Ecole Normale Supérieure
Département de Mathématiques et Applications

$e^{\pi\sqrt{163}}$ est presque un entier

Caroline Arvis

Lin Jie

Sous la direction de François Charles

22 Juin 2011

1 Introduction : calcul approché de $e^{\pi\sqrt{163}}$

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743,\ 999\,999\,999\,999\,250\,073\ \ldots$$

$$e^{\pi\sqrt{163}} \simeq 744 - (-640320)^3$$

A 10^{-12} près, $e^{\pi\sqrt{163}}$ serait un entier. Cette propriété remarquable est en fait plus qu'une simple coïncidence, et s'explique en considérant le j-invariant de la courbe elliptique sur $\mathbb{C}$ isomorphe au quotient $\mathbb{C}/(\mathbb{Z} + \frac{1+i\sqrt{163}}{2}\mathbb{Z})$.

Ceci explique qu'elle s'étend à d'autres nombres remarquables, appelés nombres de Heegner, par exemple

$$e^{\pi\sqrt{19}} \simeq 744 - (-96)^3$$

$$e^{\pi\sqrt{43}} \simeq 744 - (-960)^3$$

$$e^{\pi\sqrt{67}} \simeq 744 - (-5280)^3$$

.

Les courbes elliptiques sur $\mathbb{C}$ sont les courbes régulières, planes, projectives de degré 3, munies d'un point. Elles sont munies d'une structure de surface de Riemann.

On montre que toute courbe elliptique sur $\mathbb{C}$ est en fait isomorphe comme surface de Riemann au quotient de $\mathbb{C}$ par un réseau Λ, c'est-à-dire un $\mathbb{Z}$-module libre de rang 2 de $\mathbb{C}$ contenant une $\mathbb{R}$-base de $\mathbb{C}$. Si on note $\mathcal{H}$ le demi-plan de Poincaré, toute courbe elliptique est en fait isomorphe comme surface de Riemann à un réseau de la forme $\mathbb{Z} + \tau\mathbb{Z}$ avec $\tau \in \mathcal{H}$.

Il existe sur l'ensemble des courbes elliptiques complexes une fonction appelée j-invariant qui les classifie : deux courbes elliptiques sont isomorphes si et seulement si leur j-invariant est identique. Il apparaît alors que le j-invariant d'une courbe elliptique E dépend uniquement du complexe $\tau \in \mathcal{H}$ tel que $E \simeq \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$. En effet, elle ne dépend que l'orbit de τ sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. En particulier, elle est périodique de période 1. En notant $q = e^{2i\pi\tau}$, on obtient sa série de Fourier $j(E) = j(\tau) : j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n$ où les a_n sont des coefficients entiers. On a $a_1 = 196884$, et $a_k \leq (200\,000)^n$ pour k petit. On a par ailleurs $a_n \sim_{n\to\infty} \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{\frac{3}{4}}}$.

Notons $\mu = \frac{1+i\sqrt{163}}{2}$. On obtient $j(\mu) = -e^{\pi\sqrt{163}}+744+\sum_{n=1}^{\infty} a_n(-1)^n e^{-\pi n\sqrt{163}}$. Or $e^{-\pi\sqrt{163}} \simeq 3.8 \times 10^{-18}$, donc

$$j(\mu) \simeq -e^{\pi\sqrt{163}} + 744 + a_1 e^{-\pi n\sqrt{163}} \simeq -e^{\pi\sqrt{163}} + 744 + 8 \times 10^{-13}.$$

On pose $\Lambda = \mathbb{Z} + \mu\mathbb{Z}$ et on considère $E = \mathbb{C}/\Lambda$.

Or, l'étude du corps $K = \mathbb{Q}[\sqrt{-163}]$ montre que son anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\mu]$ est principal. On donne une méthode pour calculer le nombre de classes des corps quadratiques imaginaires. On introduit aussi la théorie de Minkowski dans l'annexe A.

On montre d'abord que $j(E)$ est algébrique sur $\mathbb{Q}$ de degré majoré par le nombre de classes de K. Pour ce faire, on démontre que $j(E)$ a une orbite de cardinal majoré par le nombre de classes de K sous l'action de $Aut(\mathbb{C})$.Donc $j(\mu)$ est un entier algébrique de degré 1, donc dans $\mathbb{Q}$.

On obtient ensuite que $j(E)$ est un entier algébrique en en construisant explicitement un polynôme annulateur unitaire. On en déduit que $j(\mu)$ est dans $\mathbb{Z}$.

De plus, pour tout E courbe elliptique à multiplication complexe, c'est-à-dire qu'il existe un complexe $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ tels que $\alpha\Lambda \subset \Lambda$, on montre que $j(E)$ est un entier algébrique.

On montre même que la racine cubique de $j(\mu)$ est dans $\mathbb{Q}(j(\mu))$, donc dans $\mathbb{Z}$; ainsi $N = (-640320)^3$. On en déduit alors

$$e^{\pi\sqrt{163}} = 744 - N + \sum_{n=1}^{\infty} a_n(-1)^n e^{-\pi n\sqrt{163}}$$

ce qui explique la valeur presque entière de $e^{\pi\sqrt{163}}$.

Nous allons ici démontrer ces différents résultats en plusieurs étapes : d'abord, nous expliquerons ce qu'est une courbe elliptique sur $\mathbb{C}$, puis donnerons la définition du j-invariant. Nous expliquerons ensuite pourquoi les courbes elliptiques sont isomorphes aux quotients de $\mathbb{C}$ par des réseaux. Ensuite, une étude des fonctions modulaires fournira la série de Fourier de j. Nous montrerons ensuite que l'anneau $\mathbb{Z}[\mu]$ est principal. Nous définirons ensuite les courbes à multiplication complexe et en déduirons que $j(E)$ est un entier algebrique, puis montrerons pour un corps quadatique imaginaire K, le degré de $j(\mathbb{C}/\mathcal{O}_K)$ est au plus h_K. Nous montrerons enfin que la racine cubique de $j(\mathbb{C}/\mathcal{O}_K)$ est dans $\mathbb{Q}(j(\mathbb{C}/\mathcal{O}_K))$.

Nous remercions François Charles pour ce sujet ainsi que pour son aide et ses conseils éclairés.

Table des matières

2 Courbes elliptiques sur $\mathbb{C}$

Dans cette section, on va définir les courbes elliptiques complexes puis les classifier à l'aide d'une fonction j définie sur $\mathcal{H}$; on établira alors un paramétrage des classes d'isomorphisme de courbes elliptiques sur $\mathbb{C}$ par $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{C}$ en montrant une correspondance entre l'ensemble des réseaux de $\mathbb{C}$ et l'ensemble de courbes elliptiques sur $\mathbb{C}$.

2.1 Définition d'une courbe elliptique

Définition 2.1. *On appelle* courbe elliptique *sur un corps k toute courbe E régulière plane projective de degré 3 munie d'un point $O \in E(k)$.*

Comme la caractéristique de $\mathbb{C}$ est différente de 2 ou 3, une courbe elliptique complexe est isomorphe à une courbe (E, O) dans $\mathcal{P}^2(\mathbb{C})$ définie par $E(a,b) : Y^2Z = X^3 + aXZ^2 + bZ^3$, munie du point $O = (0,1,0)$, avec $a, b \in \mathbb{C}$ tels que $4a^3 + 27b^2 \neq 0$. La condition $4a^3 + 27b^2 \neq 0$ est équivalente au fait que les trois racines de l'equation $x^3 + ax + b$ soient distinctes.

On peut alors définir ainsi la fonction j sur l'ensemble des courbes elliptiques sur $\mathbb{C}$: $j(E(a,b)) = \frac{1728(4a^3)}{4a^3+27b^2}$ pour $a, b \in \mathbb{C}$ avec $4a^3 + 27b^2 \neq 0$

Remarque Il existe de nombreuses manières de définir une courbe elliptique ; voir par exemple [10, pg 45].

Démonstration On considère une courbe elliptique E sur $\mathbb{C}$. On peut facilement en trouver une équation de la forme $Y^2Z + aXYZ + bYZ^2 = X^3 + cX^2Z + dXZ^2 + eZ^3$ et prendre le point $(0,1,0)$. Une telle équation s'appelle une *équation de Weierstrass* pour la courbe elliptique considérée.

On effectue alors le changement de variable $\begin{cases} X' = X \\ Y' = Y + \frac{a}{2}X \\ Z' = Z \end{cases}$. On obtient l'équation $Y'^2Z' + bY'Z'^2 = X'^3 + (c + \frac{a}{2})X'^2Z' + (d + \frac{a}{2})X'Z'^2 + eZ'^3$.

On pose ensuite $\begin{cases} x = X' + \frac{c+\frac{a}{2}}{3}Z' \\ y = Y' + \frac{b}{2}Z' \\ z = Z' \end{cases}$ pour obtenir une équation de la forme voulue.

Réciproquement, une courbe de cette forme est régulière si et seulement si $4a^3 + 27b^2 \neq 0$, d'où le résultat voulu.

□

Remarque On peut montrer sans difficulté qu'une courbe elliptique est une surface de Riemann (c'est-à-dire une variété complexe de dimension 1) compacte et connexe. On dira que deux courbes elliptiques sont isomorphes si elles le sont en tant que surfaces de Riemann.

Théorème 2.2. *Deux courbes elliptiques $E(a,b)$ et $E(a',b')$ sont isomorphes si et seulement si $j(E(a,b)) = j(E(a',b'))$. Ainsi, la fonction j donne une classification de l'ensemble de courbes elliptiques sur $\mathbb{C}$.*

Démonstration Soit $\phi : E(a,b) \to E(a',b')$ un isomorphisme de courbes elliptiques. En comparant les degrés, on obtient l'existence de $u, v, r, s \in \mathbb{C}$ avec u, r non nuls tels que $\phi(x) = ux + v$, $\phi(y) = ry + s$. Ici, x et y sont des coordonées affines. On en déduit que $(ry+s)^2 = (ux+v)^3 + a'(ux+v) + b'$. En comparant avec $y^2 = x^3 + ax + b$, on obtient $b'/b = u^3, a'/a = u^2$. Ainsi $j(E(a',b')) = \frac{1728(4a'^3)}{4a'^3+27b'^2} = \frac{1728(4u^6a^3)}{4u^6a^3+27u^6b^2} = j(E(a,b))$.

Réciproquement, si $j(E(a,b)) = j(E(a',b')$, alors soit $a = a' = 0$, soit $a \neq 0$, $a' \neq 0$ et $b^2/a^3 = b'^2/a'^3$. Donc il existe toujours $\lambda \in \mathbb{C}$ tel que $b' = \lambda^3 b$ et $a' = \lambda^2 a$. Le morphisme $(x,y) \mapsto (\lambda^2 x, \lambda^3 y)$ est alors un isomorphisme entre $E(a,b)$ et $E(a',b')$. □

Remarque Ceci est vrai pour les courbes elliptiques sur tout corps algébriquement clos de caractéristique différente de $2, 3$.

Dans la suite, on écrira $j(E)$ au lieu de $j(E(a,b))$ car j ne dépend pas du choix des paramètres (a,b).

2.2 Réseaux de $\mathbb{C}$ et courbes elliptiques associées

Définition 2.3. *Un **réseau** dans $\mathbb{C}$ est un sous-groupe de $\mathbb{C}$ engendré par deux nombres complexes linéairement indépendants sur $\mathbb{R}$, c'est-à-dire un sous-ensemble Λ de $\mathbb{C}$ de la forme $\mathbb{Z}z_1 + \mathbb{Z}z_2$, avec $\frac{z_1}{z_2} \notin \mathbb{R}$.*

Remarque On munit $\mathbb{C}/\Lambda$ d'une stucture de surface de Riemann par la stucture complexe de variété quotient.

On obtient une stucure de groupe sur $\mathbb{C}/\Lambda$ par la stucture de groupe quotient. Alors $\mathbb{C}/\Lambda$ est un groupe de Lie complexe.

Une fonction sur $\mathbb{C}/\Lambda$ se relève en une fonction doublement périodique sur $\mathbb{C}$ de périodes z_1, z_2.

Définition 2.4. *Soit Λ, Λ' deux réseaux de $\mathbb{C}$. On note O (resp. O') le point $0+\Lambda$ (resp. $0+\Lambda'$) de $\mathbb{C}/\Lambda$ (resp. $\mathbb{C}/\Lambda'$) et on note $Hom(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda')$ l'ensemble des fonctions holomorphes de $\mathbb{C}/\Lambda$ à $\mathbb{C}/\Lambda'$ qui envoient O sur O'. C'est un sous-groupe du groupe des holomorphismes entre groupes de Lie complexes. Si $\Lambda' = \Lambda$, on note $End(\mathbb{C}/\Lambda) = Hom(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda)$.*

*On dit $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont **isomorphes** si il existe une application bijective dans $Hom(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda')$. Il est facile de voir que si $f \in Hom(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda')$ est bijective, alors $f^{-1} \in Hom(\mathbb{C}/\Lambda', \mathbb{C}/\Lambda)$ et est bijective. Comme $Id \in End(\mathbb{C}/\Lambda)$, on sait que la relation d'isomorphisme est une relation équivalente.*

Proposition 2.5. *Soit Λ, Λ' deux réseaux de $\mathbb{C}$ et soit ϕ une fonction holomorphe de $\mathbb{C}/\Lambda$ dans $\mathbb{C}/\Lambda'$ qui envoit O sur O'. Alors il existe un nombre complexe α tel que $\alpha\Lambda \subset \Lambda'$ et pour chaque $z \in \mathbb{C}$, $\phi(z+\Lambda) = \alpha z + \Lambda'$. C'est-à-dire que ϕ est induit par la multiplication par α.*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\phi}} & \mathbb{C} \\ \pi \downarrow & & \downarrow \pi' \\ \mathbb{C}/\Lambda & \xrightarrow{\phi} & \mathbb{C}/\Lambda' \end{array}$$

Démonstration

On note π (resp.π') la projection canonique de $\mathbb{C}$ sur $\mathbb{C}/\Lambda$ (resp.$\mathbb{C}/\Lambda'$). Comme $\mathbb{C}$ est le revêtement universel de $\mathbb{C}/\Lambda'$, il existe une fonction holomorphe $\tilde{\phi}$ de $\mathbb{C}$ à $\mathbb{C}$ qui relève ϕ, c'est-à-dire que $\pi' \circ \tilde{\phi} = \phi \circ \pi$. Quitte à translater, on peut supposer $\tilde{\phi}(0) = 0$.

