Calcul effectif de points spéciaux

Antonin Riffaut

université de BORDEAUX

Institut de Mathématiques de Bordeaux

edmi BORDEAUX
ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

Thèse

présentée à

L'université de Bordeaux

École Doctorale de Mathématiques et Informatique

par Antonin Riffaut

pour obtenir le grade de

Docteur

Spécialité : Mathématiques pures - Théorie des nombres

Calcul effectif de points spéciaux

Soutenue le 9 juillet 2018 à l'Institut de Mathématiques de Bordeaux

devant le jury composé de :

M. Karim Belabas	Professeur	Université de Bordeaux	Co-directeur
M. Yuri Bilu	Professeur	Université de Bordeaux	Directeur
M. Cristophe Delaunay	Professeur	Université de Franche-Comté	Rapporteur
M. Philipp Habegger	Professeur	Université de Bâle	Rapporteur
M. Jean Gillibert	Professeur	Université Toulouse 2 - Jean Jaurès	

Résumé

À partir du théorème d'André en 1998, qui est la première contribution non triviale à la conjecture de André-Oort sur les sous-variétés spéciales des variétés de Shimura, la principale problématique de cette thèse est d'étudier les propriétés diophantiennes des modules singuliers, en caractérisant les points de multiplication complexe (x, y) satisfaisant un type d'équation donné de la forme $F(x, y) = 0$, pour un polynôme irréductible $F(X, Y)$ à coefficients complexes.

Plus spécifiquement, nous traitons deux équations impliquant des puissances de modules singuliers. D'une part, nous montrons que deux modules singuliers x, y tels que les nombres 1, x^m et y^n soient linéairement dépendants sur $\mathbb{Q}$, pour des entiers strictement positifs m, n, doivent être de degré au plus 2, ce qui généralise un résultat d'Allombert, Bilu et Pizarro-Madariaga, qui ont étudié les points de multiplication complexe appartenant aux droites de $\mathbb{C}^2$ définies sur $\mathbb{Q}$. D'autre part, nous montrons que, sauf cas "évidents", le produit de n'importe quelles puissances entières de deux modules singuliers ne peut être un nombre rationnel non nul, ce qui généralise un résultat de Bilu, Luca et Pizarro-Madariaga, qui ont ont étudié les points de multiplication complexe appartenant aux hyperboles $xy = A$, où $A \in \mathbb{Q}^\times$. Les méthodes que nous développons reposent en grande partie sur les propriétés des corps de classes engendrés par les modules singuliers, les estimations de la fonction j-invariant et les estimations des formes linéaires logarithmiques.

Nous déterminons également les corps engendrés par les sommes et les produits de deux modules singuliers x et y : nous montrons que le corps $\mathbb{Q}(x, y)$ est engendré par la somme $x + y$, à moins que x et y soient conjugués sur $\mathbb{Q}$, auquel cas $x + y$ engendre un sous-corps de degré au plus 2 ; le même résultat demeure pour le produit xy.

Nos preuves sont assistées par le logiciel PARI/GP, que nous utilisons pour procéder à des vérifications dans des cas particuliers explicites.

Abstract

Starting for André's Theorem in 1998, which is the first non-trivial contribution to the celebrated André-Oort conjecture on the special subvarieties of Shimura varieties, the main purpose of this thesis is to study Diophantine properties of singular moduli, by characterizing CM-points (x, y) satisfying a given type of equation of the form $F(x, y) = 0$, for an irreducible polynomial $F(X, Y)$ with complex coefficients.

More specifically, we treat two different equations involving powers of singular moduli. On the one hand, we show that two distinct singular moduli x, y such that the numbers 1, x^m and y^n are linearly dependent over $\mathbb{Q}$, for some positive integers m, n, must be of degree at most 2. This partially generalizes a result of Allombert, Bilu and Pizarro-Madariaga, who studied CM-points belonging to straight lines in $\mathbb{C}^2$ defined over $\mathbb{Q}$. On the other hand, we show that, with "obvious" exceptions, the product of any two powers of singular moduli cannot be a non-zero rational number. This generalizes a result of Bilu, Luca and Pizarro-Madariaga, who studied CM-points belonging to hyperbolas $xy = A$, where $A \in \mathbb{Q}^\times$. The methods we develop lie mainly on the properties of ring class fields generated by singular moduli, on estimations of the j-function and on estimations of linear forms in logarithms.

We also determine fields generated by sums and products of two singular moduli x and y : we show that the field $\mathbb{Q}(x, y)$ is generated by the sum $x + y$, unless x and y are conjugate over $\mathbb{Q}$, in which case $x + y$ generate a subfield of degree at most 2 ; the same holds for the product xy.

Our proofs are assisted by the PARI/GP package, which we use to proceed to verifications in particular explicit cases.

Calcul effectif de points spéciaux

Thèse de doctorat

Antonin Riffaut

Table des matières

Remerciements

Le compte est bon. Cette formule que je chéris tant me semble appropriée pour établir le bilan de cette longue aventure qu'est le doctorat, et pour adresser quelques pensées à toutes les personnes qui m'ont soutenu et accompagné, de près comme de loin, durant ces trois dernières années. Et quel meilleur endroit pour cela qu'une section dédiée aux remerciements !

Je remercie tout d'abord mes deux directeurs : d'une part, Yuri Bilu, pour m'avoir accueilli puis encadré tout au long de nos travaux ; d'autre part, Karim Belabas, pour ses conseils et discussions utiles. J'ai découvert à vos côtés les agréments de la recherche en mathématiques, et votre aide m'a été très précieuse pour mener à bien nos différents projets. Sachez que même si j'ai choisi de m'orienter vers l'enseignement, cette expérience restera marquante et déterminante dans ma carrière. Je remercie également Bernadette Faye et Florian Luca pour leur collaboration enrichissante, sans oublier Bill Allombert, Amalia Pizzaro-Madariaga, Lars Kühne, et les collègues de bureau, Florian, Jialun, Bianca et Stéphane.

J'ai bien sûr une pensée pour mes parents, ainsi que pour mon frère Adrien et ma sœur Natacha, que j'embrasse fort. Nos moments passés tous ensemble, bien qu'occasionnels, m'apportent toujours un grand réconfort.

J'aimerais ensuite accorder une attention toute particulière à deux amis très proches, Théo et Thomas, qui ont suivi cette aventure à Bordeaux en même temps que moi. Nous avons passé de nombreux moments ensemble dont je garderai un précieux souvenir. Pour n'en citer qu'un parmi les autres, sans nul doute le plus mémorable, je pense bien entendu à notre participation à Motus, Théo ; ce fut un grand instant d'amusement et de complicité (avec un joli pactole à la clé) ! Vous avez tous les deux été d'un grand soutien lors des moments difficiles, vous avez su faire preuve de patience et supporter mes excentricités (vous êtes aussi pas mal dans votre genre !), en plus de partager des passions communes ; pour tout cela, je suis heureux de vous connaître. Je vous souhaite tout le succès possible pour l'achèvement de votre doctorat et la suite de votre parcours.

Parmi mes autres amis, une mention spéciale à Salim, mon ami de longue date qui a été à mes côtés pendant presque toutes mes études dans le supérieur. J'ai beaucoup d'admiration pour toi et te souhaite également une bonne continuation !

Je tiens à saluer chaleureusement tous les copains et surtout toutes les copines du club de chiffres et lettres d'Eysines : Michèle, Annie et Annie, Marie, Françoise, Claudy, Suzette, Martine, Yvette, Simone, Catherine, Jean-Pierre, Bruno, Michel, et Olivier et son papa. Partager ma passion du jeu avec vous chaque semaine m'a bien aidé à garder les pieds sur terre. J'ai plus particulièrement beaucoup apprécié toutes nos virées dans la région pour nous illustrer à l'occasion de tournois, qui m'ont bien sûr permis de voyager et d'échapper à mon côté casanier, mais aussi de rencontrer d'autres joueurs tout aussi sympathiques. Il me serait difficile de tous les citer, mais je pense à Alain, Pierre, Céline, Loïc, Wilfrid, Dany, Laurent, Éliane, Françoise, Thierry, ... et plein d'autres encore ! Nous formons comme une famille, et j'aurai toujours

grand plaisir à vous revoir. Je n'oublie pas non plus Melia, qui m'a énormément entraîné.

De la même manière, je salue les copains du TCT, notamment Hiino, Jules, PAD et Alex. Je n'ai qu'une chose à vous dire : *show me your moves !*

Pour terminer, je remercie vivement Maryvonne Ligot et Pascale Regnault du Mottier, mes enseignantes de mathématiques et de physique-chimie au lycée respectivement, qui ont été un véritable moteur dans ma vie. C'est vous qui avez contribué en premier lieu à mon essor, qui m'avez inspiré et m'inspirent encore, et je n'en serais certainement pas arrivé jusque là sans vous. C'est à mon tour d'endosser le rôle d'enseignant à présent, et j'espère être à votre hauteur.

Merci encore à vous tous, et à tous ceux que j'aurais pu oublier !

Introduction

Soit j la fonction j-invariant sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C} \,;\, \operatorname{Im} z > 0\}$. Un *module singulier* est un nombre de la forme $j(\tau)$, où $\tau \in \mathbb{H}$ est un nombre quadratique imaginaire. Le principal théorème de la théorie de la multiplication complexe stipule que $j(\tau)$ est un entier algébrique, et combinée à la théorie des corps de classes, il apparaît que son degré est donné par

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = [\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}(\tau)] = h(\Delta),$$

le nombre de classes de l'ordre $\mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$, où $\Delta < 0$ est le discriminant du polynôme minimal de τ sur $\mathbb{Z}$. De plus, $\mathbb{Q}(\tau, j(\tau))/\mathbb{Q}(\tau)$ est une extension abélienne dont le groupe de Galois est canoniquement isomorphe au groupe des classes de l'ordre $\mathcal{O}_\Delta$. Le lien avec la multiplication complexe vient du fait que $\mathcal{O}_\Delta$ peut être interprété comme l'anneau d'endomorphismes du réseau $\langle 1, \tau \rangle$ du plan complexe $\mathbb{C}$, ou de la courbe elliptique correspondante.

Au cours des dernières décennies, motivés par la conjecture d'André-Oort sur les sous-variétés spéciales des variétés de Shimura, de nombreux travaux de recherche ont été menés afin d'étudier les propriétés diophantiennes des modules singuliers. Le point de départ est le résultat obtenu par André en 1998 [And98], qui démontre qu'une courbe plane irréductible de $\mathbb{C}^2$ non *spéciale* n'admet qu'un nombre fini de *points de multiplication complexe*, c'est-à-dire de couples de modules singuliers $(j(\tau), j(\tau'))$. Une courbe plane irréductible de $\mathbb{C}^2$ étant définie par une équation polynômiale $F(x, y) = 0$, avec $F(X, Y) \in \mathbb{C}[X, Y]$, cela revient à dire que les solutions de l'équation $F(j(\tau), j(\tau')) = 0$ sont généralement en nombre fini. Les courbes *spéciales* sont connues explicitement, et sont de l'un des types suivants :

- les droites verticales $x = j(\tau)$;
- les droites horizontales $y = j(\tau')$;
- les *courbes modulaires* $Y_0(N)$, avec $N \geq 1$ entier, réalisés comme les courbes planes d'équation $\Phi_N(x, y) = 0$, où Φ_N est le polynôme modulaire de niveau N.

Les courbes spéciales contiennent clairement une infinité de points de multiplications complexe, et André a donc prouvé qu'elles sont caractérisées par cette propriété. Son résultat est la première contribution importante à la conjecture d'André-Oort ; voir [Pil11].

Indépendemment, le même résultat a été obtenu par Edixhoven [Edi98], toutefois sous l'hypothèse de Riemann généralisée. En 2009, Pila [Pil09] fournit une preuve alternative du théorème de André, en s'appuyant sur les idées de Pila et Zannier [Pil08]. Cependant, les preuves d'André et de Pila ne sont pas effectives, puisqu'elles utilisent la borne inférieure de Siegel sur le nombre de classes [Sie35].

Aujourd'hui, des résultats plus généraux sur la conjecture de André-Oort sont disponibles, grâce aux travaux remarquables de Klinger, Pila, Tsimerman, Ullmo et Yafaev ; voir [Kli14, Pil11, Pil13, Ull14]. Hélas, à l'instar des arguments initiaux d'André et Edixhoven, leurs preuves sont soit ineffectives, soit conditionnelles à l'hypothèse de Riemann généralisée.

Des preuves effectives du théorème d'André ont été découvertes à partir de 2012 seulement,

par Kühne [Kuh12, Kuh13], et indépendemment par Bilu, Masser et Zannier [Bil13]. Ils démontrent que, si $\mathcal{C}$ est une courbe plane irréductible non spéciale d'équation $F(x,y)=0$, et si (x,y) est un point de multiplication complexe appartenant à $\mathcal{C}$, alors les discriminants Δ_x et Δ_y des modules singuliers x et y respectivement satisfont $|\Delta_x|, |\Delta_y| \leq c(F)$, où $c(F)$ est une constante effectivement calculable en fonction du polynôme F.

Ces considérations ont ouvert la possibilité de non seulement prouver la finitude de l'ensemble des solutions d'équations polynomiales impliquant des modules singuliers, mais également de résoudre certaines d'entre elles complètement. Par exemple, Kühne [Kuh12] a montré que l'équation $x+y=1$ n'admet pas de solution (sous-entendu, pas de solution avec x, y des modules singuliers), et Bilu, Masser et Zannier [Bil13] ont montré que l'équation $xy=1$ n'admet pas de solution non plus.

Ces résultats ont été généralisés dans deux articles récents [All15, Bil16]. Dans [All15], Allombert, Bilu et Pizzaro-Madariaga ont déterminé les solutions de toutes les équations linéaires de la forme $Ax+By+C=0$, avec $A, B, C \in \mathbb{Q}$. Dans [Bil16], Bilu, Lucas et Pizzaro-Madariaga ont obtenu le même résultat pour les équations de la forme $xy=A$, avec $A \in \mathbb{Q}^\times$. Dans les deux cas, il apparaît en particulier que x et y engendrent le même corps sur $\mathbb{Q}$ de degré au plus 2, ce qui caractérise essentiellement l'ensemble des solutions. Nous aurons l'occasion d'en reparler plus en détail dans le chapitre 3.

La principale problématique de la présente thèse est d'étudier des types particuliers d'équations polynomiales impliquant des modules singuliers. Par exemple, dans l'optique de généraliser les équations d'hyperboles $xy=A$, que peut-on dire d'un point de multiplication complexe (x,y) satisfaisant une équation générique de conique $Ax^2+Bxy+Cy^2+Dx+Ey+F=0$? Nous avons envisagé cette direction de recherche, notamment dans des cas plus simples tels que $Ax^2+Bxy+Cy^2+D=0$, mais ne sommes arrivés à rien de concluant dans le cas général. La piste privilégiée est de contrôler les hauteurs des nombres algébriques x et y. En utilisant les travaux de Kühne [Kuh13, Lemma 3], nous pouvons observer qu'il n'existe qu'un nombre fini de points de "petite hauteur" sur une conique, c'est-à-dire dont la hauteur est majorée explicitement en termes de la hauteur de la conique. La question demeure difficile, et nous avons par la suite choisi de la laisser en suspens, pour nous concentrer sur le cas particulier $Ax^2+By^2+C=0$.

Ce dernier cas est plus accessible, dans la mesure où les arguments d'Allombert, Bilu et Pizzaro-Madariaga [All15] peuvent être transposés afin d'obtenir le même résultat. Le point clé est le fait que toutes les puissances entières non nulles d'un module singulier engendrent le même corps (voir le corollaire 2.43), et donc que $\mathbb{Q}(x)=\mathbb{Q}(y)$ en l'occurrence. Il est alors naturel de se demander si le degré de x et y est encore majoré par 2 lorsqu'ils satisfont l'équation généralisée $Ax^m+By^n+C=0$, où les entiers m et n sont également inconnus. Ces nouvelles inconnues font obstacle au raisonnement initial d'Allombert, Bilu et Pizzaro-Madariaga, qu'il est nécessaire de voir sous un angle différent.

Nous sommes tout d'abord parvenus à montrer que le degré de x et y est majoré par 3 lorsque $x \neq y$, avec deux exceptions de degré 3 que nos méthodes ne permettent pas de traiter. Le principal apport est l'emploi des estimations connues sur les formes linéaires logarithmiques. Nos travaux ont été consignés dans un premier article [Rif18]. Sur une idée originale de Luca, les exceptions de degré 3 ont pu être éliminées, et cette collaboration a abouti à l'élaboration d'un second article [Luc17]. En somme, le degré de x et y est bien majoré par 2 comme attendu, et le résultat obtenu est optimal. Il reste le cas $x \neq y$, bien plus difficile, que nous avons écarté par manque d'outils. Un résultat similaire a été établi pour l'équation généralisée

$x^m y^n = A$, consigné lui aussi dans le premier article [Rif18].

En marge de ces équations, nous avons entrepris un projet en commun avec Faye et Luca afin d'étudier les corps engendrés par les sommes et les produits de modules singuliers. Un autre article [Fay18] s'en est ensuivi, dans lequel nous montrons qu'étant donnés deux modules singuliers x et y et $\varepsilon \in \{\pm 1\}$, les degrés $[\mathbb{Q}(x,y) : \mathbb{Q}(x+\varepsilon y)]$ et $[\mathbb{Q}(x,y) : \mathbb{Q}(xy^\varepsilon)]$ sont d'au plus 2.

Ce dernier résultat révèle toute son utilité dans la généralisation des équations $x+y=1$ et $xy=1$ à non plus deux, mais trois modules singuliers, ce qui fait l'objet d'un dernier projet toujours en cours. Précisément, il s'agit de résoudre les équations $x+y+z=A \in \mathbb{Q}$ et $xyz=B \in \mathbb{Q}^\times$, où x,y,z sont trois modules singuliers. Nous montrons cette fois-ci que les modules singuliers x,y,z sont de degré au plus 3.

La particularité de chacun des travaux mentionnés ci-dessus est le recours aux fonctionnalités du paquet PARI/GP [PARI]. En effet, le processus de résolution d'une équation consiste à réduire dans un premier temps l'ensemble potentiel des solutions à un ensemble fini (en bornant les discriminants des modules singuliers impliqués), puis à examiner les possibilités restantes au moyen d'un algorithme. Toutes les estimations réalisées doivent donc être explicites afin de procéder au calcul.

La structure du mémoire est la suivante. Les deux premiers chapitres préliminaires ont pour vocation d'introduire l'essentiel du matériel théorique à la source de notre problématique de recherche. Ainsi, dans le chapitre 1, nous revenons sur la notion d'*ordre* d'un corps quadratique en vue de définir le *groupe des classes* et le *nombre de classes* d'un ordre ; nous donnons également quelques éléments de théorie des corps de classes afin de définir le *corps de classes* d'un ordre. Puis, dans le chapitre 2, nous présentons la théorie de la multiplication complexe, dont la fonction j-invariant joue un rôle central ; nous détaillons entre autres les principales propriétés algébriques des modules singuliers et les estimations de la fonction j dont nous faisons régulièrement usage. Les deux derniers chapitres sont, quant à eux, consacrés à l'exposition de nos résultats de recherche. Le chapitre 3 reprend les articles [Rif18] et [Luc17] sur les équations $Ax^m + By^n + C = 0$ et $x^m y^n = A$, tandis que le chapitre 4 reprend l'article [Fay18] sur les corps engendrés par les sommes et les produits de modules singuliers. Les trois premières annexes apportent de multiples outils complémentaires à la réalisation de nos travaux. L'annexe A définit la hauteur d'un nombre algébrique et en donne les principales propriétés utilisées, en particulier concernant la hauteur d'un module singulier. L'annexe B revient sur la construction du domaine fondamental standard de l'action de $\mathrm{SL}(2,\mathbb{Z})$ sur le demi-plan de Poincaré $\mathbb{H}$, et décrit notamment un algorithme pour tester l'appartenance de deux éléments $\tau, \tau' \in \mathbb{H}$ à une même orbite sous cette action. L'annexe C donne quelques propriétés élémentaires des logarithmes réel et complexe, pour ensuite retracer l'historique des résultats connus sur les formes linéaires logarithmiques. Enfin, l'intégralité de nos scripts PARI est retranscrite dans l'annexe D.

Chapitre 1

Ordres de corps quadratiques imaginaires

La première étape avant de développer la théorie de la multiplication complexe est d'introduire la notion d'*ordre* d'un corps quadratique. Les ordres sont en quelque sorte une généralisation des anneaux des entiers. La majeure partie du travail de ce chapitre consiste à transposer la théorie des idéaux de l'anneau des entiers aux ordres, afin de définir notamment le groupe des classes et le corps de classes d'un ordre. La principale difficulté provient du fait que, contrairement aux anneaux des entiers, les ordres ne sont en général pas des anneaux de Dedekind.

Avant toute chose, il convient de rappeler quelques généralités au sujet des corps quadratiques et de leurs anneaux des entiers.

Un *corps quadratique* est un corps de nombres de degré 2. Un tel corps s'écrit de manière unique sous la forme $\mathbb{Q}(\sqrt{N})$, où $N \neq 0, 1$ est un entier sans facteur carré. Le *discriminant* d'un corps quadratique $K = \mathbb{Q}(\sqrt{N})$ est la quantité

$$D_K = \begin{cases} N & \text{si } N \equiv 1 \bmod 4, \\ 4N & \text{sinon.} \end{cases}$$

Remarquons que $D_K \equiv 0, 1 \bmod 4$ et que $K = \mathbb{Q}(\sqrt{D_K})$, de sorte qu'un corps quadratique est entièrement déterminé par son discriminant.

L'*anneau des entiers* $\mathcal{O}_K$ d'un corps quadratique $K = \mathbb{Q}(\sqrt{N})$ est l'ensemble des entiers algébriques de K. Il peut être décrit comme suit :

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{si } N \not\equiv 1 \bmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{N}}{2}\right] & \text{si } N \equiv 1 \bmod 4. \end{cases}$$

De manière plus concise, en termes du discriminant D_K,

$$\mathcal{O}_K = \mathbb{Z}[w_K], \quad w_K = \frac{D_K + \sqrt{D_K}}{2}. \tag{1.1}$$

L'anneau des entiers $\mathcal{O}_K$ d'un corps quadratique K est un anneau de Dedekind, si bien que ses idéaux fractionnaires non nuls sont inversibles pour la loi $(\mathfrak{a}, \mathfrak{b}) \longmapsto \mathfrak{ab}$, d'élément neutre $\mathcal{O}_K$. Les idéaux fractionnaires de $\mathcal{O}_K$ forment donc un groupe abélien I_K. Les idéaux fractionnaires principaux (i.e. de la forme $\alpha\mathcal{O}_K$, avec $\alpha \in K^\times$) forment un sous-groupe P_K de I_K. Le quotient

$$\mathrm{Cl}(\mathcal{O}_K) = I_K / P_K$$

s'appelle le *groupe des classes* de $\mathcal{O}_K$. L'ordre de $\mathrm{Cl}(\mathcal{O}_K)$, noté $h(\mathcal{O}_K)$, s'appelle le *nombre de classes* de $\mathcal{O}_K$.

Le *corps de classes de Hilbert* d'un corps quadratique K est l'extension abélienne non ramifiée maximale L/K de K. Son groupe de Galois $\mathrm{Gal}(L/K)$ est isomorphe au groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$, et en particulier, son ordre est le nombre de classes $h(\mathcal{O}_K)$.

De plus amples détails peuvent être consultés par exemple dans [Cox89, §5].

1.1 Formes quadratiques binaires

L'objet de la théorie de la réduction des formes quadratiques binaires est de déterminer les entiers représentés par une forme donnée. Notre motivation est d'introduire plus spécifiquement, étant donné un entier $\Delta \equiv 0, 1 \bmod 4$, le groupe des classes $\mathrm{Cl}(\Delta)$ correspondant à l'ensemble des classes d'équivalence propre de formes réduites de discriminant Δ, ainsi que le nombre de classes $h(\Delta)$. Le lien entre ce groupe et le groupe des classes d'un ordre est établi en 1.3. Cette section s'appuie en grande partie sur [Cox89, §2 et §3].

Détaillons tout d'abord la terminologie employée.

- Une *forme quadratique binaire*, ou plus simplement une *forme*, est une forme quadratique $f(x, y) = ax^2 + bxy + cy^2$, avec $a, b, c \in \mathbb{Z}$.
- On dit que $f(x, y)$ est *primitive* si $\mathrm{pgcd}(a, b, c) = 1$.
- On dit que $f(x, y)$ est *définie positive* (resp. *définie négative*) si $f(x, y) > 0$ (resp. $f(x, y) < 0$), pour tout $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.
- Le *discriminant* de $f(x, y) = ax^2 + bxy + cy^2$ est la quantité $\Delta = b^2 - 4ac$. Il vérifie $\Delta \equiv b^2 \bmod 4$, donc $\Delta \equiv 0, 1 \bmod 4$. Réciproquement, tout entier $\Delta \equiv 0, 1 \bmod 4$ est le discriminant d'une forme : il suffit de considérer la forme

$$F_\Delta(x, y) = x^2 + r_4(\Delta)xy + \frac{r_4(\Delta) - \Delta}{4} y^2, \tag{1.2}$$

  où $r_4(\Delta) \in \{0, 1\}$ est défini par $\Delta \equiv r_4(\Delta) \bmod 4$, et de constater qu'elle est bien de discriminant Δ. La forme $F_\Delta(x, y)$ s'appelle la *forme principale* de discriminant Δ.
- Soit m un entier non nul. On dit que m est *représenté* (resp. *représenté proprement*) par $f(x, y)$, ou que $f(x, y)$ *représente* (resp. *représente proprement*) m, si l'équation $f(x, y) = m$ admet une solution entière (x, y) (resp. une solution entière (x, y) avec $\mathrm{pgcd}(x, y) = 1$).
  En notant Δ le discriminant de $f(x, y)$, on a l'identité

$$4af(x, y) = (2ax + by)^2 - \Delta y^2.$$

  De fait, si $\Delta < 0$, alors $f(x, y)$ ne représente soit que des entiers strictement positifs, soit que des entiers strictement négatifs. En conséquence, $f(x, y)$ est respectivement définie positive ou définie négative.
- Deux formes $f(x, y)$ et $g(x, y)$ sont *équivalentes* (resp. *proprement équivalentes*) s'il existe des entiers $p, q, r, s \in \mathbb{Z}$ tels que $f(x, y) = g(px + qy, rx + sy)$ et $ps - qr = \pm 1$ (resp. $ps - qr = 1$). Cela correspond à l'équivalence usuelle de formes quadratiques, avec un changement de base donné par une matrice de passage

$$P = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$$

(resp. $P \in \mathrm{SL}(2,\mathbb{Z})$). Il s'agit en particulier d'une relation d'équivalence. Par ailleurs, il est important de noter que deux formes équivalentes (resp. proprement équivalentes) représentent (resp. représentent proprement) les mêmes entiers, et que l'équivalence préserve également le discriminant et le caractère défini positif.

- Une forme primitive définie positive $f(x,y) = ax^2 + bxy + cy^2$ est dite *réduite* si

$$-a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c.$$

Le principal résultat de réduction est le suivant :

Théorème 1.1. *Toute forme primitive définie positive est proprement équivalente à une unique forme réduite.*

Démonstration. Voir [Cox89, Theorem 2.8]. ■

Soit $f(x,y) = ax^2 + bxy + cy^2$ une forme réduite de discriminant $\Delta < 0$. Alors $b^2 \leq a^2$, $a \leq c$, et

$$-\Delta = -b^2 + 4ac \geq -a^2 + 4a^2 = 3a^2,$$

d'où

$$a \leq \sqrt{\frac{-\Delta}{3}}. \tag{1.3}$$

Comme Δ est fixé, il existe un nombre fini de choix possibles pour a puis pour b, et donc également pour $c = (b^2 - \Delta)/(4a)$. On en déduit qu'il existe un nombre fini de formes réduites de discriminant Δ. Le théorème 1.1 implique qu'il en est de même du nombre de classes d'équivalence propre de formes réduites de discriminant Δ. Ce nombre se note $h(\Delta)$. La propriété d'unicité du théorème 1.1 garantit en outre que deux formes réduites distinctes de même discriminant ne sont pas proprement équivalentes, de sorte que $h(\Delta)$ corresponde simplement au nombre de formes réduites de discriminant Δ. Remarquons enfin que pour tout entier $\Delta < 0$ avec $\Delta \equiv 0, 1 \bmod 4$, $h(\Delta) \geq 1$ grâce à la forme principale $F_\Delta(x,y)$ construite en (1.2). Nous venons de démontrer le théorème suivant :

Théorème 1.2. *Soit $\Delta < 0$ un entier avec $\Delta \equiv 0, 1 \bmod 4$. Alors le nombre $h(\Delta)$ de classes d'équivalence propre de formes réduites de discriminant Δ est fini, et de plus $h(\Delta)$ est égal au nombre de formes réduites de discriminant Δ.*

La discussion ci-dessus donne un moyen algorithmique de calculer facilement $h(\Delta)$ pour de petites valeurs de Δ. Il s'agit d'énumérer les éléments de l'ensemble T_Δ des triplets d'entiers (a,b,c) satisfaisant

$$\begin{cases} \mathrm{pgcd}(a,b,c) = 1, \text{ et} \\ -a < b \leq a < c \text{ ou } 0 \leq b \leq a = c. \end{cases} \tag{1.4}$$

L'algorithme suivant décrit une manière naïve de procéder :

Données : Un entier $\Delta < 0$ avec $\Delta \equiv 0, 1 \bmod 4$
Résultat : L'ensemble T_Δ et le nombre de classes $h(\Delta)$
$T_\Delta \leftarrow \{\}$;
pour $0 \leq b \leq \lfloor \sqrt{-\Delta}/3 \rfloor$ **faire**
  si $\Delta \equiv b^2 \bmod 4$ **alors**
    pour $a | (b^2 - \Delta)/4$ **faire**
      $c \leftarrow (b^2 - \Delta)/(4a)$;
      si $b \leq a \leq c$ *et* $\gcd(a, b, c) = 1$ **alors**
        rajouter (a, b, c) à T_Δ ;
        si $b \neq 0$ *et* $a \neq b$ *et* $a \neq c$ **alors**
          rajouter $(a, -b, c)$ à T_Δ ;
        fin
      fin
    fin
  fin
fin
retourner T_Δ et $h(\Delta) = |T_\Delta|$.

Algorithme 1 : Calcul de T_Δ et de $h(\Delta)$

En résumé, l'algorithme 1 détermine l'ensemble T_Δ, c'est-à-dire l'ensemble des formes réduites de discriminant Δ donné, pour en déduire notamment $h(\Delta)$.

En général, il n'est pas possible de caractériser explicitement les éléments de l'ensemble T_Δ. Toutefois, on pourra remarquer que la forme principale $F_\Delta(x, y)$ introduite en (1.2) est réduite, ce qui fournit un triplet

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right) \in T_\Delta. \tag{1.5}$$

Dans le cas particulier où $\Delta \equiv 1 \bmod 8$, nous disposons également du résultat pratique ci-après :

Proposition 1.3. *Soient $\Delta < 0$ un entier tel que $\Delta \equiv 1 \bmod 8$, et $n \geq 1$ un entier. Si $|\Delta| \geq 2^{2n+2}$, alors l'ensemble T_Δ admet exactement deux triplets (a, b, c) avec $a = 2^n$.*

Démonstration. Fixons $a = 2^n$. Débutons par l'observation que s'il existe des entiers b, c tels que $(a, b, c) \in T_\Delta$, alors b est une solution de l'équation

$$\Delta \equiv b^2 \bmod 4a$$

dans l'intervalle $]-a, a]$, et $c = (\Delta - b^2)/(4a)$ est uniquement déterminé par b.

Il est bien connu que

$$(\mathbb{Z}/4a\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z},$$

si bien que l'équation $\Delta \equiv b^2 \bmod 4a$ d'inconnue $b \in \mathbb{Z}/4a\mathbb{Z}$ admet exactement 4 solutions (puisque Δ est impair), que l'on représentera dans l'intervalle $]-2a, 2a]$ sous la forme $\pm b_1, \pm b_2$ avec $0 < b_1 < b_2 < 2a$ (b_1 et b_2 sont également impairs). Comme $-2a < b_1 - 2a < 0$ et

$$(b_1 - 2a)^2 = b_1^2 + 4a^2 - 4ab_1 \equiv b_1^2 \bmod 4a,$$

alors $b_1 - 2a \in \{-b_1, -b_2\}$, soit $b_1 = a$ ou $b_1 + b_2 = 2a$. Le premier cas est exclu par comparaison des parités. Ainsi, $b_1 < a$. En somme, l'équation $\Delta \equiv b^2 \bmod 4a$ admet exactement deux solutions $\pm b_1$ dans l'intervalle $]-a, a]$. On notera simplement $b = b_1$ dans la suite.

Posons $c = (\Delta - b^2)/(4a)$, de sorte que $\Delta = b^2 - 4ac$. Si $c \leq a$, alors

$$|\Delta| = 4ac - b^2 \leq 2^{2n+2} - 1.$$

Ainsi, si $|\Delta| \geq 2^{2n+2}$, alors $c > a$, et dans ce cas, les deux triplets (a, b, c) et $(a, -b, c)$ appartiennent à T_Δ. L'analyse ci-dessus prouve que ce sont les deux seuls triplets dans T_Δ ayant a comme première composante. ■

Enfin, dans le cadre général, les triplets (a, b, c) de l'ensemble T_Δ avec $a = 2$ peuvent être explicitement déterminés, et leur nombre est décrit par la proposition suivante :

Proposition 1.4. *Soit $\Delta < 0$ un entier avec $\Delta \equiv 0, 1 \bmod 4$. L'ensemble T_Δ possède au plus deux triplets (a, b, c) avec $a = 2$. Plus précisément, l'ensemble T_Δ possède :*

- *deux triplets (a, b, c) avec $a = 2$ si $\Delta \equiv 1 \bmod 8$, $\Delta \neq -7$;*
- *un triplet (a, b, c) avec $a = 2$ si $\Delta \equiv 8, 12 \bmod 16$, $\Delta \neq -4, -8$;*
- *aucun triplet (a, b, c) avec $a = 2$ si $\Delta \equiv 5 \bmod 8$ ou $\Delta \equiv 0, 4 \bmod 16$.*

Nous allons ensuite munir l'ensemble des classes d'équivalence propre de formes réduites de discriminant Δ d'une structure de groupe. Pour ce faire, le lemme suivant est requis.

Lemme 1.5. *Soient $f(x, y) = ax^2 + bxy + cy^2$ et $g(x, y) = a'x^2 + b'xy + c'y^2$ deux formes de discriminant Δ telles que $\operatorname{pgcd}(a, a', (b + b')/2) = 1$ (puisque b et b' ont la même parité, $(b + b')/2$ est bien entier). Alors il existe un unique entier B modulo $2aa'$ tel que*

$$\begin{aligned} B &\equiv b \bmod 2a, \\ B &\equiv b' \bmod 2a', \\ B^2 &\equiv \Delta \bmod 4aa'. \end{aligned}$$

Démonstration. Voir [Cox89, Lemma 3.2]. ■

Nous pouvons maintenant définir la *composition de Dirichlet* de deux formes primitives définies positives de même discriminant.

Définition 1.6. Soient $f(x, y) = ax^2 + bxy + cy^2$ et $g(x, y) = a'x^2 + b'xy + c'y^2$ deux formes primitives définies positives de discriminant $\Delta < 0$ telles que $\operatorname{pgcd}(a, a', (b + b')/2) = 1$. La *composition de Dirichlet* de $f(x, y)$ et de $g(x, y)$ est la forme

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

où B est l'entier déterminé par le lemme 1.5.

La forme $F(x, y)$ ainsi construite est de discriminant $\Delta < 0$, et donc est bien définie positive (puisque $F(1, 0) = aa' = f(1, 0)g(1, 0) > 0$). Il s'avère que cette opération induit une structure de groupe comme voulu :

Théorème 1.7. *Soit $\Delta < 0$ un entier avec $\Delta \equiv 0, 1 \bmod 4$. Soit $\mathrm{Cl}(\Delta)$ l'ensemble des classes d'équivalence propre de formes primitives définies positives de discriminant Δ. Alors la composition de Dirichlet induit une structure de groupe abélien fini sur $\mathrm{Cl}(\Delta)$, appelé* groupe des classes *de discriminant Δ, d'ordre le nombre de classes $h(\Delta)$.*

De plus, l'identité de $\mathrm{Cl}(\Delta)$ est la classe contenant la forme principale $F_0(x, y)$ définie en 1.2, et l'inverse de la classe contenant une forme $ax^2 + bxy + cy^2$ est la classe contenant la forme $ax^2 - bxy + cy^2$.

