_3^5 \\
& - 2^{13}\times 3^{14}\times 1181\times 445809677\, j_1^7 j_2^5 j_3^6 - 2^8\times 3^{13}\times 5\times 7\times 11^4 j_1^{10} j_2^6 j_3^2 - 2^7\times 3^{12}\times 13\times 73\times 1319\times 1549\, j_1^9 j_2^6 j_3^3
\end{aligned}
$$

$$+2^5\times3^{12}\times1439\times1531\times79631081\,j_1^8j_2^6j_3^4+2^{11}\times3^{14}\times449\times3900368627\,j_1^7j_2^6j_3^5+2^{21}\times3^{15}\times5\times16351469\,j_1^6j_2^6j_3^6+2^9\times3^{12}\times5\times11^4j_1^{10}j_2^7j_3$$
$$+2^5\times3^{12}\times11\times254892401\,j_1^9j_2^7j_3^2-2^7\times3^{13}\times11\times359\times19603\times41579\,j_1^8j_2^7j_3^3-2^8\times3^{12}\times47\times307\times317\times13596893\,j_1^7j_2^7j_3^4$$
$$-2^{15}\times3^{14}\times7\times6661\times763381\,j_1^6j_2^7j_3^5-2^6\times3^{11}\times5\times11^4j_1^{10}j_2^8-2^6\times3^{13}\times5^2\times139\times18149\,j_1^9j_2^8j_3+2^6\times3^{10}\times5\times53\times1901\times48725627\,j_1^8j_2^8j_3^2$$
$$+2^9\times3^{11}\times31\times1297\times707636873\,j_1^7j_2^8j_3^3+2^{13}\times3^{14}\times37\times43\times59\times1413271\,j_1^6j_2^8j_3^4+2^5\times3^8\times5\times47^2\times142981\,j_1^9j_2^9$$
$$-2^7\times3^9\times11\times17\times79\times2683\times76343\,j_1^8j_2^9j_3-2^5\times3^{12}\times7^3\times61\times24373\times55351\,j_1^7j_2^9j_3^2-2^{12}\times3^{11}\times11\times53\times1069\times5642513\,j_1^6j_2^9j_3^3$$
$$-2^{16}\times3^{14}\times37\times59\times525313\,j_1^5j_2^9j_3^4+2^5\times3^8\times5^2\times31\times149\times11455231\,j_1^8j_2^{10}+2^6\times3^9\times113\times351911687537\,j_1^7j_2^{10}j_3$$
$$+2^{14}\times3^{11}\times13\times31\times373\times1597147\,j_1^6j_2^{10}j_3^2+2^{16}\times3^{11}\times50925030661\,j_1^5j_2^{10}j_3^3-2^5\times3^8\times7\times13\times1181\times99900863\,j_1^7j_2^{11}$$
$$-2^9\times3^{10}\times53\times373\times9857\times17053\,j_1^6j_2^{11}j_3-2^{13}\times3^{10}\times139\times5132331041\,j_1^5j_2^{11}j_3^2+2^5\times3^8\times28476287051677\,j_1^6j_2^{12}$$
$$+2^{10}\times3^9\times1319\times3245505437\,j_1^5j_2^{12}j_3+2^{17}\times3^{11}\times13\times853\times180007\,j_1^4j_2^{12}j_3^2-2^7\times3^8\times53\times109\times28493\times56957\,j_1^5j_2^{13}$$
$$-2^{14}\times3^9\times5\times18371\times1132141\,j_1^4j_2^{13}j_3+2^{13}\times3^8\times47\times61\times38025503\,j_1^4j_2^{14}-2^{15}\times3^9\times7\times314130631\,j_1^3j_2^{15}-2^8\times3^{16}\times11^2j_1^9j_3^{10}$$
$$+2^{14}\times3^{17}\times967\,j_1^8j_3^{11}+2^9\times3^{15}\times5\times11^2j_1^9j_2j_3^9-2^{12}\times3^{15}\times5\times23\times1091\,j_1^8j_2j_3^{10}+2^{18}\times3^{17}j_1^7j_2j_3^{11}-2^8\times3^{16}\times5\times11^2j_1^9j_2^2j_3^8$$
$$+2^{12}\times3^{14}\times211\times2939\,j_1^8j_2^2j_3^9-2^{18}\times3^{15}\times149\times197\,j_1^7j_2^2j_3^{10}+2^{11}\times3^{14}\times5\times11^2j_1^9j_2^3j_3^7-2^8\times3^{14}\times7\times53\times26597\,j_1^8j_2^3j_3^8$$
$$+2^{14}\times3^{14}\times257\times18047\,j_1^7j_2^3j_3^9-2^9\times3^{13}\times5\times7\times11^2j_1^9j_2^4j_3^6+2^{11}\times3^{13}\times7\times113\times3121\,j_1^8j_2^4j_3^7-2^{12}\times3^{13}\times11\times191\times39239\,j_1^7j_2^4j_3^8$$