Pour $\omega \in \Lambda$, comme l' application $z \mapsto \tilde{\phi}(z+\omega) - \tilde{\phi}(z)$ est continue, et que son image est contenue dans Λ' (ensemble discret), elle est constante. D'où $\forall \omega \in \Lambda$, $\forall z \in \mathbb{C}$, $\tilde{\phi}'(z+\omega) = \tilde{\phi}'(z)$. Or $\tilde{\phi}'$ est holomorphe et doublement périodique donc bornée, elle est donc constante par le théorème de Liouville. Donc il existe $\alpha \in \mathbb{C}$ tel que $\tilde{\phi}' \equiv \alpha$. Alors $\tilde{\phi}(z) = \alpha z$ car $\tilde{\phi}$ envoie 0 sur 0. On a alors $\alpha\Lambda \subset \Lambda'$ et ϕ est induit par la multiplication par α.

□

On peut déduire directement du théorème précédent ces deux corollaires :

Corollaire 2.6. 1. *Pour tout réseau Λ, $End(\mathbb{C}/\Lambda)$ est un anneau.*

2. *Pour deux réseau Λ et Λ', $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes si et seulement s'il existe $\alpha \in \mathbb{C}$ tel que $\Lambda' = \alpha\Lambda$.*

Soit $\Lambda = \mathbb{Z}z_1 + \mathbb{Z}z_2$ est un réseau. On pose $\tau = z_1/z_2$ si $Im(z_1/z_2) > 0$ ou $\tau = z_2/z_1$ si $Im(z_1/z_2) < 0$, et $\Lambda' = \mathbb{Z} + \mathbb{Z}\tau$. Alors $\mathbb{C}/\Lambda$ est isomorphique à $\mathbb{C}/\Lambda'$. Dans la suite on se ramène donc au cas $z_1 = 1$, $z_2 = \tau$, où $\tau \in \mathcal{H}$, $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ désignant le demi-plan de Poincaré.

2.3 La fonction de Weierstrass $\mathcal{P}$

Nous avons donc paramétré les courbes elliptiques et les réseaux par classes d'isomorphisme ; nous allons à présent relier courbes elliptiques et quotients de $\mathbb{C}$ par des réseaux ; pour ce faire, on commence par construire une fonction suffisamment régulière sur $\mathbb{C}/\Lambda$ pour un réseau Λ quelconque.

Soit un réseau $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. On cherche à construire une courbe elliptique isomorphe à $\mathbb{C}/\Lambda$.On commence par construire une fonction méromorphe, doublement périodique de périodes 1, τ.

Définition 2.7. *L'application $\mathcal{P} : z \mapsto \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$ est une fonction méromorphe. En effet, la série converge absolutement dans $\mathbb{C} - \Lambda$ et est clairement méromorphe en tout point de Λ. Il est facile de voir qu'elle est doublement périodique par rapport au réseau Λ. On l'appelle* ***fonction de Weierstrass****.*

Sa dérivée $z \mapsto \sum_{\omega\in\Lambda}(\frac{-2}{(z-\omega)^3})$ est aussi une fonction méromorphe doublement périodique par rapport à Λ. Dans la suite, on considérera $\mathcal{P}$ et $\mathcal{P}'$ comme des fonctions méromorphes sur $\mathbb{C}/\Lambda$.

Pour $m \in \mathbb{N}, m > 2$, on pose $G_m(\Lambda) = \sum_{\omega\in\Lambda,\,\omega\neq 0}(\frac{1}{\omega^m})$. Pour m impair, $G_m(\Lambda) = 0$. Pour $z \in \mathcal{H}$, on pose $G_m(z) = G_m(\mathbb{Z} + z\mathbb{Z})$. G_m est holomorphe sur $\mathcal{H}$ car la série converge absolutement. Ces fonctions sont les ***séries d'Eisenstein*** *qui seront à nouveau utilisées en §3.*

Remarque La fonction $\mathcal{P}$ est paire et la fonction $\mathcal{P}'$ est impaire.

Proposition 2.8. *$\mathcal{P}$ vérifie l'équation différentielle*

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2(\Lambda)\mathcal{P}(z) - g_3(\Lambda)$$

où $g_2(\Lambda) = 60G_4(\Lambda)$, $g_3(\Lambda) = 140G_6(\Lambda)$.

Démonstration On considère le série de Laurent en 0 :

Comme $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty} \frac{n+1}{w^{n+2}z^n}$, on a alors

$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda-0}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(\Lambda)z^n.$

Donc la partie non entière de la série de Laurent de $\mathcal{P}^3$ est $\frac{1}{z^6} + \frac{9G_4(\Lambda)}{z^2} + 15G_6(\Lambda)$.

De même, on peut aussi écrire que la partie non entière de $\mathcal{P}'^2$ est $\frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda)$.

Donc la fonction $F(z) := \mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + g_2\mathcal{P}(z) + g_3$ est holomorphe en 0 et de plus, s'annule en 0. Alors F est une fonction holomorphe sur $\mathbb{C}$ et doublement périodique, donc constante. On en déduit que $F(z) = \mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + g_2(\Lambda)\mathcal{P}(z) + g_3(\Lambda) = F(0) = 0$ partout, ce que l'on cherchait.

□

On note la série de Laurent de $\mathcal{P}$ en 0 par $\frac{1}{z^2} + \sum_{n=1}^{\infty} a_n z^n$. Par la proposition précédente, on a $\mathcal{P}''(z) = 6\mathcal{P}(z)^2 - (1/2)g_2$. Donc pour $n \leq 3$, on a $2n(2n-1)a_n = 6(2a_n + \sum_{i=1}^{n-2} a_i a_{n-1-i})$. On peut alors montrer par récurrence le corollaire suivant :

Corollaire 2.9. *Tous les coefficient de la série de Fourier de $\mathcal{P}$ sont des polynômes à coefficients rationnels en g_2, g_3.*

On va montrer que toutes les fonctions méromorphes doublement périodiques de périodes 1, τ sont fonctions rationnelles de $\mathcal{P}$ et $\mathcal{P}'$.

On note $\mathcal{M}$ le corps des fonctions méromorphes sur $\mathbb{C}/\Lambda$. C'est aussi le corps des fonctions méromorphes doublement périodiques sur $\mathbb{C}$ de périodes 1, τ.

Soit $f \in \mathcal{M}$ non nulle, on note $v_x(f)$ l'ordre du zéro (ou l'opposé de l'ordre du pôle) de f en x.

On pose $div(f) = \sum_{x \in \mathbb{C}/\Lambda} v_x(f)(x)$. Comme $\mathbb{C}/\Lambda$ est compacte, le nombre des pôles et zéros de f dans $\mathbb{C}/\Lambda$ est fini. Donc il n'y a qu'un nombre fini de x dans $\mathbb{C}/\Lambda$ tel que $v_x(f)$ est non nulle.

On note $w_1 = 1/2, w_2 = \tau/2, w_3 = (1+\tau)/2$ les trois points de $\mathbb{C}/\Lambda$ d'ordre exactement 2.

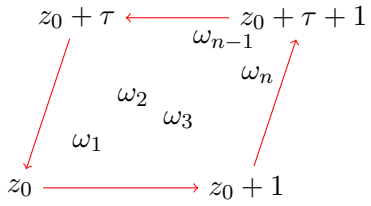
Lemme 2.10. *1. Soit $f \in \mathcal{M}$ non nulle, alors $\sum_{x \in \mathbb{C}/\Lambda} v_x(f) = 0$.*

2. Soit f et g deux éléments non nuls de $\mathcal{M}$ tels que $div(f) = div(g)$; il existe $c \in \mathbb{C}$ non nul tel que $f = cg$.

Démonstration

1. Comme le nombre des pôles et zéros de f est fini dans $\mathbb{C}/\Lambda$, il existe z_0 dans $\mathbb{C}$, tel que f n'a pas de pôles ou zéros sur le bord de $D :=$

$\{z_0 + t_1 + t_2\tau | 0 \leq t_1 \leq 1, 0 \leq t_2 \leq 1\}$.
Donc on a $\sum_{x \in \mathbb{C}/\Lambda} v_x(f) = \sum_{x \in D} v_x(f) = \sum_{x \in D} res_x(\frac{f'(z)}{f(z)})dz = \frac{1}{2\pi i}\int_{\partial D} \frac{f'(z)}{f(z)} =$ 0 puisque $\frac{f'}{f}$ est doublement périodique.
Dans la figure ci-dessous est représenté le bord du domaine D, avec les ω_i des zéros ou pôles de f.



2. Comme $div(f) = div(g)$ on a $div(f/g) = 0$, c'est-à-dire que f/g n'est pas de pôles ou zéros dans $\mathbb{C}/\Lambda$. On prend $z_1 \in \mathbb{C}/\Lambda$ tel que z_1 n'a pas pôle ou zéro de f ou g. On pose $c = f(z_1)/g(z_1)$ qui est un nombre complexe non nul. Alors $f/g - c$ n'a pas de pôles dans $\mathbb{C}/\Lambda$ et s'annule en z_1. Par 1, on a $f/g - c$ nulle partout. Donc $f = cg$.

□

On étudie alors les pôles et zéros de $\mathcal{P}$ et $\mathcal{P}'$:

Lemme 2.11. *1. Soit $a \in \mathbb{C}/\Lambda$ non nul, alors $div(\mathcal{P}(z) - \mathcal{P}(a)) = (a) + (-a) - 2(O)$.*

2. $div(\mathcal{P}'(z)) = (w_1) + (w_2) + (w_3) - 3(O)$

3. $\mathcal{P}'(z)^2 = 4(\mathcal{P}(z) - \mathcal{P}(w_1))(\mathcal{P}(z) - \mathcal{P}(w_2))(\mathcal{P}(z) - \mathcal{P}(w_3))$

4. $\mathcal{P}(w_1), \mathcal{P}(w_2), \mathcal{P}(w_3)$ sont deux à deux distincts. Donc la courbe $Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$ dans $\mathbb{P}^2(\mathbb{C})$ est une courbe elliptique.

Démonstration

1. Le seul pôle de $\mathcal{P}(z) - \mathcal{P}(a)$ et un pôle double en O. Si $a \neq -a$ dans $\mathbb{C}/\Lambda$, alors a et $-a$ sont deux zéros distincts de $\mathcal{P}(z) - \mathcal{P}(a)$. Par la première partie du lemme précedent, $\mathcal{P}(z) - \mathcal{P}(a)$ a exactement deux zéros simples a et $-a$. Si $a = -a$ dans $\mathbb{C}/\Lambda$, alors $\mathcal{P}'(a) = -\mathcal{P}'(-a) = -\mathcal{P}'(a)$ donc $= 0$. Alors a est un zéro de $\mathcal{P}(z) - \mathcal{P}(a)$ d'ordre au moins 2. Par la première partie du lemme précedent, a est le seul zéro de $\mathcal{P}(z) - \mathcal{P}(a)$ donc d'ordre exactement 2.
2. Comme $\mathcal{P}'$ est impaire, w_1, w_2, w_3 sont trois zéros distincts de $\mathcal{P}'$. Comme le seul pôle de $\mathcal{P}'$ est 0, c'est un pôle d'ordre 3. On a donc $div(\mathcal{P}'(z)) = (w_1) + (w_2) + (w_3) - 3(O)$.

3. Par 1 et 2, on a $div\mathcal{P}'(z)^2 = div((\mathcal{P}(z)-\mathcal{P}(w_1))(\mathcal{P}(z)-\mathcal{P}(w_2))(\mathcal{P}(z)-\mathcal{P}(w_3)))$. Grâce a la deuxième partie du lemme précedent, il existe un nombre complexe non nul c tel que $\mathcal{P}'(z)^2 = c(\mathcal{P}(z)-\mathcal{P}(w_1))(\mathcal{P}(z)-\mathcal{P}(w_2))(\mathcal{P}(z)-\mathcal{P}(w_3))$. En considerant la série de Laurent en O, on a $c = 4$.
4. Par 1, $div(\mathcal{P}(z)-\mathcal{P}(w_1)) = 2(w_1)-2(O)$, donc w_2 n'est pas un zéro de $\mathcal{P}(z)-\mathcal{P}(w_1)$. Donc $\mathcal{P}(w_1) \neq \mathcal{P}(w_2)$. De même, $\mathcal{P}(w_1) \neq \mathcal{P}(w_3)$ et $\mathcal{P}(w_2) \neq \mathcal{P}(w_3)$. En comparant 3 et la propsition 2.8, on obtient que la courbe $Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$ dans $\mathbb{P}^2(\mathbb{C})$ est une courbe elliptique.

□

Théorème 2.12. *1. Soit f une fonction méromorphe paire sur $\mathbb{C}/\Lambda$, alors $f \in \mathbb{C}(\mathcal{P})$.*

2. Le corps $\mathcal{M}$ est engendré par $\mathcal{P}$ et $\mathcal{P}'$.

Démonstration

1. On peut supposer que f est non nulle. Comme f est paire, il existe $N \in \mathbb{N}$, $a_1, \cdots, a_N \in \mathbb{C}/\Lambda$, $a_j \neq -a_j, 1 \leq j \leq N$ et $m_1, \cdots, m_N \in \mathbb{Z}$, $n_1, n_2, n_3 \in \mathbb{Z}$ tels que :

$$div(f) = \sum_{j=1}^{N} m_j((a_j) + (-a_j) - 2(O)) + \sum_{i=1}^{3} n_i((w_i) - (O))$$

   De plus, comme $f(z) = f(-z)$, on a que la $2k+1$ dérivée de f est impaire pour tout $k \in \mathbb{N}$. Donc la $2k+1$ dérivée de f s'annule en $w_i, 1 \leq i \leq 3$. Alors n_i est pair pour tout $1 \leq i \leq 3$.
   Donc $div(f) = div(\prod_{j=1}^{N}(\mathcal{P}(z)-\mathcal{P}(a_j))^{m_j} \cdot \prod_{i=1}^{3}(\mathcal{P}(z)-\mathcal{P}(w_i))^{n_i/2})$ par le lemme précedent. Grâce au lemme 2.10, on a alors $f \in \mathbb{C}(\mathcal{P})$.
2. Soit $g \in \mathcal{M}$, alors

$$g(z) = \frac{g(z)+g(-z)}{2} + \frac{g(z)-g(-z)}{2\mathcal{P}'(z)} \cdot \mathcal{P}'(z)$$

   Comme $\frac{g(z)+g(-z)}{2}$ et $\frac{g(z)-g(-z)}{2\mathcal{P}'(z)}$ sont deux fonction méromorphe paires de $\mathbb{C}/\Lambda$, on a alors $f \in \mathbb{C}(\mathcal{P}, \mathcal{P}')$ par 1.

□

Remarque Le corps $\mathcal{M}$ est isomorphe à $\mathbb{C}(X,Y)/(Y^2-4X^3+g_2X+g_3)$.