Démonstration. Voir [Cox89, Theorem 3.9]. ■

1.2 Ordres de corps quadratiques

Définissons à présent ce qu'est un ordre d'un corps quadratique.

Définition 1.8. Soit K un corps quadratique. Un *ordre* $\mathcal{O}$ de K est une partie de K satisfaisant les trois conditions suivantes :

(i) $\mathcal{O}$ est un sous-anneau unitaire de K ;

(ii) $\mathcal{O}$ est un $\mathbb{Z}$-module de type fini ;

(iii) $\mathcal{O}$ contient une $\mathbb{Q}$-base de K.

Puisque $\mathcal{O}$ est sans-torsion, les conditions (ii) et (iii) réunies équivalent à dire que $\mathcal{O}$ est un $\mathbb{Z}$-module libre de rang 2. En outre, par la condition (iii), K est le corps de fractions de $\mathcal{O}$.

L'anneau des entiers $\mathcal{O}_K$ de K est toujours un ordre de K. De plus, tout ordre $\mathcal{O}$ est inclus dans $\mathcal{O}_K$, de sorte que $\mathcal{O}_K$ est l'*ordre maximal* de K. Démontrons ce dernier fait.

Proposition 1.9. *Soient $\mathcal{O}$ un ordre d'un corps quadratique K. Alors $\mathcal{O} \subset \mathcal{O}_K$.*

Démonstration. Soit $x \in \mathcal{O} \setminus \{0\}$. Par la condition (i) ci-dessus, $x^n \in \mathcal{O}$, pour tout $n \geq 0$, donc $\mathbb{Z}[x]$ est un sous-$\mathbb{Z}$-module de $\mathcal{O}$. Par la condition (ii), $\mathbb{Z}[x]$ est de type fini, ce qui prouve que $x \in \mathcal{O}_K$. ■

Tout comme pour l'anneau des entiers, les ordres admettent une description explicite :

Proposition 1.10. *Soit $\mathcal{O}$ un ordre d'un corps quadratique K de discriminant D_K. Alors $\mathcal{O}$ est d'indice fini dans $\mathcal{O}_K$, et en posant $f = [\mathcal{O}_K : \mathcal{O}]$, on a*

$$\mathcal{O} = \mathbb{Z}[f w_K],$$

où w_K est défini par (1.1).

Démonstration. Puisque $\mathcal{O}$ et $\mathcal{O}_K$ sont deux $\mathbb{Z}$-modules libres de rang 2, on déduit que $[\mathcal{O}_K : \mathcal{O}] < \infty$. En posant $f = [\mathcal{O}_K : \mathcal{O}]$, on a $f\mathcal{O}_K \subset \mathcal{O}$, et donc $\mathbb{Z}[f w_K] \subset \mathcal{O}$. Pour conclure, il suffit d'observer que $\mathbb{Z}[f w_K]$ est d'indice f dans $\mathcal{O}_K = \mathbb{Z}[w_K]$. ■

L'entier f de la proposition 1.10 s'appelle le *conducteur* de l'ordre $\mathcal{O}$. Le conducteur de l'ordre maximal $\mathcal{O}_K$ est égal à 1. Un autre invariant important de $\mathcal{O}$ est son *discriminant*, défini comme suit :

Définition 1.11. Soit $\mathcal{O}$ un ordre. Soient (α, β) une $\mathbb{Z}$-base de $\mathcal{O}$, et α', β' les conjugués respectifs de α, β par l'unique automorphisme non trivial de K. Le *discriminant* de $\mathcal{O}$ est la quantité

$$\Delta = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2.$$

Le discriminant est indépendant de la base choisie, et en le calculant avec la base $(1, fw_K)$ de la proposition 1.10, on obtient la formule

$$\Delta = f^2 D_K.$$

Le discriminant satisfait donc $\Delta \equiv 0, 1 \bmod 4$. Par analogie avec D_K, le discriminant Δ détermine $\mathcal{O}$ de manière unique, et tout entier non carré $\Delta \equiv 0, 1 \bmod 4$ est le discriminant d'un ordre d'un corps quadratique. En particulier, par la proposition 1.10, $\mathcal{O}$ s'écrit en termes de son discriminant Δ

$$\mathcal{O} = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right].$$

Remarquons en outre que le discriminant de l'ordre maximal $\mathcal{O}_K$ est bien D_K, ce qui est conforme à la définition donnée précédemment ; on dira dans ce cas que Δ est *fondamental*, pour bien comprendre qu'il s'agit du discriminant de $\mathcal{O}_K$.

Intéressons-nous à présent aux idéaux d'un ordre $\mathcal{O}$. Si $\mathfrak{a}$ est un idéal non nul de $\mathcal{O}$, alors $\mathcal{O}/\mathfrak{a}$ est fini. On peut donc définir la *norme* de $\mathfrak{a}$ par $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. Il s'ensuit que $\mathcal{O}$ est noethérien et de dimension 1 (i.e. que tout idéal premier non nul de $\mathcal{O}$ est maximal). Toutefois, si le conducteur f de $\mathcal{O}$ est strictement plus grand que 1, alors $\mathcal{O}$ n'est pas intégralement clos dans K, de sorte que $\mathcal{O}$ n'est pas un anneau de Dedekind. En conséquence, les idéaux de $\mathcal{O}$ n'admettent pas en général de factorisation unique.

Pour construire la théorie des idéaux de $\mathcal{O}$, il faut donc procéder autrement. On introduit pour cela la notion d'*idéal propre* d'un ordre. Concrètement, étant donné un idéal $\mathfrak{a}$ de $\mathcal{O}$, on constate que

$$\mathcal{O} \subset \{\beta \in K \,;\, \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

L'égalité n'est cependant pas réalisée en général. Par exemple, $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ est de conducteur 2 dans $K = \mathbb{Q}(\sqrt{-3})$, et pour l'idéal $\mathfrak{a}$ de $\mathcal{O}$ engendré par 2 et $1 + \sqrt{-3}$, on a

$$\mathcal{O} \neq \{\beta \in K \,;\, \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K.$$

On dit alors qu'un idéal $\mathfrak{a}$ de $\mathcal{O}$ est *propre* lorsque l'égalité est réalisée :

Définition 1.12. Soient $\mathcal{O}$ un ordre d'un corps quadratique K, et $\mathfrak{a}$ un idéal de $\mathcal{O}$. On dit que $\mathfrak{a}$ est *propre* lorsque

$$\mathcal{O} = \{\beta \in K \,;\, \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

En particulier, tous les idéaux principaux sont propres, ainsi que tous les idéaux de l'ordre maximal $\mathcal{O}_K$.

Étendons cette terminologie idéaux fractionnaires et évoquons enfin la notion d'inversibilité :

Définition 1.13.
Soit $\mathcal{O}$ un ordre d'un corps quadratique K.

- Un *idéal fractionnaire* de $\mathcal{O}$ est un sous-$\mathcal{O}$-module non nul de K de type fini, autrement dit une partie de K de la forme $\alpha\mathfrak{a}$, avec $\alpha \in K^\times$ et $\mathfrak{a}$ un idéal de $\mathcal{O}$.
- On dit qu'un idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}$ est *propre* lorsque

$$\mathcal{O} = \{\beta \in K \,;\, \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

- On dit qu'un idéal fractionnaire $\mathfrak{a}$ de $\mathcal{O}$ est *inversible* s'il existe un autre idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{ab} = \mathcal{O}$.

Les idéaux fractionnaires principaux (c'est-à-dire de la forme $\alpha\mathcal{O}$, avec $\alpha \in K^\times$) sont notamment inversibles. Il s'avère que les notions d'idéaux propres et inversibles coïncident :

Proposition 1.14. *Soient $\mathcal{O}$ un ordre d'un corps quadratique K, et $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}$. Alors $\mathfrak{a}$ est inversible si et seulement si $\mathfrak{a}$ est propre.*

Démonstration. Voir [Cox89, Proposition 7.4]. ■

La proposition 1.14 nous permet de définir le *groupe des classes* de $\mathcal{O}$ comme suit, par analogie avec le groupe des classes de l'ordre maximal $\mathcal{O}_K$. Notons $I(\mathcal{O})$ l'ensemble des idéaux fractionnaires propres de $\mathcal{O}$, qui forment un groupe pour la loi $(\mathfrak{a}, \mathfrak{b}) \longmapsto \mathfrak{ab}$, d'élément neutre $\mathcal{O}$. Les idéaux fractionnaires principaux de $\mathcal{O}$ (i.e. de la forme $\alpha\mathcal{O}$, avec $\alpha \in K^\times$), quant à eux, forment un sous-groupe $P(\mathcal{O})$ de $I(\mathcal{O})$.

Définition 1.15. Soit $\mathcal{O}$ un ordre. Le *groupe des classes* de $\mathcal{O}$, noté $\mathrm{Cl}(\mathcal{O})$, est le groupe quotient

$$\mathrm{Cl}(\mathcal{O}) = I(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

L'ordre de $\mathrm{Cl}(\mathcal{O})$, noté $h(\mathcal{O})$, s'appelle le *nombre de classes* de $\mathcal{O}$.

Lorsque $\mathcal{O} = \mathcal{O}_K$, cette définition coïncide bien avec celle de $\mathrm{Cl}(\mathcal{O}_K)$.

1.3 Ordres et formes quadratiques

Les idéaux d'un ordre $\mathcal{O}$ de discriminant Δ sont remarquablement liés aux formes quadratiques binaires de discriminant Δ mentionnées en 1.1. C'est l'objet du prochain théorème :

Théorème 1.16. *Soit $\mathcal{O}$ un ordre de discriminant Δ d'un corps quadratique imaginaire K. Alors :*

(i) *si $f(x, y) = ax^2 + bxy + cy^2$ est une forme primitive définie positive de discriminant Δ, alors $[a, (-b + \sqrt{\Delta})/2]$ est un idéal propre de $\mathcal{O}$.*

(ii) *L'application $f(x, y) \longmapsto [a, (-b + \sqrt{\Delta})/2]$ induit un isomorphisme entre le groupe des classes $\mathrm{Cl}(\Delta)$ et le groupe des classes $\mathrm{Cl}(\mathcal{O})$. En particulier, $|\mathrm{Cl}(\mathcal{O})| = h(\Delta)$.*

(iii) *Un entier $m > 0$ est représenté par une forme $f(x, y)$ si et seulement si m est la norme $N(\mathfrak{a})$ d'un idéal $\mathfrak{a}$ dans la classe correspondante dans $\mathrm{Cl}(\mathcal{O})$.*

Démonstration. Voir [Cox89, Theorem 7.7] ■

Remarque 1.17. En combinant les théorèmes 1.1 et 1.16, on déduit que l'application $(a, b, c) \in T_\Delta \longmapsto [a, (-b + \sqrt{\Delta})/2]$ une bijection entre l'ensemble T_Δ et le groupe des classes $\mathrm{Cl}(\mathcal{O})$ (T_Δ a été défini par (1.4)).

Par commodité, on préférera souvent les notations $\mathrm{Cl}(\Delta)$ et $h(\Delta)$ à $\mathrm{Cl}(\mathcal{O})$ et $h(\mathcal{O})$. En outre, l'algorithme 1 donne un moyen de calculer $h(\mathcal{O})$, en comptant les formes réduites de discriminant Δ. Nous verrons plus tard les conséquences pratiques de la vision du groupe des classes $\mathcal{C}(\mathcal{O})$ du point de vue des formes binaires.

1.4 Idéaux premiers au conducteur

La définition précédente du groupe des classes $\mathrm{Cl}(\mathcal{O})$ d'un ordre $\mathcal{O}$ d'un corps quadratique K n'est pas entièrement satisfaisante, au sens où la théorie des idéaux de l'anneau des entiers $\mathcal{O}_K$ se transpose mal aux idéaux propres de $\mathcal{O}$. Il faut donc considérer une famille d'idéaux plus restrictive : c'est là qu'intervient la notion d'idéal *premier au conducteur*.

Définition 1.18. Soit $\mathcal{O}$ un ordre de conducteur f. On dit qu'un idéal non nul $\mathfrak{a}$ de $\mathcal{O}$ est *premier à* f si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$, autrement dit si les idéaux $\mathfrak{a}$ et $f\mathcal{O}$ sont premiers entre eux.

Les propriétés élémentaires des idéaux premiers au conducteur sont les suivantes (cf. [Cox89, Lemma 7.18]) :

Lemme 1.19. *Soit $\mathcal{O}$ un ordre de conducteur f.*

(i) *Un idéal $\mathfrak{a}$ non nul de $\mathcal{O}$ est premier à f si et seulement si sa norme $N(\mathfrak{a})$ est première à f.*

(ii) *Tout idéal non nul de $\mathcal{O}$ premier à f est propre.*

Démonstration. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}$.

(i) Soit $m_f : \mathcal{O}/\mathfrak{a} \longrightarrow \mathcal{O}/\mathfrak{a}$ la multiplication par f. Alors $\mathfrak{a}$ est premier à f si et seulement m_f est un isomorphisme. Par le théorème de structure des groupes abéliens finis, m_f est un isomorphisme si et seulement si f est premier à l'ordre $N(\mathfrak{a})$ de $\mathcal{O}/\mathfrak{a}$, ce qui prouve (i).

(ii) Supposons que $\mathfrak{a}$ soit premier à f. Soit $\beta \in K$ tel que $\beta\mathfrak{a} \subset \mathfrak{a}$. Alors $\beta \in \mathcal{O}_K$, et on a

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K.$$

Or, $f\mathcal{O}_K \subset \mathcal{O}$, d'où $\beta\mathcal{O} \subset \mathcal{O}$. Par conséquent, $\beta \in \mathcal{O}$, ce qui prouve que $\mathfrak{a}$ est propre. ■

Il s'ensuit que l'ensemble des idéaux non nuls de $\mathcal{O}$ premiers à f est inclus dans $I(\mathcal{O})$ et stable par multiplication (puisque $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, voir [Cox89, Lemma 7.14], est également premier à f si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls premiers à f). On note $I(\mathcal{O}, f) \subset I(\mathcal{O})$ le sous-groupe des idéaux fractionnaires qu'ils engendrent, ainsi que $P(\mathcal{O}, f)$ le sous-groupe de $I(\mathcal{O}, f)$ engendré par les idéaux principaux $\alpha\mathcal{O}$, où $\alpha \in \mathcal{O}$ a une norme $N(\alpha)$ première à f.

Proposition 1.20. *L'inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induit un isomorphisme*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) = \mathrm{Cl}(\mathcal{O}).$$

Démonstration. Voir [Cox89, Proposition 7.19]. ■

Les idéaux de $\mathcal{O}$ premiers au conducteur sont reliés aux idéaux de l'ordre maximal $\mathcal{O}_K$ de la manière suivante. Étant donné un entier $m > 0$, on dit qu'un idéal $\mathfrak{a}$ de $\mathcal{O}_K$ est *premier à* m si $\mathfrak{a}+m\mathcal{O}_K = \mathcal{O}_K$. Comme dans le lemme 1.19, cette condition est équivalente à $\operatorname{pgcd}(N(\mathfrak{a}), m) = 1$. L'ensemble $I_K(m)$ engendré par les idéaux de $\mathcal{O}_K$ premiers à m forme alors un sous-groupe du groupe I_K des idéaux fractionnaires de $\mathcal{O}_K$.

Proposition 1.21. *Soit $\mathcal{O}$ un ordre de conducteur f d'un corps quadratique imaginaire K. Alors :*

(i) *pour tout idéal $\mathfrak{a}$ de $\mathcal{O}_K$ premier à f, $\mathfrak{a} \cap \mathcal{O}$ est un idéal de $\mathcal{O}$ premier à f et de même norme ;*

(ii) *pour tout idéal $\mathfrak{a}$ de $\mathcal{O}$ premier à f, $\mathfrak{a}\mathcal{O}_K$ est un idéal de $\mathcal{O}_K$ premier à f et de même norme ;*

(iii) *L'application $\mathfrak{a} \longmapsto \mathfrak{a} \cap \mathcal{O}$ induit un isomorphisme de $I_K(f)$ dans $I(\mathcal{O}, f)$, d'inverse $\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_K$.*

Démonstration. Voir [Cox89, Proposition 7.20]. ■

Proposition 1.22. *Soit $\mathcal{O}$ un ordre de conducteur f d'un corps quadratique imaginaire K. On a les isomorphismes*

$$\mathrm{Cl}(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f),$$

où $P_{K,\mathbb{Z}}(f)$ est le sous-groupe de $I_K(f)$ engendré par les idéaux principaux de la forme $\alpha\mathcal{O}_K$, où $\alpha \in \mathcal{O}_K$ satisfait $\alpha \equiv a \bmod f\mathcal{O}_K$ pour un entier a premier à f.

Démonstration. [Cox89, Proposition 7.22]. ■

Le dernier isomorphisme $\mathrm{Cl}(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$ relie ainsi directement le groupe des classes $\mathrm{Cl}(\mathcal{O})$ aux idéaux de $\mathcal{O}_K$, ce qui permet comme souhaité de transposer la théorie des idéaux de $\mathcal{O}_K$ à celle de $\mathcal{O}$.

1.5 Nombre de classes

L'une des applications les plus remarquables de la proposition 1.22 est la "formule du nombre de classes", qui exprime le nombre de classes $h(\mathcal{O})$ d'un ordre $\mathcal{O}$ d'un corps quadratique imaginaire K en fonction du nombre de classes $h(\mathcal{O}_K)$ de l'ordre maximal $\mathcal{O}_K$. Avant d'énoncer la formule, nous avons besoin de définir le *symbole de Kronecker* (D_K/p) : si p est un nombre premier impair, alors (D_K/p) est simplement le symbole de Legendre, et si $p = 2$, on pose

$$\left(\frac{D_K}{2}\right) = \begin{cases} 0 & \text{si } 2 | D_K, \\ 1 & \text{si } D_K \equiv 1 \bmod 8, \\ -1 & \text{si } D_K \equiv 5 \bmod 8. \end{cases}$$

Théorème 1.23 (formule du nombre de classes)**.** *Soit $\mathcal{O}$ un ordre de conducteur f d'un corps quadratique imaginaire K. Alors*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|f} \left(1 - \left(\frac{D_K}{p}\right)\frac{1}{p}\right).$$

De plus, $h(\mathcal{O})$ est toujours un multiple entier de $h(\mathcal{O}_K)$.

Démonstration. Voir [Cox89, Theorem 7.24]. ■

Grâce au théorème 1.23, le problème de calculer $h(\Delta)$ pour un entier $\Delta < 0$ avec $\Delta \equiv 0, 1 \bmod 4$ se réduit donc à celui de calculer $h(D_K)$ pour le discriminant $D_K < 0$ d'un corps quadratique imaginaire. Ce dernier peut être obtenu par la formule classique

$$h(D_K) = -\frac{|\mathcal{O}_K^\times|}{2|D_K|} \sum_{n=1}^{|D_K|-1} \left(\frac{D_K}{n}\right) n, \tag{1.6}$$

où (D_K/n) est le symbole de Jacobi ; voir, par exemple [Bor66, Chapter 5, Section 4].

La formule (1.6) ne permet pas de décrire le comportement de $h(D_K)$ lorsque $|D_K|$ tend vers $+\infty$. Le meilleur résultat est dû à Siegel [Sie35], qui a démontré que

$$\lim_{D_K \to -\infty} \frac{\log h(D_K)}{\log |D_K|} = \frac{1}{2}.$$

En particulier, pour tout $\varepsilon > 0$, il existe une constante $C(\varepsilon) > 0$ telle que

$$h(D_K) > C(\varepsilon)|D_K|^{1/2-\varepsilon}.$$

Cependant, la constante $C(\varepsilon)$ dans la preuve de Siegel n'est pas effective. D'un autre côté, Goldfeld, Gross, Zagier et Oesterlé ont démontré dans les années 1980 la formule plus faible

$$h(D_K) > \frac{\log |D_K|}{55} \prod_{p|D_K,\, p<D_K} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right).$$

On pourra se référer à [Oes85, Oes88] et [Zag84] pour une discussion plus approfondie sur cette formule.

Il en résulte qu'il existe un nombre fini d'ordres de corps quadratiques imaginaires de nombre de classes h donné. Toutefois, même pour de petites valeurs de h, déterminer tous les ordres de nombre de classes h demeure un problème difficile. Cela étant dit, les ordres de nombre de classes 1 sont bien connus, les voici :

Théorème 1.24.

(i) *Si K est un corps quadratique imaginaire de discriminant D_K, alors*

$$h(D_K) = 1 \iff D_K \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

(ii) *Si $\Delta \equiv 0, 1 \bmod 4$ est un entier strictement négatif, alors*

$$\begin{aligned} h(D) = 1 \iff \Delta \in \{ &-3, -4, -7, -8, -11, -2^2 \cdot 3, -2^2 \cdot 4, \\ &-19, -3^2 \cdot 3, -2^2 \cdot 7, -43, -67, -163\}. \end{aligned}$$

1.6 Ordres de groupes des classes 2-élémentaire

Rappelons qu'un groupe fini G est dit 2-*élémentaire* si tous ses éléments non triviaux sont d'ordre 2, auquel cas il est abélien et isomorphe à un produit fini de groupes cycliques d'ordre 2. La question que l'on pose dans cette section est la suivante : quels sont les ordres de corps

quadratiques imaginaires dont le groupe des classes est 2-élementaire ? Une réponse partielle est fournie par Weinberger, dont nous allons citer le résultat.

Soit $\Delta < 0$ un entier avec $\Delta \equiv 0, 1 \bmod 4$. Le groupe $\mathrm{Cl}(\Delta)/\mathrm{Cl}(\Delta)^2$ s'appelle le "*genus group*" de Δ. Il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^\mu$, où $\mu = \mu(\Delta) \in \{\omega(\Delta) - 1, \omega(\Delta)\}$, et $\omega(\Delta)$ est le nombre de facteurs premiers disctincts de Δ. En outre, $\mu(\Delta) = \omega(\Delta) - 1$ lorsque Δ est fondamental.

Euler a étudié les discriminants Δ satisfaisant la propriété

$$|\mathrm{Cl}(\Delta)^2| = 1,$$

où, de manière équivalente, $\mathrm{Cl}(\Delta) \simeq (\mathbb{Z}/2\mathbb{Z})^\mu$. Chowla a démontré que l'ensemble des tels discriminants est fini. En utilisant une formule plus approfondie de Tatuzawa [Tat52] sur les zéros de Siegel, Weinberger [Wei73] a amélioré ce résultat en prouvant que les discriminants fondamentaux satisfaisant cette propriété sont bornés explicitement, avec au plus une exception. Voici l'énoncé exact de sa proposition :

Proposition 1.25 (Weinberger)**.** *Il existe un entier $D^* < 0$ tel que, pour tout discriminant D_K d'un corps quadratique imaginaire K, si $\mathrm{Cl}(D_K)$ est 2-élémentaire, alors $|D'_K| \leq 5460$ ou $D_K = D^*$.*

Ici, D'_K désigne la partie sans facteur carré de D_K :

$$D'_K = \begin{cases} D_K & \text{si } D_K \equiv 1 \bmod 4, \\ D_K/4 & \text{si } D_K \equiv 0 \bmod 4. \end{cases}$$

Les méthodes actuelles (voir [Wat04]) permettent de déterminer aisément la liste complète des discriminants fondamentaux D_K tels que $|\mathrm{Cl}(D_K)^2| = 1$ et $|D'_K| \leq 5460$. Comme le groupe $\mathrm{Cl}(D_K)$ est un quotient du groupe $\mathrm{Cl}(\Delta)$, alors si $\mathrm{Cl}(\Delta)$ est 2-élémentaire, $\mathrm{Cl}(D_K)$ l'est également. Ainsi, la liste des discriminants $\Delta = f^2 D_K$ tels que $|\mathrm{Cl}(\Delta)^2| = 1$ et $|D'_K| \leq 5460$ peut également être obtenue ; nous la reproduisons dans le tableau 1.1 ci-dessous.

Table 1.1 – Discriminants Δ connus avec $|\mathrm{Cl}(\Delta)^2| = 1$

$h(\Delta) = 1$	$-3, -3 \cdot 2^2, -3 \cdot 3^2, -4, -4 \cdot 2^2, -7, -7 \cdot 2^2, -8, -11, -19, -43, -67, -163$
$h(\Delta) = 2$	$-3 \cdot 4^2, -3 \cdot 5^2, -3 \cdot 7^2, -4 \cdot 3^2, -4 \cdot 4^2, -4 \cdot 5^2, -7 \cdot 4^2, -8 \cdot 2^2, -8 \cdot 3^2, -11 \cdot 3^2,$ $-15, -15 \cdot 2^2, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148,$ $-187, -232, -235, -267, -403, -427$
$h(\Delta) \geq 4$	$-3 \cdot 8^2, -7 \cdot 8^2, -8 \cdot 6^2, -15 \cdot 4^2, -15 \cdot 8^2, -20 \cdot 3^2, -24 \cdot 2^2, -35 \cdot 3^2, -40 \cdot 2^2,$ $-84, -88 \cdot 2^2, -120, -120 \cdot 2^2, -132, -168, -168 \cdot 2^2, -195, -228, -232 \cdot 2^2,$ $-280, -280 \cdot 2^2, -312, -312 \cdot 2^2, -340, -372, -408, -408 \cdot 2^2, -420, -435,$ $-483, -520, -520 \cdot 2^2, -532, -555, -595, -627, -660, -708, -715,$ $-760, -760 \cdot 2^2, -795, -840, -840 \cdot 2^2, -1012, -1092, -1155, -1320, -1320 \cdot 2^2,$ $-1380, -1428, -1435, -1540, -1848, -1848 \cdot 2^2, -1995, -3003, -3315, -5460$

Le corollaire suivant est ainsi une conséquence du résultat de Weinberger.

Corollaire 1.26. *Il existe un entier $D^* < 0$ tel que, pour tout discriminant Δ d'un ordre d'un corps quadratique imaginaire K de discriminant D_K, si $\mathrm{Cl}(\Delta)$ est 2-élémentaire, alors Δ apparaît dans le tableau 1.1 ou $D_K = D^*$.*

Remarque 1.27. Les nombres de classes des discriminants du tableau 1.1 valent au plus 16, et les résultats de [Wat04] impliquent que le tableau 1.1 contient tous les discriminants Δ vérifiant $|\mathrm{Cl}(\Delta)^2| = 1$ et $h(\Delta) \leq 64$. En conséquence, si Δ vérifie $|\mathrm{Cl}(\Delta)^2| = 1$ mais n'apparaît pas dans le tableau 1.1, alors $h(\Delta) \geq 128$.

1.7 Éléments de théorie des corps de classes

La théorie des corps de classes a pour but de classifier les extensions abéliennes d'un corps de nombres donnés. De telles extensions sont décrites en termes de *groupes des classes généralisés*. Dans cette section, nous ne développons pas la théorie dans un cadre général ; on pourra se référer à [Cox89, §8] pour une introduction. En revanche, nous décrivons les résultats obtenus dans le cas particulier des corps quadratiques imaginaires, et faisons ainsi le lien avec les ordres évoqués précédemment. Ce dernier point est, quant à lui, abordé dans [Cox89, §9].

Il résulte de la théorie des corps de classes le théorème d'existence suivant :

Théorème 1.28. *Soient K un corps quadratique imaginaire, et $\mathcal{O}$ un ordre de K de conducteur f et de discriminant Δ. Il existe une unique extension abélienne L/K (à isomorphisme près), non ramifiée en dehors de $f\mathcal{O}_K$, telle que*

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Gal}(L/K).$$

En particulier, $[L : K] = h(\mathcal{O})$. Le corps L sera noté $\mathrm{RiCF}(\mathcal{O})$, $\mathrm{RiCF}(\Delta)$ *ou encore* $\mathrm{RiCF}(K, f)$, *et s'appelle le* corps de classes *de $\mathcal{O}$.*

Étant donné un ordre $\mathcal{O}$ d'un corps quadratique imaginaire K, le théorème 1.28 fournit donc une extension abélienne L/K dont le groupe de Galois est isomorphe à $\mathrm{Cl}(\mathcal{O})$. Il est légitime de s'interroger alors quant à la structure du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$; c'est l'objet de la discussion ci-dessous. Nous verrons plus tard (cf. remarque 2.23) que l'extension $L/\mathbb{Q}$ est galoisienne.

On dit qu'un groupe fini G est de *type diédral* s'il existe un sous-groupe abélien H de G d'indice 2, ainsi qu'un élément $\iota \in G \setminus H$ d'ordre 2, tel que pour tout $h \in H$, on a $\iota h \iota = h^{-1}$. Le couple (H, ι) s'appelle dans ce cas une *structure diédrale* sur G, et le groupe G s'écrit comme un produit semi-direct :

$$G \simeq H \rtimes \langle \iota \rangle \simeq H \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Un groupe de type diédral peut être abélien, auquel cas il est 2-élémentaire. Par ailleurs, un groupe non abélien de type diédral ne possède essentiellement qu'une seule structure diédrale, d'après le lemme suivant dû à Hendrik Lenstra :

Lemme 1.29 (Lenstra)**.** *Soit G un groupe non abélien de type diédral, muni d'une structure diédrale (H, ι). Alors H est engendré par tous les éléments de G d'ordre > 2. En particulier, H est unique : si (H', ι') est une autre structure diédrale sur G, alors $H = H'$.*

Démonstration. Tout d'abord, G contient au moins un élément d'ordre > 2, car il serait abélien autrement. Ensuite, tout élément de G d'ordre > 2 appartient à H, car tout élément de $G \setminus H$ est de la forme ιh avec $h \in H$, et donc est d'ordre 2. Il reste à montrer que tout élément de H d'ordre 2 est produit de deux éléments d'ordre > 2. Soient $h \in H$ d'ordre 2 et $k \in H$ d'ordre > 2. Comme H est abélien, kh est aussi d'ordre > 2. En écrivant $h = k^{-1} \cdot kh$, le résultat est démontré. ∎

Il s'avère que le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ est de type diédral :

Proposition 1.30. *Soient $\mathcal{O}$ un ordre d'un corps quadratique imaginaire K, et $L = \mathrm{RiCF}(\mathcal{O})$. Alors l'extension $L/\mathbb{Q}$ est galoisienne, et son groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ est de type diédral, ayant pour structure diédrale $(\mathrm{Gal}(L/K), \iota)$, où ι est la conjugaison complexe.*

Démonstration. Voir [Cox89, Lemma 9.3]. ■

Pour terminer, décrivons le compositum de deux corps de classes :

Proposition 1.31. *Soient K un corps quadratique imaginaire de discriminant D, et $f_1, f_2 > 0$ deux entiers. Posons $f = \mathrm{ppcm}(f_1, f_2)$. Alors :*

(i) *si $D \notin \{-3, -4\}$, alors $\mathrm{RiCF}(K, f_1)\,\mathrm{RiCF}(K, f_2) = \mathrm{RiCF}(K, f)$;*

(ii) *supposons que $D \in \{-3, -4\}$. Alors $\mathrm{RiCF}(K, f_1)\,\mathrm{RiCF}(K, f_2) = \mathrm{RiCF}(K, f)$ lorsque $f_1 = 1$ ou $f_2 = 1$ ou $\mathrm{pgcd}(f_1, f_2) > 1$. Dans le cas contraire, c'est-à-dire lorsque $f_1, f_2 > 1$ et $\mathrm{pgcd}(f_1, f_2) = 1$, $\mathrm{RiCF}(K, f_1)\,\mathrm{RiCF}(K, f_2)$ est un sous-corps de $\mathrm{RiCF}(K, f)$ de degré 2 si $D = -4$, et de degré 3 si $D = -3$.*

Démonstration. Voir [All15, Proposition 3.1]. ■

Chapitre 2

Multiplication complexe

La théorie de la multiplication complexe se concentre sur l'étude des réseaux du plan complexe stables par multiplication par un nombre complexe. De tels réseaux donnent naturellement naissance à des ordres de corps quadratiques imaginaires, ce qui permet d'établir le lien entre les groupes des classes et les classes d'homothétie de réseaux. L'outil central est la fonction j-invariant, qui classifie les classes d'homothétie. Le théorème fondamental de la théorie de la multiplication complexe stipule que le j-invariant $j(\mathcal{O})$ d'un ordre $\mathcal{O}$ d'un corps quadratique imaginaire K est un entier algébrique, qui engendre le corps de classes de K. Un tel nombre s'appelle un *module singulier*.

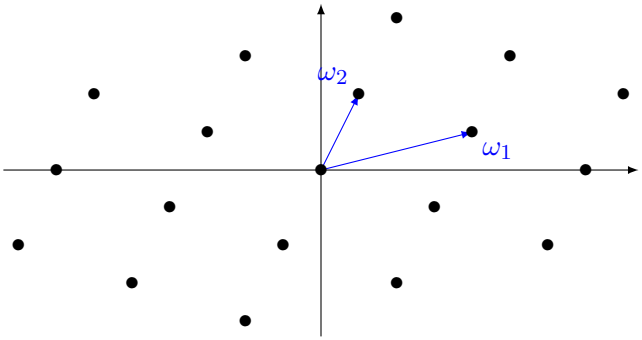
Dans ce chapitre, nous introduisons d'abord sommairement ces différents concepts dans les sections 2.1, 2.2 et 2.3. Puis, nous détaillons les principales propriétés analytiques de la fonction j dans la section 2.4, et donnons notamment quelques estimations utiles dans la section 2.5. Nous évoquons succinctement la courbe modulaire $Y_0(N)$ dans la section 2.6. Enfin, nous revenons aux propriétés algébriques des modules singuliers, en explicitant leurs conjugués dans la section 2.7, et en comparant les corps qu'ils engendrent sur $\mathbb{Q}$ dans la section 2.8.

2.1 Fonctions elliptiques et fonction $\wp$ de Weierstrass

La propriété de multiplication complexe d'un réseau s'exprime en termes des *fonctions elliptiques* pour ce réseau, et plus particulièrement d'une fonction elliptique de référence, appelée *fonction $\wp$ de Weierstrass*. Nous commençons donc par étudier ces fonctions au cours de cette section.

Il convient de rappeler ce qu'est un réseau du plan complexe.

Définition 2.1. Un *réseau* du plan complexe $\mathbb{C}$ est un sous-groupe additif L de $\mathbb{C}$ engendré par deux nombres complexes ω_1, ω_2 linéairement indépendants sur $\mathbb{R}$. On écrit $L = [\omega_1, \omega_2]$.



Les *fonctions elliptiques* pour un réseau L sont les fonctions $\mathbb{C} \longrightarrow \mathbb{C}$ méromorphes sur $\mathbb{C}$, et périodiques par rapport aux points de L. Plus précisément :

Définition 2.2. Soit L un réseau. Une *fonction elliptique* pour L est une fonction $f : \mathbb{C} \longrightarrow \mathbb{C}$ satisfaisant les deux conditions suivantes :

(i) $f(z)$ est méromorphe sur $\mathbb{C}$;

(ii) pour tout $\omega \in L$, $f(z+\omega) = f(z)$.

Remarque 2.3. Si $L = [\omega_1, \omega_2]$, la condition (ii) ci-dessus équivaut à

$$f(z+\omega_1) = f(z+\omega_2) = f(z).$$

On dit que la fonction f est *bi-périodique*.