$$-2^{18}\times3^{15}\times19^2\times41\,j_1^6j_2^4j_3^9+2^{10}\times3^{13}\times7\times11^2j_1^9j_2^5j_3^5-2^{10}\times3^{13}\times7\times17\times19501\,j_1^8j_2^5j_3^6+2^{14}\times3^{12}\times5\times41\times264643\,j_1^7j_2^5j_3^7$$
$$+2^{19}\times3^{13}\times5\times45197\,j_1^6j_2^5j_3^8-2^9\times3^{11}\times5\times7\times11^2j_1^9j_2^6j_3^4+2^{11}\times3^{11}\times7\times61\times8263\,j_1^8j_2^6j_3^5-2^9\times3^{11}\times39791\times75329\,j_1^7j_2^6j_3^6$$
$$-2^{15}\times3^{12}\times7^2\times328919\,j_1^6j_2^6j_3^7+2^{11}\times3^{10}\times5\times11^2j_1^9j_2^7j_3^3-2^9\times3^{11}\times29\times73\times1619\,j_1^8j_2^7j_3^4+2^{10}\times3^{10}\times11\times19\times2237\times3793\,j_1^7j_2^7j_3^5$$
$$+2^{13}\times3^{12}\times11\times709\times7079\,j_1^6j_2^7j_3^6+2^{19}\times3^{13}\times109\times113\,j_1^5j_2^7j_3^7-2^8\times3^{10}\times5\times11^2j_1^9j_2^8j_3^2+2^{11}\times3^9\times11\times13\times23\times401\,j_1^8j_2^8j_3^3$$
$$-2^9\times3^9\times13\times224037301\,j_1^7j_2^8j_3^4-2^{13}\times3^{10}\times270832781\,j_1^6j_2^8j_3^5-2^{19}\times3^{11}\times73\times3407\,j_1^5j_2^8j_3^6+2^9\times3^7\times5\times11^2j_1^9j_2^9j_3-2^{10}\times3^8\times907397\,j_1^8j_2^9j_3^2$$
$$+2^{11}\times3^8\times19\times21563777\,j_1^7j_2^9j_3^3+2^9\times3^9\times401\times599\times19501\,j_1^6j_2^9j_3^4+2^{15}\times3^{11}\times107\times35983\,j_1^5j_2^9j_3^5-2^8\times3^6\times11^2j_1^9j_2^{10}$$
$$+2^{11}\times3^6\times5\times7\times8069\,j_1^8j_2^{10}j_3-2^9\times3^7\times5\times23\times83\times63353\,j_1^7j_2^{10}j_3^2-2^{11}\times3^9\times7\times39893383\,j_1^6j_2^{10}j_3^3-2^{13}\times3^9\times11\times101\times67493\,j_1^5j_2^{10}j_3^4$$
$$+2^{19}\times3^{11}\times11\times677\,j_1^4j_2^{10}j_3^5-2^8\times3^5\times7\times73\times419\,j_1^8j_2^{11}+2^{10}\times3^6\times331\times199559\,j_1^7j_2^{11}j_3+2^{10}\times3^7\times765685001\,j_1^6j_2^{11}j_3^2$$
$$+2^{14}\times3^9\times3319\times3691\,j_1^5j_2^{11}j_3^3-2^{21}\times3^9\times37993\,j_1^4j_2^{11}j_3^4-2^9\times3^6\times7\times43\times14369\,j_1^7j_2^{12}-2^{11}\times3^6\times5\times11\times67\times27539\,j_1^6j_2^{12}j_3$$
$$-2^8\times3^8\times47\times53\times157\times1187\,j_1^5j_2^{12}j_3^2+2^{14}\times3^8\times17\times593\times1193\,j_1^4j_2^{12}j_3^3+2^9\times3^6\times15860233\,j_1^6j_2^{13}+2^9\times3^6\times230601383\,j_1^5j_2^{13}j_3$$
$$-2^{12}\times3^7\times56208829\,j_1^4j_2^{13}j_3^2-2^{18}\times3^9\times44491\,j_1^3j_2^{13}j_3^3-2^8\times3^5\times5\times13179643\,j_1^5j_2^{14}+2^{12}\times3^6\times5\times7\times902987\,j_1^4j_2^{14}j_3$$
$$+2^{18}\times3^7\times127\times3457\,j_1^3j_2^{14}j_3^2-2^8\times3^6\times5\times47\times233\times673\,j_1^4j_2^{15}-2^{14}\times3^6\times11\times421\times1627\,j_1^3j_2^{15}j_3+2^{12}\times3^6\times1423\times2477\,j_1^3j_2^{16}$$
$$+2^{18}\times3^7\times19763\,j_1^2j_2^{16}j_3-2^{19}\times3^5\times5\times6029\,j_1^2j_2^{17}-2^8\times3^{12}j_1^8j_3^{12}+2^{17}\times3^{13}j_1^7j_3^{13}+2^{10}\times3^{12}j_1^8j_2j_3^{11}-2^{13}\times3^{12}\times5\times41\,j_1^7j_2j_3^{12}$$
$$-2^9\times3^{11}\times11\,j_1^8j_2^2j_3^{10}+2^{15}\times3^{12}\times101\,j_1^7j_2^2j_3^{11}+2^{16}\times3^{13}j_1^6j_2^2j_3^{12}+2^{10}\times3^9\times5\times11\,j_1^8j_2^3j_3^9-2^9\times3^{10}\times5\times14009\,j_1^7j_2^3j_3^{10}-2^{20}\times3^{12}j_1^6j_2^3j_3^{11}$$