2.4 Classification des courbes elliptiques sur $\mathbb{C}$

Munis de la fonction de Weierstrass, il nous est maintenant possible d'expliciter une correspondence entre les classes d'isomorphisme des courbes elliptiques et l'ensemble $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{C}$.

Construction de $E(\Lambda)$. Soit $\tau \in \mathcal{H}$ et $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$ comme précédent. On définit une courbe dans $\mathbb{P}^2(\mathbb{C})$ par $E(\Lambda) : Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$. Par la section précédente, c'est une courbe elliptique sur $\mathbb{C}$.

$E(\Lambda)(\mathbb{C})$ est un sous-espace de $\mathbb{P}^2(\mathbb{C})$, et est donc muni d'une structure de variété complexe de dimension 1.

Proposition 2.13. *L'application*

$$\Phi : \begin{cases} \mathbb{C}/\Lambda \to E(\Lambda) \\ 0 \mapsto (0:1:0) \\ z \mapsto (\mathcal{P}(z) : \mathcal{P}'(z) : 1) \end{cases}$$

est un isomorphisme de variétés complexes.

Ainsi, à tout réseau Λ de $\mathbb{C}$ on peut associer une courbe elliptique isomorphe en tant que variété complexe à $\mathbb{C}/\Lambda$.

Démonstration Il est clair que Φ est holomorphe. Donc il suffit de montrer que Φ est bijective. On suppose par l'absurde qu'il existe z, z' deux éléments distincts de $\mathbb{C}/\Lambda$ tels que $(\mathcal{P}(z) : \mathcal{P}'(z) : 1) = (\mathcal{P}(z') : \mathcal{P}'(z') : 1)$. Alors $\mathcal{P}(z) = \mathcal{P}(z'), \mathcal{P}'(z) = \mathcal{P}'(z')$. Donc z' est un zéro de la fonction $w \mapsto \mathcal{P}(w) - \mathcal{P}(z)$. Comme $div(\mathcal{P}(w) - \mathcal{P}(z)) = (z) + (-z) - 2(O)$, on a forcément $z' = -z$. Comme $\mathcal{P}'$ est impair, on a $\mathcal{P}'(z) = \mathcal{P}'(z') = \mathcal{P}'(-z) = -\mathcal{P}'(z)$. Donc $\mathcal{P}'(z) = 0$. Alors il existe $i \in \{1,2,3\}$ tel que $z = w_i$. En particulier $z' = -z = z$, ce qui est absurde ! Donc Φ est injective. En particulier, Φ est non constante. Par le fait que Φ est holomorphe, on a $im(\Phi)$ est ouverte.

De plus, comme $\mathbb{C}/\Lambda$ est compacte, $im(\Phi)$ est compacte. Par connexité de $E(\Lambda)$, Φ est surjective donc bijective. □

Définition 2.14. *On définit la fonction j sur $\mathcal{H}$ par $j : \tau \mapsto j(E(\Lambda)) = \frac{1728 g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$ avec $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. On notera parfois $j(E(\Lambda)) = j(\Lambda) = j(\mathbb{C}/\Lambda)$.*

Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. On défint une action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}$ par $\gamma \cdot \tau = \frac{a\tau+b}{c\tau+d}$. Il est facile de voir que $\gamma \cdot \tau$ est encore dans $\mathcal{H}$.

On verra en §3 que j est invariante sous l'action du $\mathrm{SL}_2(\mathbb{Z})$, c'est-à-dire que $j(E(\mathbb{Z}+\mathbb{Z}\tau)) = j(E(\mathbb{Z}+\mathbb{Z}\gamma\tau))$. Donc on a $E(\mathbb{Z}+\mathbb{Z}\tau) \simeq E(\mathbb{Z}+\mathbb{Z}\gamma\tau)$.

Ainsi, Φ induit une application de $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ dans l'ensemble des classes d'isomorphismes de courbes elliptiques.

On a vu que j classifie les courbes elliptiques et puisque, comme on le verra en 3.6, $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \to \mathbb{C}$ est bijective, on obtient :

Théorème 2.15. *L'application de* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ *dans l'ensemble des classes d'isomorphismes des courbes elliptiques définie par* $\tau \mapsto E(\mathbb{Z}+\mathbb{Z}\tau)$ *est bijective.*

Remarque On a alors que $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ paramètre les classes d'isomorphisme des courbes elliptiques sur $\mathbb{C}$. Dans la suite, identifiera une courbe elliptique avec un tore complexe $\mathbb{C}/\Lambda$ avec $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$ pour un certain $\tau \in \mathcal{H}$.

3 Fonctions modulaires

Dans cette section, nous allons étudier plus en détail la fonction j, qui est le coeur de cet exposé.

3.1 Définition d'une fonction modulaire

Soit $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ le demi-plan supérieur de Poincaré. On va définir des fonctions sur $\mathcal{H}$ qui vérifient certaines propriétés automorphes par rapport au groupe $\Gamma := \mathrm{SL}_2(\mathbb{Z})$.

Soient $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $z \in \mathcal{H}$, on définit γz comme $\frac{az+b}{cz+d}$. Il est facile de voir que γz est encore dans $\mathcal{H}$.

Soit f une fonction méromorphe sur $\mathcal{H}$ 1-périodique, on dit que f est méromorphe en ∞ si sa série de Fourier

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$$

n'a qu'un nombre fini de a_n non nul avec n négatif. Ici, $q = \exp(2\pi i z)$.

Dans ce cas, on définit $v_\infty(f) := \inf\{n \in \mathbb{Z}, a_n \neq 0\}$.

Définition 3.1. *Soient f une fonction méromorphe sur $\mathcal{H}$ et k un entier. On dit que f est une* ***fonction modulaire pour*** Γ ***(ou simplement fonction modulaire) de poids*** *k si elle est méromorphe sur $\mathcal{H}$ et vérifie :*

1. *$f(\gamma z) = (cz+d)^k f(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et tout $z \in \mathcal{H}$.*
2. *Elle est méromorphe en ∞.*

On appelle sa série de Fourier son q-développement.

Remarque Soient f et g deux fontions modulaires de poids k et l respectivement. Alors :

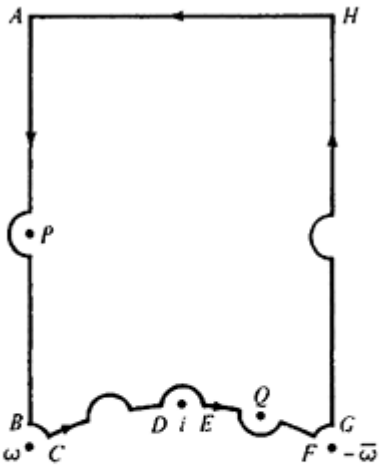
1. Le produit fg est une fonction modulaire de poids $k+l$.
2. Si g n'est pas identiquement nulle, alors le quotient f/g est une fonction modulaire de poids $k-l$.
3. Les fonctions modulaires de poids k forment un $\mathbb{C}$-espace vectoriel et les fonctions modulaires de poids 0 est un corps.

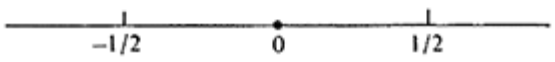
Dans la suite, on note $\mathcal{R}$ la région $\{z \in \mathcal{H} : |z| \geq 1, |Re(z)| \leq 1/2\}$. C'est le domaine fondamental de $\mathcal{H}$ sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. On sait que chaque point de $\mathcal{H}$ est équivalent à un point de $\mathcal{R}$ sous l'action du $\mathrm{SL}_2(\mathbb{Z})$. Deux points distincts z, z' dans $\mathcal{R}$ sont équivalents par l'action du $\mathrm{SL}_2(\mathbb{Z})$ si et seulement si $|Re(z)| = 1/2 et |z - z'| = 1$ ou $|z| = 1, z' = -1/z$.

Théorème 3.2. *Soit f une fonction modulaire non nulle de poids k. Pour $P \in \mathcal{H}$, on note $v_P(f)$ l'ordre de zéro (ou moins l'ordre de pôle) de f en P. Alors, on a*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\omega(f) + \sum_{P \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}, P \neq i,\omega} v_P(f) = \frac{k}{12}$$

Schéma de démonstration Voir [6] Chapter III, §2, Propositon 8. Il suffit d'intégrer $\frac{f'}{f}$ sur le chemin donné par H, qui suit à peu près le bord de $\mathcal{R}$, comme dans l'image ci-dessous, tirée de [6, pp 115].





□

On peux aussi définir des fonction modulaires par rapport au sous-groupe de Γ défini par $\Gamma_0(m) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod m\}$. Dans cet exposé, on s'intéresse seulement au cas des fonctions de poids 0.

Définition 3.3. *Soient f une fonction méromorphe sur $\mathcal{H}$ et m un entier. On dit que f est une* ***fonction modulaire pour*** $\Gamma_0(m)$ ***de poids*** 0 *si elle est méromorphe sur $\mathcal{H}$ et vérifie :*

1. *$f(\gamma z) = f(z)$ pour tout $\gamma \in \Gamma_0(m)$ et tout $z \in \mathcal{H}$.*
2. *Elle est méromorphe en tous les cusps.*

Expliquons la deuxieme condition. Soit f une fonction méromorphe sur $\mathcal{H}$ vérifiant la première condition. Alors, pour chaque $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f_\gamma(z) = f(\gamma z)$ est une fonction de z m-périodique. En effet, si $\tau = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, alors $f_\gamma(m+z) = f(\gamma\tau z) = f(\gamma\tau\gamma^{-1}\gamma z) = f(\gamma z) = f_\gamma(z)$. On dit que f_γ est méromorphe en ∞ si sa série de Fourier

$$f_\gamma(z) = \sum_{n\in\mathbb{Z}} a_n q^{n/m}$$

n'a qu'un nombre fini de a_n non nuls avec n négatif. Ici, $q = \exp(2\pi i z)$. Et on dit que f est méromorphe en tous les cusps si f_γ est méromorphe en ∞ pour tous les $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

3.2 Séries d'Eisenstein

On va maintenant expliquer pourquoi j est modulaire et calculer sa série de Fourier.

Soit k un entier plus grand que 2. Pour $z \in \mathcal{H}$, on définit les séries d'Eisenstein :

$$G_k(z) := \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^k}$$

Alors G_k est une fonction modulaire de poids k.

En effet, il est clair que G_m est holomorphe sur $\mathcal{H}$ car la série converge absolument sur $\mathcal{H}$. De plus, soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, alors

$$G_k(\gamma z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\gamma z+n)^k} = (zc+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{((ma+nc)z+mb+nd)^k}$$

$$= (cz+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^k} = (cz+d)^k G_m(z)$$

Il reste à montrer que G_k est méromorphe en ∞. Calculons sa série de Fourier dans le cas où k est pair. (En effet, G_k est nulle si k est impair.)

Proposition 3.4. *Soient k un entier pair et $z \in \mathcal{H}$, alors*

$$G_k(z) = 2\zeta(k)(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n)$$

où ζ est la fonction ζ de Riemann, B_k le k-me nombre de Bernoulli, et où $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

On rappelle que $\zeta(k) = \frac{-(2\pi i)^k}{k!}$ et que les B_k sont définis par $\frac{x}{e^x-1} = \sum_{k\in\mathbb{Z}} B_k \frac{x^k}{k!}$.

Démonstration Comme

$$\sin \pi z = \pi z \prod_{n=1}^{\infty}(1-\frac{z}{n})(1+\frac{z}{n})$$

On a :

$$\pi\frac{\cos \pi z}{\sin \pi z} = \frac{1}{z} + \sum_{n=1}^{\infty}(\frac{1}{z-n} + \frac{1}{z+n}) \tag{1}$$

Comme

$$\cos \pi z = \frac{1}{2}e^{-i\pi z}(e^{2i\pi z}+1), \sin \pi z = \frac{1}{2i}e^{-i\pi z}(e^{2i\pi z}-1)$$

On a :

$$\pi\frac{\cos \pi z}{\sin \pi z} = \pi i\frac{q+1}{q-1} = \pi i + \frac{2\pi i}{q-1} = \pi i - 2\pi i\sum_{v=0}^{\infty} q^v \tag{2}$$

où $q = e^{2\pi i z}$.
En comparant (1) et (2), on en déduit que :

$$\frac{1}{z}+\sum_{n=1}^{\infty}(\frac{1}{z-n}+\frac{1}{z+n})=\pi i-2\pi i\sum_{v=0}^{\infty}q^v$$

On dérive cette equation k fois :

$$(-1)^{k-1}(k-1)!\sum_{n=-\infty}^{\infty}(z-n)^{-k}=-\sum_{v=1}^{\infty}(2\pi i)^k v^{k-1}q^v$$

Comme k est pair, on a

$$\sum_{n=-\infty}^{\infty}(mz+n)^{-k}=\frac{(2\pi i)^k}{(k-1)!}\sum_{v=1}^{\infty}n^{k-1}q^{mv}=-\frac{2k}{B_k}\zeta(k)\sum_{v=1}^{\infty}n^{k-1}q^{mv}$$

Alors

$$\begin{aligned}
G_k(z) &= \sum_{(m,n)\neq(0,0)}(mz+n)^{-k}\\
&= \sum_{n=-\infty}^{\infty}n^{-k}+2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}(mz+n)^{-k}\\
&= 2\zeta(k)(1-\frac{2k}{B_k}\sum_{m=1}^{\infty}\sum_{v=1}^{\infty}n^{k-1}q^{mv})\\
&= 2\zeta(k)(1-\frac{2k}{B_k}\sum_{n=1}^{\infty}(\sum_{d|n}d^{k-1})q^n)\\
&= 2\zeta(k)(1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n)
\end{aligned}$$

□

En particulier, on a

$$g_2:=60G_4=\frac{(2\pi)^4}{(2^23)}(1+240X),X=\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

$$g_3:=140G_6=\frac{(2\pi)^6}{2^33^3}(1-504Y),Y=\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

Donc la fonction

$$\Delta:=g_2^3-27g_3^2=\frac{(2\pi)^6}{2^63^3}[(1+240X)^3-(1-504Y)^2]$$

est une fonction modulaire de poids 12. On observe que $[(1+240X)^3 - (1-504Y)^2] \equiv 3^2 2^4 (5X+7Y) \mod 2^6 3^3$. Comme pour tous les entiers n, $\sigma_3(n) \equiv \sigma_5(n) \mod 12$ (car $d^3 \equiv d^5 \mod 12$ pour tout d), on a $\Delta = (2\pi)^6 q(1 + \sum_{n=1}^{\infty} \tau_{n+1} q^n)$ avec $\tau_n \in \mathbb{Z}$ pour tout n.