La proposition ci-après justifie le fait de considérer des fonctions méromorphes, et non pas de se restreindre aux fonctions holomorphes :

Proposition 2.4. *Soit $L = [\omega_1, \omega_2]$ un réseau de $\mathbb{C}$. Les seules fonctions $f(z)$ elliptiques pour L et holomorphes sur $\mathbb{C}$ sont les fonctions constantes.*

Démonstration. Soit $f(z)$ une telle fonction. Sur le compact

$$\{s\omega_1 + t\omega_2 \,;\, s,t \in [0,1]\} \subset \mathbb{C},$$

la fonction $f(z)$ est bornée, donc par périodicité, elle est bornée sur $\mathbb{C}$. Par conséquent, d'après le théorème de Liouville, $f(z)$ est constante. ■

La prochaine proposition permet de construire une fonction elliptique particulière :

Proposition 2.5. *Soit L un réseau. La série*

$$\frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

converge uniformément sur tous les compacts de $\mathbb{C}\setminus L$, et définit une fonction méromorphe sur $\mathbb{C}$. Sa somme, notée $\wp_L(z)$ (ou simplement $\wp(z)$ lorsqu'il n'y a pas d'ambiguïté sur le réseau L), s'appelle la fonction $\wp$ de Weierstrass *de L.*

La fonction $\wp(z)$ est paire, de dérivée

$$\wp'(z) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3}.$$

On s'aperçoit notamment que $\wp'(z)$ est bi-périodique, et de plus impaire. Il s'agit effectivement d'une fonction elliptique :

Proposition 2.6. *Soit $L = [\omega_1, \omega_2]$ un réseau. La fonction $\wp$ de Weierstrass associée à L est bi-périodique.*

Démonstration. Comme $\wp'(z)$ est bi-périodique, on a

$$\frac{\mathrm{d}}{\mathrm{d}z}(\wp(z+\omega_1) - \wp(z)) = 0,$$

donc la fonction $\wp(z+\omega_1) - \wp(z)$ est constante. En l'évaluant en $z = -\omega_1/2$ (qui n'est pas un pôle), on obtient

$$\wp\left(\frac{\omega_1}{2}\right) - \wp\left(-\frac{\omega_1}{2}\right) = 0$$

par parité de $\wp(z)$. En procédant de même avec ω_2, on en déduit la proposition. ■

Les pôles de la fonction $\wp(z)$ d'un réseau L se déduisent aisément de l'expression de $\wp(z)$: il s'agit des points de L. L'une des propriétés les plus essentielles de la fonction $\wp(z)$ est qu'elle vérifie une équation différentielle d'ordre 1. Consignons ces différents faits :

Proposition 2.7. *Soit L un réseau.*

(i) *La fonction $\wp(z)$ de Weierstrass associée à L est une fonction elliptique pour L, dont les pôles sont les points de L et sont d'ordre 2.*

(ii) *La fonction $\wp(z)$ satisfait l'équation différentielle*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$

où les constantes $g_2(L)$ et $g_3(L)$ sont définies par

$$g_2(L) = 60\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^4},$$
$$g_3(L) = 140\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^6}.$$

Démonstration. Montrons l'assertion (ii). Posons

$$g(z) = \wp(z) - \frac{1}{z^2} = \sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Le développement en série de Laurent de $\wp$ au voisinage de 0 est de la forme

$$\wp(z) = \frac{1}{z^2} + b_2 z^2 + b_4 z^4 + \ldots,$$

puisque $\wp$ est paire et que $g(0) = 0$. En dérivant terme à terme, la fonction g permet de calculer les premiers coefficients de ce développement :

$$b_2 = 3 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4}, \quad b_4 = 5 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6}.$$

On dérive terme à terme le développement de $\wp$ pour obtenir

$$\wp'(z) = -\frac{2}{z^3} + 2b_2 z + 4b_4 z^3 + \dots,$$

relation qu'on élève au carré :

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{8b_2}{z^2} - 16b_4 + \dots$$

On obtient ainsi

$$\wp'(z)^2 - 4\wp(z)^3 = -\frac{20b_2}{z^2} - 28b_4 + \dots,$$

et donc la fonction

$$\wp'(z)^2 - 4\wp(z)^3 + 20\wp(z) + 28b_4$$

est holomorphe au voisinage de 0 et nulle en 0. Toutefois, elle est bi-périodique, donc holomorphe sur $\mathbb{C}$, et finalement constante égale à 0 en vertu de la proposition 2.4. Par ailleurs, on retrouve bien les valeurs $g_2(L) = 20b_2$ et $g_3(L) = 28b_4$ introduites ci-dessus. ■

Voici une propriété utile de la fonction $\wp(z)$:

Proposition 2.8. *Soit $\wp(z)$ la fonction de Weierstrass d'un réseau $L = [\omega_1, \omega_2]$. Pour tous $z, w \notin L$, $\wp(z) = \wp(w)$ si et seulement si $z \equiv \pm w \bmod L$.*

Démonstration. Le sens indirect de l'équivalence est immédiat puisque $\wp(z)$ est bi-périodique et paire. Intéressons-nous au sens direct. Fixons un nombre réel $-1 < \delta < 0$, et considérons le parallélogramme

$$\mathcal{P} = \{s\omega_1 + t\omega_2 \,;\, s, t \in [\delta, \delta + 1]\} \subset \mathbb{C},$$

ainsi que son bord Γ orienté dans le sens trigonométrique. Ajoutons que tout nombre complexe est congrue modulo L à un élément de $\mathcal{P}$.

Fixons $w \notin L$, et considérons la fonction $f(z) = \wp(z) - \wp(w)$. Quitte à ajuster δ, on peut supposer que $f(z)$ n'a ni zéro ni pôle sur Γ. Ainsi, par le théorème de l'indice, on a

$$\frac{1}{2i\pi} \int_\Gamma \frac{f'(z)}{f(z)} \mathrm{d}z = Z - P,$$

où Z (resp. P) est le nombre de zéros (resp. de pôles) de $f(z)$ dans $\mathcal{P}$, comptés avec multiplicités. Comme $f'(z)/f(z)$ est bi-périodique, les intégrales sur les côtés opposés de Γ s'annulent, si bien que

$$\int_\Gamma \frac{f'(z)}{f(z)} \mathrm{d}z = 0,$$

ce qui montre que $Z = P$. Toutefois, d'après le (i) de la proposition 2.7, l'unique pôle de $f(z)$ dans $\mathcal{P}$ est 0, d'ordre 2, d'où $Z = P = 2$. On en déduit que $f(z)$ a deux zéros (toujours en comptant les multiplicités) dans $\mathcal{P}$.

Distinguons à présent deux cas. Si $w \not\equiv -w \bmod L$, alors w et $-w$ sont congrus modulo L à deux zéros distincts de $f(z)$ dans $\mathcal{P}$. Dans ce cas-ci, puisque $Z = 2$, ce sont les deux seuls zéros de $f(z)$ dans $\mathcal{P}$, de multiplicité 1 chacun, c'est-à-dire $\wp'(w) \neq 0$. En revanche, si $w \equiv -w \bmod L$, alors $2w \in L$. Puisque $\wp'$ est bi-périodique et impaire, on obtient

$$\wp'(w) = \wp'(w - 2w) = \wp'(-w) = -\wp'(w),$$

soit $\wp'(w) = 0$. Ainsi, w est congru modulo L à un zéro de $f(z)$ dans $\mathcal{P}$ de multiplicité supérieure ou égale à 2. À nouveau, puisque $Z = 2$, il s'agit donc de l'unique zéro de $f(z)$ dans $\mathcal{P}$. ■

La preuve de la proposition 2.8 nous renseigne en outre sur les zéros de $\wp'$:

Corollaire 2.9. *Pour tout $w \notin L$, $\wp'(w) = 0$ si et seulement si $2w \in L$.*

2.2 j-invariant d'un réseau

Dans cette section, nous munissons l'ensemble des réseaux du plan complexe d'une relation d'équivalence préservant les fonctions elliptiques, et introduisons la fonction *j-invariant* qui caractérise les classes d'équivalence.

Définition 2.10. On dit que deux réseaux L et L' sont *homothétiques* s'il existe $\lambda \in \mathbb{C}^\times$ tel que $L' = \lambda L$.

Remarque 2.11. L'homothétie définit une relation d'équivalence sur l'ensemble des réseaux. En outre, deux réseaux homothétiques admettent "essentiellement" les mêmes fonctions elliptiques : en effet, si $f(z)$ est une fonction elliptique pour L, alors $f(\lambda^{-1}z)$ est une fonction elliptique pour λL. De plus, la fonction $\wp(z)$ de Weierstrass se transforme comme suit :

$$\wp_{\lambda L}(\lambda z) = \lambda^{-2}\wp_L(z).$$

Pour définir le *j-invariant* d'un réseau L, il faut tout d'abord définir son *discriminant* :

Définition 2.12. Soit L un réseau. Le *discriminant* de L, noté $\Delta(L)$, est la quantité définie par

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2,$$

où $g_2(L), g_3(L)$ sont les constantes apparaissant dans l'équation différentielle satisfaite par $\wp$ introduite dans la proposition 2.7.

Remarque 2.13. La quantité $\Delta(L)$ est liée au discriminant du polynôme $4X^3 - g_2(L)X - g_3(L)$ qui apparaît dans l'équation différentielle satisfaite par $\wp(z)$: en effet, on a

$$\Delta(L) = 16\,\mathrm{disc}(4X^3 - g_2(L)X - g_3(L)).$$

Le discriminant d'un réseau est toujours non nul :

Proposition 2.14. *Soit $L = [\omega_1, \omega_2]$ un réseau. Alors $\Delta(L) \neq 0$.*

Démonstration. D'après la remarque 2.13, montrer que $\Delta(L) \neq 0$ revient à montrer que le discriminant du polynôme $4X^3 - g_2(L)X - g_3(L)$ est non nul, c'est-à-dire que ce dernier admet trois racines distinctes.

Soit $w \notin L$. Si $\wp'(w) = 0$, alors

$$0 = \wp'(w)^2 = 4\wp(w)^3 - g_2(L)\wp(w) - g_3(L),$$

donc $\wp(w)$ est racine du polynôme $4X^3 - g_2(L)X - g_3(L)$. D'après le corollaire 2.9, $\wp'(w) = 0$ si et seulement si $2w \in L$. Pour chacun des éléments $w_1 = \omega_1/2, w_2 = \omega_2/2$ et $\omega_3 = (\omega_1 + \omega_2)/2$, on a $2w_i \in L$, donc $\wp(w_i)$ est une racine de ce polynôme, $i \in \{1, 2, 3\}$. La proposition 2.8 garantit que ces trois racines sont distinces, d'où le résultat. ■

Nous pouvons désormais définir le *j-invariant* :

Définition 2.15. Soit L un réseau. Le *j-invariant* de L, noté $j(L)$, est la quantité définie par

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{g_2(L)^3}{\Delta(L)}.$$

Comme annoncé, le j-invariant caractérise les classes d'homothétie de réseaux :

Théorème 2.16. *Soient L et L' deux réseaux. Alors L et L' sont homothétiques si et seulement si $j(L) = j(L')$.*

Démonstration. Voir [Cox89, Theorem 10.9]. ■

2.3 Multiplication complexe

Nous avons désormais tous les outils en main pour développer le concept de multiplication complexe.

Démarrons par l'observation suivante. Soient $\mathcal{O}$ un ordre d'un corps quadratique imaginaire K, et $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$. Par le théorème 1.16, il existe $\alpha, \beta \in K$ tels que $\mathfrak{a} = [\alpha, \beta]$. Puisque K est quadratique imaginaire, α et β sont linéairement indépendants sur $\mathbb{R}$. En conséquence, $\mathfrak{a} = [\alpha, \beta]$ est un réseau de $\mathbb{C}$, et son j-invariant $j(\mathfrak{a})$ est bien défini. Un tel nombre s'appelle un *module singulier*.

L'idée de la multiplication complexe est motivée par la proposition suivante :

Proposition 2.17. *Soient L un réseau, et $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Les assertions suivantes sont équivalentes :*

(i) *$\wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$;*

(ii) *$\alpha L \subset L$;*

(iii) *il existe un ordre $\mathcal{O}$ d'un corps quadratique imaginaire K tel que $\alpha \in \mathcal{O}$ et L est homothétique à un idéal fractionnaire propre de $\mathcal{O}$.*

De plus, si ces conditions sont satisfaites, alors $\wp(\alpha z)$ peut s'écrire sous la forme

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))},$$

où A et B sont des polynômes premiers entre eux tels que

$$\deg(A) = \deg(B) + 1 = [L : \alpha L] = N(\alpha).$$

Pour démontrer la proposition 2.17, nous allons employer le lemme suivant.

Lemme 2.18. *Soient L un réseau, et $f(z)$ une fonction elliptique pour L. Si f est paire, alors $f(z)$ est une fonction rationnelle en $\wp(z)$.*

Démonstration. Supposons dans un premier temps que $f(z)$ est holomorphe sur $\mathbb{C}\setminus L$. Comme $f(z)$ est paire, le développement en série de Laurent de $f(z)$ au voisinage de 0 est de la forme

$$f(z) = \sum_{n=1}^{N} \frac{a_n}{z^{2n}} + h(z),$$

tandis que celui de $\wp(z)$ est de la forme

$$\wp(z) = \frac{1}{z^2} + g(z)$$

avec $h(z)$ et $g(z)$ deux fonctions holomorphes sur un voisinage de 0. Posons alors

$$A(X) = \sum_{n=1}^{N} b_n X^n,$$

où l'on peut choisir les coefficients $b_1, \dots, b_N$ de sorte que la fonction $f(z) - A(\wp(z))$ soit holomorphe en 0. Elle est donc holomorphe en chaque point de L par périodicité, puis enfin sur $\mathbb{C}$ tout entier. D'après le lemme 2.4, elle est constante, ce qui prouve que $f(z)$ est un polynôme en $\wp(z)$.

Revenons au cas général. Partons de l'observation que si $f(z)$ admet un pôle d'ordre m en un point $w \in \mathbb{C}\setminus L$, alors la fonction $(\wp(z)-\wp(w))^m f(z)$ est holomorphe en w. Écrivons $L = [\omega_1, \omega_2]$, et considérons le parallélogramme

$$\mathcal{P} = \{s\omega_1 + t\omega_2 \,;\, s,t \in [0,1]\}.$$

La fonction $f(z)$ n'admet qu'un nombre fini de pôles $w_1, \dots, w_n$ sur $\mathcal{P}$, d'ordres respectifs $m_1, \dots, m_n$. Posons alors

$$B(X) = \prod_{k=1}^{n} (X - \wp(w_k))^{m_k},$$

de sorte que la fonction $B(\wp(z))f(z)$ soit holomorphe sur $\mathcal{P}\setminus(L\cap\mathcal{P})$. Elle est donc holomorphe sur $\mathbb{C}\setminus L$ par périodicité, puis enfin polynomiale en $\wp(z)$ par ce que nous avons démontré ci-dessus. ∎

Démonstration de la proposition 2.17. Démontrons seulement les 3 équivalences. Pour une preuve complète, on pourra se référer à [Cox89, Theorem 10.14].

(i) $\Longrightarrow$ (ii). Si $\wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$, il existe des polynômes A et B tels que

$$B(\wp(z))\wp(\alpha z) = A(\wp(z)). \tag{2.1}$$

Comme $\wp(z)$ et $\wp(\alpha z)$ admettent un pôle double en 0, on en déduit que

$$\deg(A) = \deg(B) + 1. \tag{2.2}$$

À présent, soit $\omega \in L$. Comme $\wp(z)$ admet un pôle double en ω, alors (2.1) et (2.2) impliquent que $\wp(\alpha z)$ admet également un pôle en ω, ce qui signifie que $\wp(z)$ admet un pôle en $\alpha\omega$. Étant donné que les pôles de $\wp(z)$ sont exactement les éléments du réseau L, on parvient à la conclusion que $\alpha\omega \in L$, puis que $\alpha L \subset L$.

(ii) $\Longrightarrow$ (i). Si $\alpha L \subset L$, alors $\wp(\alpha z)$ est une fonction elliptique pour L. De plus, $\wp(\alpha z)$ est paire puisque $\wp(z)$ l'est. D'après le lemme 2.18, $\wp(\alpha z)$ est une fonction rationnelle en $\wp(z)$.

(ii) $\Longrightarrow$ (iii). Supposons que $\alpha L \subset L$. Quitte à remplacer L par λL pour un $\lambda \in \mathbb{C}^\times$ convenable, on peut supposer que $L = [1, \tau]$ pour un $\tau \in \mathbb{C} \setminus \mathbb{R}$. Alors $\alpha L \subset L$ signifie qu'il existe des entiers a, b, c, d tels que $\alpha = a + b\tau$ et $\alpha\tau = c + d\tau$. On obtient

$$\tau = \frac{c + d\tau}{a + b\tau},$$

d'où l'on déduit que τ satisfait l'équation de degré 2

$$b\tau^2 + (a - d)\tau - c = 0.$$

Comme τ n'est pas réel, nécessairement $b \neq 0$, et $K = \mathbb{Q}(\tau)$ est un corps quadratique imaginaire. Il s'ensuit que

$$\mathcal{O} = \{\beta \in K \,;\, \beta L \subset L\}$$

est un ordre de K pour lequel L est un idéal fractionnaire propre, et puisque $\alpha \in \mathcal{O}$, l'assertion (iii) est vérifiée.

(iii) $\Longrightarrow$ (ii). Immédiat. ■

La proposition 2.17 montre que si un réseau L est stable par multiplication par un élément $\alpha \in \mathbb{C} \setminus \mathbb{R}$, alors il l'est par multiplication par tout un ordre $\mathcal{O}$ d'un corps quadratique imaginaire. On pourra noter de plus que les éléments de $\mathcal{O} \setminus \mathbb{Z}$ ne sont pas réels. Cela permet de donner un sens à la notion de *multiplication complexe* :

Définition 2.19. On dit qu'un réseau L a de la *multiplication complexe* si l'ensemble

$$\mathrm{End}(L) = \{\alpha \in \mathbb{C} \,;\, \alpha L \subset L\},$$

appelé *anneau d'endomorphismes* de L, admet un élément $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Dans ce cas, $\mathrm{End}(L)$ est un ordre du corps quadratique imaginaire $K = \mathbb{Q}(\alpha)$.

La multiplication complexe fait donc correspondre les deux principales classes d'objets que nous avons étudiés jusqu'à présent : les réseaux du plan complexe d'une part, et les ordres de corps quadratiques imaginaires d'autre part. Cette correspondance est d'autant plus profonde que les classes d'homothétie de réseaux et les groupes des classes sont reliés comme suit :

Corollaire 2.20. *Soit $\mathcal{O}$ un ordre d'un corps quadratique imaginaire. Alors il existe une correspondance bijective entre le groupe des classes $\mathrm{Cl}(\mathcal{O})$ et l'ensemble des classes d'homothétie de réseaux à multiplication complexe admettant $\mathcal{O}$ comme anneau d'endomorphismes.*

Démonstration. Soit L un réseau à multiplication complexe admettant $\mathcal{O}$ comme anneau d'endomorphismes. D'après la proposition 2.17, on peut supposer que L est un idéal fractionnaire propre de $\mathcal{O}$. Réciproquement, tout idéal fractionnaire propre de $\mathcal{O}$ est un réseau admettant $\mathcal{O}$ comme anneau d'endomorphismes. Par ailleurs, deux idéaux fractionnaires propres de $\mathcal{O}$ sont homothétiques en tant que réseaux si et seulement s'ils déterminent la même classe dans le groupes des classes $\mathcal{C}(\mathcal{O})$. Cela induit donc une correspondance bijective comme désirée. ■

Le théorème central de la multiplication complexe va encore plus loin dans la correspondance évoquée précédemment : si $\mathfrak{a}$ est un idéal fractionnaire propre d'un ordre $\mathcal{O}$ d'un corps quadratique K, alors le module singulier $j(\mathfrak{a})$ engendre le corps de classes de $\mathcal{O}$ sur K. Voici son énoncé exact :

Théorème 2.21. *Soient $\mathcal{O}$ un ordre d'un corps quadratique imaginaire K, et $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$. Alors le j-invariant $j(\mathfrak{a})$ est un entier algébrique, et $K(j(\mathfrak{a}))$ est le corps de classes de l'ordre $\mathcal{O}$:*

$$K(j(\mathfrak{a})) = \mathrm{RiCF}(\mathcal{O}).$$

En particulier, $[K(j(\mathfrak{a})) : K] = h(\mathcal{O})$. De plus,

$$[K(j(\mathfrak{a})) : K] = [\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] = h(\mathcal{O}). \tag{2.3}$$

Démonstration. Voir [Cox89, Theorem 11.1 et §11 D.]. ■

Le théorème 2.21 permet de compléter l'étude du corps de classes engagée dans la section 1.7 :

Proposition 2.22. *Soient $\mathcal{O}$ un ordre d'un corps quadratique imaginaire K, et $\mathfrak{a}$ un idéal fractionnaire propre de $\mathcal{O}$. Alors les assertions suivantes sont équivalentes :*

(i) *le groupe $\mathrm{Gal}(K(j(\mathfrak{a}))/\mathbb{Q})$ est abélien ;*

(ii) *le groupe $\mathrm{Gal}(K(j(\mathfrak{a}))/K)$ est 2-élémentaire ;*

(iii) *le groupe $\mathrm{Gal}(K(j(\mathfrak{a}))/\mathbb{Q})$ est 2-élémentaire ;*

(iv) *l'extension $\mathbb{Q}(j(\mathfrak{a}))/\mathbb{Q}$ est galoisienne ;*

(v) *l'extension $\mathbb{Q}(j(\mathfrak{a}))/\mathbb{Q}$ est abélienne.*

Démonstration. Rappelons qu'en vertu de la proposition 1.30, le groupe $\mathrm{Gal}(K(j(\mathfrak{a}))/\mathbb{Q})$ est de type diédral, avec une structure diédrale $(\mathrm{Gal}(K(j(\mathfrak{a}))/K, \iota)$. Les implications (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) en découlent immédiatement. L'implication (iii) $\Longrightarrow$ (iv) est immédiate. Pour démontrer (iv) $\Longrightarrow$ (v), il suffit d'observer que (2.3) implique l'isomorphisme $\mathrm{Gal}(K(j(\mathfrak{a}))/K) \simeq \mathrm{Gal}(\mathbb{Q}(j(\mathfrak{a}))/\mathbb{Q})$. Enfin, l'implication (v) $\Longrightarrow$ (i) est à nouveau immédiate. ■

Remarque 2.23. Puisque $K(j(\mathfrak{a}))/K$ est une extension galoisienne, elle contient, d'après (2.3), tous les conjugués de $j(\mathfrak{a})$ sur $\mathbb{Q}$. Il s'ensuit que l'extension $K(j(\mathfrak{a}))/\mathbb{Q}$ est galoisienne. L'extension $\mathbb{Q}(j(\mathfrak{a}))/\mathbb{Q}$, quant à elle, n'est en général pas galoisienne, et la proposition 2.22 fournit des conditions nécessaires et suffisantes pour qu'elle le soit.

En complément du théorème 2.21, introduisons le *polynôme de classes de Hilbert* de discriminant Δ, qui correspond au polynôme unitaire irréductible engendrant le corps de classes :

Définition 2.24. Soit $\mathcal{O}$ un ordre de discriminant Δ d'un corps quadratique imaginaire K. Le *polynôme de classes de Hilbert* de discriminant Δ, noté $H_{\mathcal{O}}(X)$ ou $H_{\Delta}(X)$, est le polynôme minimal de $j(\mathcal{O})$ sur K.

Comme $j(\mathcal{O})$ est un entier algébrique de degré $h(\mathcal{O})$, $H_{\mathcal{O}}(X)$ est un polynôme de $\mathbb{Z}[X]$ de degré $h(\mathcal{O})$. De plus, ses racines sont exactement les j-invariants des différentes classes d'idéaux de $\mathrm{Cl}(\mathcal{O})$:

Proposition 2.25. *Soit $\mathcal{O}$ un ordre d'un corps quadratique imaginaire K, et soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ des représentants pour chacune des classes d'idéaux de $\mathrm{Cl}(\mathcal{O})$ (avec $h = h(\mathcal{O})$). Alors*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)).$$

Démonstration. Voir [Cox89, Proposition 13.2]. ■

2.4 La fonction j

Dans la section 2.2, nous avons défini le j-invariant d'un réseau L en termes des constantes $g_2(L)$ et $g_3(L)$, qui caractérise les classes d'homothétie de réseaux. Tout réseau L est homothétique à un réseau de la forme $[1, \tau]$ avec $\tau \in \mathbb{H} = \{z \in \mathbb{C} \,;\, \mathrm{Im}\, z > 0\}$, ce qui nous amène à considérer la fonction $j : \mathbb{H} \longrightarrow \mathbb{C}$ définie par

$$j(\tau) = j([1, \tau]).$$

Nous nous intéressons ici aux propriétés analytiques de la fonction j.

Voici quelques premières propriétés.

Proposition 2.26.

(i) *La fonction j est holomorphe sur $\mathbb{H}$.*

(ii) *Pour tous $\tau, \tau' \in \mathbb{H}$, $j(\tau) = j(\tau')$ si et seulement s'il existe $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ tel que $\tau' = \gamma \cdot \tau$. En particulier, la fonction j est $\mathrm{SL}(2, \mathbb{Z})$-invariante.*

(iii) *La fonction $j(\tau)$ est surjective.*

Démonstration. Voir [Cox89, Theorem 11.2]. ■

L'une des conséquences de la surjectivité de la fonction $j(\tau)$ est le corollaire suivant :

Corollaire 2.27. *Soient $g_2, g_3 \in \mathbb{C}$ tels que $g_2^3 - 27 g_3^2 \neq 0$. Alors il existe un réseau L tel que $g_2(L) = g_2$ et $g_3(L) = g_3$.*

Démonstration. Voir [Cox89, Corollary 11.7]. ■

Le fait que la fonction j soit $\mathrm{SL}(2, \mathbb{Z})$-invariante nous permet de la restreindre au domaine fondamental standard $\mathcal{D}$ de l'action de $\mathrm{SL}(2, \mathbb{Z})$ sur $\mathbb{H}$, dont la construction est rappelée dans l'annexe B. La restriction $j : \mathcal{D} \longrightarrow \mathbb{C}$ est en particulier bijective, et réelle monotone sur les bords de $\mathcal{D}^+ = \{z \in \mathcal{D} \,;\, \mathrm{Re}\, z \geq 0\}$. Plus précisément :

Proposition 2.28.

(i) *On a $j(\zeta_3) = j(\zeta_6) = 0$ (où $\zeta_3 = \mathrm{e}^{2i\pi/3}$ et $\zeta_6 = \mathrm{e}^{i\pi/3}$) et $j(i) = 1728$.*

(ii) *Les fonctions $t \in [0, +\infty[\longmapsto j(\zeta_6 + it)$, $t \in [\pi/3, \pi/2] \longrightarrow j(\mathrm{e}^{it})$ et $t \in [0, +\infty[\longmapsto j(i(1+t))$ sont réelles et strictement monotones, respectivement décroissante, croissante et croissante. En particulier, $j^{-1}(\mathbb{R}) = \partial\mathcal{D}^+$, la frontière de $\mathcal{D}^+$.*

D'autre part, comme $z \longmapsto z+1 \in \mathrm{SL}(2,\mathbb{Z})$, alors $j(\tau) = j(\tau+1)$, ce qui implique que la fonction $j(\tau)$ est holomorphe en la variable $q = q(\tau) = \mathrm{e}^{2i\pi\tau}$, définie sur le domaine $0 < |q| < 1$. En conséquence, la fonction $j(\tau)$ admet un développement de Laurent de la forme

$$j(\tau) = \sum_{n=-\infty}^{+\infty} c_n q^n,$$

appelé *développement en série de Fourier* de $j(\tau)$. Ce développement peut être explicité :

Proposition 2.29. *La fonction $j(\tau)$ se développe en série de Fourier sous la forme*

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n=0}^{+\infty} c_n q^n,$$

où $c_n \geq 0$ est entier pour tout $n \geq 0$.

Démonstration. Voir [Cox89, Theorem 11.8]. ■

La formule ci-après se déduit immédiatement du développement de $j(\tau)$ en série de Fourier :

Corollaire 2.30. *Pour tout $\tau \in \mathbb{H}$,*

$$j(-\overline{\tau}) = \overline{j(\tau)}.$$

2.5 Estimations de la fonction j

Poursuivons l'investigation des propriétés analytiques de la fonction $j(\tau)$, en nous concentrant sur son comportement dans le domaine fondamental standard $\mathcal{D}$. Écrivons $\mathcal{D} = \mathcal{D}^+ \cup \mathcal{D}^-$, où

$$\mathcal{D}^+ = \{z \in \mathcal{D}\,;\, \mathrm{Re}\, z \geq 0\}, \quad \mathcal{D}^- = \{z \in \mathcal{D}\,;\, \mathrm{Re}\, z < 0\}.$$

Dans un premier temps, nous nous intéressons au comportement de $j(\tau)$ lorsque $\mathrm{Im}\,\tau$ tend vers $+\infty$. La proposition suivante est dû à Bilu, Masser et Zannier [Bil13, Lemma 1] :

Proposition 2.31. *Pour $\tau \in \mathcal{D}$, on a*

$$\big||j(\tau)| - |q|^{-1}\big| \leq 2079,$$

où $q = q(\tau) = \mathrm{e}^{2i\pi\tau}$.

Démonstration. Par la proposition 2.29, le développement en série de Fourier de $j(\tau)$ est de la forme

$$j(\tau) = q^{-1} + \sum_{n=0}^{+\infty} c_n q^n,$$

où c_n est un entier positif, pour tout $n \geq 0$. Par ailleurs, comme $\tau \in \mathcal{D}$, alors $\mathrm{Im}\,\tau \geq \sqrt{3}/2$, donc

$$|q| = \mathrm{e}^{-2\pi\,\mathrm{Im}\,\tau} \leq \mathrm{e}^{-\pi\sqrt{3}}.$$

Ainsi,

$$\big||j(\tau)| - |q|^{-1}\big| \leq \sum_{n=0}^{+\infty} c_n |q|^n \leq \sum_{n=0}^{+\infty} c_n \mathrm{e}^{-\pi\sqrt{3}} = j\left(i\frac{\sqrt{3}}{2}\right) - \mathrm{e}^{\pi\sqrt{3}} \approx 2078.813... \qquad ■$$

Proposition 2.32. *Pour $\tau \in \mathcal{D} \setminus \{e^{i\pi/3}, e^{2i\pi/3}\}$, on a*

$$|j(\tau)| = |q|^{-1} e^{v(q)}, \tag{2.4}$$

où $v(q)$ est un nombre réel satisfaisant $0 < v(q) \leq 2883|q|$ dès lors que $\operatorname{Im}\tau \geq \log 4158/2\pi = 1.326\ldots$

Démonstration. D'après la proposition 2.31, on a

$$|q|^{-1}(1 - 2079|q|) \leq |j(\tau)| \leq |q|^{-1}(1 + 2079|q|),$$

soit

$$|j(\tau)| = |q|^{-1}(1 + u(q)),$$

avec $|u(q)| \leq 2079|q| = 2079e^{-2\pi \operatorname{Im}\tau}$. Par suite, si $\operatorname{Im}\tau \geq \log 4158/2\pi$, alors $|u(q)| \leq 1/2$. Comme $|\log(1+x)| \leq 2\log(2)|x|$, pour tout $x \in]-1/2, 1/2[$, on en déduit que

$$v(q) = |\log(1 + u(q))| \leq 2\log(2)|u(q)| \leq 2883|q|. \qquad \blacksquare$$

Remarque 2.33. La formule (2.4) traduit simplement le fait que

$$|j(\tau)| = |q|^{-1} e^{O(|q|)},$$

où l'on dispose d'un contrôle précis sur le terme $O(|q|)$ d'après la proposition 2.32. Par exemple, si $\operatorname{Im}\tau \geq \log 5766/2\pi \approx 1.378$, alors $|O(|q|)| \leq 1/2$. En particulier, plus $\operatorname{Im}\tau$ est grand, et plus $|j(\tau)|$ est "proche" de $|q|^{-1}$.

À présent, examinons le comportement de $j(\tau)$ au voisinage des sommets $\zeta_3 = e^{i\pi/3}$ et $\zeta_6 = e^{2i\pi/3}$ du triangle hyperbolique délimité par $\mathcal{D}$. Rappelons que $j(\zeta_3) = j(\zeta_6) = 0$; il s'agit alors de déterminer à quelle vitesse $j(\tau)$ tend vers 0. La proposition suivante est dû à Bilu, Luca et Pizarro-Madariaga [Bil16, Proposition 2.2] :

Proposition 2.34. *Pour $z \in \mathcal{D}^+$, l'une des alternatives suivantes est vérifiée : si $|z - \zeta_6| \geq 10^{-3}$, alors $|j(z)| \geq 4.4 \cdot 10^{-5}$, et si $|z - \zeta_6| \leq 10^{-3}$, alors*

$$44000|z - \zeta_6|^3 \leq |j(z)| \leq 47000|z - \zeta_6|^3. \tag{2.5}$$

En particulier,

$$|j(z)| \geq \min\{4.4 \cdot 10^{-5}, 44000|z - \zeta_6|^3\}.$$

Remarque 2.35. Le résultat est identique (ainsi que la démonstration) pour $z \in \mathcal{D}^-$, en remplaçant simplement ζ_6 par ζ_3.

Commençons par démontrer les deux lemmes suivants.

Lemme 2.36. *Soit $f(z)$ une fonction holomorphe sur un voisinage ouvert d'un disque $D(a, R)$, avec $a \in \mathbb{C}$ et $R > 0$. Supposons que f est bornée sur $D(a, R)$ par un réel $B > 0$. Soit $l \geq 0$ le plus petit entier tel que $f^{(k)}(a) = 0$, pour tout $0 \leq k < l$, et $f^{(l)}(a) \neq 0$. Posons enfin $A = f^{(l)}(a)/l!$. Alors pour tout $z \in D(a, R)$, on a*

$$|f(z) - A(z-a)^l| \leq \frac{|A|R^l + B}{R^{l+1}}|z - a|^{l+1}.$$

Démonstration. La fonction $g(z) = (f(z) - A(z-a)^l)(z-a)^{-l-1}$ est holomorphe sur un voisinage ouvert du disque $D(a,R)$, et sur le bord du disque, on a

$$|g(z)| \leq \frac{|A|R^l + B}{R^{l+1}}.$$

Par le principe du maximum, cette dernière estimation demeure vraie sur tout le disque $D(a,R)$. Le résultat est ainsi démontré. ∎

Lemme 2.37. *Pour tout $z \in D(\zeta_6, \sqrt{3}/4)$, on a $|j(z)| \leq 23000$.*

Démonstration. On reprend la démonstration de Bilu, Masser et Zannier, voir [Bil13, Lemma 2].

On découpe le disque $D(\zeta_6, \sqrt{3}/4)$ en 6 portions délimitées par les cercles $|z| = 1$, $|z-1| = 1$ et la droite verticale passant par $1/2$. En appliquant les transformations $z, z-1, \frac{1}{1-z}, \frac{z}{1-z}, \frac{z-1}{z}, -\frac{1}{z}$ aux portions successives du disque dans le sens trigonométrique, on observe que chaque point du disque est équivalent sous l'action de $\mathrm{SL}(2,\mathbb{Z})$ à un point du domaine fondamental de partie imaginaire bornée par $y_0 = (16\sqrt{3} + \sqrt{183})/26 \approx 1.586$. Il suffit donc de borner j sur le bord de l'ensemble $\{z \in \mathcal{D}\,;\, \mathrm{Im}\, z \leq y_0\}$, et d'appliquer à nouveau le principe du maximum pour conclure. Sur les bords verticaux et circulaire, on a $|j(z)| \leq \max\{1728, -j(1/2 + iy_0)\} < 20561$ par monotonie. Sur le bord horizontal, on a $|q(z)| = \mathrm{e}^{-2\pi y_0} = q(iy_0)$, et en utilisant le développement de j en série de Fourier, on en déduit que

$$|j(z)| \leq q(iy_0)^{-1} + \sum_{n=0}^{+\infty} c_n q(iy_0)^n = j(iy_0) < 22049.$$ ∎

Démonstration de la proposition 2.34. On a $j(\zeta_6) = j'(\zeta_6) = j''(\zeta_6) = 0$ et

$$j'''(\zeta_6) = -162\Gamma(1/3)^{18}\pi^{-9}i \approx -i \cdot 274470.483,$$

voir [Wus14, page 777] par exemple. On applique alors le lemme 2.36 avec

$$a = \zeta_6, \quad R = \sqrt{3}/4, \quad A = j'''(\zeta_6)/6, \quad B = 23000,$$

la valeur de B provenant du lemme 2.37. On obtient, pour tout $z \in D(\zeta_6, \sqrt{3}/4)$,

$$|j(z) - A(z-\zeta_6)^3| \leq \frac{46000(\sqrt{3}/4)^3 + 23000}{(\sqrt{3}/4)^4}|z-\zeta_6|^4 < 761000|z-\zeta_6|^4.$$

Par suite, si $|z-\zeta_6| \leq 10^{-3}$, alors le terme de droite de l'inégalité précédente est majoré par $761|z-\zeta_6|^3$, d'où

$$(|A| - 761)|z-\zeta_6|^3 \leq |j(z)| \leq (|A| + 761)|z-\zeta_6|^3,$$

ce qui démontre l'inégalité (2.5).