$$-2^8\times3^{10}\times5\times11\,j_1^8j_2^4j_3^8+2^{10}\times3^9\times5^2\times3449\,j_1^7j_2^4j_3^9+2^{14}\times3^{11}\times19\times23\,j_1^6j_2^4j_3^{10}+2^{11}\times3^9\times11\,j_1^8j_2^5j_3^7-2^9\times3^{10}\times19\times1787\,j_1^7j_2^5j_3^8$$
$$-2^{15}\times3^{10}\times5\times173\,j_1^6j_2^5j_3^9-2^{17}\times3^{12}j_1^5j_2^5j_3^{10}-2^{10}\times3^7\times7\times11\,j_1^8j_2^6j_3^6+2^{12}\times3^8\times5\times13\times257\,j_1^7j_2^6j_3^7+2^8\times3^9\times5\times7\times59\times139\,j_1^6j_2^6j_3^8$$
$$+2^{17}\times3^{10}\times5\times7\,j_1^5j_2^6j_3^9+2^{11}\times3^7\times11\,j_1^8j_2^7j_3^5-2^{10}\times3^7\times65719\,j_1^7j_2^7j_3^6-2^{11}\times3^8\times23\times29\times97\,j_1^6j_2^7j_3^7-2^{13}\times3^{10}\times5\times191\,j_1^5j_2^7j_3^8$$
$$-2^8\times3^6\times5\times11\,j_1^8j_2^8j_3^4+2^{11}\times3^7\times5^2\times17\times19\,j_1^7j_2^8j_3^5+2^{10}\times3^7\times7\times23899\,j_1^6j_2^8j_3^6+2^{16}\times3^9\times5\times71\,j_1^5j_2^8j_3^7+2^{16}\times3^{10}\times5\,j_1^4j_2^8j_3^8$$
$$+2^{10}\times3^3\times5\times11\,j_1^8j_2^9j_3^3-2^{10}\times3^4\times5^2\times19\times167\,j_1^7j_2^9j_3^4-2^{11}\times3^6\times11\times7127\,j_1^6j_2^9j_3^5-2^{10}\times3^6\times5\times78623\,j_1^5j_2^9j_3^6-2^{20}\times3^7\times5^2j_1^4j_2^9j_3^7$$
$$-2^9\times3^3\times11\,j_1^8j_2^{10}j_3^2+2^{12}\times3^3\times13\times599\,j_1^7j_2^{10}j_3^3+2^9\times3^5\times5\times42397\,j_1^6j_2^{10}j_3^4+2^{11}\times3^6\times61\times1399\,j_1^5j_2^{10}j_3^5+2^{15}\times3^6\times5\times613\,j_1^4j_2^{10}j_3^6$$
$$+2^{10}\times3^2j_1^8j_2^{11}j_3-2^9\times3^3\times5\times11\times101\,j_1^7j_2^{11}j_3^2-2^{11}\times3^7\times5\times11\times17\,j_1^6j_2^{11}j_3^3-2^{10}\times3^5\times5\times19\times1609\,j_1^5j_2^{11}j_3^4$$
$$-2^{16}\times3^6\times5\times13\times17\,j_1^4j_2^{11}j_3^5-2^{18}\times3^7\times5\,j_1^3j_2^{11}j_3^6-2^8j_1^8j_2^{12}+2^{10}\times3\times1361\,j_1^7j_2^{12}j_3+2^{10}\times3^3\times89\times181\,j_1^6j_2^{12}j_3^2$$
$$+2^{12}\times3^3\times5\times13963\,j_1^5j_2^{12}j_3^3+2^8\times3^4\times5\times67\times3391\,j_1^4j_2^{12}j_3^4+2^{17}\times3^6\times5\times13\,j_1^3j_2^{12}j_3^5-2^9\times5\times41\,j_1^7j_2^{13}-2^{11}\times3^2\times7\times13\times17\,j_1^6j_2^{13}j_3$$
$$-2^{10}\times3^3\times5\times83\times89\,j_1^5j_2^{13}j_3^2-2^{10}\times3^3\times5\times73\times661\,j_1^4j_2^{13}j_3^3-2^{13}\times3^5\times5\times557\,j_1^3j_2^{13}j_3^4+2^8\times3^2\times19^2\,j_1^6j_2^{14}+2^{11}\times3^2\times5\times863\,j_1^5j_2^{14}j_3$$
$$+2^9\times3^3\times5\times31\times547\,j_1^4j_2^{14}j_3^2+2^{15}\times3^4\times5\times197\,j_1^3j_2^{14}j_3^3+2^{16}\times3^6\times5\,j_1^2j_2^{14}j_3^4-2^{10}\times2707\,j_1^5j_2^{15}-2^{10}\times3\times5\times23\times331\,j_1^4j_2^{15}j_3$$
$$-2^9\times3^3\times17\times2927\,j_1^3j_2^{15}j_3^2-2^{22}\times3^4j_1^2j_2^{15}j_3^3+2^8\times5^2\times13\times61\,j_1^4j_2^{16}+2^{10}\times3^2\times10399\,j_1^3j_2^{16}j_3+2^{14}\times3^7\times5\,j_1^2j_2^{16}j_3^2$$
$$-2^9\times3\times59\times61\,j_1^3j_2^{17}-2^{15}\times3^3\times47\,j_1^2j_2^{17}j_3-2^{17}\times3^4j_1j_2^{17}j_3^2+2^8\times5\times2803\,j_1^2j_2^{18}+2^{17}\times3\times19\,j_1j_2^{18}j_3-2^{13}\times157\,j_1j_2^{19}+2^{16}\times3\,j_2^{20}.$$