Comme $j = 12^3 \frac{g_2^3}{\Delta}$, on obtient

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n$$

avec tous les a_n entiers. La fonction j est donc une fonction modulaire de poids 0. Comme on a déja vu que δ est non nulle dans $\mathcal{H}$, on obtient alors :

Corollaire 3.5. *La fonction j est une fonction modulaire de poids 0. De plus, j est holomorphe sur $\mathcal{H}$ et son q-développement est donné par $\frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n$ avec les a_n entiers.*

[3] donne les valeurs suivantes pour les premiers coefficients :
$a_1 = 196884$, $a_2 = 21493760$, $a_3 = 864299970$, $a_4 = 20245856256$, $a_5 = 333202640600$.
De plus, pour les petites valeurs de $k \in \mathbb{N}$, on a $|a_k| \leq (200\,000)^n$.

Remarque Les coefficients du développement admettent l'équivalent suivant :

$$a_n \sim_{n\to\infty} \frac{e^{4\pi\sqrt{n}}}{\sqrt{2} n^{\frac{3}{4}}}.$$

On pourra voir [11] pour une preuve de cet équivalent.

3.3 La fonction j

La fonction j est exceptionnelle parmi les fonctions modulaires de poids 0. En effet, elle engendre le corps composé de ces fonctions. Plus généralement, si on fixe un entier positif m, alors $j(z)$ et $j(mz)$ engendrent le corps des fonctions modulaires pour $\Gamma_0(m)$ de poids 0. On commence par établir la bijectivité de j qu'on a utilisée en 2.15.

Proposition 3.6. *La fonction $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \to \mathbb{C}$ est bijective.*

Démonstration Pour chaque nombre complexe c, on définit $j_c(z) = j(z) - c$. Alors j_c est une fonction modulaire de poids 0. De plus, $v_\infty(j_c) = -1$. Donc par le théorème 3.2, il existe un point P dans $\mathcal{H}$, telle que $v_P(j_c) > 0$. C'est-à-dire que $j(P) = c$.

Par ailleurs, le seul pôle de $j - c$ est ∞ et c'est un pôle simple. Comme $f - c$ est encore une fonction modulaire de poids 0, on a $\frac{1}{2}v_i(j-c) + \frac{1}{3}v_\omega(j-c) + \sum_{P \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}, P \neq i,\omega} v_P(j-c) = 1$. On en déduit sans difficulté que $j - c$ s'annule en exactement un point dans $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. Donc j est injective. □

Les théorèmes fondamentaux de cette section sont les deux théorèmes suivants :

Théorème 3.7. *Soit f une fontion modulaire de poids 0.*

1. *Si on a de plus, f est holomorphe sur $\mathcal{H}$, alors $f \in \mathbb{C}[j]$. Si de plus les coefficients de la série de Fourier de f sont des entiers, alors $f \in \mathbb{Z}[j]$.*
2. *Si f est méromorphe sur $\mathcal{H}$, alors $f \in \mathbb{C}(j)$.*

Démonstration

1. On note n l'ordre du pôle de f en ∞ ; si f est holomorphe en ∞, on pose $n = 0$. On écrit la série de Fourier de f $\sum_{k=-n}^{0} c_k q^k + \sum_{k=1}^{\infty} c_k q^k$. On montre le résultat par récurrence sur n.

   Si $n = 0$, alors $f - c_0$ est une fonction modulaire de poids 0 holomorphe partout et s'annulant en ∞. Donc elle est nulle partout par le théorème 3.2. Donc $f = c_0 \in \mathbb{C}[j]$. Si de plus $c_0 \in \mathbb{Z}$, alors $f \in \mathbb{Z}[j]$.

   Si ce théorème est vrai pour un entier n, alors pour le cas $n + 1$, on pose $P(x) = c_{n+1}x^{n+1}$, et $g := f - P(j)$ est une fonction modulaire de poids 0. Comme le q-développement de j commence par $1/q$, on a $v_\infty(g) \geq -n$. Par l'hypothèse de récurrence, on a alors $g \in \mathbb{C}[j]$. Si de plus les coefficients du q-développement de f sont dans $\mathbb{Z}$, c'est vrai aussi pour g. Donc par l'hypothèse de récurrence, $g \in \mathbb{Z}[j]$. Donc $f \in Z[j]$.
2. Maintenant soit f une fonction modulaire non nulle quelconque. Comme les pôles de f sont isolés et que ∞ est un pôle de f, alors le nombre de pôles de f dans $\mathcal{R}$ est fini. On dénote les pôles de f dans $\mathcal{R}$ par $z_1, z_2, \cdots, z_N$ avec N un entier naturel, et on dénote leurs ordres par $m_1, m_2, \cdots, m_N$. Donc la fonction $g(z) := \prod_{i=1}^{N}(j(z) - j(z_i)^{m_i} f(z)$ est une fonction modulaire de poids 0 holomorphe sur $\mathcal{R}$. Comme tous les

points de $\mathcal{H}$ équivalent à un point de $\mathcal{R}$ et comme g est invariante par $\mathrm{SL}_2(\mathbb{Z})$, on en déduit que g est holomorphe sur $\mathcal{H}$. Par 1, on a alors $g \in \mathbb{C}[j]$. On en déduit $f \in \mathbb{C}(j)$.

□

Plus généralement, on a :

Théorème 3.8. *Soit f une fonction modulaire pour $\Gamma_0(m)$ de poids 0, alors f est une fonction rationelle de $j(z)$ et $j(mz)$. De plus, si tous les coefficients du q-développement de f sont rationnels, alors $f(z) \in \mathbb{Q}(j(z), j(mz))$*

On montrera ce théorème après avoir construit les équations modulaires. On explique tout d'abord pourquoi $j(mz)$ est effectivement une fonction modulaire pour $\Gamma_0(m)$ de poids 0.

Lemme 3.9. *La fonction $z \mapsto j(mz)$ est une fonction modulaire pour $\Gamma_0(m)$ de poids 0.*

Démonstration On montre d'abord que $j(mz)$ est invariante par $\Gamma_0(m)$. En effet, soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(m)$; on pose $\gamma' = \begin{pmatrix} a & bm \\ c/m & d \end{pmatrix}$, alors $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. De plus,

$$j(m\gamma z) = j(\frac{m(az+b)}{cz+d}) = j(\frac{a(mz)+mb}{c/m(mz)+d}) = j(\gamma'(mz)) = j(mz)$$

Donc la fonction $z \mapsto j(mz)$ est invariante par $\Gamma_0(m)$.

On fixe $\tau \in \mathrm{SL}_2(\mathbb{Z})$. On sait qu'il existe $\tau' \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\tau' \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \tau = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. On pose $\sigma := \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$. Alors $AD = det(\sigma) = m$.

On a $j(m\tau z) = j(\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \tau z) = j(\tau'^{-1}\sigma z) = j(\sigma z)$. On pose $\zeta = e^{2\pi i/m}$, et alors $q(\sigma z) = e^{2\pi i(az+b)/d} = \zeta^{ab}(q^{1/m})^{a^2}$. On pose $Q = q^{1/m}$ et on obtient alors le q-développement de $z \mapsto j(m\tau z) = j(\sigma z)$:

$$\frac{\zeta^{-ab}}{Q^{a^2}} + 744 + \sum_{n=1}^{\infty} c_n \zeta^{abn} Q^{a^2 n}$$

où les c_n sont les coefficients du q-développement de j. Alors la fonction $z \mapsto j(m\tau z)$ est méromorphe à ∞. On en déduit que la fonction $z \mapsto j(mz)$ est une fonction modulaire pour $\Gamma_0(m)$ de poids 0. □

Les résultats des deux sections suivantes vont servir à démontrer l'intégralité du j-invariant puis l'intégralité de sa racine cubique dans certains cas ; on peut se reporter à 5.1 pour une définition de la multiplication complexe et à §5 pour un aperçu des enjeux de ce qui suit.

3.4 Equations modulaires

On en arrive à un des théorèmes principaux de cet exposé :

Théorème 3.10. *Soit E une courbe elliptique à multiplication complexe. Alors $j(E)$ est un entier algébrique.*

On définira la multiplication complexe en 5.1.

Dans cette section, on va constuire explicitement un polynôme unitaire tel que $j(E)$ en soit une des racines.

Définition 3.11. *Soit $n \in \mathbb{N}$. On pose $D_n = \{M \in \mathcal{M}_2(\mathbb{Z}) : \det M = n\}$, $S_n = \{\begin{pmatrix} a & d \\ 0 & b \end{pmatrix} : ab = n, b \in \mathbb{N}^*, 0 \leq d < b\}$. Il est facile de voir que $S_n = \mathrm{SL}_2(\mathbb{Z})\backslash D_n$. Comme S_n est fini, on peut définir $F_n(X) := \prod_{M \in S_n} (X - j \circ M) = \sum_{m \in \mathbb{N}} s_m X^m$.*

On verra que les coefficients s_m sont dans $\mathbb{Z}[j]$. Par le théorème 3.7, il suffit de montrer les deux lemmes suivantes :

Lemme 3.12. *Les coefficents de F_n sont des fonctions modulaires de poids 0 et holomorphes sur $\mathcal{H}$.*

Lemme 3.13. *Les séries de Fourier des coefficients de F_n sont à coefficients entiers.*

Démonstration du lemme 3.12 Les coefficients s_m sont des fonctions symétriques de l'ensemble $\{j \circ M | M \in S_n\}$, donc holomorphes sur $\mathcal{H}$.

On montre d'abord que s_m est invariant par $\mathrm{SL}_2(\mathbb{Z})$. On fixe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Comme $S_n = \mathrm{SL}_2(\mathbb{Z})\backslash D_n$, on a pour tout $M \in S_n$, l'existence d'un unique δ_M dans $\mathrm{SL}_2(\mathbb{Z})$, tel que $\delta_M M\gamma \in S_n$. De plus, si M, M' sont deux éléments dans S_n tels que $\delta_M M\gamma = \delta_{M'} M'\gamma$, on a $M' = \delta M$ avec $\delta \in \mathrm{SL}_2(\mathbb{Z})$, alors on a forcément que $M = M'$. On en déduit que l'ensemble $\{\delta_M M\gamma\} = S_n$. Donc $\{j \circ (M\gamma) : M \in S_n\} = \{j \circ (\delta_M^{-1}) \circ (\delta_M M\gamma) : M \in S_n\} = \{j \circ (\delta_M M\gamma) : M \in S_n\} = \{j \circ M : M \in S_n\}$. La deuxime égalité vient du fait que j est

invariant par $\mathrm{SL}_2(\mathbb{Z})$.

Il reste de montrer que s_m est méromorphe à ∞. Pour chaque $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$, comme $j = \frac{1}{q} + \sum_{k=0}^{\infty} a_k q^k$, on a

$$j \circ M(z) = e^{-2\pi i \frac{az+b}{d}} + \sum_{k=0}^{\infty} a_k e^{2\pi i k \frac{az+b}{d}}$$

Alors $q^{n+1} j \circ M(z) \to 0$ quand q tend vers 0 car $|a/d| \leq n$. Par le fait que S_n est fini, il existe un entier N tel que $q^N s_m(z) \to 0$ quand q tend vers 0. Ce qui revient à dire que s_m est méromorphe à ∞.

□

Démonstration du lemme 3.13 On note $\zeta = e^{\frac{2i\pi}{n}}$, $Q = q^{\frac{1}{n}} = e^{\frac{2i\pi z}{n}}$; $G = Gal(\mathbb{Q}[\zeta]/\mathbb{Q})$. On remarque que s_m se développe en une série entiére en Q ; comme elle est 1-périodique, c'est en fait une série en q. On va montrer que les coefficients du développement en Q des s_m sont à la fois dans $\mathbb{Z}[\zeta]$ et dans $\mathbb{Q}$.

Soit $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$.

Alors $q \circ M(z) = \zeta^{ab} Q^{a^2}$, puis $j \circ M(z) = \zeta^{-ab} Q^{-a^2} + \sum_{k=0}^{\infty} a_k \zeta^{abk} Q^{a^2 k}$, où les a_k sont les coefficients (entiers !) du développement de Fourier en q de$j$. Les $a_k \zeta^{abk}$ sont bien dans $\mathbb{Z}[\zeta]$. Par définition, les coefficients des développements des s_m sont bien dans $\mathbb{Z}[\zeta]$.

De plus, si $\sigma \in G$, alors $\sigma(\zeta) = \zeta^{p_\sigma}$ pour un p_σ premier avec n. Alors $(j \circ M)^\sigma = \zeta^{-p_\sigma ab} Q^{-a^2} + \sum_{k=0}^{\infty} a_k \zeta^{p_\sigma abk} Q^{a^2 k}$. On a alors $\left(j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right)^\sigma = \left(j \circ \begin{pmatrix} a & p_\sigma b \\ 0 & d \end{pmatrix} \right)$. Or $\{p_\sigma b | 0 \leq b < d\} = \mathbb{Z}/d\mathbb{Z}$ car p_σ est premier avec d, puisque $ad = n$. j étant invariant sous l'action de $\mathrm{SL}_2(\mathbb{Z})$, on en déduit $\{(j \circ M)^\sigma | M \in S_n\} = \{(j \circ M) | M \in S_n\}$. Donc les s_m sont invariants sous l'action de G, donc leurs développements de Fourier en Q sont à coefficients dans $\mathbb{Q}$.

Ainsi les coefficients du développement en Q (donc en q) des s_m sont dans $\mathbb{Z} = \mathbb{Z}[\zeta] \cap \mathbb{Q}$.

□

On en déduit le théorème suivant :

Théorème 3.14. *Il existe $F_n \in \mathbb{Z}[X,Y]$ tel que $F_n(j,X) = \prod_{M\in S_n}(X - j\circ M)$.*

Pour la propriété d'intégralité, on a aussi besoin de la propriété unitaire suivante :

Proposition 3.15. *Soit $n \in \mathbb{N}$ tel que $n \notin \mathbb{N}^2$. Alors $H_n(X) = F_n(X,X)$ est non constant, de coefficient dominant dans $\{-1, 1\}$.*

Démonstration On écrit le développement en série de Fourier en Q de $j - j\circ M$ pour $M \in S_n$; on obtient que le partie négative de la série de Fourier de $j - j\circ M$ est $Q^{-n} - \zeta^{ab}Q^{-a^2}$, non nulle et de coefficient dominant une racine n-ème de l'unité car n n'est pas un carré. On en déduit que $F_n(j,j)$ est non constant, de coefficient dominant une racine de l'unité. Comme on a déja vu que $F_n(j,j) \in \mathbb{Z}[j]$, on en déduit que $F_n(X,X)$ est non-constant et de coefficient dominant -1 ou 1. □

3.5 Fonctions modulaires sur $\Gamma_0(m)$ de poids 0

On fixe m un entier positif. On montre maintenant le théorème 3.8 :

Soit f une fonction modulaire pour $\Gamma_0(m)$ de poids 0 ; alors f est une fonction rationnelle de $j(z)$ et $j(mz)$. De plus, si on a tous les coefficients du q-développement de f rationnels, on a $f(z) \in \mathbb{Q}(j(z), j(mz))$.