En particulier, sur le cercle $|z-\zeta_6| = 10^{-3}$, on a $|j(z)| \geq 4.4 \cdot 10^{-5}$. Par monotonie de j sur les bords de $\mathcal{D}^+$, on en déduit que la minoration $|j(z)| \geq 4.4 \cdot 10^{-5}$ reste vraie sur le bord de l'ensemble $\mathcal{D}^+ \cap \{z \in \mathbb{C}\,;\, |z-\zeta_6| \geq 10^{-3}\}$. Par le principe du maximum, on en conclut que si $|z-\zeta_6| \geq 10^{-3}$, alors $|j(z)| \geq 4.4 \cdot 10^{-5}$ comme voulu. ∎

2.6 La courbe modulaire $Y_0(N)$

Soit $N > 0$ un entier. La *courbe modulaire classique* de niveau N, notée $Y_0(N)$, est la courbe algébrique correspondant au quotient de $\mathbb{H}$ par l'action du sous-groupe de congruence

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,;\, c \equiv 0 \bmod N \right\}$$

de $\mathrm{SL}(2,\mathbb{Z})$. Elle peut être réalisée comme une courbe algébrique de $\mathbb{C}^2$ d'équation

$$\Phi_N(x,y) = 0,$$

où $\Phi_N(X,Y) \in \mathbb{C}[X,Y]$ est appelé le *polynôme modulaire classique* de niveau N.

Le polynôme $\Phi_N(X,Y)$ admet la caractérisation suivante. Considérons l'ensemble de matrices

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,;\, ad = N,\, a > 0,\, 0 \le b < d,\, \mathrm{pgcd}(a,b,d) = 1 \right\}.$$

Pour

$$\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$$

et $\tau \in \mathbb{H}$, on écrit

$$\sigma \cdot \tau = \frac{a\tau + b}{d} \in \mathbb{H}.$$

Alors pour tout $\tau \in \mathbb{H}$, on a

$$\Phi_N(X, j(\tau)) = \prod_{\sigma \in C(N)} (X - j(\sigma \cdot \tau)). \tag{2.6}$$

En particulier, comme

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in C(N),$$

on déduit que pour tout $\tau \in \mathbb{H}$,

$$\Phi_N(j(N\tau), j(\tau)) = 0.$$

Il s'agit d'une propriété importante du polynôme $\Phi_N(X,Y)$. La proposition suivante énumère d'autres propriétés arithmétiques remarquables de ce polynôme.

Proposition 2.38. *Soit $N > 0$ un entier.*

(i) $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$.

(ii) $\Phi_N(X,Y)$ *est irréductible en tant que polynôme en* X.

(iii) $\Phi_N(X,Y) = \Phi_N(Y,X)$ *si* $N > 1$.

Démonstration. Voir [Cox89, Theorem 11.18]. ■

Calculer explicitement le polynôme modulaire $\Phi_N(X,Y)$ ne fait pas partie de nos problématiques. Il existe toutefois des méthodes pour y parvenir ; on pourra voir par exemple [Bru16, Algorithm 1.1 et Corollary 3.4]. En guise d'illustration, on peut donner $\Phi_1(X,Y)$ et $\Phi_2(X,Y)$:

$$\begin{aligned}\Phi_1(X,Y) =& X - Y,\\ \Phi_2(X,Y) =& -X^2Y^2 + X^3 + Y^3 + 1488X^2Y + 1488XY^2 + 40773375XY\\ &- 162000X^2 - 162000Y^2 + 8748000000X + 8748000000Y\\ &- 157464000000000\end{aligned}$$

La caractérisation (2.6) de $\Phi_N(X,Y)$ nous intéresse davantage. Elle permet notamment d'identifier les couples de modules singuliers $(j(\tau), j(\tau'))$ appartenant à la courbe modulaire $Y_0(N)$. Par exemple, pour $N = 2$, on détermine aisément

$$C(2) = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\},$$

ce qui fournit, pour tout $\tau \in \mathbb{H}$,

$$\Phi_2(X, j(\tau)) = (X - j(2\tau)) \left(X - j\left(\frac{\tau}{2}\right)\right) \left(X - j\left(\frac{\tau+1}{2}\right)\right).$$

En conséquence, $(j(\tau), j(\tau')) \in Y_0(2)$ si et seulement si

$$j(\tau) \in \left\{ j(2\tau'), j\left(\frac{\tau'}{2}\right), j\left(\frac{\tau'+1}{2}\right) \right\}.$$

Cette dernière condition peut être vérifiée en utilisant l'algorithme 4 décrit dans l'annexe B. Cela étant dit, lorsque τ, τ' appartiennent au domaine fondamental $\mathcal{D}$, et de plus $\operatorname{Im}\tau' \geq 2$, elle est très simple à vérifier : en effet, dans ce cas, chacun des éléments $2\tau', \tau'/2$ et $(\tau'+1)/2$ appartient à $\mathcal{D}$, et donc la condition est équivalente à

$$\tau \in \left\{ 2\tau', \frac{\tau'}{2}, \frac{\tau'+1}{2} \right\}.$$

En particulier, on obtient le lemme suivant.

Lemme 2.39. *Soient $j(\tau), j(\tau')$ deux modules singuliers, avec $\tau, \tau' \in \mathcal{D}$. Supposons que $(j(\tau), j(\tau')) \in Y_0(2)$ et que $\operatorname{Im}\tau' \geq 2$. Alors $\operatorname{Im}\tau / \operatorname{Im}\tau' \in \{2, 1/2\}$.*

2.7 Les conjugués de $j(\tau)$

Nous avons précédemment énoncé le théorème central de la multiplication complexe 2.21, selon lequel un module singulier $j(\mathfrak{a})$, pour un idéal fractionnaire propre $\mathfrak{a}$ d'un ordre $\mathcal{O}$, est un entier algébrique de degré le nombre de classes $h(\mathcal{O})$. Nous souhaitons à présent expliciter les conjugués de $j(\mathfrak{a})$ sur $\mathbb{Q}$. Pour cela, nous nous appuyons sur l'isomorphisme établi en 1.3 entre le groupe des classes $\mathrm{Cl}(\mathcal{O})$ et le groupe des classes d'équivalence propre de formes quadratiques binaires réduites de discriminant Δ, où Δ est le discriminant de l'ordre $\mathcal{O}$.

Dans toute la suite, on appellera désormais *module singulier* le j-invariant $j(\tau) = j([1, \tau])$ d'un nombre quadratique imaginaire $\tau \in \mathbb{H}$. Par abus de langage, on dira que le *discriminant* du module singulier $j(\tau)$ est le discriminant de l'anneau d'endomorphismes $\mathrm{End}([1, \tau])$, et on parlera également de son *nombre de classes* $h(\Delta)$.

Les conjugués d'un module singulier $j(\tau)$ sur $\mathbb{Q}$ sont donnés explicitement par la proposition suivante :

Proposition 2.40. *Soit $j(\tau)$ un module singulier de discriminant Δ. L'application*

$$(a, b, c) \longmapsto j\left(\frac{b + \sqrt{\Delta}}{2a}\right)$$

définit une bijection de l'ensemble T_Δ défini par (1.4) dans l'ensemble des conjugués de $j(\tau)$ sur $\mathbb{Q}$.

Démonstration. Soit $\mathcal{O}$ l'ordre de discriminant Δ. La proposition 2.25 dit que les conjugués de $j(\tau)$ sont exactement les $j(\mathfrak{a})$ pour $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$. La remarque 1.17 permet de conclure. ∎

Remarque 2.41. Pour tout $(a, b, c) \in T_\Delta$, l'élément $\tau(a, b, c) = (b + \sqrt{\Delta})/(2a)$ appartient au domaine fondamental standard $\mathcal{D}$. En effet,

$$\begin{cases} \mathrm{Re}(\tau(a, b, c)) = \frac{b}{2a}, \\ |\tau(a, b, c)| = \sqrt{\frac{c}{a}}, \end{cases}$$

donc :

- si $-a < b \leq a < c$, alors $-1/2 < \mathrm{Re}(\tau(a, b, c)) \leq 1/2$ et $|\tau(a, b, c)| > 1$;
- si $0 \leq b \leq a = c$, alors $0 \leq \mathrm{Re}(\tau(a, b, c)) \leq 1/2$ et $|\tau(a, b, c)| = 1$.

De fait, $j(\tau(a, b, c)) \in \mathbb{R}$ si et seulement si $a = b$, $a = c$ ou $b = 0$ (cf. proposition 2.28). Dans le cas contraire, d'après le corollaire 2.30,

$$j(\tau(a, -b, c)) = j(-\overline{\tau(a, b, c)}) = \overline{j(\tau(a, b, c))},$$

donc $j(\tau(a, -b, c))$ et $j(\tau(a, b, c))$ sont des conjugués complexes.

En tout cas, les estimations établies en section 2.5 peuvent s'appliquer directement aux conjugués $j(\tau(a, b, c))$ de $j(\tau)$.

Dans la section 1.1, nous avons exhibé l'unique triplet $(a, b, c) \in T_\Delta$ avec $a = 1$, donné explicitement par (1.5). Le conjugué de $j(\tau)$ correspondant,

$$j\left(\frac{r_4(\Delta) + \sqrt{\Delta}}{2}\right),$$

sera nommé la *j-valeur dominante* de discriminant Δ, et on dira plus simplement qu'il est *dominant*. Il possède en effet la propriété d'être bien plus grand en valeur absolue que tous ses autres conjugués.

Proposition 2.42. *Soit $j(\tau)$ la j-valeur dominante de discriminant Δ, avec $|\Delta| \geq 11$. Soit $j(\tau')$ un conjugué de $j(\tau)$ sur $\mathbb{Q}$, $j(\tau) \neq j(\tau')$. Alors $|j(\tau')| \leq 0.1|j(\tau)|$.*

Démonstration. On peut supposer que $\tau = (r_4(\Delta)+\sqrt{\Delta})/2$ et $\tau' = (-b+\sqrt{\Delta})/2a$, avec $a \geq 2$. On a $|q(\tau)|^{-1} = \mathrm{e}^{\pi|\Delta|^{1/2}} \geq \mathrm{e}^{\pi\sqrt{11}} > 33506$ et $|q(\tau')|^{-1} \leq |q(\tau)|^{-1/2}$. D'après la proposition 2.31, on en déduit que

$$\frac{|j(\tau')|}{|j(\tau)|} \leq \frac{|q(\tau')|^{-1}+2079}{|q(\tau)|^{-1}-2079} \leq \frac{33506^{1/2}+2079}{33506-2079} < 0.1,$$

comme attendu. ■

Dans le cas particulier où $\Delta \equiv 1 \bmod 8$, la proposition 1.3 permet d'expliciter d'autres conjugués de $j(\tau)$.

L'existence de la j-valeur dominante garantit qu'un module singulier engendre le même corps sur $\mathbb{Q}$ que n'importe laquelle de ses puissances entières :

Corollaire 2.43. *Soit $j(\tau)$ un module singulier de discriminant Δ, et $n \neq 0$ un entier. Alors $\mathbb{Q}(j(\tau)^n) = \mathbb{Q}(j(\tau))$.*

Démonstration. Si $|\Delta| < 11$, alors $j(\tau) \in \mathbb{Q}$, donc le résultat est vrai.

Considérons maintenant que $|\Delta| \geq 11$, et notons $x = j(\tau)$. Puisque $\mathbb{Q}(x^n) = \mathbb{Q}(x^{-n})$, il suffit de prouver la proposition pour $n \geq 2$. Supposons que $\mathbb{Q}(x) \neq \mathbb{Q}(x^n)$, ce qui signifie que $\mathbb{Q}(x^n)$ est un sous-corps strict de $\mathbb{Q}(x)$. Soit L une clôture galoisienne de l'extension $\mathbb{Q}(x)/\mathbb{Q}$. Par le théorème de correspondance de Galois, le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}(x))$ est un sous-groupe strict de $\mathrm{Gal}(L/\mathbb{Q}(x^n))$. Il existe donc un automorphisme $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma(x^n) = x^n = \sigma(x)^n$ et $\sigma(x) \neq x$. À présent, choisissons $\sigma_0 \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma_0(x)$ soit la j-valeur dominante de discriminant Δ. On a alors $(\sigma_0\sigma)(x)^n = \sigma_0(x)^n$ et $(\sigma_0\sigma)(x) \neq \sigma_0(x)$. Cela contredit la proposition 2.42, selon laquelle $|(\sigma_0\sigma)(x)| < |\sigma_0(x)|$, d'où $|(\sigma_0\sigma)(x)^n| < |\sigma_0(x)^n|$. ■

On dira enfin d'un module singulier de discriminant Δ qu'il est *sous-dominant* s'il correspond à un triplet $(a,b,c) \in T_\Delta$ avec $a = 2$; il est alors de la forme

$$j\left(\frac{-b+\sqrt{\Delta}}{4}\right). \tag{2.7}$$

Le nombre de modules singuliers sous-dominants de discriminant Δ est donné par la proposition 1.4 : rappelons notamment qu'il est d'au plus deux.

2.8 Comparaison des corps engendrés par un module singulier

Dans cette section, nous nous intéressons aux paires de modules singuliers $j(\tau_1), j(\tau_2)$ satisfaisant la propriété $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$. Nous distinguons deux cas : d'une part, le cas $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$, où nous pouvons lister toutes les possibilités ; d'autre part, le cas $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$, où nous établissons que les discriminants respectifs Δ_1 et Δ_2 de $j(\tau_1)$ et $j(\tau_2)$ sont "quasiment identiques". Nous reprenons les travaux effectués dans [All15, Section 4].

2.8.1 Le cas $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$

Il s'avère que la condition $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ et $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ est très forte, et conduit à une caractérisation explicite de tous les cas possibles.

Proposition 2.44. *Soient $\tau_1, \tau_2 \in \mathbb{H}$ deux nombres quadratiques imaginaires tels que $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ mais $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$. Alors les discriminants respectifs Δ_1 et Δ_2 des modules singuliers $j(\tau_1)$ et $j(\tau_2)$ apparaissent tous les deux dans le tableau 1.1.*

Démonstration. Notons $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$, ainsi que D_1 et D_2 les discriminants respectifs des corps $\mathbb{Q}(\tau_1)$ et $\mathbb{Q}(\tau_2)$. Si l'extension $L/\mathbb{Q}$ est galoisienne, alors le groupe $\mathrm{Cl}(\Delta) \simeq \mathrm{Cl}(\Delta')$ est 2-élémentaire d'après la proposition 2.22. On peut alors appliquer le corollaire 1.26 : puisque $D \neq D'$, au moins l'un des deux discriminants D et D' est distinct de D^*, disons D. Dans ce cas, Δ figure dans le tableau 1.1, et la remarque 1.27 implique que Δ' y figure également.

À présent, supposons que l'extension $L/\mathbb{Q}$ ne soit pas galoisienne, et aboutissons à une contradiction. Soit M la clôture galoisienne de $L/\mathbb{Q}$; alors $M = \mathbb{Q}(\tau_1, j(\tau_1)) = \mathbb{Q}(\tau_2, j(\tau_2)) = \mathrm{RiCF}(\Delta) = \mathrm{RiCF}(\Delta')$. D'après la proposition 1.30, le $\mathrm{Gal}(M/\mathbb{Q})$ est de type diédral :

$$\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(M/\mathbb{Q}(\tau_1)) \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Gal}(M/\mathbb{Q}(\tau_2)) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Toutefois, le lemme de Lenstra 1.29 implique que $\mathrm{Gal}(M/\mathbb{Q}(\tau_1)) = \mathbb{Q}(M/\mathbb{Q}(\tau_2))$, et donc que $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$, ce qui est exclu par hypothèse. La proposition est démontrée. ■

La proposition 2.44 permet ainsi de produire la liste complète des corps $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ possibles avec $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$, en examinant toutes les paires de corps déterminés par les discriminants du tableau 1.1.

Corollaire 2.45. *Soit L un corps de nombres satisfaisant la propriété suivante : il existe deux nombres quadratiques $\tau_1, \tau_2 \in \mathbb{H}$ tels que $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ mais $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$. Alors L est l'un des corps présentés dans le tableau 2.1 ci-après.*

TABLE 2.1 – Corps $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ avec $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$

Corps L	$[L : \mathbb{Q}]$	Δ	$\mathrm{Cl}(\Delta)$
$\mathbb{Q}$	1	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$	trivial
$\mathbb{Q}(\sqrt{2})$	2	$-24, -32, -64, -88$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{3})$	2	$-36, -48$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{5})$	2	$-15, -20, -35, -40, -60, -75, -100, -115, -235$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{13})$	2	$-52, -91, -403$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{17})$	2	$-51, -187$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	$-96, -192, -288$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	4	$-180, -240$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	4	$-195, -520, -715$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	4	$-120, -160, -280, -760$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	4	$-340, -595$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	8	$-480, -960$	$(\mathbb{Z}/2\mathbb{Z})^3$

2.8.2 Le cas $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$

Examinons à présent le cas $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ et $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. Dans ce cas, les discriminants Δ_1 et Δ_2 sont reliés de la manière suivante :

Proposition 2.46. *Soient $\tau_1, \tau_2 \in \mathbb{H}$ deux nombres quadratiques tels que $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$ et $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. Notons D le discriminant du corps quadratique $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$, et $\Delta_i = f_i^2 D$ le discriminant du module singulier $j(\tau_i)$, $i \in \{1, 2\}$. Alors soit*

$$f_1/f_2 \in \{1, 2, 1/2\},$$

soit $D = -3$ et $f_1, f_2 \in \{1, 2, 3\}$ (auquel cas $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = \mathbb{Q}$).

Démonstration. Notons $K = \mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$. Soit $f = \mathrm{ppcm}(f_1, f_2)$. Lorsque $D \neq -3, -4$, d'après la proposition 1.31,

$$\mathrm{RiCF}(K, f_1)\,\mathrm{RiCF}(K, f_2) = \mathrm{RiCF}(K, f),$$

donc

$$h(f^2 D) = [K(j(\tau_1), j(\tau_2)) : K]. \tag{2.8}$$

Comme $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$, on obtient

$$h(f_1^2 D) = h(f_2^2 D) = h(f^2 D).$$

Ainsi, par la formule du nombre de classes 1.23,

$$\frac{f}{f_1} \prod_{p|f,\, p\nmid f_1} \left(1 - \left(\frac{D}{p}\right) p^{-1}\right) = 1.$$

Notons que f/f_1 est entier, et que pour tout nombre premier p, si $p|f$ et $p \nmid f_1$ alors $p|(f/f_1)$. Le nombre

$$N = \frac{f}{f_1} \prod_{p|f,\, p\nmid f_1} p^{-1}$$

est donc entier, et on a

$$N \prod_{p|f,\, p\nmid f_1} \left(p - \left(\frac{D}{p}\right)\right) = 1.$$

En conséquence, $N = 1$, et pour tout nombre premier p, si $p|f$ et $p \nmid f_1$ alors $p - \left(\frac{D}{p}\right) = 1$, ce qui implique $p = 2$. On en déduit finalement que $f/f_1 \in \{1, 2\}$. De la même manière, $f/f_2 \in \{1, 2\}$. Ainsi, $f_1/f_2 \in \{1, 2, 1/2\}$.

Supposons désormais que $D \in \{-3, -4\}$. Si $\mathrm{pgcd}(f_1, f_2) > 1$, alors l'égalité (2.8) est à nouveau vérifiée et $f_1/f_2 \in \{1, 2, 1/2\}$ par le même argument que précédemment.

Si $f_1 = 1$ par exemple, alors soit $D = -4$ et $f_2 \in \{1, 2\}$, soit $D = -3$ et $f_2 \in \{1, 2, 3\}$.

Enfin, supposons que $f_1, f_2 > 1$ et $\mathrm{pgcd}(f_1, f_2) = 1$. Alors $f = f_1 f_2$, et la proposition 1.31 implique cette fois que

$$h(f_1^2 D) = h(f_2^2 D) = l^{-1} h(f^2 D),$$

où $l = 2$ si $D = -4$ et $l = 3$ si $D = -3$. Par la formule du nombre de classes, on a

$$f_i \prod_{p|f_i} \left(1 - \left(\frac{D}{p}\right) p^{-1}\right) = l, \quad i \in \{1, 2\},$$

d'où l'on déduit aisément que $D = -3$ et $\{f_1, f_2\} = \{2, 3\}$. ∎

Chapitre 3

Équations aux puissances de modules singuliers

Le présent chapitre consigne la majeure partie de nos travaux de recherche réalisés durant le doctorat. Les résultats de ces recherches ont mené à la rédaction de deux articles [Rif18] et [Luc17]. La problématique au cœur de nos travaux est détaillée ci-après.

Un *point de multiplication complexe* dans $\mathbb{C}^2$ est un couple $(j(\tau), j(\tau'))$, où $j(\tau)$ et $j(\tau')$ sont des modules singuliers, c'est-à-dire que $\tau, \tau' \in \mathbb{H}$ sont des nombres quadratiques imaginaires. Nous nous intéressons aux points de multiplication complexe $(j(\tau), j(\tau'))$ solutions d'une équation de la forme $F(x, y) = 0$, pour un polynôme irréductible $F(X, Y) \in \mathbb{C}[X, Y]$ donné. De manière équivalente, d'un point de vue plus géométrique, nous étudions les points de multiplications complexes appartenant à une courbe algébrique plane irréductible donnée de $\mathbb{C}^2$. André [And98] a démontré qu'à quelques exceptions explicites près, une telle courbe ne contient qu'un nombre fini de points de multiplication complexe. Précisément :

Théorème 3.1 (André)**.** *Soit $\mathcal{C}$ une courbe plane irréductible de $\mathbb{C}^2$. Alors $\mathcal{C}$ contient un nombre fini de points de multiplication complexe, sauf si elle est de l'un des types suivants :*

- *les droites verticales $x = j(\tau)$;*
- *les droites horizontales $y = j(\tau')$;*
- *les courbes modulaires $Y_0(N)$ pour $N \geq 1$ entier.*

Les trois types de courbes mentionnées ci-dessus sont dites *spéciales*, et contiennent clairement une infinité de points de multiplication complexe. Le théorème de André 3.1 est le point de départ de nos travaux. Concrètement, nous recherchons à caractériser les points de multiplication complexe appartenant à une courbe ou une famille de courbes donnée. Par exemple, Kühne [Kuh13] a démontré que l'équation $x + y = 1$ n'admet pas de solution (sous-entendu, pas de solution avec x, y des modules singuliers), et Bilu, Masser et Zannier [Bil13] ont obtenu le même résultat pour l'équation $xy = 1$.

Ces résultats ont été généralisés dans deux articles récents [All15, Bil16]. Dans [All15], Allombert, Bilu et Pizzaro-Madariaga ont déterminé les solutions de toutes les équations linéaires de la forme $Ax + By = C$, avec $A, B, C \in \mathbb{Q}$. Dans [Bil16], Bilu, Lucas et Pizzaro-Madariaga ont obtenu le même résultat pour les équations de la forme $xy = A$, avec $A \in \mathbb{Q}^\times$. Voici les énoncés des principaux théorèmes de [All15, Bil16].

Théorème 3.2 (Allombert et al. [All15])**.** *Soient $A, B, C \in \mathbb{Q}$, avec $AB \neq 0$, et x, y deux modules singuliers. Supposons que $Ax + By = C$. Alors l'une des options suivantes est satisfaite :*

(le cas trivial) $A + B = C = 0$ *et* $x = y$ *;*

(le cas rationnel) $x, y \in \mathbb{Q}$ *;*

(le cas quadratique) $x \neq y$ *et* x *et* y *engendrent le même corps de nombres sur* $\mathbb{Q}$ *de degré* 2*.*

Théorème 3.3 (Bilu et al. [Bil16])**.** *Soient* x, y *deux modules singuliers tels que* $xy \in \mathbb{Q}^\times$*. Alors l'une des options suivantes est satisfaite :*

(le cas rationnel) $x, y \in \mathbb{Q}^\times$ *;*

(le cas quadratique) $x \neq y$*, et* x *et* y *sont de degré* 2 *et conjugués sur* $\mathbb{Q}$*.*

Ces résultats sont les meilleurs possibles : en effet, dans les cas rationnel et quadratique du théorème 3.2, on trouve aisément $A, B, C \in \mathbb{Q}$ avec $AB \neq 0$ tels que $Ax + By = C$; de même, dans les cas rationnel et quadratique du théorème 3.3, on a $xy \in \mathbb{Q}^\times$. Par ailleurs, les liste des modules singuliers de degrés 1 et 2 sur $\mathbb{Q}$ sont connus et peuvent être facilement calculés en PARI. En particulier, il existe 13 modules singuliers rationnels, et 29 paires de modules singuliers distincts de degré 2 et conjugués sur $\mathbb{Q}$; voir [Bil16, Section 1] pour davantage de détails. Cela signifie que les théorèmes 3.2 et 3.3 fournissent une caractérisation explicite des solutions des équations.

Dans le cadre de nos recherches, nous nous sommes intéressés à une généralisation des théorèmes 3.2 et 3.3, en introduisant des exposants : c'est-à-dire, au lieu des équations $Ax + By = C$ et $xy = A$, de considérer les équations plus générales $Ax^m + By^n = C$ et $x^m y^n = 1$, où les exposants entiers m et n sont également inconnus. Dans un premier temps, nous avons obtenu le résultat suivant :

Théorème 3.4 ([Rif18])**.** *Soient* x, y *deux modules singuliers* distincts *de discriminants respectifs* Δ_x *et* Δ_y*, et* $m, n \geq 1$ *deux entiers. Supposons qu'il existe* $A, B, C \in \mathbb{Q}^\times$ *tels que* $Ax^m + By^n = C$*. Alors* x *et* y *engendrent le même corps de nombres sur* $\mathbb{Q}$ *de degré au plus* 3*. De plus, si* $h = 3$*, alors soit* $\{\Delta_x, \Delta_y\} = \{-23, -4 \cdot 23\}$*, soit* $\{\Delta_x, \Delta_y\} = \{-31, -4 \cdot 31\}$*.*

Les méthodes que nous avons développées dans [Rif18] ne permettent pas de traiter les deux cas suivants. Premièrement, le cas $x = y$, qui équivaut à la question suivante : un module singulier de degré 3 ou plus peut-il être racine d'un trinôme à coefficients rationnels ? Nous n'avons pas été en mesure de répondre à cette question, qui demeure en suspens. Deuxièmement, le cas où x et y sont de degré 3, auquel cas il ne reste que deux paires de modules singuliers à examiner comme indiqué dans l'énoncé du théorème 3.4. Sur une idée originale de Luca, nous avons éliminé ces deux paires, ce qui a conduit à l'élaboration d'un second article [Luc17]. En conséquence, le résultat final obtenu est le suivant :

Théorème 3.5. *Soient* x, y *deux modules singuliers* distincts *de discriminants respectifs* Δ_x *et* Δ_y*, et* $m, n \geq 1$ *deux entiers. Supposons qu'il existe* $A, B, C \in \mathbb{Q}^\times$ *tels que* $Ax^m + By^n = C$*. Alors* x *et* y *engendrent le même corps de nombres sur* $\mathbb{Q}$ *de degré au plus* 2*.*

D'autre part, pour ce qui est de l'équation $x^m y^n = A$ avec $A \in \mathbb{Q}^\times$, nous avons plus aisément généralisé le théorème 3.3 en nous appuyant majoritairement sur les arguments exposés dans [Bil16], et le résultat que nous obtenons est le meilleur possible :

Théorème 3.6. *Soient* x, y *deux modules singuliers non nuls, et* m, n *deux entiers non nuls. Supposons que* $x^m y^n \in \mathbb{Q}^\times$*. Alors l'une des options suivantes est satisfaites :*

(le cas d'égalité) $x = y$ *et* $m + n = 0$ *;*

(le cas rationnel) $x, y \in \mathbb{Q}^\times$;

(le cas quadratique) $m = n$, $x \neq y$, *et* x *et* y *sont de degré* 2 *et conjugués sur* $\mathbb{Q}$.

L'objet de ce chapitre est de retracer les démonstrations des théorèmes 3.5 et 3.6 dans les sections 3.2 et 3.3 respectivement.

3.1 Indépendance multiplicative de nombres algébriques

Dans cette section préliminaire, nous investiguons la notion d'*indépendance multiplicative* de nombres algébriques. Notre but est de développer un procédé algorithmique permettant de prouver l'indépendance multiplicative de deux nombres algébriques donnés, en cas de succès.

Soient α, β deux nombres algébriques non nuls d'un corps de nombres L. On dit que α et β sont *multiplicativement indépendants* si, pour tous entiers m, n, l'égalité $\alpha^m \beta^n = 1$ implique $m = n = 0$. Autrement, on dit qu'ils sont *multiplicativement dépendants*.

Si l'un des deux nombres algébriques α ou β est une racine de l'unité, disons α, alors α et β sont évidemment multiplicativement dépendants, puisque dans ce cas, il suffit de considérer $n = 0$ et m tel que $\alpha^m = 1$. Nous exclurons cette possibilité dans la suite.

Supposons que α et β sont multiplicativement dépendants, et considérons deux entiers m, n non simultanément nuls tels que

$$\alpha^m = \beta^n. \tag{3.1}$$

Notons d'abord que $m, n \neq 0$, puisque α et β ne sont pas des racines de l'unité par hypothèse. L'égalité (3.1) implique alors que les idéaux fractionnaires $\alpha\mathcal{O}_L$ et $\beta\mathcal{O}_L$ partagent les mêmes idéaux premiers dans leur décomposition en produits d'idéaux premiers de $\mathcal{O}_L$. Si leur décomposition n'est pas triviale, on peut donc choisir un idéal premier non nul $\mathfrak{p}$ de $\mathcal{O}_L$ divisant à la fois $\alpha\mathcal{O}_L$ et $\beta\mathcal{O}_L$. Pour cet idéal $\mathfrak{p}$, on a

$$\frac{m}{n} = \frac{v_\mathfrak{p}(\beta\mathcal{O}_L)}{v_\mathfrak{p}(\alpha\mathcal{O}_L)},$$

ce qui permet en pratique de calculer une valeur théorique k/l sous forme irréductible de la fraction m/n. Ensuite, en remarquant que

$$\left(\frac{\alpha^k}{\beta^l}\right)^{m/k} = 1,$$

c'est-à-dire que α^k/β^l est une racine de l'unité de L, il reste à calculer l'ensemble des racines de l'unité de L, et les comparer à α^k/β^l. Si aucune ne correspond, on peut en conclure que α et β sont multiplicativement indépendants.

En résumé, voici l'algorithme que nous proposons :

Données : Deux nombres algébriques α et β d'un corps de nombres L qui ne sont pas des unités
Résultat : Succès si le test réussit, Échec sinon
$\mathfrak{a} \leftarrow \alpha\mathcal{O}_L + \beta\mathcal{O}_L$;
si $\mathfrak{a} = 0$ **alors**
  retourner Succès
sinon
  $\mathfrak{p} \leftarrow$ un idéal premier de $\mathcal{O}_L$ divisant $\mathfrak{a}$;
  $k/l \leftarrow v_\mathfrak{p}(\beta\mathcal{O}_L)/v_\mathfrak{p}(\alpha\mathcal{O}_L)$;
  $S \leftarrow$ l'ensemble des racines de l'unité de L ;
  si $\alpha^k/\beta^l \notin S$ **alors**
    retourner Succès
  sinon
    retourner Échec
  fin
fin

Algorithme 2 : Test de l'indépendance multiplicative de deux nombres algébriques

En cas de succès, l'algorithme 2 prouve que α et β sont multiplicativement indépendants. Toutefois, en cas d'échec, il ne permet pas de dire s'ils sont multiplicativement dépendants ou pas. Notons par ailleurs que la condition requise $\alpha, \beta \notin \mathcal{O}_L^\times$ équivaut à ce que les idéaux $\alpha\mathcal{O}_L$ et $\beta\mathcal{O}_L$ soient effectivement non triviaux, ce qui se produit dans toutes nos applications. Dans ce cas, leurs diviseurs communs sont les diviseurs de l'idéal $\mathfrak{a} = \alpha\mathcal{O}_L + \beta\mathcal{O}_L \neq 0$. Il convient donc, lors du test, de vérifier dans un premier temps que l'idéal $\mathfrak{a}$ n'est pas trivial ; dans le cas contraire, le test conclut directement que α et β ne sont pas multiplicativement indépendants. Ajoutons enfin que PARI dispose de toutes les routines nécessaires pour effectuer des opérations sur les idéaux, les factoriser, mais aussi déterminer l'ensemble des racines de l'unité d'un corps de nombres.

Voici une seconde méthode pour tester l'indépendance multiplicative de deux nombres algébriques α et β d'un corps de nombres L, qui a l'avantage de n'imposer aucune restriction sur α et β. Son inconvénient, néanmoins, est de recourir à des calculs numériques, là où l'algorithme 2 ne procéde quant à lui qu'à des calculs formels. Soient $\sigma_1, \ldots, \sigma_r : L \longrightarrow \mathbb{C}$ les plongements de L dans $\mathbb{C}$, en ne comptant qu'un seul plongement par paire de plongements complexes conjugués. Si α et β sont multiplicativement dépendants, il existe deux entiers m, n non simultanément nuls tels que $\alpha^m\beta^n = 1$, et alors, pour tout $i \in \{1, \ldots, r\}$, $(\alpha^{\sigma_i})^m(\beta^{\sigma_i})^n = 1$, d'où

$$m \log|\alpha^{\sigma_i}| + n \log|\beta^{\sigma_i}| = 0.$$

Il s'ensuit que pour tous $i, j \in \{1, \ldots, r\}$, $i \neq j$, le vecteur (m, n) appartient au noyau de la matrice

$$\begin{pmatrix} \log|\alpha^{\sigma_i}| & \log|\beta^{\sigma_i}| \\ \log|\alpha^{\sigma_j}| & \log|\beta^{\sigma_j}| \end{pmatrix}$$

donc cette dernière n'est pas inversible. Autrement dit,

$$\log|\alpha^{\sigma_i}| \log|\beta^{\sigma_j}| - \log|\alpha^{\sigma_j}| \log|\beta^{\sigma_i}| = 0. \tag{3.2}$$

Ainsi, l'algorithme consiste à calculer les membres de gauche de l'égalité (3.2) pour $i, j \in \{1, \ldots, r\}$, $i \neq j$, jusqu'à trouver un membre plus grand qu'une valeur arbitraire $\varepsilon > 0$ en

valeur absolue, ε étant choisi pour pallier l'imprécision des calculs effectués. À nouveau, si ce test échoue, on ne peut rien dire quant à l'indépendance multiplicative de α et β. Comme évoqué précédemment, dans toutes nos applications, nous utilisons l'algorithme 2.

Munis de ces différentes méthodes, et dans l'optique de généraliser la notion d'indépendance multiplicative, le problème que l'on se pose à présent est le suivant : étant donné deux nombres algébriques non nuls α, β d'un corps de nombres L, existe-t-il deux entiers m, n non simultanément nuls tels que $\alpha^m \beta^n \in \mathbb{Q}^\times$? Si la réponse est négative, on dira que α et β sont *fortement multiplicativement indépendants*. Cette question est avant tout motivée par la démonstration du théorème 3.6, qui requiert d'éliminer des cas particuliers. La méthode que nous proposons pour y répondre est la suivante.

On peut supposer que l'extension L est galoisienne. Une routine en PARI permet de calculer le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$. S'il existe deux entiers m, n non simultanément nuls tels que $\alpha^m \beta^n \in \mathbb{Q}^\times$, alors pour tout automorphisme $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, on a

$$\left(\frac{\alpha}{\alpha^\sigma}\right)^m \left(\frac{\beta}{\beta^\sigma}\right)^n = 1,$$

ce qui signifie que les nombres algébriques α/α^σ et β/β^σ sont multiplicativement dépendants. En conséquence, il suffit d'exhiber un automorphisme $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que α/α^σ et β/β^σ franchissent l'un des tests précédents avec succès ; si un tel automorphisme n'existe pas, on ne peut rien conclure. Voici l'algorithme correspondant, dans lequel on fait référence aux précédents tests par l'appellation `mult_ind` :

Données : Deux nombres algébriques α et β d'un corps de nombres L galoisien sur $\mathbb{Q}$ qui ne sont pas des racines de l'unité
Résultat : Succès si le test réussit, Échec sinon
$\{\sigma_1, \ldots, \sigma_r\} \leftarrow \mathrm{Gal}(L/\mathbb{Q})$;
$i \leftarrow 1$;
tant que $i \leq r$ *et* `mult_ind`$(\alpha/\alpha^\sigma, \beta/\beta^\sigma)$ = Échec **faire**
  $i \leftarrow i + 1$;
fin
si $i \leq r$ **alors**
  retourner Succès
sinon
  retourner Échec
fin

Algorithme 3 : Test de l'indépendante multiplicative forte de deux nombres algébriques

3.2 Indépendance linéaire de puissances modules singuliers

Cette section est consacrée à la démonstration du théorème 3.5, dont nous rappelons l'énoncé.