Conclusion

Dans ce mémoire, nous avons d'une part étudié de manière relativement théorique les suites de Borchardt sur les nombres complexes, dont les suites AGM peuvent être vues comme un cas particulier. D'autre part, nous nous sommes intéressé à un certain nombre d'applications de ces suites en théorie algorithmique des nombres.

D'un point de vue théorique, nos contributions sont les suivantes : nous avons démontré la convergence de toute suite de Borchardt sur les complexes, et donné un critère permettant de décider de la nullité de la limite. Dans le cas où la limite est non nulle, nous avons montré que la convergence est quadratique. Dans le cas particulier des suites de Borchardt de quatre éléments, nous avons entièrement déterminé l'ensemble des limites des suites de Borchardt associées à un quadruplet de nombres complexes fixé. Ces résultats peuvent être vus comme des généralisations de résultats connus dans le cas de l'AGM.

D'un point de vue algorithmique, nous avons donné une borne quantitative sur l'approximation du logarithme complexe donnée par l'AGM. Nous avons donné un algorithme rapide d'évaluation de fonctions modulaires en genre 1 (utilisant l'AGM et des itérations de Newton), et avons analysé finement sa complexité. Nous avons donné un algorithme rapide d'évalution de matrices de Riemann associées à des courbes hyperelliptiques en genre quelconque (et même à des courbes non hyperelliptiques en genre 3) utilisant les suites de Borchardt. Enfin, à partir de ce dernier algorithme et en utilisant des itérations de Newton, nous avons donné un algorithme rapide pour l'évaluation de certaines fonctions modulaires et des theta constantes en genre 2. Nous avons appliqué ces algorithmes au calcul explicite de polynômes modulaires en genre 2.

Un certain nombre de prolongements de ces travaux sont possibles. En ce qui concerne les relations entre les suites de Borchardt de quatre éléments et les theta constantes en genre 2 par exemple, nous n'avons pas réussi à généraliser *tous* les résultats connus pour l'AGM. En particulier, il serait intéressant de déterminer l'ensemble

$$\left\{ \tau \in \mathcal{H}_2 : B_2\left(b_1(\tau), b_2(\tau), b_3(\tau)\right) = \frac{1}{\theta_0^2(\tau)} \right\},$$

et à l'intérieur de cet ensemble un ensemble fondamental pour l'action de Γ_b sur $\mathcal{H}_2$. Ceci permettrait au passage de démontrer la validité de la Conjecture 9.1 (ou un résultat analogue). Concernant le calcul de polynômes modulaires en genre 2 (ou supérieur), nos travaux restent très prospectifs : il serait intéressant de connaître des propriétés de ces polynômes, de pouvoir les calculer plus rapidement, de déterminer des invariants plus adaptés que les invariants d'Igusa (*i.e.*, pour lesquels les polynômes modulaires associés sont "plus petits"), de pouvoir les utiliser pour généraliser les idées d'Elkies et Atkin au genre supérieur,...

Bibliographie

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203) :29–68, July 1993.

[Atk88] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Draft, 1988.

[Atk92] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (II). Draft. Available on `http ://listserv.nodak.edu/archives/nmbrthry.html`, 1992.

[BB84] J. M. Borwein and P. B. Borwein. The arithmetic-geometric mean and fast computation of elementary functions. *SIAM Review*, 26 :351–366, 1984.

[BB87] J. M. Borwein and P. B. Borwein. *Pi and the AGM.* John Wiley, 1987.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I : The user language. *J. Symbolic Comput.*, 24(3) :235–265, 1997.

[BCSS97] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation.* Springer-Verlag, 1997.

[BGS72] M. Beeler, R. Gosper, and R. Schroeppel. HAKMEM, 1972. MIT Artificial Intelligence Lab. Memo 239, available at `http://www.inwap.com/pdp10/hbaker/hakmem/hakmem.html`, Item 143 : AGM for elliptic integrals, log and pi.