Tout d'abord, construisons un nouveau type d' équation modulaire.

Construction de $\Phi_m(X,Y)$ Dans la suite, on fixe $\{\gamma_i, i \in I\}$ des éléments de $\mathrm{SL}_2(\mathbb{Z})$ qui représentent les classes à droite de $\Gamma_0(m)$ dans $\mathrm{SL}_2(\mathbb{Z})$ telles que $\gamma_1 = Id$. Et on note $\sigma_0 := \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$. On pose $T_m = \{\begin{pmatrix} a & d \\ 0 & b \end{pmatrix} : ab = n,\ b \in \mathbb{N}^*, 0 \le d < b,\ pgcd(a,b,d) = 1\}$. C'est un sous-ensemble de S_m.

Comme $\mathrm{SL}_2(\mathbb{Z})\backslash D_n = S_n$, on a pour chaque $i \in I$, l'existence d'un unique $\sigma_i \in S_n$ tel que $\gamma_i'\sigma_i = \sigma_0\gamma_i$ avec $\gamma_i' \in \mathrm{SL}_2(\mathbb{Z})$. Alors σ_i est dans T_n car le pgcd des coefficients de σ_i est égal au pgcd des coefficients de σ_0, donc 1. Pour $i = 1$, on a $\sigma_1 = \sigma_0 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$. De plus, $j(\sigma_i z) = j(\gamma_i'\sigma z) = j(\sigma_0\gamma_i z) = j(m\gamma_i z)$.

Par ailleurs, soit $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ un élément de T_m, alors il existe $\alpha, \beta \in \mathbb{Z}$ tels que $pgcd(\alpha d, \beta a - \alpha b) = 1$. En effet, on pose $c = (a, b)$ et $a' = a/c$, $b' = b/c$. Alors, il existe $u, v \in \mathbb{Z}\backslash 0$ tels que $va' - ub' = 1$. En particulier, u est premier avec a'. Donc pour tout nombre premier p, soit p ne divise pas u, soit p ne divise pas $u + a'$. Par le théorème chinois, il existe un entier k tel que $u + ka'$ est premier avec c. On pose $\alpha = u + ka'$, $\beta = v + kb'$, alors $pgcd(\alpha d, \beta a - \alpha b) = pgcd(\alpha d, c) = pgcd(\alpha, c) = 1$.

Manitenant posons $x = \alpha d$, $y = \beta a - \alpha b$. Comme $pgcd(x, y) = 1$, il existe deux entiers z, w tels que la matrice $\gamma' := \begin{pmatrix} x & y \\ z & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, de plus $\gamma'\sigma = \begin{pmatrix} \alpha ad & \beta ad \\ za & zb + wd \end{pmatrix}$. Comme $m = ad$, il existe alors $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma'\sigma = m\gamma$. On écrit $\gamma\ \delta\gamma_i$ avec un $i \in I$ et $\delta \in \Gamma_0(m)$. Alors $j(\sigma z) = j(\gamma'\sigma z) = j(\sigma_0\gamma_i z) = j(m\delta\gamma_i z) = j(m\gamma z)$ car $z \mapsto j(mz)$ est invariante par $\Gamma_0(m)$. Il est facile de voir que ce γ_i est unique.

On en déduit que le lemme suivant :

Lemme 3.16. *Il existe une correspondance entre* $\Gamma_0(m)\backslash\mathrm{SL}_2(\mathbb{Z}) = \{\gamma_i, i \in I\}$ *et* $T_m = \{M_i : i \in I\}$ *tel que* $j(m\gamma_i z) = j(\sigma_i z)$. *De plus, comme l'ensemble* T_m *est fini,* I *est fini. On peut donc supposer que* $I = \{1, 2, \cdots, N\}$ *avec un entier positif* N.

On peut maintenant définir une équation modulaire comme dans la section précédente :

On pose $\Phi_m(X) = \prod_{ß=1}^{N}(X - j \circ \sigma_i)$. Par le lemme précédent, $\Phi_m(X) = \prod_{i=1}^{N}(X - j \circ (m\gamma_i))$.

Soit γ un élément de $\mathrm{SL}_2(\mathbb{Z})$. Comme $\gamma_i\gamma, i \in I$ représentent les classes à droites de $\Gamma_0(m)$ dans $\mathrm{SL}_2(\mathbb{Z})$ et comme l'application $z \mapsto j(mz)$ est invariante sous l'action de $\Gamma_0(m)$, on a alors $\prod_{i=1}^{N}(X - j\circ(m\gamma_i)) = \prod_{i=1}^{N}(X - j\circ(m\gamma_i\gamma))$. Donc les coéfficients de Φ sont invariants sous l'action de $\mathrm{SL}_2(\mathbb{Z})$.

On a vu dans la section précédent que $q^{n+1} j \circ (M_i)(z) \to 0$ quand $q \to 0$ pour tout $i \in I$. Les coéfficients de Φ sont donc mérompprphes en ∞.

On en déduit que les coéfficients du Φ sont des fonctions modulaires de poids 0 holomorphes sur $\mathcal{H}$. Donc ils sont dans $\mathbb{C}[j]$.

Comme dans la section précédente, on peut en déduire que les coéfficients du Φ sont dans $\mathbb{Z}[j]$. On obtient le théorème suivant :

Théorème 3.17. *Il existe* $\Phi_m \in \mathbb{Z}[X, Y]$ *tel que* $\Phi_m(j, X) = \prod_{i=1}^{N}(X - j \circ \sigma_i) = \prod_{i=1}^{N}(X - j \circ (m\gamma_i))$.

On peut alors démontrer le théorème 3.8.

Démonstration du théorème 3.8

Soit f une fonction modulaire pour $\Gamma_0(m)$ de poids 0 ; on pose

$$G(X) = \Phi_m(j(z), X) \prod_{i=1}^{N} \frac{f(\gamma_i z)}{X - j(m\gamma_i z)} = \sum_{i=1}^{N} (f(\gamma_i z) \prod_{j \neq i} (X - j(m\gamma_j z)))$$

Comme on l'a fait pour Φ_m, on montre que coéfficients de G sont des fonction modulaires de poids 0, donc dans $\mathbb{C}(j)$ par le théorème 3.7, c'est-à-dire que $G(j(z), X) \in \mathbb{C}(j(z))[X]$.

En remplaçant X par $j(\sigma_1 z)$, on a alors

$$G(j(z), j(mz)) = f(z) \prod_{j \neq 1} (j(mz) - j(m\gamma_j z)) = f(z) \prod_{j \neq 1} (j(\sigma_1 z) - j(\sigma_j z))$$

Comme σ_j et σ_1 ne sont pas dans la même orbite pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ dans D_n pour tout $j \neq 1$, on a alors que $j(\sigma_1 z) - j(\sigma_j z)$ est non nulle pour tout $j \neq 1$. Donc

$$f(z) = \frac{G(j(z), j(mz))}{\prod_{j \neq 1} (j(\sigma_1 z) - j(\sigma_j z))} \in \mathbb{C}(j(z), j(mz))$$

comme on veut.

Si de plus les coefficients du q-développement de f sont dans $\mathbb{Q}$, comme on a déja $\prod_{j \neq 1} (j(\sigma_1 z) - j(\sigma_j z)) = \Phi'_m(j(mz)) \in \mathbb{Z}[j(z), j(mz)]$, il suffit de montrer que $G(j(z), j(mz)) \in \mathbb{Q}(j(x), j(mz)$.

En effet, comme on a vu que $G(j(z), j(mz)) \in \mathbb{C}(j(x))[j(mz]$, il existe deux polynômes $P \in \mathbb{C}[X, Y]$ et $Q \in C[X], Q \neq 0$ tels que $G(j(z), j(mz)) = \frac{P(j(z), j(mz))}{Q(j(z))}$. On écrit P et Q comme $P(X, Y) = \sum_{i=1}^{N} \sum_{k=1}^{M} a_{ik} X^i Y^k$ et $Q(X) = \sum_{l=1}^{L} b_l X^l$. Alors $G = P/Q$ est équivalent à

$$\sum_{i=1}^{N} \sum_{k=1}^{M} a_{ik} j(z)^i j(mz)^k = f(z) \Phi'_m(j(mz)) (\sum_{l=1}^{L} b_l (j(z))^l)$$

En considérant les q-développements, on sait qu'il est équivalent à un système linéaire homogène en les a_{ik} et b_l. Comme tous les coefficients des

q-développements de $j(z)$, $j(mz)$, $f(z)$ et $\Phi'_m(j(mz))$ sont dans $\mathbb{Q}$, les coefficients de ce système linéaire sont dans dans $\mathbb{Q}$. De plus, il a une solution dans $\mathbb{C}$ tel que les b_l ne sont pas tous nuls. Alors il existe une solution de ce système dans $\mathbb{Q}$ qui rendre les b_l non tous nuls. C'est-à-dire que $G(j(z), j(mz)) \in \mathbb{Q}(j(z), j(mz))$. □

4 Groupe des classes d'un corps quadratique imaginaire

On va donner une méthode de calcul du nombre de classes d'idéaux de l'anneau des entiers d'un corps quadratique imaginaires. En particulier, on montrera que l'anneau des entiers du corps $\mathbb{Q}[\sqrt{-163}]$ est principal.

4.1 Corps de nombres quadratiques

Définition 4.1. *On appelle corps de nombres toute extension finie de $\mathbb{Q}$.*

On dit que K est un corps de nombres quadratique si c'est une extension algébrique finie de degré 2 de $\mathbb{Q}$.

Il existe alors $d \in \mathbb{Z}^*$ tel que $\sqrt{d} \notin K$ et $K = \mathbb{Q}[\sqrt{d}]$. En effet, si $z \in K \backslash \mathbb{Q}$, z est élément primitif de K, et il existe a, $b \in \mathbb{Q}$ tels que $z^2 + az + b = 0$. Alors $\mathbb{Q}[z] = \mathbb{Q}[\sqrt{a^2 - 4b}]$. Or $a^2 - 4b = \frac{p}{q}$ est un rationnel. On peut écrire $\frac{p}{q} = \frac{pq}{q^2}$, puis $K = \mathbb{Q}[\sqrt{pq}]$, où pq est bien un entier relatif.

Si $d > 0$, K est dit réel ; sinon, K est dit imaginaire.

K est donc le corps de décomposition du polynôme séparable $X^2 - d$; l'extension $\mathbb{Q} \hookrightarrow K$ est galoisienne, et on a de plus $Gal(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. On note σ l'élément de $Gal(K/\mathbb{Q})$ différent de l'identité.

Proposition 4.2. *Pour deux entiers relatifs a et b, on a*

$$\mathbb{Q}[\sqrt{a}] = \mathbb{Q}[\sqrt{b}] \Leftrightarrow \exists r \in \mathbb{Q} : a = r^2 b$$

Démonstration Si on suppose $\mathbb{Q}[\sqrt{a}] = \mathbb{Q}[\sqrt{b}]$, alors $Gal(\mathbb{Q}[\sqrt{a}]/\mathbb{Q}) = Gal(\mathbb{Q}[\sqrt{b}]/\mathbb{Q}) = G$. On en déduit $G = \{id; \sigma\}$, avec $\sigma_{|\mathbb{Q}} = id_{|\mathbb{Q}}$, $\sigma(\sqrt{a}) = -\sqrt{a}$, $\sigma(\sqrt{b}) = -\sqrt{b}$. Donc $r = \sqrt{\frac{a}{b}}$ est invariant sous l'action de G, puis $r \in \mathbb{Q}$.

Le sens réciproque est clair.

□

On note $\mathcal{A} = \mathbb{Q}^*/\mathbb{Q}^{*2}$ l'ensemble des entiers sans carrés parmi leurs facteurs entiers.

Proposition 4.3. *L'ensemble des extensions quadratiques de $\mathbb{Q}$ est $(\mathbb{Q}[\sqrt{d}])_{d \in \mathcal{A}}$.*

□

On fixe $d \in \mathcal{A}$ et on note $K = \mathbb{Q}[\sqrt{d}]$.

Définition 4.4. *On note $\mathcal{O}_K$ et on appelle anneau des entiers de K la clôture intégrale de $\mathbb{Z}$ dans K.*

Proposition 4.5. *On a*

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] \Leftrightarrow d \equiv 2, 3\,[4]$$

$$\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \Leftrightarrow d \equiv 1\,[4]$$

Démonstration Soit $y \in \mathcal{O}_K$. Alors y s'écrit $a+b\sqrt{d}$ pour un couple (a, b) de rationnels. On note $G = Gal(K/\mathbb{Q})$. $G = \{id, \sigma\}$. On a $\sigma(y) = a - b\sqrt{d}$.

Comme $\mathcal{O}_K$ est un anneau, $y + \sigma(y) \in \mathcal{O}_K$ et $y\sigma(y) \in \mathcal{O}_K$. Or ces deux quantités sont stables sous l'action de G, donc sont dans $\mathbb{Q}$. Ce sont donc des entiers relatifs. Puis $2a \in \mathbb{Z}$ et $a^2 - b^2 d \in \mathbb{Z}$.

On en déduit successivement $4a^2 \in \mathbb{Z}$ puis $4b^2 d \in \mathbb{Z}$. On a alors, comme d n'a pas de diviseur carré, $2b \in \mathbb{Z}$.

Si $d \equiv 2\,[4]$, $db \in \mathbb{Z}$ car alors $d \equiv 0\,[2]$. On en déduit que $2b \times bd \in \mathbb{Z}$, puis $2a^2 \in \mathbb{Z}$; puisque $2a \in \mathbb{Z}$ et $2a^2 = 2a \times a$, on a nécéssairement $a \in \mathbb{Z}$. Alors $b^2 d \in \mathbb{Z}$ puis comme $bd \in \mathbb{Z}$, $b \in \mathbb{Z}$. Donc $y \in \mathbb{Z}[\sqrt{d}]$.

Réciproquement, si $z = p + q\sqrt{d}$,avec p, $q \in \mathbb{Z}$, $P = X^2 - 2pX + p^2 - dq^2$ est un polynôme unitaire á coefficients entiers annulant z.

Donc $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

Si $d \equiv 3\,[4]$, on suppose que $2b$ est impair. Alors $4b^2 \equiv 1\,[4]$, donc $4(a^2 - db^2) \equiv 3\,[4]$, ce qui est absurde. Donc $b \in \mathbb{Z}$. Donc $a^2 \in \mathbb{Z}$, puis $a \in \mathbb{Z}$. Donc $y \in \mathbb{Z}[\sqrt{d}]$.