Théorème 3.5. *Soient x, y deux modules singuliers distincts, et $m, n > 0$ deux entiers. Supposons qu'il existe $A, B, C \in \mathbb{Q}^\times$ tels que $Ax^m + By^n = C$. Alors x et y engendrent le même corps de nombres sur $\mathbb{Q}$ de degré au plus 2.*

Remarques 3.7.

- La condition $ABC \neq 0$ n'est pas restrictive. En effet, si $A = 0$ et $B \neq 0$, alors $y^n \in \mathbb{Q}$, donc $y \in \mathbb{Q}$ d'après la proposition 2.43. De même, si $A \neq 0$ et $B = 0$, alors $x^m \in \mathbb{Q}$, donc $x \in \mathbb{Q}$. Enfin, si $AB \neq 0$ et $C = 0$, alors $x^m y^{-n} \in \mathbb{Q}$; ce dernier cas est traité par le théorème 3.6 ci-après.
- Le résultat du théorème 3.5 est optimal pour des modules singuliers x, y distincts : s'ils engendrent le même corps de nombres K sur $\mathbb{Q}$ de degré au plus 2, alors K est un $\mathbb{Q}$-espace vectoriel de dimension au plus 2, donc quels que soient $m, n > 0$, la famille $1, x^m, y^n$ d'éléments de K est liée.

3.2.1 Réduction du problème

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts de discriminants respectifs Δ_x, Δ_y, et $m, n > 0$ deux entiers. Supposons qu'il existe $A, B, C \in \mathbb{Q}^\times$ tels que

$$Ax^m + By^n = C. \tag{3.3}$$

Tout d'abord, l'équation (3.3) implique que $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, d'où $\mathbb{Q}(x) = \mathbb{Q}(y)$ d'après la proposition 2.43. En particulier, les discriminants Δ_x et Δ_y ont le même nombre de classes $h = h(\Delta_x) = h(\Delta_y)$. De plus, l'orbite du point (x, y) sous l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ possède exactement h éléments, et chaque conjugué de x apparaît exactement une fois comme première coordonnée d'un point de l'orbite, tout comme chaque conjugué de y apparaît exactement une fois comme seconde coordonnée d'un point de l'orbite. Enfin, l'équation (3.3) étant définie sur $\mathbb{Q}$, chaque point de l'orbite la vérifie également. Dans toute la suite, on suppose que $h \geq 3$, et on a alors $|\Delta_x|, |\Delta_y| \geq 23$.

Par ailleurs, l'équation (3.3) signifie que les conjugués sur $\mathbb{Q}$ du point (x^m, y^n) sont tous colinéaires. Autrement dit, pour tous $\sigma, \sigma', \sigma'' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$\begin{vmatrix} 1 & (x^\sigma)^m & (y^\sigma)^n \\ 1 & (x^{\sigma'})^m & (y^{\sigma'})^n \\ 1 & (x^{\sigma''})^m & (y^{\sigma''})^n \end{vmatrix} = 0. \tag{3.4}$$

Cette relation de colinéarité joue un rôle central dans la démonstration, et sera réécrite de plusieurs manières différentes en temps voulu. On peut déjà en tirer la première conséquence suivante.

Lemme 3.8. *Sous les hypothèses ci-dessus, le point (x, y) est conjugué sur $\mathbb{Q}$ à un point (x', y'), dont les deux coordonnées x' et y' sont les j-valeurs dominantes de discriminants respectifs Δ_x et Δ_y.*

Démonstration. Quitte à conjuguer, on peut supposer que x est dominant. Supposons que y ne soit pas dominant. Le point (x, y) est alors conjugué à un point (x^σ, y^σ), où y^σ est dominant mais pas x^σ. Comme $h \geq 3$, il existe un troisième conjugué $(x^{\sigma'}, y^{\sigma'})$, dont les deux coordonnées sont toutes deux non dominantes.

Maintenant, la relation de colinéarité (3.4) appliquée à ces trois points s'écrit

$$\begin{vmatrix} 1 & x^m & y^n \\ 1 & (x^\sigma)^m & (y^\sigma)^n \\ 1 & (x^{\sigma'})^m & (y^{\sigma'})^n \end{vmatrix} = 0.$$

Le déterminant ci-dessus est une somme de 6 termes : le "terme dominant" $x^m(y^\sigma)^n$ et 5 autres termes. Chacun de ces autres termes est majoré par $0.1|x^m(y^\sigma)^n|$ en module d'après la proposition 2.42, si bien que le déterminant ne peut s'annuler. Il s'agit d'une contradiction, ce qui prouve finalement le lemme. ■

Suite au lemme 3.8, on peut supposer sans perte de généralité que x et y sont les j-valeurs dominantes de discriminants respectifs Δ_x, Δ_y. À ce stade, la démonstration consiste à examiner les deux cas suivants : $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$ et $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$.

3.2.2 Le cas $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$

Dans cette partie, nous nous intéressons au cas $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$. La proposition 2.46 s'applique dans ce cas, et fournit $\Delta_x/\Delta_y \in \{1, 4, 1/4\}$. Si $\Delta_x = \Delta_y$, alors x et y sont conjugués, mais comme ils sont tous les deux dominants, cela signifierait que $x = y$, ce qui est exclu par hypothèse. On peut alors supposer par exemple que $\Delta_x = 4\Delta_y$, et on écrira simplement $\Delta = \Delta_y$. Comme x et y sont dominants, on peut choisir

$$\tau = \frac{r_4(4\Delta) + \sqrt{4\Delta}}{2} = \sqrt{\Delta}, \quad \tau' = \frac{r_4(\Delta) + \sqrt{\Delta}}{2}.$$

On s'aperçoit alors que $\tau' = \frac{1}{2}\gamma \cdot \tau$, où

$$\gamma = \begin{pmatrix} 1 & r_4(\Delta) \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Par conséquent, le point (x, y) appartient à la courbe modulaire $Y_0(2)$. Cette dernière étant définie sur $\mathbb{Q}$, elle contient également tous les conjugués sur $\mathbb{Q}$ de (x, y).

Observons en outre que $\Delta \equiv 1 \bmod 8$, en vertu du lemme suivant.

Lemme 3.9. *Soit Δ le discriminant d'un ordre d'un corps quadratique imaginaire tel que $h(4\Delta) = h(\Delta)$. Alors soit $\Delta \in \{-3, -4\}$, soit $\Delta \equiv 1 \bmod 8$.*

Démonstration. On peut vérifier aisément que $h(-3) = h(-4 \cdot 3)$ et $h(-4) = h(-4 \cdot 4)$. Pour $\Delta \notin \{-3, -4\}$, d'après la formule du nombre de classes,

$$h(4\Delta) = 2h(\Delta)\left(1 - \frac{1}{2}\left(\frac{\Delta}{2}\right)\right),$$

soit $(\Delta/2) = 1$ après simplification par $h(4\Delta) = h(\Delta)$, c'est-à-dire $\Delta \equiv 1 \bmod 8$. ■

Élimination des grands discriminants

Nous allons tout d'abord exhiber une contradiction lorsque $|\Delta|$ est suffisamment grand. Il restera ensuite à examiner un nombre fini de discriminants Δ.

L'idée est la suivante. La relation de colinéarité (3.4) entre trois conjugués donnés du point (x, y) permet d'encadrer la fraction m/n en utilisant les estimations du j-invariant étudiées en section 2.5, comme nous allons le voir. Pour peu que $|\Delta|$ soit suffisamment grand, cette opération peut être réitérée en choisissant un autre triplet de conjugués de (x, y), pour obtenir un deuxième encadrement de m/n. En obtenant deux encadrements incompatibles, on soulève une contradiction. Le tout est d'expliciter dans un cadre général des conjugués de (x, y).

On dispose déjà du conjugué (x, y), correspondant aux j-valeurs dominantes x et y de discriminants respectifs 4Δ et Δ. On pose $(x_1, y_1) = (x, y)$. Par la proposition 1.3, pour $|\Delta| \geq 2^{2\times 3+2} = 256$, il existe 3 autres conjugués (x_i, y_i), $i \in \{2, 3, 4\}$, de la forme suivante :

TABLE 3.1 – Conjugués de (x, y) sur $\mathbb{Q}$ pour $|\Delta| \geq 256$, avec a_2, a_3, a_4 inconnus

i	x_i	y_i
1	$j(\sqrt{\Delta})$	$j\left(\frac{1+\sqrt{\Delta}}{2}\right)$
2	$j\left(* + \frac{\sqrt{\Delta}}{a_2}\right)$	$j\left(\frac{1+\sqrt{\Delta}}{4}\right)$
3	$j\left(* + \frac{\sqrt{\Delta}}{a_3}\right)$	$j\left(* + \frac{\sqrt{\Delta}}{8}\right)$
4	$j\left(* + \frac{\sqrt{\Delta}}{a_4}\right)$	$j\left(* + \frac{\sqrt{\Delta}}{16}\right)$.

Les "$*$" sont des valeurs réelles qui n'ont pas d'incidence sur les estimations que nous allons effectuer ensuite. Il nous faut en revanche déterminer les valeurs des entiers a_2, a_3, a_3. Commençons par un lemme :

Lemme 3.10. *Soit Δ le discriminant d'un corps quadratique imaginaire tel que $\Delta \equiv 1 \bmod 8$. Alors l'ensemble $T_{4\Delta}$ ne possède aucun triplet (a, b, c) avec $a = 2$ ou $a = 4$, et exactement deux triplets (a, b, c) avec $a = 8$ si $|\Delta| > 63$.*

Démonstration. Supposons qu'il existe un triplet $(a, b, c) \in T_{4\Delta}$ avec $a = 2$. On a $4\Delta = b^2 - 8c$. Comme $4\Delta \equiv 4 \bmod 8$ et $|b| \leq 2$, on en déduit que $b^2 \equiv 4 \bmod 8$ et donc que $b = 2$. Par suite, $\Delta - 1 = -2c \equiv 0 \bmod 8$, donc c est pair, ce qui contredit $\operatorname{pgcd}(a, b, c) = 1$.

Le raisonnement est simimaire pour montrer qu'il n'existe aucun triplet $(a, b, c) \in T_{4\Delta}$ avec $a = 4$.

Supposons à présent qu'il existe $(a, b, c) \in T_{4\Delta}$ avec $a = 8$. On a $4\Delta = b^2 - 32c$. Comme $4\Delta \equiv 4 \bmod 32$ et $|b| \leq 8$, on en déduit que $b^2 \equiv 4 \bmod 32$, et donc que $b = \pm 2$ ou $b = \pm 6$. Par suite,

$$c = \frac{b^2 - 4\Delta}{32} \in \left\{ \frac{4 - 4\Delta}{32}, 1 + \frac{4 - 4\Delta}{32} \right\},$$

une seule des deux valeurs ci-dessus étant impaire, ce qui permet d'exclure l'une des deux possibilités $b = \pm 2$ ou $b = \pm 6$. Enfin, l'hypothèse $|\Delta| > 63$ garantit que $(4 - 4\Delta)/32 > 8$ et donc que $c > 8$. Cette analyse prouve que l'ensemble $T_{4\Delta}$ possède au plus deux triplets (a, b, c) avec $a = 8$, et construit les deux triplets explicites en question dont on vérifie qu'ils sont bien des éléments de $T_{4\Delta}$. ■

Revenons-en à la détermination des valeurs a_2, a_3, a_4. Sous l'hypothèse $|\Delta| \geq 1024$, le lemme 2.39 assure que $a_i/2^i \in \{2, 1/2\}$, pour chaque $i \in \{2, 3, 4\}$.

- Pour $i = 2$, cela signifie que $a_2 \in \{2, 8\}$, le cas $a_2 = 2$ étant exclu puisque l'ensemble $T_{4\Delta}$ ne possède aucun triplet (a, b, c) avec $a = 2$ en vertu du lemme 3.10 ci-dessus. Ainsi, $a_2 = 8$.
- Pour $i = 3$, cela signifie que $a_3 \in \{4, 16\}$, le cas $a_3 = 4$ étant exclu toujours d'après le lemme 3.10. Ainsi, $a_3 = 16$.

- Pour $i = 4$, cela signifie que $a_4 \in \{8, 32\}$. On utilise à nouveau le lemme 3.10, pour remarquer que les deux triplets (a, b, c) de l'ensemble $T_{4\Delta}$ avec $a = 8$ correspondent déjà à x_2 et $\overline{x_2}$, ce qui permet d'exclure le cas $a_4 = 8$. Ainsi, $a_4 = 32$.

Par conséquent, pour $|\Delta| \geq 1024$, chaque (x_i, y_i), $i \in \{1, 2, 3, 4\}$, est de la forme

$$(x_i, y_i) = \left(j\left(* + \frac{\sqrt{\Delta}}{a_i} \right), j\left(* + \frac{\sqrt{\Delta}}{a_i'} \right) \right),$$

où les a_i, a_i' sont résumés dans le tableau ci-après.

TABLE 3.2 – Valeurs des entiers a_i, a_i'

i	a_i	a_i'
1	1	2
2	8	4
3	16	8
4	32	16

On suppose dans tout ce paragraphe que $|\Delta| \geq 1024$, et on dispose alors des conjugués explicites décrits ci-dessus.

En utilisant la proposition 2.32, on a les estimations suivantes :

$$\left|\frac{x_i}{x_j}\right| = \mathrm{e}^{2\pi|\Delta|^{1/2}a_{i,j}+O(1)}, \quad \left|\frac{y_i}{y_j}\right| = \mathrm{e}^{2\pi|\Delta|^{1/2}a'_{i,j}+O(1)}, \quad 1 \leq i < j \leq 4, \tag{3.5}$$

où $O(1)$ est un terme dépendant de $|\Delta|$ avec $|O(1)| \leq 1$ dans chacune des estimations, et $a_{i,j} = a_i^{-1} - a_j^{-1}$, $a'_{i,j} = a_i'^{-1} - a_j'^{-1}$.

Nous allons appliquer la relation de colinéarité (3.4), successivement aux triplets de conjugués (x_i, y_i) pour $i \in \{1, 2, 3\}$ puis pour $i \in \{1, 3, 4\}$. Pour $1 \leq i < j < k \leq 4$, cette relation se réécrit comme suit :

$$\left(\frac{x_i}{x_j}\right)^m \left(\frac{y_i}{y_j}\right)^{-n} - 1 = \frac{\left(\frac{y_k}{y_j}\right)^n + \left(\frac{x_k}{x_i}\right)^m - \left(\frac{y_k}{y_i}\right)^n - \left(\frac{x_k}{x_j}\right)^m}{1 - \left(\frac{y_k}{y_j}\right)^n - \left(\frac{x_k}{x_i}\right)^m}. \tag{3.6}$$

D'après les estimations (3.5), on a

$$\left|\left(\frac{y_k}{y_j}\right)^n + \left(\frac{x_k}{x_i}\right)^m\right| \leq \mathrm{e}^{2\pi\sqrt{1024}a'_{k,j}+1} + \mathrm{e}^{2\pi\sqrt{1024}a_{k,i}+1} \leq 0.001,$$

d'où

$$\left|\left(\frac{x_i}{x_j}\right)^m \left(\frac{y_i}{y_j}\right)^{-n} - 1\right| \leq 2.004\left(\mathrm{e}^{2n\pi|\Delta|^{1/2}a_{k,j}+n} + \mathrm{e}^{2m\pi|\Delta|^{1/2}a'_{k,j}+m}\right) \leq \frac{1}{2}. \tag{3.7}$$

On en déduit que

$$\left|2\left(ma_{i,j} - na'_{i,j}\right)\pi|\Delta|^{1/2} + mO(1) + nO(1)\right| \leq 4.008\left(\mathrm{e}^{n\pi|\Delta|^{1/2}a_{k,j}+n} + \mathrm{e}^{m\pi|\Delta|^{1/2}a'_{k,j}+m}\right) \leq \frac{1}{2},$$

puis

$$\left|ma_{i,j} - na'_{i,j}\right| \leq \frac{0.001 + m + n}{2\pi\sqrt{1024}} \leq 0.001 + 0.01(m+n),$$

et enfin

$$\frac{a'_{i,j} - 0.011}{a_{i,j} + 0.01} \leq \frac{m}{n} \leq \frac{a'_{i,j} + 0.011}{a_{i,j} - 0.01}.$$

Finalement, pour $(i,j,k) = (1,2,3)$, on obtient

$$0.27 \leq \frac{m}{n} \leq 0.31,$$

tandis que pour $(i,j,k) = (1,3,4)$, on obtient

$$0.38 \leq \frac{m}{n} \leq 0.42.$$

Ces deux encadrements se contredisent l'un l'autre. On peut en conclure que $|\Delta| < 1024$.

Élimination des petits discriminants

Nous nous intéressons à présent aux discriminants Δ tels que $|\Delta| < 1024$. Voici la liste exhaustive des discriminants Δ tels que $|\Delta| < 1024$ et $h(4\Delta) = h(\Delta) \geq 3$, qui peut être obtenue par une simple routine en PARI :

TABLE 3.3 – Discriminants Δ tels que $|\Delta| \leq 1024$ et $h(4\Delta) = h(\Delta) \geq 3$

$h(\Delta)$	Δ
3	$-23, -31$
4	$-39, -55, -63$
5	$-47, -79, -103, -127$
6	$-87, -135, -175, -207, -247$
7	$-71, -151, -223, -343, -463, -487$
8	$-95, -111, -183, -295, -583$
9	$-199, -367, -823$
10	$-119, -143, -159, -303, -319, -375, -415, -423, -847$
11	$-167, -271, -967$
12	$-231, -255, -279, -327, -351, -543, -567, -655, -687, -775$
13	$-191, -263, -607, -631, -727$
14	$-215, -287, -391, -447, -511, -535, -639, -703, -807$
15	$-239, -439, -751$
16	$-399, -407, -471, -495, -559, -663, -735, -799, -855, -895, -903, -943, -975, -1015, -1023$
17	$-383, -991$
18	$-335, -519, -527, -575, -679, -783$
19	$-311, -359, -919$
20	$-455, -615, -711, -927$
21	$-431, -503, -743, -863$
22	$-591, -623, -767, -871, -879$
23	-647
24	$-695, -759, -999$
25	$-479, -599$
26	$-551, -951$
27	-983
28	$-831, -935$
29	-887
30	$-671, -815, -1007$
31	$-719, -911$
32	-791
33	-839
36	-959

Pour chacun de ces discriminants, on peut calculer numériquement tous les conjugués de (x, y) sur $\mathbb{Q}$, en exploitant leur appartenance à la courbe modulaire $Y_0(2)$. Si (x_i, y_i), $i \in \{1, 2, 3\}$, sont 3 conjugués avec $|x_i| \neq |x_j|$ et $|y_i| \neq |y_j|$, pour tous $i \neq j$, on peut alors, comme précédemment, obtenir un encadrement de la fraction m/n, en utilisant la relation de colinéarité (3.4). Pour peu que (x, y) possède suffisamment de conjugués, on obtient une contradiction en exhibant deux encadrements incompatibles. Décrivons ce processus en détail.

Considérons un système maximal de conjugués $(x, y) = (x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)$, $r \leq h$, de conjugués de (x, y) sur $\mathbb{Q}$ satisfaisant $|x_1| > |x_2| > \cdots > |x_r|$ et $|y_i| \neq |y_j|$, pour tous $i \neq j$. Un tel système s'obtient en ne conservant qu'un seul conjugué, pour chaque paire de conjugués $(x^\sigma, y^\sigma), (x^{\sigma'}, y^{\sigma'})$ qui sont des conjugués complexes, c'est-à-dire tels que $\overline{x^\sigma} = x^{\sigma'}$ et $\overline{y^\sigma} = y^{\sigma'}$: cela peut être vérifié avec PARI pour chaque discriminant du tableau 3.3.

Il apparaît que $r \geq 3$, excepté pour $\Delta \in \{-23, -31\}$, les deux discriminants du tableau 3.3 de nombre de classes 3. Ces deux discriminants requièrent un traitement spécial qui fera l'objet du prochain paragraphe. Pour le moment, supposons que $r \geq 3$.

Soient $1 \leq i < j < k \leq r$. Rappelons l'égalité (3.6) :

$$\left(\frac{x_i}{x_j}\right)^m \left(\frac{y_i}{y_j}\right)^{-n} - 1 = \frac{\left(\frac{y_k}{y_j}\right)^n + \left(\frac{x_k}{x_i}\right)^m - \left(\frac{y_k}{y_i}\right)^n - \left(\frac{x_k}{x_j}\right)^m}{1 - \left(\frac{y_k}{y_j}\right)^n - \left(\frac{x_k}{x_i}\right)^m}, \tag{3.6}$$

qui se réécrit également comme suit :

$$\left(\frac{x_i}{x_j}\right)^m \left(\frac{y_i}{y_k}\right)^{-n} + 1 = \frac{\left(\frac{x_k}{x_j}\right)^m \left(-1 + \left(\frac{y_j}{y_i}\right)^n\right) + \left(\frac{y_j}{y_k}\right)^n + \left(\frac{x_j}{x_i}\right)^m}{-1 + \left(\frac{y_j}{y_k}\right)^n + \left(\frac{x_j}{x_i}\right)^m}. \tag{3.8}$$

- Si $|y_j| > |y_k|$, alors d'après (3.6), $|(x_i/x_j)^m (y_i/y_j)^{-n} - 1|$ est majoré par une constante effective $0 < M < 1$, donnée par

$$M = \frac{\left|\frac{y_k}{y_j}\right| + \left|\frac{x_k}{x_i}\right| + \left|\frac{y_k}{y_i}\right| + \left|\frac{x_k}{x_j}\right|}{1 - \left|\frac{y_k}{y_j}\right| - \left|\frac{x_k}{x_i}\right|}. \tag{3.9}$$

  Il s'ensuit que

$$\frac{-M + (1 - M) \log |y_i/y_j|}{(1 - M) \log |x_i/x_j|} \leq \frac{m}{n} \leq \frac{M + (1 - M) \log |y_i/y_j|}{(1 - M) \log |x_i/x_j|}. \tag{3.10}$$

- Si $|y_j| < |y_k|$, alors d'après (3.8) cette fois-ci, $|(x_i/x_j)^m (y_i/y_k)^{-n} + 1|$ est majoré par une constante effective $0 < M < 1$, donnée par

$$M = \frac{\left|\frac{x_k}{x_j}\right| \left(1 + \left|\frac{y_j}{y_i}\right|\right) + \left|\frac{y_j}{y_k}\right| + \left|\frac{x_j}{x_i}\right|}{1 - \left|\frac{y_j}{y_k}\right| - \left|\frac{x_j}{x_i}\right|}. \tag{3.11}$$

  Il s'ensuit que

$$\frac{-M + (1 - M) \log |y_i/y_k|}{(1 - M) \log |x_i/x_j|} \leq \frac{m}{n} \leq \frac{M + (1 - M) \log |y_i/y_k|}{(1 - M) \log |x_i/x_j|}. \tag{3.12}$$

Ainsi, les inégalités (3.10) et (3.12) fournissent un encadrement de m/n pour chaque triplet (i,j,k) avec $1 \leq i < j < k \leq r$. En particulier, lorsque $r \geq 4$, on obtient plusieurs encadrements. Il s'agit alors de vérifier avec PARI que dans ce cas, il est toujours possible de trouver deux encadrements incompatibles.

Considérons désormais le cas $r = 3$. On a alors $h \in \{4,5\}$, et les discriminants Δ correspondants sont exactement ceux donnés par les entrées $h(\Delta) = 4$ et $h(\Delta) = 5$ du tableau 3.3

Posons $\alpha = x_1/x_2$, et

$$\beta = \begin{cases} y_1/y_2 & \text{si } |y_2| > |y_3|, \\ y_1/y_3 & \text{si } |y_2| < |y_3|. \end{cases}$$

Les relations (3.6) et (3.8) permettent d'estimer $\alpha^m\beta^{-n}$:

$$|\alpha^m\beta^{-n} + (-1)^\varepsilon| \leq M, \tag{3.13}$$

où

$$\varepsilon = \begin{cases} 1 & \text{si } |y_2| > |y_3|, \\ 0 & \text{si } |y_2| < |y_3|, \end{cases}$$

et $0 < M < 1$ est la constante définie par (3.9) et (3.11). Les encadrements (3.10) et (3.12), définissent également deux constantes effectives $0 < c_1 < c_2 < 1$ telles que

$$c_1 \leq m/n \leq c_2; \tag{3.14}$$

le fait que $c_2 < 1$ se vérifie en pratique. En particulier, $m \leq n$.

À nouveau d'après (3.6) et (3.8), il existe deux constantes effectives $c_3, c_4 > 0$ telles que

$$|\alpha^m\beta^{-n} + (-1)^\varepsilon| \leq c_3 \cdot c_4^n. \tag{3.15}$$

Explicitement :

- si $|y_2| > |y_3|$,

$$|\alpha^m\beta^{-n} - 1| \leq 2\frac{\left|\frac{x_3}{x_2}\right|^m + \left|\frac{y_3}{y_2}\right|^n}{1 - \left|\frac{y_3}{y_2}\right| - \left|\frac{x_3}{x_1}\right|} \leq \frac{4\left(\max\left\{\left|\frac{x_3}{x_2}\right|^{c_1}, \left|\frac{y_3}{y_2}\right|\right\}\right)^n}{1 - \left|\frac{y_3}{y_2}\right| - \left|\frac{x_3}{x_1}\right|},$$

  d'où

$$c_3 = \frac{4}{1 - \left|\frac{y_3}{y_2}\right| - \left|\frac{x_3}{x_1}\right|},$$
$$c_4 = \max\left\{\left|\frac{x_3}{x_2}\right|^{c_1}, \left|\frac{y_3}{y_2}\right|\right\};$$

- si $|y_2| < |y_3|$,

$$|\alpha^m\beta^{-n} + 1| \leq \frac{2\left|\frac{x_3}{x_2}\right|^m + \left|\frac{x_2}{x_1}\right|^m + \left|\frac{y_2}{y_3}\right|^n}{1 - \left|\frac{y_2}{y_3}\right| - \left|\frac{x_2}{x_1}\right|} \leq \frac{4\left(\max\left\{\left|\frac{x_3}{x_2}\right|^{c_1}, \left|\frac{x_2}{x_1}\right|^{c_1}, \left|\frac{y_2}{y_3}\right|\right\}\right)^n}{1 - \left|\frac{y_2}{y_3}\right| - \left|\frac{x_2}{x_1}\right|},$$

d'où

$$c_3 = \frac{4}{1 - \left|\frac{y_2}{y_3}\right| - \left|\frac{x_2}{x_1}\right|},$$
$$c_4 = \max\left\{\left|\frac{x_3}{x_2}\right|^{c_1}, \left|\frac{x_2}{x_1}\right|^{c_1}, \left|\frac{y_2}{y_3}\right|\right\}.$$

Suite à l'inégalité (3.15), on déduit

$$|m\log\alpha - n\log\beta + (2k-1+\varepsilon)i\pi| \leq c_3' \cdot c_4^n, \tag{3.16}$$

avec $c_3' = c_3/(1-M)$ et k entier. Ici, on choisit la détermination principale du logarithme (définie sur $\mathbb{C}\setminus\mathbb{R}^-$) pour $\log\alpha$ et $\log\beta$, et l'entier k satisfait $|2k| \leq m+n$ (cf. proposition C.7).

L'inégalité (3.16) nous amène à considérer la forme linéaire logarithmique $\Lambda = m\log\alpha - n\log\beta + (2k-1+\varepsilon)i\pi$, tout en sachant que $i\pi = \log(-1)$. Nous allons appliquer le théorème C.9 pour minorer $|\Lambda|$, et nous pourrons en déduire une majoration de n. La première étape consiste à s'assurer que $\Lambda \neq 0$. Le fait que $\Lambda = 0$ signifie que $\alpha^m\beta^n = (-1)^\varepsilon$, c'est-à-dire que les nombres algébriques α et β sont multiplicativement indépendants. L'algorithme 2 décrit en section 3.1 permet d'écarter cette possibilité.

Il s'agit ensuite d'estimer tous les paramètres intervenant dans le théorème C.9.

- En remarquant que $\mathbb{Q}(\alpha,\beta) \subset K(x_1,y_1) = K(x_1)$, où $K = \mathbb{Q}(\tau) = \mathbb{Q}(\tau')$, on a

$$d = [\mathbb{Q}(\alpha,\beta,-1):\mathbb{Q}] \leq [K(x_1):\mathbb{Q}] = 2h \leq 10.$$

- On a (d'après la proposition A.5)

$$\mathrm{h}(\alpha) \leq 2\mathrm{h}(x_1) \leq 9|\Delta_x|^{1/2} = 18|\Delta|^{1/2}.$$

  En outre,

$$|\log\alpha|/d \leq |\log|\alpha||/d + \pi/d \leq \mathrm{h}(\alpha) + \pi/d \leq 19|\Delta|^{1/2}.$$

  On peut donc choisir $A_1 = 19|\Delta|^{1/2}$. De la même manière, on peut choisir $A_2 = 10|\Delta|^{1/2}$, et $A_3 = 1$.
- Enfin, $H = \max\{m,n,|2k-1+\varepsilon|\} \leq m+n+1 \leq n(1+c_2)+1 \leq 3n$.

Par conséquent,

$$|\Lambda| > \mathrm{e}^{-c_5 h^5 |\Delta| \log(2eh)\log(3en)}, \tag{3.17}$$

où

$$c_5 = \min\left\{\frac{1}{8}\mathrm{e}^2 30^6 3^{5.5}, 2^{38}\right\} \cdot 19 \cdot 10 \cdot 1 \cdot 2^5 = 1671257674219520.$$

Finalement, en combinant la majoration (3.16) et la minoration (3.17), on obtient

$$\frac{n}{\log(3en)} < \frac{-c_5 h^5 |\Delta| \log(2eh) - \log c_3'}{\log c_4} = c_6, \tag{3.18}$$

et on aboutit, en utilisant la propriété C.1, à

$$n < \left(1 + \frac{1}{\mathrm{e}}\right) c_6 \log(3(1+\mathrm{e})c_6) = c_7. \tag{3.19}$$

Il s'ensuit que m est également majoré d'après (3.14), et donc qu'il y a un nombre fini de couples (m, n) possibles. Toutefois, en pratique, les majorations obtenues sur m et n sont beaucoup trop grandes pour pouvoir énumérer tous les couples (m, n) possibles. Voici comment contourner cet obstacle.

En reprenant l'inégalité (3.15), écrivons

$$\left|\theta - \frac{m}{n}\right| \leq \frac{c_3' \cdot c_4^n}{n \log|\alpha|}, \tag{3.20}$$

avec $\theta = \log|\beta|/\log|\alpha|$. On obtient une estimation précise du nombre réel θ par le nombre rationnel m/n. Deux situations peuvent alors se produire.

- Si $|\theta - m/n| \leq 1/(2n^2)$, alors d'après le théorème de Legendre (voir [Sch80, Theorem 5C]), en écrivant m/n sous forme irréductible p/q, la fraction p/q est une réduite du développement en fraction continue de θ.
- Sinon, l'inégalité (3.20) impose que

  $$\frac{1}{2n^2} < \frac{c_3' \cdot c_4^n}{n \log|\alpha|},$$

  d'où

  $$n \leq \frac{\log(2c_3' n/\log|\alpha|)}{\log(c_4^{-1})} \leq \frac{\log(2c_3' c_7/\log|\alpha|)}{\log(c_4^{-1})} = c_7',$$

  la dernière inégalité découlant de (3.19). Ce procédé peut être réitéré jusqu'à obtenir une majoration de n strictement plus petite que 1 : en effet, si $c_7' > 1$, on a

  $$n \leq \frac{\log(2c_3' c_7'/\log|\alpha|)}{\log(c_4^{-1})} = c_7'',$$

  et ainsi de suite, chaque nouvelle majoration étant plus fine que la précédente. On observe alors que cette situation ne peut se produire.

En conséquence, tous les couples (m, n) possibles se déduisent du développement en fraction continue de θ et de la majoration (3.19) sur n. Le terme de droite de l'inégalité (3.20) converge plus rapidement vers 0 que son terme de gauche lorsque n croît, ce qui nous suggère le processus suivant en PARI. On commence par calculer θ avec une précision suffisante pour obtenir toutes ses réduites p/q vérifiant $q < c_7$, la majoration obtenue en (3.19) ; pour cela, on peut utiliser l'algorithme de Lehmer (voir [Coh96, Algorithm 1.3.13]), qui repose sur la division euclidienne. Pour chaque réduite p/q, on vérifie que

$$\log|\theta q - p| > q \log(c_4') + \log\left(\frac{c_3'}{\log|\alpha|}\right), \tag{3.21}$$

ce qui contredit (3.20) pour le couple (p, q) donné. Comme le terme de droite de (3.21) décroît en fonction de q, alors si (3.21) est satisfaite pour (p, q), elle l'est également pour tous les multiples (m, n) de (p, q). Il suffit donc de vérifier que (3.21) est satisfaite pour toutes les réduites p/q telles que $q < c_7$.

Élimination des discriminants de nombre de classes 3

Il reste à traiter les cas $\Delta = -23$ et $\Delta = -31$, pour lesquels $h(\Delta) = 3$, et (x, y) admet deux conjugués qui sont des conjugués complexes. Comme précédemment, notons $(x_1, y_1) = (x, y)$,

le couple correspondant aux j-valeurs dominantes de discriminants respectifs 4Δ et Δ, ainsi que $(x_2, y_2), (x_3, y_3)$ les deux autres conjugués, qui vérifient alors $\overline{x_2} = x_3$ et $\overline{y_2} = y_3$. Notons également L la clôture galoisienne de $\mathbb{Q}(x) = \mathbb{Q}(y)$, qui contient par définition tous les x_i et les y_i, et qui est de degré 6 sur $\mathbb{Q}$.

D'après (3.4), les trois points (x_i, y_i), $i \in \{1, 2, 3\}$, vérifient la relation de colinéarité

$$\begin{vmatrix} 1 & x_1^m & y_1^n \\ 1 & x_2^m & y_2^n \\ 1 & x_3^m & y_3^n \end{vmatrix} = 0, \tag{3.22}$$

qui se réécrit sous la forme

$$\left(\frac{x_1}{x_2}\right)^{-m} \left(\frac{y_1}{y_2}\right)^{n} = \frac{1 - \left(\frac{y_3}{y_2}\right)^n - \left(\frac{x_3}{x_1}\right)^m}{1 - \left(\frac{y_3}{y_1}\right)^n - \left(\frac{x_3}{x_2}\right)^m}. \tag{3.23}$$

Focalisons-nous dans un premier temps sur le cas $\Delta = -23$. Le second cas se traitera de manière analogue.