[BK01] H. Baier and G. Köhler. How to compute the coefficients of the elliptic modular function $j(z)$. *Experiment. Math.*, 12(1) :115–121, 2001.

[BLS03] P. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degree. In S. Cimato, C. Galdi, and G. Persiano, editors, *SCN 2002*, volume 2576 of *Lecture Notes in Comput. Sci.*, pages 257–267. Springer-Verlag, 2003. Third International Conference on Security in Communication Networks, Amalfi, Italy, September 2002.

[BM88] J.-B. Bost and J.-F. Mestre. Moyenne arithmético-géométrique et périodes de courbes de genre 1 et 2. *Gaz. Math.*, 38 :36–64, 1988.

[Bor79] C.-W. Borchardt. Sur un système de trois équations différentielles totales qui définissent la moyenne arithmético-géométrique de quatre éléments. *Bull. Soc. Math. France*, 7 :124–129, 1878–79.

[Bor61] C.-W. Borchardt. Ueber das arithmetisch-geometrisch Mittel. *Borchardt's Journal*, 58 :127–137, 1861.

[Bor76] C.-W. Borchardt. Ueber das arithmetisch-geometrische Mittel aus vier Elementen. *Monatsbericht der Akademie der Wissenschaften zu Berlin*, pages 611–621, November 1876.

[Bor78] C.-W. Borchardt. Theorie des arithmetisch-geometrisches Mittels aux vier Elementen. *Mathematische Abhandlungen der Akademie der Wissenschaften zu Berlin*, pages 33–96, 1878.

[Bor88] C.-W. Borchardt. *Gesammelte Werke, auf Verandlassung der königlich Preussischen Akademie der Wissenschaften*, chapter Sur deux algorithmes analogues à celui de la moyenne arithmético-géométrique de deux éléments, pages 453–462. G. Reimer, Berlin, 1888.

[BP94] D. Bini and V. Pan. *Polynomial and Matrix Computations*, volume 1, Fundamental Algorithms. Birkhaüser, Boston, 1994.

[Bre75] R. P. Brent. *Analytic computational complexity*, chapter Multiple-precision zero-finding methods and the complexity of elementary function evaluation, pages 151–176. Academic Press, New York, 1975.

[Bre76] R. P. Brent. Fast multiple-precision evaluation of elementary functions. *J. ACM*, 23(2) :242–251, 1976.

[BS04] R. Bröker and P. Stevenhagen. Elliptic curves with a given number of points. In D. Buell, editor, *ANTS VI*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 117–131. Springer-Verlag, 2004. Proceedings of the 6th Algorithmic Number Theory Symposium, Burlington, VT, USA, June 2004.

[BSS99] I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*, volume 265 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1999.

[BSS05] I. Blake, G. Seroussi, and N. Smart. *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 2005.

[BW05] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1) :133–141, 2005.

[CC87] D. Chudnovsky and G. Chudnovsky. *Number Theory (New York 1984–85)*, volume 1240 of *Lecture Notes in Math.*, chapter Computer assisted number theory with applications, pages 1–68. Springer–Verlag, 1987.

[CH02] J.-M. Couveignes and T. Hénocq. Action of modular correspondences around CM points. In C. Fieker and D. Kohel, editors, *ANTS V*, Lecture Notes in Comput. Sci., pages 234–243. Spring-Verlag, 2002. Proceedings of the 5th Algorithmic Number Theory Symposium, Sydney, Australia, July 2002.

[Coh84] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95 :389–402, 1984.

[Com05] Computer algebra group. Magma. `http ://www.maths.usyd.edu.au/magma/`, 2005.

[Cou03] W. Couwenberg. A simple proof of the modular identity for theta functions. *Proc. Amer. Math. Soc.*, 131 :3305–3307, 2003.

[Cox84] D. A. Cox. The arithmetic-geometric mean of Gauss. *Enseign. Math.*, 30 :275–330, 1984.

[Cox89] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[DEM05] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *J. of Cryptology*, 18(2) :79–89, 2005.

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14 :197–272, 1941.

[DHB+04] B. Deconinck, M. Heil, A. Bobenko, M. van Hoeij, and M. Schmies. Computing Riemann theta functions. *Math. Comp.*, 73 :1417–1442, 2004.

[DR84] P. Davis and P. Rabinowitz. *Methods of Numerical Integration, 2nd ed.* Academic Press, New York, 1984.

[Dup05] R. Dupont. Fast evaluation of modular functions using Newton iterations and the AGM, 2005. To appear in *Math. Comp.*

[Dur68] E. Durand. *Solution numérique des équations algébriques*, volume 1. Masson, Paris, 1968.

[DvH01] B. Deconinck and M. van Hoeij. Computing Riemann matrices of algebraic curves. *Physica D*, 152–153 :28–46, 2001.

[Elk98] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory : Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[EM02] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratic fields. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer-Verlag, 2002. 5th International Symposium, ANTS–V, Sydney, Australia, July 7-12, 2002. Proceedings.

[Eng05a] A. Enge. The complexity of class polynomial computation via floating point approximations, 2005. In preparation.