Réciproquement, si $z = p + q\sqrt{d}$,avec p, $q \in \mathbb{Z}$, $P = X^2 - 2pX + p^2 - dq^2$ est un polynôme unitaire á coefficients entiers annulant z.

Donc $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

Si $d \equiv 1\,[4]$, on pose $\tau = \frac{1+\sqrt{d}}{2}$. On pose $\beta = 2b$ et $\alpha = a - b$. Alors $y = \alpha + \beta\tau$. On a alors $\beta \in \mathbb{Z}$ et $2\alpha \in \mathbb{Z}$.

De plus $4(\alpha^2 + \alpha\beta + \frac{\beta^2(d-1)}{4}) \in \mathbb{Z}$. Donc en développant, $4\alpha^2 + 4\alpha\beta \equiv 0[4]$. On en déduit que 2α est pair. Donc $\alpha \in \mathbb{Z}$. Puis $y \in \mathbb{Z}[\tau]$.

Réciproquement, si $z = p + q\tau$,avec p, $q \in \mathbb{Z}$, $P = X^2 - (2p+q)X + p^2 - pq - \frac{q^2(d-1)}{4}$ est un polynôme unitaire á coefficients entiers annulant z.

Puis $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

□

Définition 4.6. *On appelle discriminant de $\mathbb{Q}[\sqrt{d}]$, noté $\mathcal{D}$, le nombre défini par $\mathcal{D} = 4d$ si $d \equiv 2, 3\,[4]$ et $\mathcal{D} = d$ si $d \equiv 1\,[4]$.*

Remarque On donne dans l'annexe des détails sur la signification de $\mathcal{D}$ et sa valeur dans un corps de nombres quelconque.

4.2 Nombre des classes, triplet réduit

Soit A un anneau de Dedekind et F son corps des fractions ; on suppose $A \neq F$.

On peut munir l'ensemble des idéaux de A d'une relation d'équivalence Δ : pour deux idéaux I, J de A, on a $I\Delta J$ si et seulement s'il existe a, $b \in A$ tels que $(a)I = (b)J$ où (c) dénote l'idéal engendré par c. Δ est clairement une relation d'équivalence.

Les classes de Δ sont appelées les classes d'idéaux de A. On note $Cl(A)$ l'ensemble des classes, $h(A)$ le cardinal de $Cl(A)$ quand il est fini.

Remarque A est principal si et seulement s'il n'a qu'une seule classe d'idéaux.

Proposition 4.7. *Si I, J sont des idéaux de A, et si on note $[I]$, $[J]$ leurs classes respectives par Δ, alors on a $[I] \cdot [J] = [I \cdot J]$. $Cl(A)$ est donc un monoïde abélien d'élément neutre $[A]$.*

On note $Cl(K) = Cl(\mathcal{O}_K)$ l'ensemble des classes d'équivalence de Δ pour un corps quadratique K.

Proposition 4.8. *L'ensemble $Cl(K)$ est un groupe abélien sous l'opération $\cdot$, et la classe de $\mathcal{O}_K$ en est l'élément neutre.*

On montre d'abord un lemme.

Lemme 4.9. *Soit I un élément de $\mathcal{I}$. Alors il existe trois entiers m, a, b tels que $a \geq |b|$, $4a \mid b^2 - \mathcal{D}$ et $I = m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$.*

Démonstration On sait que l'idéal $I \bigcap \mathbb{Z}$ de $\mathbb{Z}$ est non-nul car pour chaque élément non-nul x de I, l'entier $x \cdot \overline{x}$ est un élément non-nul de $I \bigcap \mathbb{Z}$. On note n son générateur positif. Pour x un élément de I, il existe m, l dans $\mathbb{Z}$ tel que $x = \frac{l+m\sqrt{\mathcal{D}}}{2}$. On choisit un x dans $I \backslash \mathbb{Z}$ tel que la valeur absolue de m soit minimale. Il est clair que $I =< n, \frac{l+m\sqrt{\mathcal{D}}}{2} >$. En remplaçant l par $l + 2kn$ pour un certain entier k, on peut supposer que $|l| \leq n$.

Comme I est un idéal de $\mathcal{O}_K$, on a $n\frac{-\tau+\sqrt{\mathcal{D}}}{2} \in < n, \frac{l+m\sqrt{\mathcal{D}}}{2} >$. En particulier on a m divise n. De même on a $\frac{l+m\sqrt{\mathcal{D}}}{2}\frac{-\tau+\sqrt{\mathcal{D}}}{2} \in < n, \frac{l+m\sqrt{\mathcal{D}}}{2} >$, et donc

m divise $\frac{-m\tau+l}{2}$, donc divise l. On pose $a = n/m$ et $b = l/m$. Alors on en déduit que $I = m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$ et $a \geq |b|$. Comme $m^{-1}I =< a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$ est encore un idéal de $\mathcal{O}_K$, on a $(\frac{-b+\sqrt{\mathcal{D}}}{2})(\frac{b+\sqrt{\mathcal{D}}}{2}) = \frac{b^2-\mathcal{D}}{4} \in < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$. Alors on a bien $4a \mid b^2 - \mathcal{D}$. □

Démonstration de la proposition 4.8 Il suffit de montrer que tous les idéaux sont inversible dans $Cl(K)$. Soit I un élément de $\mathcal{I}$. Par le lemme 4.9, il existe trois entiers m, a, b, tels que $a \geq |b|$, $4a \mid b^2 - \mathcal{D}$ et $I = m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$. On pose $J :=< a, \frac{b+\sqrt{\mathcal{D}}}{2} >$, c'est encore un idéal de $\mathcal{O}_K$. De plus, $[I] \cdot [J] = \left[m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >< a, \frac{b+\sqrt{\mathcal{D}}}{2} >\right] = \left[m < a^2, -ab, a\sqrt{\mathcal{D}}, \frac{b^2-\mathcal{D}}{4} >\right] = \left[ma < a, -b, \sqrt{\mathcal{D}}, \frac{b^2-\mathcal{D}}{4a} >\right]$. On pose $g = pgcd(a, b, \frac{b^2-\mathcal{D}}{4a})$, alors g^2 divise $\mathcal{D}$. Comme d est sans facteur carré, on a $g = 1$ ou $g = 2$. Si $g = 2$, on a $d \equiv 2, 3$ modulo 4 et 4 divise $(\frac{b}{2})^2 - d$. C'est impossible. Donc on a $g = 1$. On en déduit que $[I] \cdot [J] = [ma\mathcal{O}_K] = [\mathcal{O}_K]$. □

On va donner un algorithme de calcul du nombre de classes d'un corps quadratique imaginaire à l'aide de triplets réduits.

Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique de discriminant $\mathcal{D}$ et d'anneau des entiers $\mathcal{O}_K$. On note $\mathcal{I}$ l'ensemble des idéaux de $\mathcal{O}_K$.

Définition 4.10. *On dit un triplet d'entiers (a, b, c) est **réduit** si $4ac - b^2 = -D$, $c \geq a \geq |b|$ où les deux égalités ne peuvent pas être atteintes en même temps et si une des égalités est atteinte, on a $b \geq 0$.*

On va montrer que le nombre de triplets réduits est égal au nombre de classes.

Lemme 4.11. *Le nombre des triplets réduits est fini.*

Démonstration Comme $c \geq a \geq |b|$, on a $-\mathcal{D} \geq 4a^2 - a^2 = 3a^2$. Donc le nombre de a dans les triplets est fini. Comme $a \geq |b|$ et c est uniquement déterminé par a, b, le nombre des triplets réduit est fini. □

Exemple 4.12. *Si $d = -163$, alors $\mathcal{D} = -163$. Le seule triplet réduit est $(1, 1, 41)$.*

En effet, si (a, b, c) est un triplet réduit, alors $163 \geq 3a^2 \geq 3b^2$, donc $|b| \leq 7$. Si b est pair, alors $4ac$ est impair, ce qui est absurde. Si $|b| = 1$, alors $164 = 4ac$, donc $ac = 41$, puis $a = 1$, $c = 41$, d'où $(a, b, c) = (1, 1, 41)$. Si $b^2 = 9$, $ac = 43$. Or 43 est premier, donc $a = 1$, ce qui est absurde car $|b| \leq a$. De même, si $b^2 = 25$, $ac = 47$, qui est également premier. Si $|b| = 7$, alors $ac = 55$, donc $a = 1$ ou $a = 5$, ce qui est impossible.

Le seul triplet réduit est bien $(1, 1, 41)$.

Proposition 4.13. *On suppose que* $\mathcal{D} < -4$. *Soit* $\mathcal{A}$ *une classe d'idéaux de* $\mathcal{O}_K$. *Alors il existe un unique triplet réduit* (a, b, c) *tel que l'idéal* $< a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$ *est dans* $\mathcal{A}$. *En particulier, le cardinal de* $Cl(K)$ *est égal au nombre de triplets réduits, et donc le cardinal de* $Cl(K)$ *est fini.*

Démonstration On montre d'abord l'existence d'un tel triplet. On choisit un élément I dans $\mathcal{A}$ tel que la norme de I soit minimale dans $\mathcal{A}$. Par le lemme 4.9, il existe des entiers m, a, b tels que $a \geq |b|$, $4a \mid b^2 - \mathcal{D}$ et $I = m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$. Comme l'idéal $m^{-1}I$ est encore dans $\mathcal{A}$ et $N(m^{-1}I) = a$, $N(I) = m^2 a$ d'aprés l'exemple **??**, on a $I = m^{-1}I$ par le choix de I.

Maintenant on pose $c = \frac{b^2-\mathcal{D}}{4a}$. Alors on a $4ac - b^2 = -\mathcal{D}$. Comme l'idéal $J = \frac{b+\sqrt{\mathcal{D}}}{2a} I =< c, \frac{b+\sqrt{\mathcal{D}}}{2} >$ est encore dans $\mathcal{A}$ et la norme de J est égale à c, on a $c \geq a$.

On suppose par absurde que $c = a = |b|$, alors on a $-\mathcal{D} = 3a^2$. Comme d est sans facteur carré, on a $a = 1$ ou $a = 2$. Alors $\mathcal{D} = -3$ ou $\mathcal{D} = -12$. Ils sont tous impossibles sous l'hypothèses $\mathcal{D} < -4$ et d est sans facteur carré. Si on a $a = |b|$, alors l'idéal $< a, \frac{b+\sqrt{\mathcal{D}}}{2} >$ est le même que l'idéal I. Donc on peut supposer que $b \geq 0$. Si on a $c = a$, on a l'idéal $J =< a, \frac{b+\sqrt{\mathcal{D}}}{2} >$ est dans $\mathcal{A}$. Donc on peut aussi supposer que $b \geq 0$.

Il reste à montrer que le triplet réduit est unique. En effet, si (a, b, c) et (a', b', c') sont deux triplets réduits tels que $I =< a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$ et $I' =< a', \frac{-b'+\sqrt{\mathcal{D}}}{2} >$ sont dans la même classe, il existe λ un élément non-nul de K, tel que $I' = \lambda I$. Comme (a, b, c) est réduit, il est facile de voir que $\pm a$ ont une norme minimale dans I et $\pm\frac{-b+\sqrt{\mathcal{D}}}{2}$ ont une norme minimale dans $I \setminus \mathbb{Z}$. On observe que $|\frac{-b+\sqrt{\mathcal{D}}}{2}| = \sqrt{ac}$.

Si $c > a$, alors $\pm a$ sont les deux seuls éléments de I qui ont la plus petite valeur absolue. Donc $a' = \pm\lambda a$. En remplaçant λ par $-\lambda$, on peut supposer que $a' = \lambda a$. En particulier, $\lambda \in \mathbb{R}_{>0}$. En considérant la partie imaginaire de I' et λI, on a $\lambda = 1$. Donc on a $b - b'$ est un multiple de $2a$. Par la définition de triplet réduit, on a forcément que $b = b'$. Donc on a $(a, b, c) = (a', b', c')$.

Si $c = a$, il y a exactement quatre éléments dans I qui ont la plus petite valeur absolue, c'est $\pm a, \pm\frac{-b+\sqrt{\mathcal{D}}}{2}$. Comme $I' = \lambda I$, on a $\pm a', \pm\frac{-b'+\sqrt{\mathcal{D}}}{2}$ sont les seuls quatres éléments dans I' qui ont la plus petite valeur absolue. Donc on a soit $\lambda a\mathbb{Z}{=}a'\mathbb{Z}$, $\lambda\frac{-b+\sqrt{\mathcal{D}}}{2}\mathbb{Z} = \frac{-b'+\sqrt{\mathcal{D}}}{2}\mathbb{Z}$, soit $\lambda a\mathbb{Z} = \frac{-b'+\sqrt{\mathcal{D}}}{2}\mathbb{Z}$, $\lambda\frac{-b+\sqrt{\mathcal{D}}}{2}\mathbb{Z} = a'\mathbb{Z}$. Dans le premier cas, on montre comme le cas précédent que $\lambda = \pm 1$. Alors $a = a'$ et $c = c'$. Donc $b^2 = b'^2$, et donc $b = b'$ car $b \geq 0$ et $b' \geq 0$. Dans le deuxième cas, on a $\frac{-b'+\sqrt{\mathcal{D}}}{2a} = \pm\frac{2a'}{-b+\sqrt{\mathcal{D}}}$, et donc $(-b+\sqrt{\mathcal{D}})(-b'+\sqrt{\mathcal{D}})) \in \mathbb{R}$. Mais $b \geq 0$ et $b' \geq 0$, on a forcément que $b = 0$ et $b' = 0$. Alors $4a^2 = -\mathcal{D}$, c'est impossible car $\mathcal{D} < -4$ et d est sans facteur carré.

On en déduit l'existence et l'unicité du triplet réduit voulu.

On a donc une bijection entre l'ensemble des triplets réduits et le groupe des classes, d'où la conclusion. □

Corollaire 4.14. *Si $K = \mathbb{Q}(\sqrt{-163})$, alors $\mathcal{O}_K$ est principal.* □

4.3 Finitude du nombre des classes, formule du nombre de classes

En fait, pour tout corps de nombres K, on peut définir la notion d'anneau des entiers $\mathcal{O}_K$ comme clôture algébrique de $\mathbb{Z}$.

Proposition 4.15. *Cet anneau $\mathcal{O}_K$ est toujours de Dedekind.*

Démonstration On le démontre d'abord pour $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique.

$\mathcal{O}_K$ est intégralement clos par construction.