En utilisant PARI pour factoriser les idéaux $x_i\mathcal{O}_L$ et $y_i\mathcal{O}_L$ dans $\mathcal{O}_L$, on peut trouver un idéal premier $\mathfrak{p}$ au-dessus de $p = 23$ tel que $\mathfrak{p} | x_2\mathcal{O}_L$, $\mathfrak{p} | x_3\mathcal{O}_L$, mais $\mathfrak{p} \nmid x_1y_2y_3\mathcal{O}_L$. Ainsi, modulo $\mathfrak{p}^m$, la relation (3.22) aboutit à

$$1 - \alpha^n = 0 \bmod \mathfrak{p}^m,$$

avec $\alpha = y_3/y_2$. D'une part, on en déduit que $m \leq v_\mathfrak{p}(1 - \alpha^n)$. D'autre part, on applique la proposition C.11, en vérifiant tout d'abord que $1 - \alpha = 0 \bmod \mathfrak{p}$, $v_\mathfrak{p}(1 - \alpha) = 1$, et $v_\mathfrak{p}(p) = 2 < [L : \mathbb{Q}] < p - 1$. En écrivant $n = p^s r$ avec $\operatorname{pgcd}(p, r) = 1$, on obtient

$$v_\mathfrak{p}(1 - \alpha^n) = sv_\mathfrak{p}(p) + 1 = 2s + 1.$$

Par conséquent,

$$m \leq 2\frac{\log n}{\log 23} + 1. \tag{3.24}$$

À présent, nous allons majorer en valeur absolue le terme de droite de la relation (3.23) en fonction de m et de n (en fait, seulement en fonction de n grâce à l'inégalité (3.24)). La principale difficulté est de minorer son dénominateur. Comme y_3/y_1 est proche de 0, il dépend essentiellement de la quantité $1 - \beta^m$, avec $\beta = x_3/x_2$. En remarquant que $|\beta| = 1$ et que β n'est pas une racine de l'unité, alors conformément au théorème C.10, il existe une constante effective $c_1(\beta) > 0$ telle que

$$|1 - \beta^m| > 0.99\mathrm{e}^{-c_1(\beta)(\log m)^2}.$$

Explicitement, pour $m \geq 13$, on peut choisir $c_1(\beta) = 4973.14$. Il s'ensuit que

$$\begin{aligned} \left|1 - \left(\frac{y_3}{y_1}\right)^n - \left(\frac{x_3}{x_2}\right)^m\right| &> 0.99\mathrm{e}^{-4973.14(\log m)^2} - \left|\frac{y_3}{y_1}\right|^n \\ &> 0.99\mathrm{e}^{-4973.14\left(\log\left(2\frac{\log n}{\log 23}+1\right)\right)^2} - \left|\frac{y_3}{y_1}\right|^n \end{aligned}$$

(la dernière inégalité provient de (3.24)). Par un rapide calcul, on observe que le dernier terme de la précédente inégalité est positif pourvu que $n > 2074$. Plus spécifiquement, si $n > 2075$, alors

$$\left|1 - \left(\frac{y_3}{y_1}\right)^n - \left(\frac{x_3}{x_2}\right)^m\right| > 0.98\mathrm{e}^{-4973.14\left(\log\left(2\frac{\log n}{\log 23}+1\right)\right)^2}.$$

Finalement, pour $m \geq 13$ et $n > 2075$, on a

$$\left|\frac{x_1}{x_2}\right|^{-m}\left|\frac{y_1}{y_2}\right|^{n} \leq 2.05\mathrm{e}^{4973.14\left(\log\left(2\frac{\log n}{\log 23}+1\right)\right)^2},$$

puis

$$-\left(2\frac{\log n}{\log 23}+1\right)\log\left|\frac{x_1}{x_2}\right| + n\log\left|\frac{y_1}{y_2}\right| \leq \log 2.05 + 4973.14\left(\log\left(2\frac{\log n}{\log 23}+1\right)\right)^2.$$

Cette dernière inégalité induit $n \leq 2092$, et ainsi (3.24) donne $m \leq 5$. Ceci contredit les précédentes hypothèses $m \geq 13$ et $n > 2075$. En conséquence, soit $m < 13$, soit $n \leq 2075$. Dans les deux cas, $m < 13$, et pour chaque m possible, on peut calculer explicitement une constante $c_2(m)$ telle que

$$\left|\frac{x_1}{x_2}\right|^{-m}\left|\frac{y_1}{y_2}\right|^{n} \leq c_2(m), \tag{3.25}$$

ce qui permet de majorer n. Le tableau ci-dessous détaille toutes les constantes $c_2(m)$ et toutes les majorations que nous obtenons.

TABLE 3.4 – Constantes $c_2(m)$ et majorations de n pour chaque $m < 13$, dans le cas $\Delta = -23$

m	$c_2(m)$	Majoration de n
1	1.15	2
2	1.21	5
3	11.97	8
4	1.10	10
5	1.28	13
6	6.00	16
7	1.07	18
8	1.38	21
9	4.02	24
10	1.04	26
11	1.50	29
12	3.04	32

À nouveau, l'inégalité (3.24) élimine toutes les entrées du tableau 3.4 correspondant à $m \geq 3$. Il reste donc $m = 1$ et $n \leq 2$, ou $m = 2$ et $n \leq 5$. Pour chacun de ces couples (m, n), un calcul direct montre que le déterminant dans la relation (3.22) ne s'annule pas.

Pour finir, on répète ce procédé pour $\Delta = -31$. Dans ce cas, on peut trouver un idéal premier $\mathfrak{p}$ de $\mathcal{O}_L$ au-dessus de $p = 11$ tel que $\mathfrak{p}|x_2\mathcal{O}_L$, $\mathfrak{p}|x_3\mathcal{O}_L$, mais $\mathfrak{p} \nmid x_1y_2y_3\mathcal{O}_L$ comme précédemment, et on obtient

$$m \leq \frac{\log n}{\log 11} + 2. \tag{3.26}$$

On obtient de même, pour $m \geq 13$ et $n > 1440$,

$$\left|\frac{x_1}{x_2}\right|^{-m} \left|\frac{y_1}{y_2}\right|^{n} \leq 2.05\mathrm{e}^{4820.16\left(\log\left(\frac{\log n}{\log 11}+2\right)\right)^2},$$

puis

$$-\left(\frac{\log n}{\log 11}+2\right)\log\left|\frac{x_1}{x_2}\right| + n\log\left|\frac{y_1}{y_2}\right| \leq \log 2.05 + 4820.16\left(\log\left(\frac{\log n}{\log 11}+2\right)\right)^2,$$

ce qui induit $n \leq 1720$ et $m \leq 5$. Il s'agit à nouveau d'une contradiction. Pour chaque $m < 13$ possible, on calcule une constante $c_2(m)$ comme définie par (3.25), de laquelle on déduit une majoration de n. Voici la table que nous obtenons :

TABLE 3.5 – Constantes $c_2(m)$ et majorations de n pour chaque $m < 13$, dans le cas $\Delta = -31$

m	$c_2(m)$	Majoration de n
1	1.13	3
2	1.25	6
3	6.17	10
4	1.06	13
5	1.44	16
6	3.13	19
7	1.02	22
8	1.76	26
9	2.13	29
10	1.01	32
11	2.33	36
12	1.65	39

L'inégalité (3.26) élimine toutes les entrées du tableau 3.5 correspondant à $m \geq 3$. Il reste donc $m = 1$ et $n \leq 3$, ou $m = 2$ et $n \leq 6$. Un calcul identique montre que le déterminant dans la relation (3.22) ne s'annule pas.

3.2.3 Le cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

Pour achever la preuve, il nous reste à examiner le cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$. Dans ce cas, d'après le corollaire 2.45, les discriminants Δ_x et Δ_y figurent dans une même entrée du tableau 2.1, et de plus le corps $L = \mathbb{Q}(x) = \mathbb{Q}(y)$ correspondant est connu. Rappelons qu'on ne s'intéresse qu'aux entrées avec $h = [L : \mathbb{Q}] \geq 3$, et que $\Delta_x \neq \Delta_y$, puisque x et y sont distincts et dominants, donc non conjugués sur $\mathbb{Q}$.

Pour déterminer les conjugués de (x, y) sur $\mathbb{Q}$, on ne peut plus exploiter la courbe modulaire $Y_0(2)$ comme précédemment. Toutefois, comme L est explicite, on peut calculer toutes les racines des polynômes minimaux de x et y sur $\mathbb{Q}$ dans une $\mathbb{Q}$-base de L, puis isoler la plus grande racine en valeur absolue de chacun d'entre eux pour identifier x et y, les j-valeurs dominantes de discriminants respectifs Δ_x et Δ_y. Il ne reste plus qu'à calculer l'orbite de (x, y)

sous l'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$, lui aussi explicite, pour obtenir les conjugués de (x, y). À cet effet, le tableau 3.6 ci-après recense les j-valeurs dominantes pour tous les discriminants Δ_x et Δ_y possibles.

TABLE 3.6 – j-valeur dominante J_Δ de discriminant Δ, pour chaque discriminant Δ du tableau 2.1 avec $[\mathbb{Q}(J_\Delta) : \mathbb{Q}] \geq 3$

$\mathbb{Q}(J_\Delta)$	$h(\Delta)$	Δ	J_Δ
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	-96	$2382143496408\sqrt{6} + 4125993565824\sqrt{2} + 3368859648336\sqrt{3} + 5835036074184$
		-192	$820762881440077125\sqrt{6} + 1421603011620136125\sqrt{2} + 1160733998424384000\sqrt{3} + 2010450259344609000$
		-288	$14557905935176475872000\sqrt{6} + 25215032731534167067000\sqrt{2}$
			$+20587988013278347844000\sqrt{3} + 35659441264617127693000$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	4	-180	$130293882068147200\sqrt{15} + 291345976946585600\sqrt{3} + 225675623657419520\sqrt{5} + 504626034652280000$
		-240	$176909828043375943425\sqrt{15}/2 + 395582401392793626375\sqrt{3}/2$
			$+153208405264700298240\sqrt{5} + 342584408896212090600$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	4	-195	$-3499147465371648000\sqrt{65} - 1261635560680734720\sqrt{5} - 782433159587020800\sqrt{13} - 2821102876514304000$
		-520	$4018381031399327507713784832000\sqrt{65} + +1448847885306213805432286292480\sqrt{5}$
			$+898537314570460818298560345600\sqrt{13} + 323972236060151457410558618400 0$
		-715	$-942329738208550995435756855103488000\sqrt{65} - 339761818950548816661251871815516160\sqrt{5}$
			$-210711335185390092224195686717440000\sqrt{13} - 75973052333240341185619278937497600 0$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	4	-120	$69812648236800\sqrt{10} + 156105837619200\sqrt{2} + 98729993940480\sqrt{5} + 220766992776000$
		-160	$14324763611604600\sqrt{10} + 32031145197162000\sqrt{2} + 20258274977314560\sqrt{5} + 45298879956160200$
		-280	$5349622500401814835200\sqrt{10} + 11962119564768883910400\sqrt{2}$
			$+756550869358634767872 0\sqrt{5} + 16916991723354765960000$
		-760	$32448928746539631437917228871833238400\sqrt{10} + 72558010474309659689396015191902720 00\sqrt{2}$
			$+458897151178345420042368300179456256 0\sqrt{5} + 10261252247157780777921455637033556800$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	4	-340	$3900205112587637974848 00\sqrt{85} + 160809576407728512735744 0\sqrt{5}$
			$+872112375793358009856000\sqrt{17} + 3595811442804377657668800$
		-595	$-5175436520569735560861169827840 0\sqrt{85} - 213388714329881678626101264875520\sqrt{5}$
			$-1157262787322891733040029462528 00\sqrt{17} - 47715167087289891652690584576000 0$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	8	-480	$17796623907585076180678031400\sqrt{30} + 39794460827358165511539222000\sqrt{6}$
			$+308246568111323198630979552 00\sqrt{10} + 25168226894560081669417869600\sqrt{15}$
			$+689260280127937634235200256 00\sqrt{2} + 562778662093747746009508404 00\sqrt{3}$
			$+435926477177995261631308531 20\sqrt{5} + 97476123616200805300027650 00$
		-960	$171421206755988867365461163073786995317425\sqrt{30}/4 + 383309471091437312167077928802762245715025\sqrt{6}/4$
			$+296910239596142001955918718194079103568275\sqrt{10}/4 + 606065488681704711123811066188142512384 00\sqrt{15}$
			$+663911478952723221826832037231245502051375\sqrt{2}/4 + 135520363150892113690629628530924963456000\sqrt{3}$
			$+104973621911077290593933617351429680783360\sqrt{5} + 23472815443753020569492697234995778431 4600$

Les estimations des formes logarithmes décrites en partie 3.2.2 peuvent être reproduites ici, en choisissant trois conjugués (x_i, y_i), $i \in \{1, 2, 3\}$, de (x, y) sur $\mathbb{Q}$, avec $(x_1, y_1) = (x, y)$ et $|x_1| > |x_2| > |x_3|$ comme précédemment. La différence réside dans l'inégalité (3.17) résultant de l'application du théorème C.9, qui devient

$$|\Lambda| > \mathrm{e}^{-c_5 h^5 |\Delta_x|^{1/2} |\Delta_y|^{1/2} \log(eh) \log(3en)},$$

où c_5 est donné cette fois par

$$c_5 = \min\left\{\frac{1}{8}\mathrm{e}^2 30^6 3^{5.5}, 2^{38}\right\} \times 10 \times 10 \times 1 = 27487790694400$$

($[\mathbb{Q}(\alpha, \beta, -1) : \mathbb{Q}] = [\mathbb{Q}(x_1) : \mathbb{Q}] = h$, $A_1 = A_2 = 10$, $A_3 = 1$). La constante c_6 définie par (3.18) change en conséquence :

$$\frac{n}{\log(3en)} < \frac{-c_5 h^5 |\Delta_x|^{1/2} |\Delta_y|^{1/2} \log(eh) - \log c_3'}{\log c_4} = c_6.$$

On effectue alors le même procédé en PARI qu'en partie 3.2.2 pour éliminer toutes les paires de discriminants restantes.

3.3 Indépendance multiplicative forte de modules singuliers

Démontrons à présent le théorème 3.6, dont nous rappelons l'énoncé.

Théorème 3.6. *Soient x, y deux modules singuliers, et m, n deux entiers non nuls. Supposons que $x^m y^n \in \mathbb{Q}^\times$. Alors l'une des assertions suivantes est vérifiée :*

(cas d'égalité) *$x = y$ et $m + n = 0$;*

(cas rationnel) *$x, y \in \mathbb{Q}^\times$;*

(cas quadratique) *$m = n$ et x, y sont de degré 2 et conjugués sur $\mathbb{Q}$.*

Remarque 3.11. La condition $m, n \neq 0$ n'est pas restrictive. En effet, si $m = 0$ et $n \neq 0$, alors $y^n \in \mathbb{Q}$ donc $y \in \mathbb{Q}$ d'après la proposition 2.43 ; de même, si $m \neq 0$ et $n = 0$, alors $x^m \in \mathbb{Q}$ donc $x \in \mathbb{Q}$.

3.3.1 Réduction du problème

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers de discriminants respectifs Δ_x, Δ_y, et m, n deux entiers non nuls. Supposons que

$$x^m y^n = A \in \mathbb{Q}^\times. \tag{3.27}$$

Tout d'abord, l'équation (3.27) implique que $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, d'où $\mathbb{Q}(x) = \mathbb{Q}(y)$ d'après le corollaire 2.43. Posons $h = h(\Delta_x) = h(\Delta_y)$. Le cas $h = 1$ correspond au "cas rationnel" du théorème 3.6. Par ailleurs, si $x = y$, alors $x^{m+n} \in \mathbb{Q}$, donc soit $m + n = 0$, ce qui correspond au "cas d'égalité", soit $m + n \neq 0$ et $x = y \in \mathbb{Q}$.

Le déroulement de la démonstration du théorème 3.6 est similaire à celle du théorème 3.5, dans la mesure où nous commençons par exhiber une contradiction dans le cas général, pour se restreindre à un nombre fini de paires de discriminants $\{\Delta_x, \Delta_y\}$ à examiner.

Voyons tout d'abord comment "éliminer" une paire de discriminants $\{\Delta_x, \Delta_y\}$ donnée ; par "éliminer", on entend montrer que pour tous modules singuliers $x = j(\tau)$ et $y = j(\tau')$ de discriminants respectifs Δ_x et Δ_y, on a $x^m y^n \notin \mathbb{Q}^\times$. Considérons L la clôture galoisienne de $\mathbb{Q}(x) = \mathbb{Q}(y)$, c'est-à-dire $L = \mathbb{Q}(x, \tau)$ si $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$, $L = \mathbb{Q}(x)$ sinon et L est l'un des corps du tableau 2.1. "Éliminer" la paire $\{\Delta_x, \Delta_y\}$ revient alors à fixer arbitrairement deux modules singuliers x et y de discriminants respectifs Δ_x et Δ_y, et à montrer que pour tout automorphisme σ du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$, on a $x^m (y^\sigma)^n \notin \mathbb{Q}^\times$. L'algorithme 2 expliqué en section 3.1 permet de procéder à cette vérification.

En particulier, en appliquant cette méthode, nous pouvons d'emblée éliminer les paires $\{\Delta_x, \Delta_y\}$ données par le tableau 2.1 avec $h \geq 3$ (correspondantes au cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$), et les paires avec $\Delta_x \neq \Delta_y$ et $h = 2$. Dans le cas $\Delta_x = \Delta_y$ et $h = 2$, x et y sont conjugués sur $\mathbb{Q}$, et comme $x \neq y$, ils satisfont

$$\left(\frac{x}{y}\right)^{m-n} = 1.$$

Toutefois, x ou y est la j-valeur dominante de discriminant $\Delta_x = \Delta_y$, donc $|x| \neq |y|$, ce qui implique $m = n$. Cela correspond au "cas quadratique" du théorème 3.6.

Dans toute la suite, nous supposons que $h \geq 3$ et $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$. Rappelons qu'alors $\Delta_x/\Delta_y \in \{1, 4, 1/4\}$ d'après la proposition 2.46. La preuve se divise à ce stade en deux cas : les cas $mn < 0$ et $mn > 0$.

3.3.2 Le cas $mn < 0$

Supposons que $mn < 0$. Le point (x, y) satisfait l'équation

$$x^m - Ay^{-n} = 0$$

si $m > 0$ et $n < 0$, et à l'équation

$$Ax^{-m} - y^n = 0$$

si $m < 0$ et $n > 0$, ce qui correspond, dans un cas comme dans l'autre, à la situation du théorème 3.5 avec $C = 0$. En particulier, la réduction effectuée en 3.2.1 est toujours valide : d'après le lemme 3.8, (x, y) est conjugué sur $\mathbb{Q}$ à un point dont les coordonnées sont les j-valeurs dominantes de discriminants respectifs Δ_x et Δ_y. Comme $x \neq y$, on a $\Delta_x \neq \Delta_y$, et d'après la proposition 2.46, on pose $\Delta = \Delta_y$ et on peut supposer $\Delta_x = 4\Delta$ sans perte de généralité. Il s'ensuit à nouveau que le point (x, y) et tous ses conjugués sur $\mathbb{Q}$ appartiennent à la courbe modulaire $Y_0(2)$.

Si $|\Delta| \geq 256$, le tableau 3.2 fournit 3 conjugués explicites (x_i, y_i), $i \in \{1, 2, 3\}$, du point (x, y) sur $\mathbb{Q}$. Ces conjugués vérifient

$$\left(\frac{x_1}{x_i}\right)^m = \left(\frac{y_1}{y_i}\right)^{-n}, \quad i \in \{2, 3\},$$

soit

$$-\frac{m}{n} = \frac{\log|y_1/y_i|}{\log|x_1/x_i|}, \quad i \in \{2, 3\}.$$

Grâce aux estimations (3.5), on en déduit

$$\frac{1/2 + O(1)}{7/4 + O(1)} = \frac{3/4 + O(1)}{15/8 + O(1)}, \tag{3.28}$$

où $|O(1)| \leq 0.001$ ici. On s'aperçoit aisément que le terme de gauche de (3.28) est strictement plus petit que le terme de droite en valeurs absolues, ce qui aboutit à une contradiction lorsque $|\Delta| \geq 256$.

Pour $|\Delta| < 256$, on applique ensuite l'algorithme 3 pour éliminer tous les Δ possibles.

3.3.3 Le cas $mn > 0$

Supposons à présent que $mn > 0$. Puisque $x^{-m}y^{-n} \in \mathbb{Q}^\times$, on peut supposer sans perte de généralité que $m, n > 0$, et de plus que $m \geq n$.

D'une part, quitte à conjuguer sur $\mathbb{Q}$, on peut supposer que x est la j-valeur dominante de discriminant Δ_x, et on déduit de la proposition 2.31 que

$$|x| \geq \mathrm{e}^{\pi|\Delta_x|^{1/2}} - 2079 \geq 0.999\mathrm{e}^{\pi|\Delta_x|^{1/2}}.$$

D'autre part, pour minorer $|y|$, on utilise la proposition 2.34. On peut supposer que $\tau' \in \mathcal{D}^+$, le cas $\tau' \in \mathcal{D}^-$ étant en tous points analogue. Pour estimer $|\tau' - \zeta_6|$, notons d'abord que $\tau' \neq \zeta_6$ puisque $y \neq 0$, et comme $\tau' \in \mathcal{D}^+$, en écrivant $\tau' = \tau(a', b', c') = (-b' + \sqrt{\Delta_y})/(2a')$ avec $(a', b', c') \in T_{\Delta_y}$, on a

$$\frac{\sqrt{|\Delta_y|}}{2a'} = \operatorname{Im}\tau' > \frac{\sqrt{3}}{2} = \operatorname{Im}\zeta_6.$$

Ainsi,

$$|\tau' - \zeta_6| \geq \left| \frac{\sqrt{|\Delta_y|}}{2a'} - \frac{\sqrt{3}}{2} \right| = \frac{||\Delta_y| - 3a'^2|}{2a' \left(\sqrt{|\Delta_y|} + a'\sqrt{3} \right)} \geq \frac{1}{2a' \left(\sqrt{|\Delta_y|} + a'\sqrt{3} \right)} \geq \frac{\sqrt{3}}{4|\Delta_y|},$$

la dernière inégalité provenant de (1.3). On en déduit que

$$|y| \geq \min\{4.4 \cdot 10^{-5}, 3500|\Delta_y|^{-3}\}. \tag{3.29}$$

On obtient ainsi une minoration de $|A|$:

$$|A| \geq \left(0.999\mathrm{e}^{\pi|\Delta_x|^{1/2}}\right)^m \left(\min\{4.4 \cdot 10^{-5}, 3500|\Delta_y|^{-3}\}\right)^n \geq \left(3000\mathrm{e}^{\pi|\Delta_x|^{1/2}} \min\{10^{-8}, |\Delta_y|^{-3}\}\right)^m. \tag{3.30}$$

Nous allons ensuite majorer $|A|$ aussi finement que possible. Pour ce faire, nous nous intéressons à l'existence d'un conjugué (x^σ, y^σ) de (x, y) sur $\mathbb{Q}$ avec $|x^\sigma|, |y^\sigma|$ suffisamment petits. Concrètement, les conjugués de (x, y) étant de la forme

$$\left(j\left(\frac{b + \sqrt{\Delta_x}}{2a} \right), j\left(\frac{b' + \sqrt{\Delta_y}}{2a'} \right) \right), \quad (a, b, c) \in T_{\Delta_x}, \quad (a', b', c') \in T_{\Delta_y}, \tag{3.31}$$

cela revient à trouver un tel conjugué avec a et a' suffisamment grands. Distinguons les 3 cas $\Delta_x = \Delta_y$, $\Delta_x = 4\Delta_y$ et $\Delta_y = 4\Delta_x$.

Le cas $\Delta_x = \Delta_y$. Notons $\Delta = \Delta_x = \Delta_y$. L'ensemble T_Δ possède au plus deux triplets (a, b, c) avec $a = 2$. Si $h > 6$, le point (x, y) admet donc un conjugué sur $\mathbb{Q}$ de la forme (3.31) avec $a, a' \geq 3$. Pour un tel conjugué, on a

$$|A| \leq \left(\mathrm{e}^{\pi|\Delta|^{1/2}/3} + 2079\right)^m \left(\mathrm{e}^{\pi|\Delta|^{1/2}/3} + 2079\right)^n \leq \left(1.71\mathrm{e}^{2\pi|\Delta|^{1/2}/3}\right)^m. \tag{3.32}$$

En combinant (3.30) et (3.32), on obtient

$$3000\mathrm{e}^{\pi|\Delta|^{1/2}/3} \min\{10^{-8}, |\Delta|^{-3}\} \leq 1.71,$$

ce qui implique $|\Delta| \leq 109$.

Le cas $\Delta_x = 4\Delta_y$. Notons $\Delta = \Delta_y$. Rappelons que $\Delta \equiv 1 \bmod 8$ (cf. lemme 3.9), et qu'alors l'ensemble T_Δ possède exactement deux triplets (a', b', c') avec $a' = 8$ si $|\Delta| \geq 256$, tandis que l'ensemble $T_{4\Delta}$ ne possède aucun triplet (a, b, c) avec $a = 2$. Pour $|\Delta| \geq 256$, le point (x, y) admet donc un conjugué sur $\mathbb{Q}$ de la forme (3.31) avec $a \geq 3$ et $a' = 8$. Pour un tel conjugué, on a

$$|A| \leq \left(\mathrm{e}^{2\pi|\Delta|^{1/2}/3} + 2079\right)^m \left(\mathrm{e}^{\pi|\Delta|^{1/2}/8} + 2079\right)^n \leq \left(345.83\mathrm{e}^{19\pi|\Delta|^{1/2}/24}\right)^m. \tag{3.33}$$

En combinant (3.30) et (3.33), on obtient

$$3000\mathrm{e}^{29\pi|\Delta|^{1/2}/24} \min\{10^{-8}, |\Delta|^{-3}\} \leq 345.83,$$

ce qui implique $|\Delta| \leq 18$ et contredit l'hypothèse $|\Delta| \geq 256$. En conséquence, $|\Delta| < 256$.

Le cas $\Delta_y = 4\Delta_x$. Notons $\Delta = \Delta_x$. En inversant simplement les rôles de Δ_x et Δ_y dans le cas précédent, le point (x, y) admet un conjugué sur $\mathbb{Q}$ de la forme (3.31) avec $a = 8$ et $a' \geq 3$, et l'estimation (3.33) reste valable pour $|\Delta| \geq 256$. En combinant (3.30) et (3.33), on obtient

$$3000\mathrm{e}^{5\pi|\Delta|^{1/2}/24} \min\{10^{-8}, |\Delta|^{-3}/8\} \leq 345.83,$$

ce qui implique $|\Delta| \leq 992$.

L'étude précédente nous a permis de réduire le nombre de paires $\{\Delta_x, \Delta_y\}$ possibles à un nombre fini. Récapitulons ce que sont les paires restantes :

- les paires $\{\Delta, \Delta\}$, avec soit $h(\Delta) > 6$ et $|\Delta| \leq 109$, soit $h(\Delta) \leq 6$.
- les paires $\{4\Delta, \Delta\}$ avec $h(\Delta) = h(4\Delta)$ et $|\Delta| < 256$;
- les paires $\{\Delta, 4\Delta\}$ avec $h(\Delta) = h(4\Delta)$ et $|\Delta| \leq 992$.

Pour chacune de ces paires, on applique l'algorithme 3 pour conclure.

Chapitre 4

Sommes et produits de modules singuliers

Les travaux présentés dans ce chapitre sont le fruit d'une collaboration avec Faye et Luca, de laquelle a résulté un nouvel article [Fay18]. La problématique de ce projet commun est la suivante.

Dans la continuité des théorèmes 3.2 et 3.3, il apparaît légitime de s'interroger d'une manière plus générale sur le degrés des corps engendrés par les sommes et les produits de deux modules singuliers. Plus précisément, étant donnés deux modules singuliers x, y, que peut-on dire des degrés $[\mathbb{Q}(x,y) : \mathbb{Q}(x+y)]$ et $[\mathbb{Q}(x,y) : \mathbb{Q}(xy)]$? On sait que $[\mathbb{Q}(x,y) : \mathbb{Q}(x+y)] \leq 2$ lorsque $x + y \in \mathbb{Q}$, de même que $[\mathbb{Q}(x,y) : \mathbb{Q}(xy)] \leq 2$ lorsque $xy \in \mathbb{Q}^\times$. Il s'avère que, dans le cas général, ces degrés sont toujours majorés par 2, et que $x + y$ et xy engendrent chacun le corps $\mathbb{Q}(x,y)$ la plupart du temps. Voici les énoncés exacts de nos résultats :

Théorème 4.1. *Soient x, y deux modules singuliers de discriminants respectifs Δ_x, Δ_y. Alors $\mathbb{Q}(x+y) = \mathbb{Q}(x,y)$ si $\Delta_x \neq \Delta_y$, et $[\mathbb{Q}(x,y) : \mathbb{Q}(x+y)] \leq 2$ si $\Delta_x = \Delta_y$.*

Théorème 4.2. *Soient x, y deux modules singuliers de discriminants respectifs Δ_x, Δ_y. Alors $\mathbb{Q}(x+y) = \mathbb{Q}(xy)$ si $\Delta_x \neq \Delta_y$, et $[\mathbb{Q}(x,y) : \mathbb{Q}(xy)] \leq 2$ si $\Delta_x = \Delta_y$.*

Les théorèmes 4.1 et 4.2 sont démontrés respectivement dans les sections 4.1 et 4.2.

Dans tout ce chapitre, nous emploierons les notations suivantes : on notera Δ_z le discriminant d'un module singulier z, ainsi que $K_z = \mathbb{Q}(\sqrt{\Delta_z})$ et D_z le discriminant du corps quadratique K_z. En outre, nous utiliserons fréquemment l'estimation 2.31 sans mention particulière.

4.1 Sommes de modules singuliers

En vue de démontrer le théorème 4.1, nous allons plutôt établir l'énoncé un peu plus général suivant.

Théorème 4.3. *Soient x, y deux modules singuliers distincts de discriminants respectifs Δ_x, Δ_y, et $\varepsilon \in \{1, -1\}$. Alors $\mathbb{Q}(x + \varepsilon y) = \mathbb{Q}(x,y)$, sauf si $\varepsilon = 1$ et $\Delta_x = \Delta_y$, auquel cas $[\mathbb{Q}(x,y) : \mathbb{Q}(x+y)] \leq 2$.*

Nous ferons entre autres appel à la proposition ci-après :

Proposition 4.4. *Soient x, x', y, y' des modules singuliers tels que*

$$\Delta_x = \Delta_{x'}, \quad \Delta_y = \Delta_{y'}, \quad \text{et } D_x \neq D_y.$$

Supposons que $\mathbb{Q}(x, x') = \mathbb{Q}(y, y')$. Alors $\mathbb{Q}(x) = \mathbb{Q}(y)$.

Démonstration. Si l'extension $\mathbb{Q}(x)/\mathbb{Q}$ est galoisienne, alors $\mathbb{Q}(x, x') = \mathbb{Q}(x)$ et $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$ est 2-élémentaire par la proposition 2.22. Par suite, $\mathrm{Gal}(\mathbb{Q}(y, y')/\mathbb{Q})$ est également 2-élémentaire, ce qui implique que $\mathbb{Q}(y)/\mathbb{Q}$ est galoisienne, et enfin que $\mathbb{Q}(y, y') = \mathbb{Q}(y)$. En conséquence, $\mathbb{Q}(x) = \mathbb{Q}(y)$.

Supposons à présent que l'extension $\mathbb{Q}(x)/\mathbb{Q}$ n'est pas galoisienne. Nous allons exhiber une contradiction dans ce cas. Comme $K_x(x)/\mathbb{Q}$ est galoisienne et $[K_x(x) : \mathbb{Q}(x)] \leq 2$, le corps $K_x(x)$ est la clôture galoisienne de $\mathbb{Q}(x)/\mathbb{Q}$. Soit L la clôture galoisienne de $\mathbb{Q}(x, x')/\mathbb{Q}$. Puisque

$$\mathbb{Q}(x) \subset \mathbb{Q}(x, x') \subset K_x(x),$$

on déduit $L = K_x(x)$. Comme $\mathbb{Q}(x, x') = \mathbb{Q}(y, y')$, on a de la même manière $L = K_y(y)$. Posons $H_x = \mathrm{Gal}(L/K_x)$ et $H_y = \mathrm{Gal}(L/K_y)$. Alors (H_x, ι) et (H_y, ι) sont deux structures diédrales sur $G = \mathrm{Gal}(L/\mathbb{Q})$, où ι est la conjugaison complexe. En outre, le groupe G n'est pas abélien d'après la proposition 2.22, et le lemme 1.29 implique alors que $H_x = H_y$, soit $K_x = K_y$, ce qui contredit l'hypothèse $D_x \neq D_y$. ∎

Reprenons les notations du théorème 4.3. Soit L la clôture galoisienne de $\mathbb{Q}(x, y)/\mathbb{Q}$. Considérons les groupes de Galois

$$G = \mathrm{Gal}(L/\mathbb{Q}(x + \varepsilon y)) \quad \text{et} \quad H = \mathrm{Gal}(L/\mathbb{Q}(x, y)).$$

Remarquons que

$$H = \{\sigma \in G\,;\, x^\sigma = x\} = \{\sigma \in G\,;\, y^\sigma = y\}.$$

On veut montrer que $G = H$, sauf si $\varepsilon = 1$ et $\Delta_x = \Delta_y$, auquel cas $[G : H] \leq 2$.

4.1.1 Discriminants égaux

Nous nous intéressons dans cette partie au cas $\Delta_x = \Delta_y = \Delta$. Pour tout $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\mathbb{Q}(x, y)^\sigma = \mathbb{Q}(x^\sigma, y^\sigma) \simeq \mathbb{Q}(x, y)$, de même que $\mathbb{Q}(x + \varepsilon y)^\sigma = \mathbb{Q}(x^\sigma + \varepsilon y^\sigma) \simeq \mathbb{Q}(x + \varepsilon y)$. Ainsi, quitte à conjuguer sur $\mathbb{Q}$, on peut supposer que x est dominant et que y ne l'est pas (puisque $x \neq y$ par hypothèse). D'après la proposition 2.31, il s'ensuit que

$$|x| \geq \mathrm{e}^{\pi|\Delta|^{1/2}} - 2079,$$
$$|y| \leq \mathrm{e}^{\pi|\Delta|^{1/2}/2} + 2079$$

d'où

$$|x + \varepsilon y| \geq \mathrm{e}^{\pi|\Delta|^{1/2}} - \mathrm{e}^{\pi|\Delta|^{1/2}/2} - 4158. \tag{4.1}$$

Le cas $\varepsilon = 1$

Considérons d'abord le cas $\varepsilon = 1$, et montrons que $[G : H] \leq 2$. Si $[G : H] > 2$, alors il existe $\sigma \in G$ tel que $x^\sigma \neq x$ et $x^\sigma \neq y$. Puisque $x + y = x^\sigma + y^\sigma$ par définition du groupe G, on a aussi $y^\sigma \neq x$. Ainsi, ni x^σ ni y^σ ne sont dominants, de sorte que

$$|x^\sigma|, |y^\sigma| \leq \mathrm{e}^{\pi|\Delta|^{1/2}/2} + 2079,$$

puis

$$|x + y| = |x^\sigma + y^\sigma| \leq 2\mathrm{e}^{\pi|\Delta|^{1/2}/2} + 4158. \tag{4.2}$$

En combinant (4.1) et (4.2), on obtient

$$\mathrm{e}^{\pi|\Delta|^{1/2}} - 3\mathrm{e}^{\pi|\Delta|^{1/2}/2} \leq 8316,$$

ce qui aboutit à $|\Delta| \leq 8$. Or, pour $|\Delta| \leq 8$, on a $h(\Delta) = 1$, et donc $G = H$ est le groupe trivial.

Le cas $\varepsilon = -1$

Considérons à présent le cas $\varepsilon = -1$, et montrons que $G = H$. Si $G \neq H$, alors il existe $\sigma \in G$ tel que $x^\sigma \neq x$. On a aussi $y^\sigma \neq x$, puisque dans le cas contraire, on aurait $2x = x^\sigma + y$, ce qui est impossible car x est dominant, mais x^σ et y ne le sont pas. Ainsi, comme précédemment, ni x^σ ni y^σ ne sont dominants, de sorte que l'inégalité (4.2) soit encore valide et aboutisse à nouveau à $|\Delta| \leq 8$ combinée à (4.1), soit $G = H$.

4.1.2 Discriminants fondamentaux égaux

Nous étudions dans cette partie le cas $D_x = D_y = D$ et $\Delta_x \neq \Delta_y$. Sans perte de généralité, supposons par exemple que $|\Delta_x| > |\Delta_y|$, et à nouveau que x est dominant. Notons f_x et f_y les conducteurs respectifs des discriminants Δ_x et Δ_y, c'est-à-dire $\Delta_x = f_x^2 D$ et $\Delta_y = f_y^2 D$.

Comme $|\Delta_x| > |\Delta_y|$, alors $f_x \geq f_y + 1$, donc

$$|\Delta_y|^{1/2} = |D|^{1/2} f_y \leq |D|^{1/2} f_x - |D|^{1/2} \leq |\Delta_x|^{1/2} - \sqrt{3}.$$

Ainsi,

$$|x| \geq \mathrm{e}^{\pi|\Delta_x|^{1/2}} - 2079,$$
$$|y| \leq \mathrm{e}^{\pi|\Delta_x|^{1/2} - \pi\sqrt{3}} + 2079 \leq 0.01\mathrm{e}^{\pi|\Delta_x|^{1/2}} + 2079$$

d'où

$$|x + \varepsilon y| \geq 0.99\mathrm{e}^{\pi|\Delta_x|^{1/2}} - 4158. \tag{4.3}$$

Si $G \neq H$, il existe $\sigma \in G$ tel que $x^\sigma \neq x$. En particulier, x^σ n'est pas dominant, et on a

$$|x^\sigma| \leq \mathrm{e}^{\pi|\Delta_x|^{1/2}/2} + 2079,$$
$$|y^\sigma| \leq \mathrm{e}^{\pi|\Delta_x|^{1/2} - \pi\sqrt{3}} + 2079 \leq 0.01\mathrm{e}^{\pi|\Delta_x|^{1/2}} + 2079,$$

puis

$$|x + \varepsilon y| = |x^\sigma + \varepsilon y^\sigma| \leq 0.01\mathrm{e}^{\pi|\Delta_x|^{1/2}} + \mathrm{e}^{\pi|\Delta_x|^{1}/2/2} + 4158. \tag{4.4}$$

En combinant (4.3) et (4.4), on obtient

$$0.98\mathrm{e}^{\pi|\Delta_x|^{1/2}} - \mathrm{e}^{\pi|\Delta_x|^{1/2}/2} \leq 8316,$$

ce qui aboutit à $|\Delta_x| \leq 8$, et donc $|\Delta_y| \leq 8$ également. En conséquence, $h(\Delta_x) = h(\Delta_y) = 1$, et le groupe $G = H$ est trivial.