[Eng05b] A. Enge. The complexity of modular polynomial computation via floating point evaluation and interpolation, 2005. In preparation.

[ES04] A. Enge and R. Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *J. Théor. Nombres Bordeaux*, 16 :555–568, 2004.

[Eul14] L. Euler. *Leonhardi Euleri opera omnia. Series prima. Opera mathematica*, volume 3, chapter Evolutio producti infiniti $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)$ etc. in seriem simplicem, pages 472–479. B. G. Teubneri, 1914. Translation available at `http://www.arxiv.org/abs/math.HO/0411454`.

[EZ04] A. Enge and P. Zimmermann. MPC – Multiprecision Complex arithmetic library version 0.4, 2004. Available at `http://www.loria.fr/~zimmerma/free/`.

[Fay73] J. Fay. *Theta functions on Riemann surfaces*, volume 352 of *Lecture Notes in Math.* Springer-Verlag, Berlin, 1973.

[Gar02] F. Garvan. *The Maple book*. Chapman & Hall/CRC, 2002.

[Gau01] C.-F. Gauss. *Disquisitiones Arithmeticae*. G. Fleischer, 1st edition, 1801. Leipzig ; English translation by A. A. Clarke, Yale Univ. Press, New York, 1966 ; revised English translation by W. C. Waterhouse, Springer-Verlag, New York, 1988.

[Gau27] C.-F. Gauss. *Werke*, volume 3. Dieterich, Göttingen, 1868–1927.

[Gau00] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*. Thèse, École polytechnique, December 2000.

[Gau05] P. Gaudry. `mpn_AMD64`, 2005. Routines assembleur (AMD Athlon 64 et Opteron) permettant d'optimiser les performances de GMP 4.1.4, disponible à l'adresse `http://www.loria.fr/~gaudry/mpn_AMD64/`.

[Gep28] H. Geppert. Zur Theorie des arithmetisch-geometrischen Mittels. *Math. Ann.*, 99 :162–180, 1928.

[GG99] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[GHK+05] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic CM method for genus 2, 2005. In preparation.

[Got59] E. Gottschling. Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades. *Math. Ann.*, 138 :103–124, 1959.

[GR65] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals, Series and Products*. Academic Press, New York, 1965.

[Gra02] T. Granlund *et al.* GMP – GNU Multiprecision library version 4.1, 2002. Available at `http://www.swox.com/gmp/`.

[HLPZ04] G. Hanrot, V. Lefèvre, P. Pélissier, and P. Zimmermann. MPFR – Multiple Precision Floating point computations with exact Rounding library, version 2.1.0, 2004. Disponible à l'adresse `http://www.mpfr.org`.

[Igu60] J. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72 :612–649, 1960.

[Igu62] J.-I. Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84 :175–200, 1962.

[Igu72] J.-I. Igusa. *Theta functions*, volume 194 of *Die Grundlehren der mathematischen Wissenschaften*. Springer, 1972.

[Jac91] C. G. Jacobi. *C. G. Jacobi's gesammelte Werke*, volume 1, chapter Fundamenta Nova Theoriae Functionum Ellipticarum, pages 49–239. G. Reimer, Berlin, 1881–1891.

[Ker66] I. Kerner. Ein Gesamtschrittverfahren zur Berechnung der Nullstellen von Polynomen. *Numer. Math.*, 18 :290–294, 1966.

[Kli90] H. Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1990.

[KO63] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doklady*, 7 :595–596, 1963.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177) :203–209, January 1987.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *J. of Cryptology*, 1 :139–150, 1989.

[Kön65] L. Königsberger. Über die Transformation der Abelschen Functionen erster Ordnung. *J. Reine Angew. Math.*, 64 :17–42, 1865.

[Lag67] J. Lagrange. *Oeuvres de Lagrange*, volume 2, chapter Sur une nouvelle méthode de calcul intégral pour les différentielles affectées d'un radical carré sous lequel la variable ne passe pas le quatrième degré, pages 253–312. Gauthier-Villars, Paris, 1867.

[Leg28] A. Legendre. *Traité des fonctions elliptiques et des intégrales eulériennes, avec des tables pour en faciliter le calcul numérique*. Huzard-Courcier, Paris, 1825–1828.

[Mes91] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94 of *Progress in mathematics*, pages 313–334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17–21, 1990.

[Mes00] J.-F. Mestre. Lettre adressée à Gaudry et Harley, décembre 2000. Disponible à l'adresse `http://www.math.jussieu.fr/~mestre/lettreGaudryHarley.ps`.

[Mes02] J.-F. Mestre. Algorithmes pour compter des points de courbes en petite caractéristique et en petit genre, mars 2002. Notes d'un exposé donné au séminaire de cryptographie de Rennes, rédigé par David Lubicz. Disponible à l'adresse `http://www.math.jussieu.fr/~mestre/rennescrypto.ps`.

[Mes04] J.-F. Mestre. Autour de la moyenne arithmético-géométrique, 2004. Cours donné lors du trimestre spécial "Méthodes Explicites en Théorie des Nombres" à l'Institut Henri Poincaré, Paris.