On a, selon le reste modulo 4 de d, $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - d)$ ou $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - X + \frac{1-d}{4})$; $\mathbb{Z}$ étant noethérien car principal, $\mathcal{O}_K$ est noethérien en tant que $\mathbb{Z}$-algèbre d'après le théorème de Hilbert.

Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_K$. Soit $x \in \mathfrak{P} \setminus \{0\}$. On considére $\mu = X^2 + a_1X + a_0$ le polynôme minimal de x dans $\mathbb{Z}[X]$. Alors $a_0 \neq 0$. On a clairement $a_0 \in x\mathcal{O}_K \cap \mathbb{Z} \subset \mathfrak{P} \cap \mathbb{Z}$.

Or pour $x, y \in \mathbb{Z}$,

$$xy \in \mathfrak{P} \cap \mathbb{Z} \Rightarrow xy \in \mathfrak{P} \Rightarrow x \in \mathfrak{P} \text{ ou } y \in \mathfrak{P} \Rightarrow x \in \mathfrak{P} \cap \mathbb{Z} \text{ ou } y \in \mathfrak{P} \cap \mathbb{Z}.$$

Donc $\mathfrak{P} \cap \mathbb{Z}$ est premier, donc maximal, car $\mathbb{Z}$ est de Dedekind puisque principal. Ainsi $\mathbb{Z}/\mathfrak{P}\cap\mathbb{Z}$ est un corps, isomorphe à un sous-anneau de $\mathcal{O}_K/\mathfrak{P}$.

Comme tout élément de $\mathcal{O}_K$ est entier sur $\mathbb{Z}$, tout élément de $\mathcal{O}_K/\mathfrak{P}$ est entier sur $\mathbb{Z}/\mathfrak{P}\cap\mathbb{Z}$ (on dit alors qu'un anneau est entier sur son sous-anneau).

Or si $A \subset B$ sont deux anneaux intégres, avec B entier sur A, B est un corps si et seulement si A en est un. (Démonstration aisée). Donc $\mathcal{O}_K/\mathfrak{P}$ est un corps, puis $\mathfrak{P}$ est maximal.

Donc $\mathcal{O}_K$ est de Dedekind.

On procède comme pour un corps quadratique. Le point difficile est le fait que l'anneau soit noethérien. Pour cela, on pourra voir [12] ou le TD d'algèbre 2.

□

Soit A un anneau, F son corps des fractions.

Définition 4.16. *On appelle idéal fractionnaire sur A tout sous-A-module I de F tel qu'il existe $d \in A \setminus \{0\}$ tel que $dI \subset A$. Quand $d = 1$, on dit que l'idéal est entier (c'est alors un idéal de A au sens usuel).*

L'ensemble $I(A)$ des idéaux fractionnaires forme un monoïde commutatif.

Remarque En fait, on montre même que $I(A) \setminus \{0\}$ est un groupe commutatif ; voir [12] pages 60-61.

Définition 4.17. *Alors, si on note $D(A) = \{xA | x \in F^*\}$, alors $D(A)$ est un sous-groupe de $I(A)$ et on a $Cl(A) = I(A)/D(A)$. On appelle $Cl(A)$ le groupe des classes de l'anneau A.*

Soit K un corps de nombres, $\mathcal{O}_K$ son anneau des entiers, $h_K = card(Cl(\mathcal{O}_K))$.

On a alors un théorème fondamental :

Théorème 4.18. *h_K est fini.*

Démonstration Ceci est démontré en 7.25.

□

Par ailleurs, il existe une formule donnant directement le nombre de classes pour un corps quadratique imaginaire. Si $\mathbb{Q}[\sqrt{d}]$ est un corps quadratique imaginaire de nombre de classes h et de déterminant $\mathcal{D} < -4$, alors

$$h = \frac{-1}{|\mathcal{D}|} \sum_{x=1,\, x \in P_{\mathcal{D}}}^{|\mathcal{D}|-1} \chi(x) x$$

où $P_{\mathcal{D}}$ est l'ensemble des entiers premiers avec $\mathcal{D}$ et où χ est une fonction valant 1 ou -1 selon le reste de x modulo $|d|$.

On l'explique dans l'annexe en 7.6.

Remarque Il en existe une généralisation à tout corps de nombres, mais ceci dépasse largement le cadre de l'exposé. On pourra voir par exemple [2] à ce sujet.

5 Courbes elliptiques à multiplication complexe

5.1 Endomorphismes d'une courbe elliptique sur $\mathbb{C}$

Les propriétés démontrées en §3 concernent particulièrement un certain type de courbes elliptiques, dites à multiplication complexe, que nous allons enfin définir.

Soient $\tau \in \mathcal{H}$ et $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ comme précédent. On pose $E = \mathbb{C}/\Lambda$.

D'après la proposition 2.5, tout endomorphisme de variété complexe de $\mathbb{C}/\Lambda$ est de la forme $z \mapsto \alpha z$ pour un certain $\alpha \in \mathbb{C}$.

On s'identifie $\mathbb{Z}$ à un sous-anneau de $End(\mathbb{C}/\Lambda)$ via $n \mapsto (z \mapsto nz)$.

De plus, $End(\mathbb{C}/\Lambda)$ s'identifie à un sous-anneau de $\mathbb{Q}[\tau]$ contenant $\mathbb{Z}$ via $(\phi : z \mapsto \alpha z) \mapsto \alpha$.

Définition 5.1. *On dit que $\mathbb{C}/\Lambda$ est **à multiplication complexe** si $End(\mathbb{C}/\Lambda) \neq \mathbb{Z}$. On dit que le réseau Λ est à multiplication complexe si $\mathbb{C}/\Lambda$ l'est.*

Définition 5.2. *Soit K un corps quadratique imaginaire. On appelle **ordre** de K tout sous-anneau unitaire de K qui est un réseau de $\mathbb{C}$.*

Théorème 5.3. *Le réseau Λ est à multiplication complexe si et seulement si $\mathbb{Q}(\tau)$ est un corps quadratique imaginaire.*

Dans ce cas, $End(\mathbb{C}/\Lambda)$ est un ordre de K.

Démonstration *Sens direct*

$$\exists \alpha \in \mathbb{C} \setminus \mathbb{Z} : \alpha\Lambda \subset \Lambda \Rightarrow \exists a, b, c, d \in \mathbb{Z}, a \neq 0 : \begin{cases} \alpha = a\tau + b \\ \alpha\tau = c\tau + d \end{cases}$$

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

$$\Rightarrow [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$$

Sens réciproque

Si $[\mathbb{Q}[\tau] : \mathbb{Q}] = 2$, alors il existe $A, B, C \in \mathbb{Z}, A \neq 0$ tels que $A\tau^2 + B\tau + C = 0$.

Soit $x \in \mathbb{Z}$; alors $x \notin -\tau A + \mathbb{Z}$. On pose $\alpha = A\tau + x$. Soit $a\tau + b \in \Lambda$. Alors

$$\begin{aligned} \alpha(a\tau + b) &= a(A\tau^2 + x\tau) + b(A\tau + x) \\ &= a(-C + (x - B)\tau) + bA\tau + xb \\ &= (xb - aC) + \tau(ax - aB + bA). \end{aligned}$$

Alors $\alpha\Lambda \subset \Lambda$, et $\alpha \notin \mathbb{Z}$.

Dans ce cas, $End(\mathbb{C}/\Lambda) \subset \Lambda$ est un sous-groupe discret de C. Alors on peut prendre $\alpha \in End(\mathbb{C}/\Lambda) \setminus \mathbb{Z}$, tel que pour tout $\alpha' \in End(\mathbb{C}/\Lambda)$, $Im(\alpha') \supset Im(\alpha)$. On peut vérifier sans problème que $End(\mathbb{C}/\Lambda) = \mathbb{Z} + \mathbb{Z}\alpha$ est un réseau, donc un ordre.

□

Définition 5.4. *Soit K un corps quadratique, soit $\mathcal{O}$ un ordre de K. On dit qu'un idéal fractionnaire I de $\mathcal{O}$ est propre si $\mathcal{O} = \{\alpha \in K : \alpha I \subset I\}$.*

Théorème 5.5. *Soit $\tau \in \mathcal{H}$; on pose $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. Soit $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Alors $\alpha\Lambda \subset \Lambda$ si et seulement s'il existe un corps quadratique (imaginaire) K et un ordre $\mathcal{O}$ de K tel que $\alpha \in \mathcal{O}$ et tel que Λ soit un idéal fractionnaire propre de $\mathcal{O}$.*

Démonstration

$\Leftarrow$ Clair.

$\Rightarrow$ On suppose $\alpha\Lambda \subset \Lambda$. Alors $\exists a, b, c, d \in \mathbb{Z}, a \neq 0 : \begin{cases} \alpha = a\tau + b \\ \alpha\tau = c\tau + d \end{cases}$. On en déduit $a\tau^2 + (b-c)\tau + d = 0$.

On pose $K = \mathbb{Q}[\tau]$, puis $\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$, qui est un ordre de K. Or Λ est un idéal fractionnaire propre de $\mathcal{O}$ (en effet, $\frac{1}{a}\Lambda \subset \mathcal{O}$, et Λ est clairement propre), et $\alpha \in \mathcal{O}$, d'où la conclusion.

□

5.2 Le j-invariant est un nombre algébrique

On va montrer $j((1 + i\sqrt{163})/2) \in \mathbb{Q}$. Plus généralement :

Théorème 5.6. *Soit K un corps quadratique, $\mathcal{O}_K$ son anneau des entiers, et I un idéal fractionnaire non nul de $\mathcal{O}_K$. Alors $j(\mathbb{C}/I)$ est un nombre algébrique de degré au plus h_K.*

Corollaire 5.7. *On pose $\tau = (1 + i\sqrt{163})/2$. Alors $j(\tau) \in \mathbb{Q}$.*

Démonstration On applique le théorème précédent à $K = \mathbb{Q}[i\sqrt{163}]$, qui d'après le corollaire 4.14 est d'anneau des entiers principal $\mathcal{O}_K = \mathbb{Z}[\tau]$; $j(\tau) = j(\mathbb{C}/\mathcal{O}_K)$ est algébrique de degré au plus 1, donc dans $\mathbb{Q}$. □

On définit l'action de $Aut(\mathbb{C})$ sur les courbe elliptiques. Soit $\sigma \in Aut(\mathbb{C})$. Si une courbe E est donnée par les zéros d'un polynôme P, alors E^σ est donnée par les zéros du polynôme P^σ dont les coefficients sont les images de ceux de P par σ. Ainsi, on obtient $j(E^\sigma) = \sigma(j(E))$.

L'idée de la démonstration est que pour tout $\sigma \in Aut(\mathbb{C})$, j^σ est le j-invariant d'une courbe elliptique à multiplication complexe pour laquelle $\mathcal{O}_K$ est l'anneau des endomorphismes. On va montrer d'abord que cette courbe elliptique est isomorphe à $\mathbb{C}/I$ pour un certain I idéal de $\mathcal{O}_K$. Donc il y a au plus h_K possibilités de classes d'isomorphismes de $\mathbb{C}/I$, et j^σ prend au plus h_K valeurs quand σ varie, d'où la conclusion.

Lemme 5.8. *Soit K un corps quadratique. Alors on a une bijection entre le groupe des classes $Cl(\mathcal{O}_K)$ et les classes d'isomorphismes des réseaux à multiplication complexe pour lesquels $\mathcal{O}_K$ est l'anneau des endomorphismes.*

Démonstration On montre d'abord que tous les réseaux à multiplication complexe pour lesquels $\mathcal{O}_K$ est l'anneau des endomorphismes sont isomorphes à un idéal de $\mathcal{O}_K$. En notant δ le générateur de $\mathcal{O}_K$, on a $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\delta$. Soit $\Lambda = \mathbb{Z} + \mathbb{Z}z$ un réseau de $\mathbb{C}$ tel que $End(\mathbb{C}/\Lambda) = \mathcal{O}_K$. Comme $\delta \in \Lambda$, on a forcément $z \in \mathbb{Q}[\delta]$. Donc il existe un entier n tel que $n\Lambda \subset \mathcal{O}_K$. Alors $n\Lambda$ est un idéal de $\mathcal{O}_K$.

Réciproquement, soit I un idéal non nul de $\mathcal{O}_K$. Par le lemme 4.9, il existe $m, a, b \in \mathbb{Z}$, m, a non nuls tels que $I = m < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$. Donc I est vraiment un réseau de $\mathbb{C}$ et $\mathcal{O}_K \subset End(\mathbb{C}/I)$. De plus, soit $\lambda \in End(\mathbb{C}/I)$, on a $\lambda^k a \in < a, \frac{-b+\sqrt{\mathcal{D}}}{2} >$ pour tous les entiers k. Donc on a forcément $\lambda \in \mathcal{O}_K$.Alors $End(\mathbb{C}/I) = \mathcal{O}_K$.

Comme deux idéaux I et J sont isomorphes comme réseaux si et seulement s'ils sont dans la même classe d'équivalence d'idéaux. On obtient alors la bijection voulue.

□

Démonstration du théorème 5.6 Par le corollaire 2.9 on peut écrire ainsi le développement de Laurent de la fonction de Weierstrass :

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} a_n(g_2, g_3) z^{2n}$$

où pour tout $n \in \mathbb{N}^*$, $a_n \in \mathbb{Q}[X, Y]$.

Soit $\alpha \in End(\mathbb{C}/I) = \mathcal{O}_K$. Alors $\alpha I \subset I$, donc $\phi : z \mapsto \mathcal{P}(\alpha z)$ est méromorphe, paire, doublement périodiquepar rapport à I. D'après 2.12, $\phi \in \mathbb{C}(\mathcal{P})$. Donc on peut écrire

$$\mathcal{P}(\alpha z; g_2, g_3) = \frac{A(\mathcal{P}(z; g_2, g_3))}{B(\mathcal{P}(z; g_2, g_3))},$$

pour un certain couple $(A, B) \in \mathbb{C}[X]$.

Soit $\sigma \in Aut(\mathbb{C})$. On note A^σ, B^σ l'image des polynômes sous l'action de σ qui consiste à appliquer σ à leurs coefficients. Cette action se prolonge au corps des fractions de séries formelles $\mathbb{C}((X))$, et donc σ y induit un automorphisme. En appliquant σ à l'égalité précédente, on obtient :

$$\mathcal{P}(\sigma(\alpha)z; \sigma(g_2), \sigma(g_3)) = \frac{A^\sigma(\mathcal{P}(z; \sigma(g_2), \sigma(g_3)))}{B^\sigma(\mathcal{P}(z; \sigma(g_2), \sigma(g_3)))}.$$

On a $g_2^3 - 27g_3^2 \neq 0$, donc $\sigma(g_2)^3 - 27\sigma(g_3)^2 \neq 0$; par surjectivité de j, il existe Λ un réseau tel que $g_2(\Lambda) = \sigma(g_2)$; $g_3(\Lambda) = \sigma(g_3)$. En particulier, on a $j(\Lambda) = \sigma(j(I))$.