4.1.3 Discriminants fondamentaux distincts

Pour terminer, il nous reste à considérer le cas $D_x \neq D_y$. Si $G \neq H$, il existe $\sigma \in G$ tel que $x^\sigma \neq x$. Pour un tel σ, on a $x - x^\sigma = \varepsilon(y^\sigma - y)$. En particulier, $\mathbb{Q}(x - x^\sigma) = \mathbb{Q}(y - y^\sigma)$. Or, conformément à ce que nous avons démontré en partie 4.1.1 pour $\varepsilon = -1$, on a $\mathbb{Q}(x - x^\sigma) = \mathbb{Q}(x, x^\sigma)$ et $\mathbb{Q}(y - y^\sigma) = \mathbb{Q}(y, y^\sigma)$, donc $\mathbb{Q}(x, x^\sigma) = \mathbb{Q}(y, y^\sigma)$. La proposition 4.4 implique alors que $\mathbb{Q}(x) = \mathbb{Q}(y)$. Les discriminants Δ_x et Δ_y figurent ainsi dans une même entrée du tableau 2.1 en vertu du corollaire 2.45, et le résultat peut être vérifié directement en PARI.

4.2 Produits de modules singuliers

Comme précédemment, en vue de démontrer le théorème 4.2, nous allons établir l'énoncé un peu plus général suivant.

Théorème 4.5. *Soient x, y deux modules singuliers distincts non nuls de discriminants respectifs Δ_x, Δ_y, et $\varepsilon \in \{1, -1\}$. Alors $\mathbb{Q}(xy^\varepsilon) = \mathbb{Q}(x, y)$, sauf si $\varepsilon = 1$ et $\Delta_x = \Delta_y$, auquel cas $[\mathbb{Q}(x, y) : \mathbb{Q}(xy)] \leq 2$.*

Reprenons les notations du théorème 4.5. Soit L la clôture galoisienne de $\mathbb{Q}(x, y)/\mathbb{Q}$. Considérons les groupes de Galois

$$G = \mathrm{Gal}(L/\mathbb{Q}(xy^\varepsilon)) \quad \text{et} \quad H = \mathrm{Gal}(L/\mathbb{Q}(x, y)).$$

Remarquons que

$$H = \{\sigma \in G\,;\, x^\sigma = x\} = \{\sigma \in G\,;\, y^\sigma = y\}.$$

On veut montrer que $G = H$, sauf si $\varepsilon = 1$ et $\Delta_x = \Delta_y$, auquel cas $[G : H] \leq 2$.

4.2.1 Discriminants égaux

Nous nous intéressons dans cette partie au cas $\Delta_x = \Delta_y = \Delta$. On peut supposer que x est dominant et que y ne l'est pas.

Le cas $\varepsilon = 1$

Considérons d'abord le cas $\varepsilon = 1$, et montrons que $[G : H] \leq 2$. D'une part,

$$|x| \geq \mathrm{e}^{\pi|\Delta|^{1/2}} - 2079,$$

et d'autre part, d'après la proposition 2.34 et (3.29),

$$|y| \geq \min\{4.4 \cdot 10^{-5},\, 3500|\Delta|^{-3}\},$$

si bien que

$$|xy| \geq 3000 \mathrm{e}^{\pi|\Delta|^{1/2}} \min\{10^{-8}, |\Delta|^{-3}\}. \tag{4.5}$$

Si $[G : H] > 2$, il existe $\sigma \in G$ tel que $x^\sigma \neq x$ et $x^\sigma \neq y$. Puisque $xy = x^\sigma y^\sigma$ par définition de G, on a aussi $y^\sigma \neq x$. Ainsi, ni x^σ ni y^σ ne sont dominants.

Distinguons deux possibilités. Si au moins l'un des deux modules singuliers x^σ ou y^σ n'est pas sous-dominant (voir (2.7)), alors on a

$$|xy| = |x^\sigma y^\sigma| \leq \left(\mathrm{e}^{\pi|\Delta|^{1/2}/2} + 2079\right)\left(\mathrm{e}^{\pi|\Delta|^{1/2}/3} + 2079\right), \tag{4.6}$$

ce qui aboutit à $|\Delta| \leq 395$ combiné à (4.5).

Supposons à présent que x^σ et y^σ sont tous les deux sous-dominants. Alors $\Delta \equiv 1 \bmod 8$, et $(x^\sigma, y^\sigma) = (j(\tau_{x^\sigma}), j(\tau_{y^\sigma}))$, avec

$$\{\tau_{x^\sigma}, \tau_{y^\sigma}\} = \left\{\frac{-1+\sqrt{\Delta}}{4}, \frac{1+\sqrt{\Delta}}{4}\right\}.$$

En particulier, $\tau_{x^\sigma} - \tau_{y^\sigma} = \pm 1/2$, ce qui implique que le point (x^σ, y^σ) appartienne à la courbe modulaire $Y_0(4)$. Puisque $Y_0(4)$ est définie sur $\mathbb{Q}$, (x, y) est également un point de cette courbe. Or, pour tout $\tau \in \mathbb{H}$,

$$\Phi_4(X, j(\tau)) = \left(X - j\left(\frac{\tau}{4}\right)\right)\left(X - j\left(\frac{\tau+1}{4}\right)\right)\left(X - j\left(\frac{\tau+2}{4}\right)\right) \times \left(X - j\left(\frac{\tau+3}{4}\right)\right)(X - j(4\tau))\left(X - j\left(\tau + \frac{1}{2}\right)\right).$$

Comme $x = j((1+\sqrt{\Delta})/2)$, on a donc $y = j((b+\sqrt{\Delta})/8)$ pour un certain entier b. Dans ce cas, on obtient une minoration plus fine que (4.5) :

$$|xy| \geq \left(\mathrm{e}^{\pi|\Delta|^{1/2}} - 2079\right)\left(\mathrm{e}^{\pi|\Delta|^{1/2}/4} - 2079\right). \tag{4.7}$$

On a également la majoration suivante :

$$|xy| = |x^\sigma y^\sigma| \leq \left(\mathrm{e}^{\pi|\Delta|^{1/2}/2} + 2079\right)^2. \tag{4.8}$$

En comparant les deux bornes données par (4.7) et (4.8), on en déduit que $|\Delta| \leq 94$.

Par conséquent, dans tous les cas, $|\Delta| \leq 395$, et la condition $[G : H] \leq 2$ peut être vérifiée par un calcul direct en PARI.

Le cas $\varepsilon = -1$

Considérons à présent le cas $\varepsilon = -1$, et montrons que $G = H$. Si $G \neq H$, il existe $\sigma \in G$ tel que $x^\sigma \neq x$. On a $xy^\sigma = x^\sigma y$, où x^σ et y sont tous les deux non dominants. Si x^σ ou y n'est pas sous-dominant, les bornes (4.5) et (4.6) restent valides en remplaçant $|xy|$ par $|x^\sigma y|$, et aboutissent à nouveau à $|\Delta| \leq 395$.

Si x^σ et y sont tous les deux sous-dominants, alors le point (x^σ, y) appartient à $Y_0(4)$, donc $(x, y^{\sigma^{-1}})$ également. On a $xy^{\sigma^{-1}} = x^{\sigma^{-1}} y$, où $x^{\sigma^{-1}}$ et y sont tous les deux non dominants. En reprenant les arguments précédents, $|xy^{\sigma^{-1}}|$ est minoré par le membre de droite de (4.7), tandis que $|x^{\sigma^{-1}}|$ est majoré par le membre de droite de (4.8), ce qui aboutit à $|\Delta| \leq 95$.

Dans tous les cas, $|\Delta| \leq 395$, et on vérifie en PARI que $G = H$.

4.2.2 Discriminants fondamentaux égaux

Nous étudions dans cette partie le cas $D_x = D_y = D$ et $\Delta_x \neq \Delta_y$. Sans perte de généralité, supposons par exemple que $|\Delta_x| > |\Delta_y|$, et à nouveau que x est dominant.

Supposons que $G \neq H$. Il existe alors $\sigma \in G$ tel que $x^\sigma \neq x$, ce qui implique aussi que $y^\sigma \neq y$. On a $x/x^\sigma = (y^\sigma/y)^\varepsilon$, et, en particulier, $\mathbb{Q}(x/x^\sigma) = \mathbb{Q}(y/y^\sigma)$. D'après ce que nous avons démontré en partie 4.2.1, on en déduit que $\mathbb{Q}(x, x^\sigma) = \mathbb{Q}(y, y^\sigma)$, puis $K(x, x^\sigma) = K(y, y^\sigma)$, où $K = K_x = K_y = \mathbb{Q}(\sqrt{D})$. Comme les extensions $K(x)/\mathbb{Q}$ et $K(y)/\mathbb{Q}$ sont galoisiennes, on obtient $K(x) = K(y)$. Finalement, d'après la proposition 2.46, soit $h(\Delta_x) = h(\Delta_y) = 1$, ce qui impossible étant donné que $G \neq H$, soit $\Delta_x = 4\Delta_y$.

Notons $\Delta = \Delta_y$. Rappelons que $\Delta \equiv 1 \bmod 8$ (cf. lemme 3.9), et en particulier qu'il n'y a pas de module singulier sous-dominant de discriminant 4Δ, donc que x^σ n'est pas sous-dominant.

On a

$$\begin{cases} xy = x^\sigma y^\sigma & \text{si } \varepsilon = 1, \\ xy^\sigma = x^\sigma y & \text{si } \varepsilon = -1. \end{cases}$$

Puisque x est dominant, $|xy|$ et $|xy^\sigma|$ sont tous les deux minorés de la manière suivante :

$$|xy|, |xy^\sigma| \geq 3000\mathrm{e}^{\pi|\Delta_x|^{1/2}} \min\{10^{-8}, |\Delta_y|\} = 3000\mathrm{e}^{2\pi|\Delta|^{1/2}} \min\{10^{-8}, |\Delta|\}. \tag{4.9}$$

Par ailleurs, puisque x^σ n'est ni dominant, ni sous-dominant, $|x^\sigma y^\sigma|$ et $|x^\sigma y|$ sont tous les deux majorés de la manière suivante :

$$|x^\sigma y^\sigma|, |x^\sigma y| \leq \left(\mathrm{e}^{\pi|\Delta_x|^{1/2}/3} + 2079\right)\left(\mathrm{e}^{\pi|\Delta_y|^{1/2}} + 2079\right) = \left(\mathrm{e}^{2\pi|\Delta|^{1/2}/3} + 2079\right)\left(\mathrm{e}^{\pi|\Delta|^{1/2}} + 2079\right). \tag{4.10}$$

Quel que soit ε, les bornes supérieure et inférieure données par (4.9) et (4.10) peuvent être comparées pour aboutir à $|\Delta| \leq 98$. La condition $G = H$ peut être vérifiée directement en PARI pour chacun des discriminants Δ restants.

4.2.3 Discriminants fondamentaux distincts

Pour terminer, il nous reste à considérer le cas $D_x \neq D_y$. Nous raisonnons de la même manière qu'en partie 4.1.3. Si $G \neq H$, il existe $\sigma \in G$ tel que $x^\sigma \neq x$. Pour un tel σ, on a $x/x^\sigma = (y^\sigma/y)^\varepsilon$. En particulier, $\mathbb{Q}(x/x^\sigma) = \mathbb{Q}(y/y^\sigma)$. Or, conformément à ce que nous avons démontré en partie 4.2.1, on a $\mathbb{Q}(x/x^\sigma) = \mathbb{Q}(x, x^\sigma)$ et $\mathbb{Q}(y/y^\sigma) = \mathbb{Q}(y, y^\sigma)$, donc $\mathbb{Q}(x, x^\sigma) = \mathbb{Q}(y, y^\sigma)$. Le corollaire 4.4 implique alors que $\mathbb{Q}(x) = \mathbb{Q}(y)$. Les discriminants Δ_x et Δ_y figurent ainsi dans une même entrée du tableau 2.1 en vertu du corollaire 2.45, et le résultat peut être vérifié directement en PARI.

Annexe A

Hauteur d'un nombre algébrique

L'objet de cette annexe est de rappeler succinctement la définition ainsi que quelques propriétés de la *hauteur* d'un nombre algébrique, qui intervient dans nos estimations de formes linéaires logarithmiques (cf. annexe C section C.3). Nous donnons de plus une estimation élémentaire de la hauteur d'un module singulier. Pour une introduction plus approfondie aux hauteurs, on pourra se référer par exemple à [Bom06].

Soit K un corps de nombres. Soit M_K l'ensemble des places de K. À chaque $v \in M_K$, on associe la valeur absolue $|\cdot|_v$ normalisée comme suit : pour $x \in K$ et $v|p$,

$$|x|_v = |N_{K_v/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}]},$$

où $|\cdot|_p$ est la valeur absolue ordinaire sur $\mathbb{Q}$ si $p = \infty$ et $|\cdot|_p$ est la valeur absolue p-adique sur $\mathbb{Q}$ (avec $|p|_p = 1/p$) si p est premier.

L'ensemble M_K ainsi construit satisfait la "formule du produit" :

Proposition A.1 ("formule du produit")**.** *Pour tout $x \in K \setminus \{0\}$,*

$$\prod_{v \in M_K} |x|_v = 1.$$

Démonstration. La "formule du produit" pour K se déduit essentiellement de celle pour $\mathbb{Q}$, qui elle-même découle directement de la décomposition de tout entier en produit de facteurs premiers. Voir [Bom06, Proposition 1.4.2 et Proposition 1.4.4] pour plus de précisions. ■

Définition A.2. Soit α un nombre algébrique non nul. La *hauteur logarithmique* (ou simplement *hauteur*) de α, notée $\mathrm{h}(\alpha)$, est la quantité

$$\mathrm{h}(\alpha) = \sum_{v \in M_K} \log \max\{1, |\alpha|_v\},$$

avec K n'importe quel corps de nombres contenant α.

La hauteur de α est indépendante du choix de K ; voir [Bom06, Lemma 1.5.2]. Par ailleurs, la hauteur est invariante sous l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

Proposition A.3. *Soit α un nombre algébrique non nul. Pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,*

$$\mathrm{h}(\alpha^\sigma) = \mathrm{h}(\alpha).$$

Démonstration. Voir [Bom06, Proposition 1.5.17]. ■

Plus précisément, la hauteur d'un nombre algébrique peut s'exprimer en fonction de ses conjugués sur $\mathbb{Q}$:

Proposition A.4. *Soit α un nombre algébrique non nul de degré d sur $\mathbb{Q}$, et soient $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \in \overline{\mathbb{Q}}$ ses conjugués distincts sur $\mathbb{Q}$. Alors*

$$\mathrm{h}(\alpha) = \frac{1}{d}\left(\log|a_d| + \sum_{k=1}^{d} \log\max\{1, |\alpha_k|\}\right),$$

où a_d est le coefficient dominant du polynôme minimal de α sur $\mathbb{Z}$. En particulier, lorsque α est un entier algébrique, alors

$$\mathrm{h}(\alpha) = \frac{1}{d}\sum_{k=1}^{d} \log\max\{1, |\alpha_k|\}. \tag{A.1}$$

Dans nos applications, la formule (A.1) est d'un intérêt pratique puisqu'elle permet de calculer numériquement la hauteur d'entiers algébriques donnés (en l'occurrence, de modules singuliers).

Voici quelques propriétés utiles de la hauteur :

Proposition A.5.

(i) *Pour tout nombre algébrique non nul α et tout $\lambda \in \mathbb{Q}$, on a $\mathrm{h}(\alpha^\lambda) = |\lambda|\mathrm{h}(\alpha)$. En particulier, $\mathrm{h}(1/\alpha) = \mathrm{h}(\alpha)$.*

(ii) *Pour tous nombres algébriques non nuls α, β, on a $\mathrm{h}(\alpha\beta) \leq \mathrm{h}(\alpha) + \mathrm{h}(\beta)$.*

Démonstration.

(i) Voir [Bom06, Lemma 1.5.18].

(ii) Résulte de l'inégalité

$$\max\{1, xy\} \leq \max\{1, x\}\max\{1, y\},$$

satisfaite pour tous nombres réels $x, y > 0$. ■

Pour terminer, nous allons estimer la hauteur d'un module singulier :

Proposition A.6. *Soit x un module singulier de discriminant Δ. On a*

$$\mathrm{h}(x) \leq \frac{9|\Delta|^{1/2}}{2}. \tag{A.2}$$

Démontrons tout d'abord le lemme suivant :

Lemme A.7. *Pour tout $\tau \in \mathcal{D}$, on a*

$$\log|j(\tau)| \leq 9\,\mathrm{Im}\,\tau.$$

Démonstration. Tout d'abord, en utilisant la proposition 2.31, on a

$$\log|j(\tau)| \leq \log\left(2079 + |q|^{-1}\right).$$

Puisque la fonction $x \longmapsto \log(2079 + x)/\log x$ est décroissante sur l'intervalle $[1, +\infty[$, et $|q|^{-1} = \mathrm{e}^{2\pi \operatorname{Im}\tau} \geq \mathrm{e}^{\pi\sqrt{3}}$, on obtient

$$\log\left(2079 + |q|^{-1}\right) \leq \log\left(|q|^{-1}\right) \frac{\log\left(2079 + \mathrm{e}^{\pi\sqrt{3}}\right)}{\pi\sqrt{3}} \leq 9 \operatorname{Im}\tau. \qquad \blacksquare$$

Démonstration de la proposition A.6. Notons h le degré de x. D'après la proposition 2.40, on a

$$\mathrm{h}(x) = \frac{1}{h} \sum_{(a,b,c)\in T_\Delta} \log\max\left\{1, \left|j\left(\frac{-b+\sqrt{\Delta}}{2a}\right)\right|\right\}.$$

En appliquant le lemme A.7, on déduit

$$\mathrm{h}(x) \leq \frac{9|\Delta|^{1/2}}{2h} \sum_{(a,b,c)\in T_\Delta} \frac{1}{a} \leq \frac{9|\Delta|^{1/2}}{2}. \qquad \blacksquare$$

Remarque A.8. L'estimation (A.2) n'est pas optimale, mais suffit amplement pour nos applications. Pour un contrôle plus précis de la hauteur d'un module singulier, on pourra consulter [Kuh13, Lemma 3].

Annexe B

Action de $\mathrm{SL}(2,\mathbb{Z})$ sur le demi-plan de Poincaré

Dans cette annexe, on rappelle la définition du *domaine fondamental standard* de l'action du groupe $\mathrm{SL}(2,\mathbb{Z})$ sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C}\,;\, \mathrm{Im}\, z > 0\}$, et on donne un algorithme permettant de déterminer si deux nombres imaginaires quadratiques $\tau, \tau' \in \mathbb{H}$ appartiennent à une même orbite.

Le groupe $\mathrm{SL}(2,\mathbb{Z})$ agit naturellement sur $\mathbb{H}$ par homographie : pour

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

et $\tau \in \mathbb{H}$, on pose

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

L'identité

$$\mathrm{Im}(\gamma \cdot \tau) = \mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}\,\tau}{|c\tau + d|^2} \tag{B.1}$$

garantit que $\gamma \cdot \tau \in \mathbb{H}$, et donc que l'action est bien définie. Par ailleurs, on identifie un élément $\gamma \in \mathrm{SL}(2,\mathbb{Z})$ avec la transformation $z \longmapsto (az + b)/(cz + d)$ de $\mathbb{H}$ qu'il induit.

Le *domaine fondamental standard* de l'action de $\mathrm{SL}(2,\mathbb{Z})$ sur $\mathbb{H}$, que l'on notera $\mathcal{D}$, est l'union du triangle hyperbolique ouvert de sommets

$$\zeta_3 = \mathrm{e}^{2i\pi/3}, \quad \zeta_6 = \mathrm{e}^{i\pi/3}, \quad \infty,$$

et des géodésiques reliant ζ_6 à i et à ∞ (voir figure B.1 ci-après).

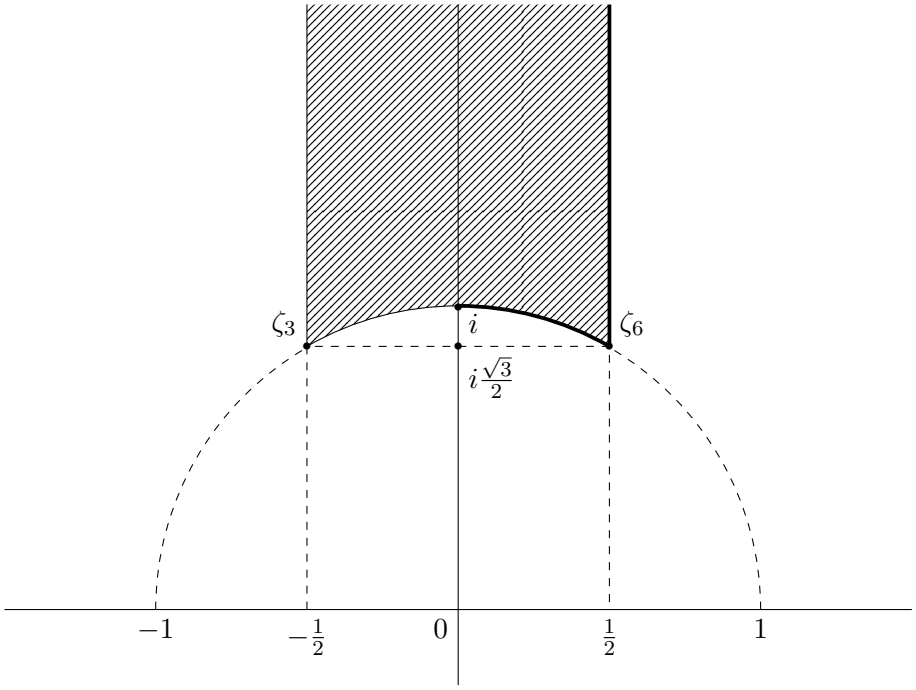


FIGURE B.1 – Domaine fondamental $\mathcal{D}$

Le domaine fondamental $\mathcal{D}$ porte son nom du fait que l'orbite de tout élément de $\mathbb{H}$ sous l'action de $\mathrm{SL}(2,\mathbb{Z})$ rencontre $\mathcal{D}$ en un unique point :

Proposition B.1. *Pour tout $\tau \in \mathbb{H}$, il existe un unique $\gamma \in \mathrm{PSL}(2,\mathbb{Z})$ tel que $\gamma \cdot \tau \in \mathcal{D}$.*

Démonstration. Fixons $\tau \in \mathbb{H}$. L'idée est d'exhiber un élément $\tau' \in \mathbb{H}$ de partie imaginaire maximale dans l'orbite de τ, puis de le translater à l'aide de la transformation $T : z \longmapsto z+1 \in \mathrm{SL}(2,\mathbb{Z})$ pour le ramener dans la bande $\{z \in \mathbb{H}\,;\, -1/2 < \mathrm{Re}(z) \leq 1/2\}$.

Pour ce faire, la relation (B.1) nous indique qu'il s'agit de minimiser la quantité $|c\tau + d|$ pour $(c,d) \in \mathbb{Z}^2$. Toutefois, le nombre de couples $(c,d) \in \mathbb{Z}^2$ tels que $|c\tau+d| \leq 1$ est fini : en effet, pour un tel couple, on a

$$|c| \operatorname{Im}\tau = |\mathrm{Im}(c\tau+d)| \leq |c\tau+d| \leq 1$$

d'où

$$|c| \leq \frac{1}{\operatorname{Im}\tau}$$
$$|d| \leq |c\tau+d| + |c\tau| \leq 1 + \frac{|\tau|}{\operatorname{Im}\tau}.$$

On en déduit qu'il existe $\gamma_0 \in \mathrm{SL}(2,\mathbb{Z})$ tel que $\mathrm{Im}(\gamma_0 \cdot \tau)$ soit maximal. Noter que le couple $(c,d) \in \mathbb{Z}^2$ retenu doit vérifier de plus $\mathrm{pgcd}(c,d) = 1$ pour pouvoir construire $a, b \in \mathbb{Z}$ tels que $ad - bc = 1$, et ainsi γ_0.

Posons $\tau' = \gamma_0 \cdot \tau$, ainsi que

$$N = \left\lfloor \frac{1}{2} - \operatorname{Re}\tau' \right\rfloor,$$

de sorte que

$$-\frac{1}{2} < \operatorname{Re}\tau' + N \leq \frac{1}{2}.$$

Posons alors $\tau'' = T^N \cdot \tau'$. Par construction,

$$-\frac{1}{2} < \operatorname{Re} \tau'' \leq \frac{1}{2}.$$

Vérifions que $|\tau''| \geq 1$. Si $|\tau''| < 1$, alors en appliquant la transformation $S : z \longmapsto -1/z \in \mathrm{SL}(2, \mathbb{Z})$, on aurait

$$\operatorname{Im}(S \cdot \tau'') = \frac{\operatorname{Im} \tau''}{|\tau''|^2} < \operatorname{Im} \tau'' = \operatorname{Im} \tau',$$

ce qui contredirait la maximalité de $\operatorname{Im} \tau'$. Pour terminer, si $\operatorname{Re} \tau'' < 0$ et $|\tau''| = 1$, on applique à nouveau la transformation S pour obtenir $S \cdot \tau'' \in \mathcal{D}$, sinon $\tau'' \in \mathcal{D}$. ■

La démonstration de la proposition B.1 suggère l'algorithme suivant pour déterminer l'unique représentant $\tau'' \in \mathcal{D}$ de l'orbite d'un nombre quadratique imaginaire $\tau \in \mathbb{H}$ sous l'action de $\mathrm{SL}(2, \mathbb{Z})$:

Données : Un nombre quadratique imaginaire $\tau \in \mathbb{H}$
Résultat : L'unique représentant $\tau'' \in \mathcal{D}$ de l'orbite de τ sous l'action de $\mathrm{SL}(2, \mathbb{Z})$
$(c, d) \leftarrow \max\{(c, d) \in \mathbb{Z}^2 \,;\, \operatorname{pgcd}(c, d) = 1,\ |c| \leq \lfloor 1/\operatorname{Im} \tau \rfloor,\ |d| \leq 1 + \lfloor |\tau|/\operatorname{Im} \tau \rfloor\}$;
Déterminer $(a, b) \in \mathbb{Z}^2$ tel que $ad - bc = 1$ par l'algorithme d'Euclide généralisé ;
$\tau' \leftarrow (a\tau + b)/(c\tau + d)$;
$\tau'' \leftarrow \tau' + \lfloor 1/2 - \operatorname{Re} \tau' \rfloor$;
si $\operatorname{Re} \tau'' < 0$ *et* $|\tau''| = 1$ **alors**
  retourner $-1/\tau''$;
sinon
  retourner τ''.
fin

Algorithme 4 : Calcul du représentant d'un nombre quadratique imaginaire dans le domaine fondamental

La proposition B.1 implique que pour que deux nombres quadratiques imaginaires $\tau, \tau' \in \mathbb{H}$ soient dans la même orbite sous l'action de $\mathrm{SL}(2, \mathbb{Z})$, il faut et il suffit que leurs représentants respectifs dans le domaine fondamental $\mathcal{D}$ coïncident. Il s'agit alors d'appliquer l'algorithme 4 à τ et à τ', et de comparer les éléments obtenus. On ajoutera que pour que τ et τ' soient dans la même orbite, il faut que $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$, condition nécessaire qui peut être vérifiée au préalable ; en outre, tous les calculs sont exacts dans le corps quadratique $K = \mathbb{Q}(\tau) = \mathbb{Q}(\tau')$.

Annexe C

Logarithmes réel et complexe, formes linéaires logarithmiques

Cette annexe est consacrée aux logarithmes réel et complexe, dont nous décrivons quelques propriétés élémentaires mais néanmoins utiles en sections C.1 et C.2, avant d'aborder les estimations des formes linéaires logarithmes en section C.3.

C.1 Une propriété utile du logarithme réel

Proposition C.1. *Pour tous nombres réels $x, A > 1$, on a*

$$x \log x \leq A \implies x \leq \left(1 + \frac{1}{\mathrm{e}}\right) \frac{A}{\log A}. \tag{C.1}$$

Démonstration. Nous allons plutôt démontrer la contraposée de (C.1) :

$$x > \left(1 + \frac{1}{\mathrm{e}}\right) \frac{A}{\log A} \implies x \log x > A.$$

Nous allons également expliquer comment est obtenue cette constante $1 + 1/\mathrm{e}$. Fixons un réel $C > 1$. Si $x > CA/\log A$, alors

$$x \log x > \frac{CA}{\log A}(\log C + \log A - \log\log A).$$

On voudrait que le terme de droite de cette inégalité soit $> A$, ce qui nous amène à considérer la fonction

$$f(A) = C(\log C + \log A - \log\log A) - \log A = (C-1)\log A - C\log\log A + C\log C$$

(après multiplication par $\log A/A$). Dérivons f pour en déduire ses variations :

$$f'(A) = \frac{C-1}{A} - \frac{C}{A\log A},$$

d'où

$$f'(A) > 0 \iff A > \exp\left(\frac{C}{C-1}\right).$$

Ainsi, f est décroissante sur l'intervalle $]1, \exp(C/(C-1))]$, et croissante sur l'intervalle $[\exp(C/(C-1)), +\infty[$, donc admet un minimum global sur l'intervalle $]1, +\infty[$ en $A_0 = \exp(C/(C-1))$. Calculons ce minimum :

$$f(A_0) = C - C\log\left(\frac{C}{C-1}\right) + C\log C = C(1 + \log(C-1)).$$

En choisissant enfin C de sorte que $f(A_0) = 0$, on obtient la constante désirée

$$C = 1 + \frac{1}{\mathrm{e}},$$

qui garantit que $f(A) \geq 0$, pour tout $A > 1$. La contraposée de (C.1) est par conséquent établie. ■

C.2 Logarithme complexe

L'objet de cette section est de définir les déterminations du logarithme complexe, plus particulièrement de rappeler la construction de la détermination principale, et d'en donner quelques propriétés.

C.2.1 Déterminations de l'argument et du logarithme

Dans toute cette partie, U désigne un ouvert connexe de $\mathbb{C}^*$.

Définition C.2.

- Une *détermination de l'argument* sur U est une application continue $\theta : U \longrightarrow \mathbb{R}$ telle que, pour tout $z \in U$,
$$\mathrm{e}^{i\theta(z)} = \frac{z}{|z|}.$$
- Une *détermination du logarithme* sur U est une application continue $l : U \longrightarrow \mathbb{C}$ telle que, pour tout $z \in U$,
$$\mathrm{e}^{l(z)} = z.$$

Ainsi, l est une détermination du logarithme sur U si et seulement si l'application $\theta : U \longrightarrow \mathbb{C}$ définie par

$$\theta(z) = \frac{l(z) - \log|z|}{i}$$

est une détermination de l'argument sur U. Cela permet d'établir un lien entre les déterminations de l'argument et du logarithme sur U. En outre, une détermination du logarithme sur U permet de toutes les obtenir :

Proposition C.3. *Soient l_1, l_2 deux déterminations du logarithme sur U. Alors il existe un entier $k \in \mathbb{Z}$ tel que $l_2 = l_1 + 2ik\pi$.*

Démonstration. Pour tout $z \in U$, $\mathrm{e}^{l_1(z)} = \mathrm{e}^{l_2(z)}$, donc il existe un entier $k(z) \in \mathbb{Z}$ tel que $l_2(z) = l_1(z) + 2ik(z)\pi$. Cela définit une application $k : U \longrightarrow \mathbb{C}$ continue sur U et à valeurs entières. Par connexité de U, elle est constante, d'où le résultat. ■

Les déterminations du logarithme sur U sont caractérisées par leur première dérivée :

Proposition C.4. *Soit $l : U \longrightarrow \mathbb{C}$ une application. Les assertions suivantes sont équivalentes :*

(i) *l est une détermination du logarithme sur U ;*

(ii) *l est holomorphe sur U, $l'(z) = 1/z$ pour tout $z \in U$, et il existe $a \in U$ tel que $\mathrm{e}^{l(a)} = a$.*

Démonstration.

(i) $\Longrightarrow$ (ii) Soit $z_0 \in U$. On pose $w_0 = l(z_0)$. Par continuité de l, on obtient

$$\begin{aligned}\lim_{z\to z_0} \frac{l(z) - l(z_0)}{z - z_0} &= \lim_{z\to z_0} \frac{l(z) - l(z_0)}{\mathrm{e}^{l(z)} - \mathrm{e}^{l(z_0)}} \\ &= \lim_{w\to w_0} \frac{w - w_0}{\mathrm{e}^{w} - \mathrm{e}^{w_0}} \\ &= \frac{1}{\mathrm{e}^{w_0}} = \frac{1}{z_0}.\end{aligned}$$

On en déduit que l est dérivable en z_0, de dérivée $l'(z_0) = 1/z_0$, puis que l est holomorphe sur U.

(ii) $\Longrightarrow$ (i) Lapplication $f : U \longrightarrow \mathbb{C}$ définie par

$$f(z) = z\mathrm{e}^{-l(z)}$$

est holomorphe sur U, de dérivée nulle. Elle est donc constante sur U par connexité de U. En outre, $f(a) = 1$, d'où l'on déduit que

$$\mathrm{e}^{l(z)} = z, \quad \forall z \in U,$$

c'est-à-dire que l est une détermination du logarithme sur U.

■

Enfin, l'existence d'une détermination du logarithme sur U impose des restrictions sur U. En effet :

Proposition C.5. *Il n'existe pas de détermination du logarithme sur $\mathbb{C}^*$.*

Démonstration. Supposons qu'il existe une détermination $l : \mathbb{C}^* \longrightarrow \mathbb{C}$ du logarithme sur $\mathbb{C}^*$. Pour tout $t \in \mathbb{R}$, on a

$$\mathrm{e}^{l(\mathrm{e}^{it})} = \mathrm{e}^{it},$$

donc il existe un entier $k(t)$ tel que $l(\mathrm{e}^{it}) = it + 2ik(t)\pi$. À nouveau, cela définit une application $k : \mathbb{R} \longrightarrow \mathbb{C}$ continue sur $\mathbb{R}$ et à valeurs entières. Par connexité de $\mathbb{R}$, elle est constante, ce qui est en contradiction avec le fait que l'application $t \longmapsto l(\mathrm{e}^{it})$ est 2π-périodique. ■

C.2.2 Déterminations principales de l'argument et du logarithme

Nous avons vu qu'il n'existe pas de détermination du logarithme sur $\mathbb{C}^*$ (et donc pas non plus de détermination de l'argument sur $\mathbb{C}^*$). Toutefois, il est possible de construire une détermination du logarithme sur $\mathbb{C}$ privé d'une demi-droite passant par l'origine. Nous allons procéder à cette construction sur $\mathbb{C} \setminus \mathbb{R}^-$, afin d'obtenir la *détermination principale du logarithme*.

Définition C.6. L'application $\arg : \mathbb{C} \setminus \mathbb{R}^- \longrightarrow]-\pi, \pi[$ définie par

$$\arg(z) = \begin{cases} \arccos\left(\frac{\operatorname{Re} z}{|z|}\right) & \text{si } \operatorname{Im} z > 0, \\ 0 & \text{si } \operatorname{Im} z = 0, \\ -\arccos\left(\frac{\operatorname{Re} z}{|z|}\right) & \text{si } \operatorname{Im} z < 0, \end{cases}$$

est une détermination de l'argument sur $\mathbb{C} \setminus \mathbb{R}^-$, appelée *détermination principale de l'argument*.

On appelle alors *détermination principale du logarithme* l'application $\log : \mathbb{C} \setminus \mathbb{R}^- \longrightarrow \mathbb{C}$ définie par

$$\log(z) = \log|z| + i \arg(z).$$

Pour que la définition ci-dessus soit valide, il faut s'assurer que arg est bien une détermination de l'argument sur $\mathbb{C} \setminus \mathbb{R}^-$, c'est-à-dire qu'elle est continue et que pour tout $z \in \mathbb{C} \setminus \mathbb{R}^-$,

$$\mathrm{e}^{i \arg(z)} = \frac{z}{|z|},$$

ce qui ne soulève pas de difficulté particulière.