[Mil87] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1987. Proceedings, Santa Barbara (USA), August 11–15, 1986.

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, E84-A(5), May 2001.

[Mor95] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux*, 7 :255–282, 1995.

[Mor05] F. Morain. Computing #(E(GF(10^2004 + 4863))). Email to the `NMBRTHRY` mailing list. Available at `http://listserv.nodak.edu/archives/nmbrthry.html`, December 2005.

[Mum84a] D. Mumford. *Tata lectures on theta I.* Birkhauser, 1984.

[Mum84b] D. Mumford. *Tata lectures on theta II.* Birkhauser, 1984.

[Ric36] F. Richelot. Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes. *C. R. Acad. Sci. Paris Sér. I Math.*, 2 :622–627, 1836.

[Rit03] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* Thèse, Université Paris 7 Denis Diderot, juin 2003.

[Rit04] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In D. Buell, editor, *Algorithmic Number Theory*, volume 3066 of *Lecture Notes in Comput. Sci.*, pages 379–394. Springer-Verlag, 2004. Sixth International Symposium on Algorithmic Number Theory, ANTS VI, Burlington, VT, USA, June 2004, Proceedings.

[Run97] B. Runge. Level-two-structures and hyperelliptic curves. *Osaka J. Math.*, 34 :21–51, 1997.

[Sal76] E. Salamin. Computation of π using arithmetic-geometric mean. *Math. Comp.*, 30 :565–570, 1976.

[Sch74] B. Schoeneberg. *Elliptic modular functions*, volume 203 of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen.* Springer–Verlag, 1974.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7 :219–254, 1995.

[Sch02] R. Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14(1) :325–343, 2002.

[Ser70] J.-P. Serre. *Cours d'arithmétique.* PUF, 1970.

[Sie35] C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1 :83–86, 1935.

[Sie39] C. L. Siegel. Einführung in die Theorie der Modulfunktionen n-ten Grades. *Math. Ann.*, 116 :617–657, 1939.

[Sie89] C. L. Siegel. *Lectures on the Geometry of Numbers.* Springer-Verlag, 1989. Réécrit par K. Chandrasekharan.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts in Math.* Springer, 1986.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Grad. Texts in Math.* Springer-Verlag, 1994.

[SS71] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing*, 7 :281–292, 1971.

[Tho70] J. Thomae. Beitrag zur Bestimmung von $\theta(0,\ldots,0)$ durch die KlassenModuln algebraischer Funktionen. *J. Reine Angew. Math.*, 71 :201–222, 1870.

[vD28] L. von David. Arithmetisch-geometrisches Mittel und Modulfunktion. *J. Reine Angew. Math.*, 159 :154–170, 1928.

[vdH99] J. van der Hoeven. Fast evaluation of holonomic functions. *Theoret. Comput. Sci.*, 210(1) :199–215, 1999.

[vW99a] P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225) :307–320, January 1999.

[vW99b] P. van Wamelen. Proving that a genus 2 curve has Complex Multiplication. *Math. Comp.*, 68(228) :1663–1677, 1999.

[vW00] P. van Wamelen. Poonen's question concerning isogenies between Smart's genus 2 curves. *Math. Comp.*, 69(232) :1685–1697, 2000.

[Web02] H. Weber. *Lehrbuch der Algebra*, volume III. Chelsea Publishing Company, New York, 1902.

[Wen01] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. Phd thesis, Universität GH Essen, October 2001.

[Wen03] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72 :435–458, 2003.

[WW27] E. T. Whittaker and G. N. Watson. *A Course of Modern Analysis*. Cambridge University Press, fourth edition, 1927. Reprinted 1973.

Index

B_g (moyenne de Borchardt) 164
$D(\tau)$ 173
D_2 224
D_3 227
$H_{K,j}$, $j \in [1,3]$ 215
J 122
N-représentation d'un nombre 17
S, T (générateurs de Γ_1) 40
Δ_a 42
$\mathcal{F}_g$ 124
$\mathcal{F}, \mathcal{F}'$ 40
$\Gamma^0(N)$ 62
Γ_1 (groupe modulaire elliptique) 40
Γ_b 146
Γ_g 123
$\Gamma_{k'}$ 57
$\mathcal{H}_g$ (demi-espace de Siegel) 121
$\mathcal{H}$ (demi-plan de Poincaré) 39
$\mathcal{I}_g$ 153
$\mathfrak{J}$ 131
$\mathfrak{G}_j$, $j \in [1,9]$ 147
$\mathfrak{N}_j$ 132
$\mathrm{Rep}_N(z)$ 17
$\Phi_\ell(X,Y)$ 64
$\Phi_{j,p}$, $j \in [1,3]$ 220
$\mathcal{R}(N)$ 17
$\mathbb{C}^{r+}$ 99
$\mathfrak{S}$ 131
$\mathfrak{T}$ 131
$M(z)$
  sur les complexes 69
  sur les réels positifs 68
$\mathrm{AGM}(a,b)$ 67
η (fonction η de Dedekind) 56
$\Phi(\gamma,.)$ 143
$\Psi(\gamma,.)$ 143
$\kappa(\gamma)$ 143
$\mathcal{B}_1$ 70
$\mathcal{B}_g$ 162
$\mathcal{C}$ 59
$\mathcal{C}_p$ 219
$\mathcal{C}_{a,b}$ 43
$\mathcal{F}_b$ 171
$\mathcal{F}_{1,B^-}$ 173
$\mathcal{F}_{2,B^+}$ 173
$\mathcal{F}_{2,B^-,M^+}$ 174
$\mathcal{F}_{2,B^-,M^-}$ 174
$\mathcal{F}_{2,B^-}$ 173
$\mathcal{F}_{k'}$ 57
$\mathcal{G}$ 171
$\mathcal{G}_1$ 171
$\mathcal{G}_2$ 172
$\mathcal{G}_3$ 172
$\mathcal{G}_{k'}$ 57
$\mathfrak{M}_1$ 131
$\mathfrak{M}_2$ 131
$\mathfrak{M}_3$ 131
$\mathrm{Sp}(2g,\mathbb{Z})$ 122
$\rho(.)$ 141
θ
  en genre 1 49
  en genre g 121
θ_j, $j \in [0,15]$ (en genre 2) 136
θ_j, $j \in [0,2]$ (en genre 1) 48
$\theta_{a,b}$ (en genre g) 121
ϑ_j, $j \in [0,2]$ 131
$\lambda(\tau)$ 121
b_j, $j \in [0,15]$ 146
j (fonction modulaire elliptique) 60
j_1, j_2, j_3 (invariants d'Igusa) 148
k, k' (fonctions modulaires) 57
q 48

AGM
  de deux nombres complexes 69
  de deux réels positifs 67

domaine fondamental 40

ensemble fondamental 40

fonction
  finiment décomposable 22
  itérée 22

modulaire 48
modulaire de Siegel 125
forme modulaire 47
de Siegel 125

invariants d'Igusa 148
itération de Borchardt 153

nombres N-représentables 17

opérations élémentaires 19

polygone élémentaire 42
polynôme modulaire 62
classique 64
précision
absolue 18
relative 18

suite de Borchardt 153

theta constantes
en genre 1 48
en genre g 121

Résumé

L'étude de la moyenne arithmético-géométrique (AGM), introduite il y a plus de deux siècles par Legendre, Lagrange et Gauss, est intimement liée aux theta constantes ainsi qu'à certaines fonctions modulaires. Ceci est le point de départ des travaux présentés dans la première partie de ce mémoire, où nous utilisons cette relation pour concevoir un algorithme rapide d'évaluation de fonctions modulaires en genre 1 utilisant l'AGM et des itérations de Newton. Nous nous intéressons aussi à l'utilisation de l'AGM pour l'évaluation rapide du logarithme complexe : plus précisément, nous donnons une borne explicite sur la précision de l'approximation du logarithme qui peut être obtenue *via* l'AGM.

Dans la seconde partie, nous nous intéressons aux itérations de Borchardt, procédé qui, par ses relations avec les theta constantes, peut être vu comme une généralisation de l'AGM à un genre quelconque. En particulier, nous démontrons des propriétés de convergence des suites de Borchardt sur les complexes et étudions les limites possibles des suites de Borchardt de quatre éléments, généralisant un résultat connu concernant l'AGM. Enfin, nous proposons un algorithme utilisant les suites de Borchardt pour l'évaluation de matrices de Riemann associées à des courbes hyperelliptiques en genre quelconque, ainsi qu'un algorithme pour l'évaluation rapide de fonctions modulaires en genre 2. Pour illustrer l'intérêt de ces algorithmes, nous les utilisons pour calculer des polynômes modulaires en genre 2 par des techniques d'évaluation/interpolation.

Abstract

The study of the arithmetic-geometric mean (AGM), introduced more than two centuries ago by Legendre, Lagrange et Gauss, is intimately linked to theta constants and to some modular functions. This is the starting point of the work presented in the first part of this thesis, where we use this relation to devise a fast algorithm for the evaluation of modular functions in genus 1, using the AGM and Newton iterations. We also study the use of the AGM to evaluate complex logarithms. More precisely, we give an explicit bound on the precision of the approximation of the logarithm obtained *via* the AGM.

In the second part, we focus on Borchardt iterations, a process which, through its link with theta constants, can be seen as a generalization of the AGM to arbitrary genus. In particular, we prove some convergence properties of Borchardt sequences over the complex numbers and study the numbers that arise as limits of Borchardt sequences of four elements, thus generalizing a well-known result concerning the AGM. Finally, we propose an algorithm using Borchardt sequences for the evaluation of Riemann matrices associated with hyperelliptic curves in any genus, as well as an algorithm for the evaluation of modular functions in genus 2. To illustrate the power of these algorithms, we apply them to the computation of modular polynomials in genus 2 using evaluation/interpolation techniques.