L'application $\log : \mathbb{C} \setminus \mathbb{R}^- \longrightarrow \mathbb{C}$ prolonge ainsi la fonction logarithme réelle usuelle définie sur $\mathbb{R}^+$. Par ailleurs, d'après la proposition C.3, les autres déterminations du logarithme sur $\mathbb{C} \setminus \mathbb{R}^-$ sont de la forme $\log + 2ik\pi$, avec $k \in \mathbb{Z}$.

Remarquons enfin que pour tout $z \in \mathbb{C} \setminus \mathbb{R}^-$,

$$|\operatorname{Im}(\log(z))| < \pi, \tag{C.2}$$

et plus précisément que log réalise un biholomorphisme de $\mathbb{C} \setminus \mathbb{R}-$ dans la bande $\{z \in \mathbb{C}\,;\, |\operatorname{Im} z| < \pi\}$, d'inverse l'exponentielle.

Voyons comment s'étend la propriété de transformation d'un produit en somme du logarithme réel au logarithme complexe.

Proposition C.7. *Soient $\alpha, \beta \in \mathbb{C} \setminus \mathbb{R}^-$, et $m, n \in \mathbb{Z}$ tels que $\alpha^m \beta^n \notin \mathbb{R}^-$. Alors*

$$\log(\alpha^m \beta^n) = m \log(\alpha) + n \log(\beta) + 2ik\pi,$$

où $k \in \mathbb{Z}$ est un entier satisfaisant $|2k| \leq m + n$.

Démonstration. Il est clair que

$$\mathrm{e}^{\log(\alpha^m \beta^n)} = \mathrm{e}^{m \log(\alpha) + n \log(\beta)} = \alpha^m \beta^n,$$

donc qu'il existe un entier $k \in \mathbb{Z}$ tel que $\log(\alpha^m \beta^n) = m \log(\alpha) + n \log(\beta) + 2ik\pi$. D'après (C.2), k est l'unique entier tel que

$$|m \operatorname{Im}(\log(\alpha)) + n \operatorname{Im}(\log(\beta)) + 2k\pi| < \pi.$$

Comme $|\operatorname{Im}(\log(\alpha))| < \pi$ et $|\operatorname{Im}(\log(\beta))| < \pi$ également, cette inégalité implique que $|2k| < m + n + 1$, soit $|2k| \leq m + n$. ∎

Mentionnons enfin une propriété utile d'accroissements du logarithme complexe.

Proposition C.8. *Pour tous $z \in \mathbb{C} \setminus \mathbb{R}^-$ et $M \in]0,1[$,*

$$|z-1| \leq M \implies |\log z| \leq \frac{|z-1|}{1-M}, \tag{C.3}$$

$$|z+1| \leq M \implies |\log z - i\pi| \leq \frac{|z+1|}{1-M}. \tag{C.4}$$

Démonstration. Démontrons l'implication (C.3), l'autre implication (C.4) se traitant de manière similaire. Il s'agit d'une simple application du théorème des accroissements finis à l'application log : si $|z-1| \leq M$, alors

$$|\log z| \leq \max_{z \in D(1,M)} \left|\frac{1}{z}\right| \cdot |z-1|.$$

Or, la valeur maximale de $|1/z|$ sur le disque $D(1,M)$ est obtenue en $z = 1-M$, d'où

$$|\log z| \leq \frac{|z-1|}{1-M}.$$

■

C.3 Formes linéaires logarithmiques

Une *forme linéaire logarithmique* en des nombres algébriques non nuls $\alpha_1, \ldots, \alpha_r$ est une expression de la forme

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_r \log \alpha_r,$$

où $b_1, \ldots, b_r \in \mathbb{Z}$, et chaque $\log \alpha_i$, $i \in \{1, \ldots, r\}$, est une valeur du logarithme de α_i pour une détermination arbitraire (pas forcément principale).

Les premiers résultats d'estimations de formes linéaires logarithmiques sont dûs à Baker dans les années 1960, qui résout alors la conjecture de Gelfond ; voir [Bak67] et [Bak69]. Ses estimations sont effectives, néanmoins pas assez fines pour nos applications. Plus tard, en 2000, Matveev [Mat00] établit de meilleures estimations. Nous reproduisons ci-dessous l'énoncé de son résultat [Mat00, Corollary 2.3] que nous utilisons en pratique :

Théorème C.9 (Matveev)**.** *Supposons que $\Lambda \neq 0$. Soient $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}]$, $H = \max\{|b_1|, \ldots, |b_r|\}$, et $A_1, \ldots, A_r$ des nombres réels tels que*

$$A_j \geq \max\{\mathrm{h}(\alpha_j), |\log \alpha_j|/d, 0.16/d\}, \quad j \in \{1, \ldots, r\}.$$

Alors

$$\log |\Lambda| > -C(r) d^{2+r} A_1 \cdots A_r \log(\mathrm{e}d) \log(\mathrm{e}H),$$

où

$$C(r) = \min\left\{ \frac{1}{\chi} \left(\frac{1}{2}\mathrm{e}r\right)^{\chi} 30^{r+3} r^{3.5}, 2^{6r+20} \right\},$$

avec $\chi = 1$ si $\mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subset \mathbb{R}$, $\chi = 2$ sinon.

Dans le cas particulier des formes linéaires en deux logarithmiques (c'est-à-dire avec seulement deux nombres algébriques α_1, α_2), Laurent, Mignotte et Nesterenko obtiennent des estimations encore plus fines, voir [Lau95] et [Lau08]. Mignotte en donne une variante, voir [Bil01, Theorem A.1.2 et Theorem A.1.3], que nous adaptons pour nos besoins en un énoncé plus compact et plus aisé à mettre en œuvre :

Théorème C.10. *Soient α un nombre algébrique tel que $|\alpha| = 1$ mais qui n'est pas une racine de l'unité, et $m > 1$ un entier. Alors il existe une constante effective $c_1(\alpha)$, dépendant uniquement du degré d de α sur $\mathbb{Q}$ et de sa hauteur logarithmique $\mathrm{h}(\alpha)$, telle que*

$$|1 - \alpha^m| > 0.99\mathrm{e}^{-c_1(\alpha)(\log m)^2}.$$

Démonstration. On applique [Bil01, Theorem A.1.2 et Theorem A.1.3] à la forme linéaire logarithmique

$$\Lambda = 2i\pi - m \log \alpha,$$

où l'on choisit la détermination principale du logarithme pour $\log \alpha$. On a

$$\log |\Lambda| > -(9.03\mathcal{H}^2 + 0.23)(D\mathrm{h}(\alpha) + 25.84) - 2\mathcal{H} - 2\log \mathcal{H} - 0.7D + 2.07,$$

où $D = d/2$ et $\mathcal{H} = D(\log m - 0.96) + 4.49 \leq c_1'(d) \log m$ pour $m \geq 13$, avec

$$c_1'(d) = D + \max\left\{0, \frac{4.49 - 0.96D}{\log 13}\right\} > 0.$$

Ainsi,

$$\log |\Lambda| > -(\log m)^2 \left(9.03c_1'(d)^2(D\mathrm{h}(\alpha) + 25.84) + \frac{2c_1'(d)}{\log m} + \frac{2\log\log m}{(\log m)^2} + \frac{0.23(D\mathrm{h}(\alpha) + 25.84) + 2\log c_1'(d) + 0.7D - 2.07}{(\log m)^2}\right) > -c_1(\alpha)(\log m)^2,$$

avec

$$c_1(\alpha) = 9.03c_1'(d)^2(D\mathrm{h}(\alpha) + 25.84) + \frac{2c_1'(d)}{\log 13} + \frac{2\log\log 13}{(\log 13)^2} + \frac{0.23(D\mathrm{h}(\alpha) + 25.84) + 2\log c_1'(d) + 0.7D - 2.07}{(\log 13)^2}.$$

Il s'ensuit que

$$|1 - \alpha^m| > \frac{\mathrm{e}^{-c_1(\alpha)(\log m)^2}}{1 + \mathrm{e}^{-c_1(\alpha)(\log m)^2}} > 0.99\mathrm{e}^{-c_1(\alpha)(\log m)^2},$$

en conséquence du théorème des accroissements finis. ∎

Il existe également des résultats d'estimations de formes linéaires logarithmiques en p-adique ; parmi les références disponibles à ce sujet, on pourra citer [Poo76]. Ces estimations ne nous sont néanmoins pas indispensables pour nos travaux, et l'on se contentera de la proposition suivante :

Proposition C.11. *Soient α un nombre algébrique qui n'est pas une racine de l'unité d'un corps de nombres L de degré d, et $m > 0$ un entier. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_L$ au-dessus d'un nombre premier p. Supposons que $\mathfrak{p} \nmid \alpha\mathcal{O}_L$. Notons $m_0 \geq 1$ l'ordre de α dans $\mathcal{O}_L/\mathfrak{p}$, c'est-à-dire le plus petit entier naturel non nul tel que $1 - \alpha^{m_0} \equiv 0 \bmod \mathfrak{p}$, et $v_0 = v_\mathfrak{p}(1 - \alpha^{m_0})$. Alors, sous l'hypothèse que $p > d + 1$, on a*

$$v_\mathfrak{p}(1 - \alpha^m) = \begin{cases} 0 & \text{si } m_0 \nmid m \\ sv_\mathfrak{p}(p) + v_0 & \text{si } m = m_0 p^s r,\ \mathrm{pgcd}(p, r) = 1. \end{cases}$$

Démonstration. Si $m_0 \nmid m$, il est clair que $1 - \alpha^m \not\equiv 0 \bmod \mathfrak{p}$, donc $v_\mathfrak{p}(1-\alpha^m) = 0$ dans ce cas. Sinon, écrivons $m = m_0 p^s r$, avec $\mathrm{pgcd}(p, r) = 1$. Nous allons procéder par récurrence sur $s \geq 0$.

- Pour $s = 0$, on factorise $1 - \alpha^{m_0 r}$ de la manière suivante :

$$1 - \alpha^{m_0 r} = (1 - \alpha^{m_0}) \left(\sum_{k=0}^{r-1} \alpha^{m_0 k} \right).$$

  Puisque $\alpha^{m_0 k} \equiv 1 \bmod \mathfrak{p}$, pour tout $k \in \{0, \ldots, r-1\}$, on observe que

$$\sum_{k=0}^{r-1} \alpha^{m_0 k} \equiv r \bmod \mathfrak{p} \not\equiv 0 \bmod \mathfrak{p},$$

  et on en déduit que

$$v_\mathfrak{p}(1 - \alpha^{m_0 r}) = v_\mathfrak{p}(1 - \alpha^{m_0}) = v_0.$$

- Supposons à présent la propriété vraie à un rang $s \geq 0$. Posons $\beta = \alpha^{m_0 p^s r}$, et écrivons $\beta = 1 + \lambda$, où $\lambda \in \mathfrak{p}$. On a

$$\frac{\beta^p - 1}{\beta - 1} = \frac{(1+\lambda)^p - 1}{\lambda} = \lambda^{p-1} + p + \sum_{k=2}^{p-1} \binom{p}{k} \lambda^{k-1}.$$

  D'une part, pour tout $k \in \{2, \ldots, p-1\}$,

$$v_\mathfrak{p}\left(\binom{p}{k} \lambda^{k-1} \right) = v_\mathfrak{p}(p) + (k-1) v_\mathfrak{p}(\lambda) > v_\mathfrak{p}(p).$$

  D'autre part, $v_\mathfrak{p}(\lambda^{p-1}) = (p-1) v_\mathfrak{p}(\lambda) \geq p - 1 > d \geq v_\mathfrak{p}(p)$. On en déduit que

$$v_\mathfrak{p}\left(\frac{\beta^p - 1}{\beta - 1} \right) = v_\mathfrak{p}(p),$$

  soit, par hypothèse de récurrence,

$$v_\mathfrak{p}(1 - \alpha^{m_0 p^{s+1} r}) = v_\mathfrak{p}(1 - \alpha^{m_0 p^s r}) + v_\mathfrak{p}(p) = (s+1) v_\mathfrak{p}(p) + v_0.$$

En conclusion, la relation est démontrée. ■

Annexe D

Scripts PARI

L'intégralité de nos scripts PARI utilisés pour les démonstrations des théorèmes 3.5, 3.6, 4.3 et 4.5, est retranscrite dans cette dernière annexe. Les fichiers sources sont disponibles auprès de l'auteur.

D.1 Fonctions auxiliaires

```
quadredtrip(D) =
/* computes the set T_D of the triples (a, b, c) corresponding
 * to the reduced binary forms ax^2 + bxy + cy^2 of discriminant
 * D < 0, b >= 0 */
{
  my (TD = List());
  forstep (b = D % 2, floor(sqrt(-D/3)), 2,
    my (ac = (b^2-D) / 4);
    fordiv (ac, a,
      my(c = ac / a);
      if (a > c, break);
      if (b > a || gcd([a,b,c]) != 1, next);
      listput(TD, [a,b,c]);
      if (b != a && b && a != c, listput(TD, [a,-b,c]));
    );
  );
  listsort(TD); return(TD);
}

elljevaltrip(D, T) = my ([a,b] = T); abs( ellj((-b + sqrt(D)) / (2*a)) );

nfeval(nf, x) = abs(nfeltembed(nf, x, 1));

isOpm1(x) = x == 0 || x == 1 || x == -1;

algnumdegree(L, G, x) =
/* computes the degree over Q of an algebraic number x belonging to a number
 * field L, with given Galois group G=Gal(L/Q); L/Q must be a Galois
 * extension */
```

```
{
  my(stab = 0);
  for(i = 1, #G,
    if(nfgaloisapply(L, G[i], x) == x, stab++);
  );
  return(#G / stab);
}
```

D.2 Démonstration du théorème 3.5

D.2.1 Le cas $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$

```
modcurve(T1, T2, D) =
/* given two triples T1 and T2 of the respective sets T_{4D} and
 * T_D, checks if the corresponding CM-point (j(t1), j(t2))
 * belongs to the modular curve Y_0(2) */
{
  my ([a1,b1] = T1, [a2,b2] = T2, w = quadgen(D));
  my(u1 = -b1 / (2*a1), v1 = 1 / a1, t1 = u1 - v1 + 2*v1*w);
  my(u2 = -b2 / (2*a2), v2 = 1 / (2*a2), t2 = u2 - v2 + 2*v2*w);
  is0pm1(t1 - 2*t2)
     || is0pm1(2*t1 - t2)
     || is0pm1(t1 + 2 / t2)
     || is0pm1(t1 + 2 / (t2+1))
     || is0pm1(t1 + 1 / ((t2+1)/2 - 1));
}

conjcm(D) =
/* returns the full list of the conjugates of (j(t1), j(t2)),
 * where j(t1) and j(t2) are the dominant j-values of respective
 * discriminants 4D and D, keeping only one conjugate for each
 * pair of complex conjugates */
{
  my(TD1 = quadredtrip(4*D), TD2 = quadredtrip(D), C = List());
  for (i = 1, #TD1,
    my(j = 1, T = TD1[i], U);
    if (T[2] < 0, next);
    until(modcurve(T, U, D), U = TD2[j]; j++);
    listput(C, [elljevaltrip(4*D,T), elljevaltrip(D,U), T, U]);
  );
  return(C);
}

boundmn(C, i, j) =
/* given the set C of conjugates of (j(tau), j(tau')), computes
 * an interval for m / n given by c,d such that |m/n - c| < d;
 * with respect to the collinearity of the points C[1], C[i] and
 * C[j], where m and n are positive integers such that 1,
```

```
 * j(tau)^m and j(tau')^n are linearly dependent */
{
  my(M, b);
  my([a1,b1] = C[1], [ai,bi] = C[i], [aj,bj] = C[j]);
  if (bi > bj,
    M = (bj/bi + aj/a1 + bj/b1 + aj/ai) / (1 - bj/bi - aj/a1);
    b = bi;
 ,
    M = (aj/ai * (1 + bi/b1) + bi/bj + ai/a1) / (1 - bi/bj - ai/a1);
    b = bj;
  );
  return([log(b1/b)/log(a1/ai), M / ((1-M) * log(a1/ai))]);
}

checkbounds(C) =
/* computes all bounds on m / n for the set of conjugates of
 * (j(tau), j(tau')), where j(tau) and j(tau') are the dominant
 * j-values of respective discriminants 4* D and D, with respect
 * to the previous function boundmn, and checks if two bounds
 * are contradicting each other. In this case, the discriminant
 * D can be eliminated */
{
  my(B = List());
  for(i = 2, #C - 1,
    for(j = i + 1, #C, listput(B, boundmn(C, i, j)));
  );
  for(i = 1, #B - 1,
    my([ci,di] = B[i]);
    for(j = i + 1, #B,
      my([cj,dj] = B[j]);
      if (abs(ci-cj) > di+dj, return(1));
    );
  );
  return(0);
}

approx(alpha, c4,c6,c7) =
{
  my (N = ceil(log(c6)/log((1+sqrt(5))/2)));
  my (pq = contfracpnqn(contfrac(alpha), N));
  for (i = 2, #pq,
    my ([p,q] = pq[,i]);
    if (log(abs(alpha * q - p)) <=  c7 + q * c4, return (0));
    if (q > c6, break)
  );
  return(1);
}

/* C = conjcm(D) */
```

```
checklogform(C, D) =
{
  if (D == -23 || D == -31, return (1)); /* two unsolved cases */
  my(h, a, b, M, c1, c3, c4, c5, c6);
  my ([J1,j1, T1,t1] = C[1]);
  my ([J2,j2, T2,t2] = C[2]);
  my ([J3,j3, T3,t3] = C[3]);
  h = qfbclassno(D);
  a = J1 / J2;
  if (j2 > j3,
    b = j1/j2;
    M = (j3/j2 + J3/J1 + j3/j1 + J3/J2) / (1 - j3/j2 - J3/J1)
  ,
    b = j1/j3;
    M = (J3/J2 * (1+j2/j1) + j2/j3 + J2/J1) / (1 - j2/j3 - J2/J1);
  );
  c1 = (-M + (1-M) * log(b)) / ((1-M) * log(a));
  if (j2 > j3,
    c3 = 4 / (1 - j3/j2 - J3/J1);
    c4 = log( max(j3/j2, (J3/J2)^c1) )
  ,
    c3 = 4 / (1 - j2/j3 - J2/J1);
    c4 = log( vecmax([(J3/J2)^c1, j2/j3, (J2/J1)^c1]) );
  );
  c5 = (-2^(6*3+20)*10*19*(2*h)^5 * abs(D) * log(2*exp(1)*h)
       - log(c3/(1-M))) / c4;
  c6 = floor((1 + exp(-1)) * c5 * log(3 * (1 + exp(1)) * c5));

  if (1, \\ block for localbitprec, high accuracy
    localbitprec(floor(log(c6)/log(2)) + 64);
    a = log(elljevaltrip(4*D, T1) / elljevaltrip(4*D, T2));
    b = log(elljevaltrip(D, t1) /
            elljevaltrip(D, if (j2>j3, t2,t3)));
  );
  my (c7 = log(c3 / (a*(1 - M))));
  return (approx(b/a, c4,c6,c7));
}

checkDall() =
/* apply checkbounds(D) on all remaining discriminants |D| <
 * 1024, and prints the list of discriminants that cannot be
 * eliminated this way */
{
  forstep(D = -1023, -1, 8,
    if (qfbclassno(D) < 3, next);
    my (C = conjcm(D));
    if (!checkbounds(C) && !checklogform(C,D), error(D));
  );
}
```

D.2.2 Le cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

```
conjcmbis(D1, D2) =
/* returns the full list of the conjugates of (j(t1), j(t2)),
 * where j(t1) and j(t2) are the dominant j-values of respective
 * discriminants D1 and D2, D1 and D2 belonging to a common
 * entry of Table 2.1 with [L : Q] >= 4 */

{
  my(C, H1 = polclass(D1,0,'X), H2 = polclass(D2,0,'X));
  my (L = nfinit(polredbest(subst(H1, X, Y))));
  my (k0, x = nfroots(L, H1), x0 = apply(u -> nfeval(L,u), x));
  my (l0, y = nfroots(L, H2), y0 = apply(u -> nfeval(L,u), y));
  vecmax(x0, &k0);
  vecmax(y0, &l0);
  C = apply(s ->
    my(a = nfgaloisapply(L, s, x[k0]));
    my(b = nfgaloisapply(L, s, y[l0]));
    [nfeval(L,a), nfeval(L,b), a, b], nfgaloisconj(L));
  return([L, vecsort(C, (a,b)->sign(b[1]-a[1]))]);
}

checklogformbis(pair) =
{
  my ([D1,D2] = pair);
  my([L,C] = conjcmbis(D1,D2), h, a, b, M, c1, c3, c4, c5, c6, c7, c8 = 0);
  my([J1,j1, T1,t1] = C[1]);
  my([J2,j2, T2,t2] = C[2]);
  my([J3,j3, T3,t3] = C[3]);

  my( t, p0 = 0, p1 = 1, q0 = 1, q1 = 0, p_aux, q_aux, i = 2);
  h = qfbclassno(D1);
  a = J1 / J2;
  if(j2 > j3,
    b = j1/j2;
    M = (j3/j2 + J3/J1 + j3/j1 + J3/J2) / (1 - j3/j2 - J3/J1),
    b = j1 / j3;
    M = (J3/J2 * (1+j2/j1) + j2/j3 + J2/J1) / (1 - j2/j3 - J2/J1);
  );
  c1 = (-M + (1 - M) * log(b)) / ((1 - M) * log(a));
  if(j2 > j3,
    c3 = 4 / (1 - j3/j2 - J3/J1);
    c4 = log( max(j3 / j2, (J3/J2)^c1) )
  ,
    c3 = 4 / (1 - j2/j3 - J2/J1);
    c4 = log( vecmax([(J3/J2)^c1, j2/j3, (J2/J1)^c1]) );
  );
```

```
  c5 = (- 2748779069440 * h^5 * abs(D1*D2)^(1/2) * log(exp(1) * h)
       - log(c3 / (1 - M))) / c4;
  c6 = floor((1 + exp(-1)) * c5 * log(3 * (1 + exp(1)) * c5));

  if (1, \\ block for localbitprec, high accuracy
    localbitprec(floor(log(c6)/log(2)) + 64);
    a = log(nfeval(L,T1) / nfeval(L,T2));
    b = log(nfeval(L,t1) / nfeval(L, if(j2>j3, t2,t3)));
  );
  my (c7 = log(c3 / (a*(1-M))));
  return (approx(b/a, c4,c6,c7));
}

checklogformall() =
/* checks if checklogformbis(D1, D2) = 1, for each pair of
 * discriminants {D1, D2} given by a common entry of Table 2.1
 * with [L : Q] >= 4 */
{
  localprec(50);
  my(LD = [[-96,-192], [-96,-288], [-192,-288], [-180,-240], [-195,-520],
  [-195,-715], [-520,-715], [-120,-160], [-120,-280], [-120,-760], [-160,-280],
  [-160,-760], [-280,-760], [-340,-595], [-480,-960]]);
  for(k = 1, #LD,
    if (!checklogformbis(LD[k]), error(LD[k]));
  );
}
```

D.3 Démonstration du théorème 3.6

```
multind(L, x, y) =
/* checks if the algebraic numbers x and y of the number field L
 * are multiplicatively independent or not. x and y are two
 * algebraic numbers of modulus <> 1 */
{
  my (p, fa, f, k, l, u0, u, v);
  fa = idealfactor(L, idealadd(L,x,y));
  if (!fa,
    if (idealhnf(L,x) != 1 || idealhnf(L,y) != 1, return (1));
    error("unit case, not handled");
  );
  p = fa[1,1];
  f = idealval(L, y, p) / idealval(L, x, p);
  k = numerator(f);
  l = denominator(f);
  x = nfbasistoalg(L,x);
  y = nfbasistoalg(L,y); v = x^k / y^l;
  u0 = nfbasistoalg(L, nfrootsof1(L)[2]);
  u = u0;
```

```
  while(u <> 1 && u <> v, u *= u0);
  return(u == 1);
}

elimmultind(pair) =
/* checks if j(tau)^m * j(tau')^n is not rational, for any
 * singular moduli j(tau) and j(tau') of respective
 * discriminants D1 and D2, and for any integers m, n <> 0 */
{
  my ([D1,D2] = pair);
  my (H1 = polclass(D1,0,'y), H2 = polclass(D2,0,'y), L, x, y);
  print(pair);
  if (quaddisc(D1)==quaddisc(D2),
    L = subst(rnfequation(polredbest(H1), 'x^2-D1), 'x,'y)
  , L = H1);
  L = nfinit(polredbest(L));
  x = nfroots(L, subst(H1,'y,'x));
  y = nfroots(L, subst(H2,'y,'x));
  if (#y < #x, return(1));
  /* Gx[i] = sigma_i . x */
  my (G = nfgaloisconj(L));
  Gx = [ apply(t->nfgaloisapply(L,s,t),x) | s <- G ];
  for (i = if (D1<>D2, 1, 2), #x,
    my(k = 1);
    while (k <= #G,
      my (sx = Gx[k]);
      if (sx[1] != x[1] &&
          (D1<>D2 || [sx[i],sx[1]] <> [x[1],x[i]]), break);
      k++;
    );
    if (k > #G || !multind(L, x[1] / Gx[k][1],
                              nfgaloisapply(L, G[k], y[i]) / y[i]),
      return(0);
    );
  );
  return(1);
}

elimmultindall() =
/* checks if elimmultind(D1, D2) = 1, for each remaining pair
 * {D1, D2} */
{
  my(LD2 = List(), LD);
  LD = List([[-71,-71], [-95,-95], [-96,-96],
  [-96,-192],  [-96,-288],  [-192,-192], [-192,-288], [-288,-288],
  [-180,-180], [-180,-240], [-240,-240], [-195,-195], [-195,-520],
  [-195,-715], [-520,-520], [-520,-715], [-715,-715], [-120,-120],
  [-120,-160], [-120,-280], [-120,-760], [-160,-160], [-160,-280],
  [-160,-760], [-280,-280], [-280,-760], [-760,-760], [-340,-340],
```

```
  [-340,-595], [-595,-595], [-480,-480], [-480,-960], [-960,-960]
  ]);
  for (D = -427, -1,
    if (D%4 <= 1 && qfbclassno(D) == 2, listput(LD2, D));
  );
  for (k = 1, #LD2-1,
    for (l = k+1, #LD2, listput(LD, [LD2[k], LD2[l]]));
  );
  forstep (D = -255, -1, 8,
    if (qfbclassno(D) >= 3, listput(LD, [D, 4*D]));
  );
  for (D = -4075, -1,
    if (D % 4 > 1, next);
    my (h = qfbclassno(D));
    if (h >= 3 && h <= 6,
      listput(LD, [D, D]);
      if (D % 8 == 1, listput(LD, [D, 4*D]));
    );
  );
  forstep (D = -303, -1, 4,
    if (qfbclassno(D) > 6, listput(LD, [D, 4*D]));
  );
  for (k = 1, #LD,
    if (!elimmultind(LD[k]), error(LD[k]));
  );
}
```

D.4 Démonstration du théorème 4.3

```
checksumgen(D1, D2) =
/* checks if Q(x+y)=Q(x,y), for all pair (x,y) of singular moduli of respective
 * discriminants D1 and D2; D1 and D2 must be two distinct discriminants of the
 * same entry in Table 2.1 */
{
  my(H1, H2, L, x, y, G);
  H1 = polclass(D1, 0, 'y);
  H2 = polclass(D2, 0, 'y);
  L = nfinit(polredbest(H1));
  x = nfroots(L, subst(H1, 'y, 'x));
  y = nfroots(L, subst(H2, 'y, 'x));
  G = nfgaloisconj(L);
  for(i = 1, #x,
    for(j = 1, #x,
      if(algnumdegree(L,G,x[i]+y[j]) < #x || algnumdegree(L,G,x[i]-y[j]) < #x,
        return(0)
      );
    );
  );
```

```
  return(1);
}

checksumgenall() =
/* checks if checksumgen(D1,D2)=1, for all pair (D1,D2) of discriminants given
 * by a common entry in Table 2.1 */
{
  my(LD=[[-24,-32,-64,-88],[-36,-48],[-15,-20,-35,-40,-60,-75,-100,-115,-235],
        [-52,-91,-403],[-51,-187],[-96,-192,-288],[-180,-240],[-195,-520,-715],
  [-120,-160,-280,-760],[-340,-595],[-480,-960]]);
  for(i = 1, #LD,
    for(j1 = 1, #LD[i] - 1,
      for(j2 = j1 + 1, #LD[i],
        if(!checksumgen(LD[i][j1], LD[i][j2]), return(0));
      );
    );
  );
  return(1);
}
```

D.5 Démonstration du théorème 4.5

```
checkprodgen(D1,D2) =
/* checks if Q(x,y)=Q(x/y) and either [Q(x,y):Q(xy)]<=2 if D1=D2, or
 * Q(x,y)=Q(xy) if D1<>D2, for all pair (x,y) of distinct singular moduli of
 * respective discriminants D1 and D2 */
{
  my(H1, H2, L, x, y, G, d1, d2, d3);
  H1 = polclass(D1, 0, 'y);
  H2 = if(D1 == D2, H1, polclass(D2, 0, 'y));
  if(quaddisc(D1) == quaddisc(D2),
    L = subst(rnfequation(polredbest(H1), 'x^2-D1), 'x, 'y),
    L = H1;
  );
  L = nfinit(polredbest(H1));
  x = nfroots(L, subst(H1, 'y, 'x));
  y = if(D1 == D2, x, nfroots(L, subst(H2, 'y, 'x)));
  G = nfgaloisconj(L);
  for(i = 1, #x,
    for(j = 1, #x,
      if(D1 == D2 && j <= i, next);
      d1 = algnumdegree(L, G, x[i] - y[j]);
      /* x[i]-y[i] generates Q(x[i],y[j]) by Theorem 1.2 */
      d2 = algnumdegree(L, G, x[i] * y[j]);
      d3 = algnumdegree(L, G, x[i] / y[j]);
      if(((D1 <> D2 || d1 / d2 > 2) && d1 <> d2) || d1 <> d3, return(0));
    );
  );
```

```
  return(1);
}

checkprodgenall() =
/* checks if checkprodgen(D1,D2)=1, for all pair (D1,D2) satisfying one of the
 * following conditions:
 * (i) D1=D2 and |D1|<=395;
 * (ii) D1=4*D2 and |D2|<99;
 * (iii) D1 and D2 are given by a common entry in Table 2.1 */
{
  my(LD=[[-24,-32,-64,-88],[-36,-48],[-15,-20,-35,-40,-60,-75,-100,-115,-235],
        [-52,-91,-403],[-51,-187],[-96,-192,-288],[-180,-240],[-195,-520,-715],
  [-120,-160,-280,-760],[-340,-595],[-480,-960]]);
  for(D = -395, -1,
    if(D % 4 <= 1 && !checkprodgen(D, D), return(0));
  );
  for(i = 1, #LD,
    for(j1 = 1, #LD[i] - 1,
      for(j2 = j1 + 1, #LD[i],
        if(!checkprodgen(LD[i][j1], LD[i][j2]), return(0));
      );
    );
  );
  forstep(D = -95, -15, 8,
    if(!checkprodgen(4 * D, D), return(0));
  );
  return(1);
}
```

Bibliographie

[All15] B. Allombert, Yu. Bilu, A. Pizarro-Madariaga, CM-Points on Straight Lines, in : C. Pomerance, M. T. Rassias (editors), *Analytic Number Theory In Honor of Helmut Maier's 60th Birthday*, Springer, 2015, to appear ; `arXiv:1406:1274`.

[And98] Y. André, Finitudes des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203-208.

[Bak67] A. Baker, Linear forms in the logarithms of algebraic numbers I, II, III, *Mathematika* **13**(1966), 204-216 ; *ibid.* **14** (1967), 102-107 ; *ibid.* **14** (1967), 220-228.

[Bak69] A. Baker, H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford SER (2)* **20** (1969), 129-137.

[Bor66] Z. I. Borevich, I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[Bil01] Yu. Bilu, G. Hanrot, P. M. Voutier, M. Mignotte, Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew. Math.* **539** (2001), 75-122.

[Bil13] Yu. Bilu, D. Masser, U. Zannier, An effective "Theorem of André" for CM-points on a plane curve, *Math. Proc. Cambridge Philos. Soc.* **154** (2013), 145-152.

[Bil16] Yu. Bilu, F. Luca, A. Pizarro-Madariaga, Rational Products of Singular Moduli, *Journal of Number Theory* **158** (2016), 397-410.

[Bom06] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge University Press, 2006.

[Bre01] F. Breuer, Heights of CM points on complex affine curves, *Ramanujan J.* **5** (2001), 311-317.

[Bru16] J. H. Bruinier, K. Ono, A. V. Sutherland, Class polynomials for nonholomorphic modular functions, *Journal of Number Theory* **161** (2016), 204-229.

[Coh96] H. Cohen, A Course in Computanional Algebraic Number Theory, Springer, 1996.

[Cox89] D. A. Cox, Primes of the form $x^2 + ny^2$, Wiley, NY, 1989.

[Edi98] B. Edixhoven, Special points on the product of two modular curves, *Compos. Math.* **114** (1998), 315-328.

[Fay18] B. Faye, A. Riffaut, Fields generated by sums and products of singular moduli, `arXiv:1712.06502`, 2018.

[Lau95] M. Laurent, M. Mignotte, Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *Journal of Number Theory* **55** (1995), 285-321.

[Lau08] M. Laurent, Linear forms in two logarithms and interpolation determinants II, *Acta Arith.* **133** (2008), 325-348.

[Kli14] B. Klinger, A. Yafaev, The André-Oort conjecture, *Ann. Math. (2)* **180** (2014), 867-925.

[Kuh12] L. Kühne, An effective result of André-Oort type, *Ann. Math. (2)* **176** (2012), 651-671.

[Kuh13] L. Kühne, An effective result of André-Oort type II, *Acta Arith.* **161** (2013), 1-19.

[Luc17] F. Luca, A. Riffaut, Linear independance of powers of singular moduli of degree 3, `arXiv:1712.06929`, 2017.

[Mat00] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II (Russian), *Izv. RAN, Ser. Mat.* **64** (2000), 125-180 ; (=*Izv. Math.* **64** (2000), 1217-1269.)

[Oes85] J. Oesterlé, Nombres des classes des corps quadratiques imaginaires, *Asterisque* **121-122** (1985), 309-323.

[Oes88] J. Oesterlé, Le problème de Gauss sur le nombre de classes, *L'Ens. Math.* **34** (1988), 43-67.

[Pil08] J. Pila, U. Zannier, Rational points in periodic analytic sets and the Manin-Mumford conjecture, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **19** (2008), 149-162.

[Pil09] J. Pila, Rational points of definable sets and results of André-Oort-Manin-Mumford type, *Int. Math. Res. Notices* 2009, 2476-2507.

[Pil11] J. Pila, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$, *Ann. Math. (2)* **173** (2011), 1779-1840.

[Pil13] J. Pila, J. Tsimerman, The André-Oort conjecture for the moduli space of abelian surfaces, *Compos. Math.* **149** (2013), 204–216.

[Poo76] A. J. Van Der Poorten, Linear forms in logarithms in the p-adic case, Transcendence theory : advances and applications, *Academic Press*, London, 1977, 29-57.

[Rif18]] A. Riffaut, Equations with powers of singular moduli, `arXiv:1710.03547`, 2018.

[Sch80] W. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, NY, 1980.

[Sie35] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arithmetica* **1** (1935), 83-86.

[Tat52] T. Tatuzawa, On a Theorem of Siegel, *Jap. J. Math.* **21** (1951), 163-178 (1952).

[Ull14] E. Ullmo, A. Yafaev, Galois orbits and equidistribution of special subvarieties : towards the André-Oort conjecture, *Ann. Math. (2)* **180** (2014), 823–865.

[Wat04] M. Watkins, Class numbers of imaginary quadratic fields, *Math. Comp.* **73** (2004), 907-938.

[Wei73] P. J. Weinberger, Exponents of the class group of the complex quadratic fields, *Acta Arith.* **22** (1973), 117-123.

[Wus14] G. Wüstholz (with an appendix by L. Kühne) A Note on the Conjectures of André-Oort and Pink, *Bull. Inst. Math. Acad. Sinica (N.S.)* **9** (2014), 735-779.

[Zag84] D. Zagier, L-Series of elliptic curves, the Birch-Swinnerton-Dyer conjecture, and the class number problem of Gauss, *Notices of the AMS* **31** (1984), 739-743.

[PARI] The PARI Group, PARI/GP version 2.7.1 (2014), Bordeaux; available from `http://pari.math.u-bordeaux.fr/`