Alors $\mathcal{P}(z,\, \Lambda) = \mathcal{P}(z;\, \sigma(g_2);\, \sigma(g_3))$

On montre que Λ est à multiplication complexe par $\sigma(\alpha)$. En effet, $\mathcal{P}(\sigma(\alpha)z,\, \Lambda) = \frac{A^\sigma(\mathcal{P}(z,\Lambda))}{B^\sigma(\mathcal{P}(z,\Lambda))}$. Donc $A^\sigma(\mathcal{P}(z)) = \mathcal{P}(\sigma(\alpha)z)B^\sigma(\mathcal{P}(z))$.
$z \mapsto \mathcal{P}(\sigma(\alpha)z)$ a un pôle double en 0, donc $deg(A^\sigma) = deg(B^\sigma) + 1$. Si $\omega \in \Lambda$, alors comme $\mathcal{P}$ a un pôle en ω, d'après les deux formules précédentes, $z \mapsto \mathcal{P}(\sigma(\alpha)z)$ aussi. Dons $\mathcal{P}$ a un pole en $\sigma(\alpha)\omega$, alors $\sigma(\alpha)\omega \in \Lambda$. Donc Λ est à multiplication complexe par $\sigma(\alpha)$.

On déduit de ce qui précéde $\sigma(End(\mathbb{C}/I)) \subset End(\mathbb{C}/\Lambda)$. En considérant σ^{-1}, on obtient que $End(\mathbb{C}/\Lambda) = \sigma(End(\mathbb{C}/I)) = \sigma(\mathcal{O}_K) = \mathcal{O}_K$ comme l'extension $\mathbb{Q} \hookrightarrow K$ est normale.

Or par 5.8, il existe au plus h_K valeurs possibles de $j(\Lambda)$, donc de $\sigma(j(\mathbb{C}/I))$. Ainsi, $j(\mathbb{C}/I)$ est un nombre algébrique de degré au plus h_K. □

Remarque En fait, et c'est démontré dans [3], le degré de $j(\mathbb{C}/\mathcal{O}_K)$ est exactement h_K. De plus, $K(j(\mathbb{C}/\mathcal{O}_K))$ est le corps de classe de Hilbert du corps K, c'est-à-dire l'extension non-ramifiée maximale de K. On sait que le corps de Hilbert du corps K est abelien sur K.

Plus généralement, soient $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K et I un idéal fractionnaire de $\mathcal{O}$. Alors $K(j(\mathbb{C}/I))$ est le "ring class field" de $\mathcal{O}$. En particulier, par le théorème 5.5, on a $j(E)$ est un nombre algébrique pour tout les courbes elliptiques à multiplication complexe.

5.3 Intégralité du j-invariant

On montre ensuite que j est un entier algèbrique.

Théorème 5.9. *Soit E une courbe elliptique à multiplication complexe. Alors $j(E)$ est un entier algébrique.*

Démonstration Soit $E = \mathbb{C}/\Lambda$ une courbe elliptique à multiplication complexe. On pose $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

On pose $K = \mathbb{Q}(\frac{\omega_1}{\omega_2})$. Alors il existe un entier négatif sans facteur carré d tel que $K = \mathbb{Q}(\sqrt{d})$. On peut supposer $\Lambda \subset \mathcal{O}_K$.

On suppose le résultat vrai quand $\Lambda = \mathcal{O}_K$; $\mathcal{O}_K = \mathbb{Z}[\tau]$ pour un certain $\tau \in \mathcal{H}$. $j(\tau)$ est donc entier sur $\mathbb{Z}$ par hypothése. Alors, quite à permuter ω_1 et ω_2, il existe $n \in \mathbb{N}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D_n$ tels que $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}$. On peut trouver $P \in \mathrm{SL}_2(\mathbb{Z})$ tel que $PM \in S_n$. Avec les notations du théorème, $j \circ PM$ annule $F_n(j, X)$; or $j \circ PM = j \circ M$ par invariance de j sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. On en déduit que $F_n[j(\tau), j \circ M(\tau)] = 0$. Alors $j(M(\tau)) = j(E)$ est intégre sur $\mathbb{Z}[M(\tau)]$ donc sur $\mathbb{Z}$.

On se ramène donc à $\Lambda = \mathcal{O}_K$.

On pose $\alpha = \sqrt{d}$ et $n = |\alpha|^2$. Alors n n'est pas un carré.

De plus, comme $\alpha\mathbb{Z}[\tau] \in \mathbb{Z}[\tau]$, il existe alors $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telle que $\alpha \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}$. En considérant le conjugué complexe, on a $\bar{\alpha} \begin{pmatrix} \bar{\tau} \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{\tau} \\ 1 \end{pmatrix}$

Donc $\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \tau & \bar{\tau} \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau & \bar{\tau} \\ 1 & 1 \end{pmatrix}$. Comme $\det \begin{pmatrix} \tau & \bar{\tau} \\ 1 & 1 \end{pmatrix} = \tau - \bar{\tau} \neq 0$, on a alors $n = |\alpha|^2 = \det \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Comme $M\tau = (a\tau + b)/(c\tau + d) = (\alpha\tau)/(\alpha)$, on a $j(M\tau) = j(\tau) = j(E)$. On obtient avec les notations du théorème $H_n(j(E)) = F_n(j(E), j(E)) = F_n(j(\tau), j(M(\tau))) = 0$ car $\mathcal{M}_2(\mathbb{Z}) \in D_n$. Comme n n'est pas un carré, par le proposition 3.15, $j(E)$ est un entier algébrique.

□

Remarque Comme on l'a vu dans la démonstration précedente, si $f : E \to E'$ est une isogénie de degré n (c'est-à-dire un morphisme surjectif de courbes elliptiques avec un noyau fini de cardinal n), alors $F_n(j(E), j(E')) = 0$. Une courbe elliptique E est à multiplication complexe si et seulement s'il existe une isogénie $E \to E$ de degré non carré.

Corollaire 5.10. *Soient K est un corps quadratique imaginaire tel que $h_K = 1$ et I un idéal non nul de $\mathcal{O}_K$. On pose $E = \mathbb{C}/I$. Alors $j(E) \in \mathbb{Z}$.*

Démonstration Par 5.7, on a $j(E) \in \mathbb{Q}$, et par 5.9, on a que $j(E)$ est un entier algébrique. Donc $j(E) \in \mathbb{Z}$. □

Corollaire 5.11. *$e^{\pi\sqrt{163}}$ est presque un entier.*

Démonstration On pose $\tau = \frac{1+i\sqrt{163}}{2}$, et on considère le réseau $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ et la courbe elliptique $E = \mathbb{C}/\Lambda$. Par le lemme précédent, $j(E) \in Z$.

Or par 3.5, on a en posant $q = e^{2i\pi\tau} = -e^{-\pi\sqrt{163}}$

$$j(E) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n.$$

On en déduit $e^{\pi\sqrt{163}} \simeq -j(E) + 744 + 8 \times 10^{-13}$.

□

5.4 Racine cubique du j-invariant

On va montrer que les racines cubiques de $j(\mathcal{O}_K)$ sont encores des entiers algébriques de degré au plus h_K pour un corps quadratique imaginaire K.

Voici quelques exemples sans calcul ; pour les détails, on pourra voir [3].

Exemple 5.12. *Il est connu que les 9 corps quadratiques imaginaires de nombre des classes 1 sont les $\mathbb{Q}(\sqrt{d})$ avec $d = -1, -2, -3, -7, -11, -19, -43, -67$ et -163. Leurs valeurs pour j sont :*

$$j(1 + \sqrt{-1}) = 12^3$$

$$j(1 + \sqrt{-2}) = 20^3$$

$$j(\frac{1}{2}(1 + \sqrt{-3})) = 0^3$$

$$j(\frac{1}{2}(1 + \sqrt{-7})) = (-15)^3$$

$$j(\frac{1}{2}(1+\sqrt{-11})) = (-32)^3$$

$$j(\frac{1}{2}(1+\sqrt{-19})) = (-96)^3$$

$$j(\frac{1}{2}(1+\sqrt{-43})) = (-960)^3$$

$$j(\frac{1}{2}(1+\sqrt{-67})) = (-5280)^3$$

$$j(\frac{1}{2}(1+\sqrt{-163})) = (-640320)^3$$

Fixons d un entier negatif sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$, $\tau_0 = \frac{3+\sqrt{d}}{2}$ si $d \equiv 1$ [4] ou $\tau_0 = \sqrt{d}$ si $d \equiv 2, 3$ [4]. Alors on a $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau_0$. Donc $j(\mathcal{O}_K) = j(\tau_0)$.

On suppose de plus que 3 ne divise pas d. Pour le cas général, on peut voir [13].

On note que pour $\tau \in i\mathbb{R}$, on a $q(\tau) = e^{2\pi i\tau} \in \mathbb{R}$, et donc $\Delta(z) \in \mathbb{Q}[[q]] \subset \mathbb{R}$. Puisque Δ est une fonction holomorphe non nulle sur $\mathcal{H}$ qui est simplement connexe, il existe Θ une fonction holomorphe sur $\mathcal{H}$ qui est réelle sur $i\mathbb{R}$ tel que $\Theta^3 = \Delta$.

On pose alors $\gamma_2(\tau) = 12\frac{g_2(\tau)}{\Theta(\tau)}$, puis $\gamma_2^3 = j$. On montre maintenant que γ_2 est une fonction modulaire pour $\Gamma_0(9)$ de poids 0 et que les coefficients de son q-développement sont dans $\mathbb{Q}$.

Proposition 5.13. *La fonction γ_2 est une fonction modulaire pour $\Gamma_0(9)$ de poids 0. De plus, les coefficients de son q-développement sont des nombres rationnels.*

Démonstration On sait que le q-développement de j est $q^{-1} + \sum_{n=0}^{\infty} c_n q^n$ avec les coefficients c_n entiers. On pose $f(q) := 1 + \sum_{n=0}^{\infty} c_n q^{n+1}$ qui est une fonction holomorphe sur la boule unité de valeur 1 en 0. Donc il existe une fonction g holomorphe dans un voisinage de 0, telle que $g^3 = f$ et $g(0) = 0$. On écrit $g = 1 + \sum_{n=1}^{\infty} a_n q^n$. Pour tout n entier positif, en considerant le coefficient de q^n dans g^3, on a alors $3a_n + P(a_1, a_2, \cdots, a_{n-1}) = c_{n-1} \in \mathbb{Z}$ avec P un polynôme à coefficients entiers. Donc on peut déduire par récurrence que tous les a_n sont dans $\mathbb{Q}$. Comme le cube de $q^{-1/3}g$ est j etque $q^{-1/3}g$ est réel quand q est réel, alors par construction du γ_2, on a $\gamma_2(q) = q^{-1/3}g$.

Maintenant on considère l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur γ_2. Soient $z \in \mathcal{H}$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. On pose $\zeta = e^{2\pi i/3}$. On vérifie que $\gamma_2(\gamma z) = \zeta^{ac-ab+a^2cd-cd}\gamma_2(z)$.

En effet, $\gamma_2(-1/z) = \gamma_2(z)$ car $-1/z \in i\mathbb{R}$ si $z \in \mathbb{R}$. $\gamma_2(z+1) = q(z+1)^{-1/3}g(q(z+1)) = \zeta^{-1}q(z)g(q(z)) = \zeta^{-1}\gamma_2(z)$. Donc l'égalité est vraie pour $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. De plus, il est facile de vérifier que si γ et γ' sont deux matrices dans $\mathrm{SL}_2(\mathbb{Z})$ tel que cette égalité est vraie, alors on a la même pour $\gamma\gamma'$. Comme $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ engendrent $\mathrm{SL}_2(\mathbb{Z})$, cette égalité est toujours vraie.

Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(9)$, on a $\gamma_2(3\gamma z) = \gamma_2(\frac{3az+3b}{cz+d}) = \gamma_2(\frac{a(3z)+b}{c/3(3z)+d}) = \gamma_2(\begin{pmatrix} a & 3b \\ c/3 & d \end{pmatrix}(3z)) = \gamma_2(3z)$ car 3 divise $c/3$.

Il reste à voir que $\gamma_2(3z)$ est méromorphe en tous les cusps. En effet, soit $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, comme $j(3z)$ est une fonction modulaire pour $\Gamma_0(3)$, on a que $(j(3\gamma z))$ est méromorphe en ∞. Donc c'est aussi vrai pour sa racine cubique $\gamma_2(3\gamma z)$.

On a déja vu dans le premier paragraphe que tous les coefficients du q-développement du γ_2 sont dans $\mathbb{Q}$. On a alors fini la démonstration. □

Par le théorème 3.8, on a $\gamma_2(3z) \in \mathbb{Q}(j(9z), j(z))$. Soit z_0 comme précédemment, on a de plus :

Corollaire 5.14. *Le nombre $\gamma_2(z_0)$ est dans $\mathbb{Q}(j(3z_0), j(z_0/3))$.*

Démonstration Comme on l'a vu dans la démonstration du théorème 3.8, $\gamma_2(z_0)\prod_{k\neq 1}(j(\sigma_1(z_0/3)) - j(\sigma_k(z_0/3)) = G(j(z_0/3), j(3z_0)) \in \mathbb{Q}(j(3z_0), j(z_0/3))$ et $\prod_{k\neq 1}(j(\sigma_1(z_0/3)) - j(\sigma_k(z_0/3)) \in \mathbb{Z}[j(3z_0), j(z_0/3)]$, il suffit de montrer que pour tout $\sigma = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T_9$, $\sigma \neq \sigma_0$ où $\sigma_0 = \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}$, on a $j(\sigma(z_0/3)) \neq j(\sigma_0(z_0/3))$. On suppose par l'absurde que $j(\sigma(z_0/3)) = j(\sigma_0(z_0/3))$. Alors il existe $\delta \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\sigma_0(z_0/3) = \delta\sigma(z_0/3)$. On peut écrire $\delta\sigma$ comme $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. Donc on a $3z_0 = \frac{Az_0+3B}{Cz_0+3D}$.

- Si $d \equiv 1$ [4], on a $z_0 = \frac{3+\sqrt{d}}{2}$. Alors $A\frac{3+\sqrt{d}}{2} + 3B = 3C\frac{9+D+6\sqrt{d}}{4} + 9D\frac{3+\sqrt{d}}{2}$.
  Ainsi $3A/2 + 3B = 3C(9+d)/4 + 27D/2$ et $A/2 = 9C/2 + 9D/2$. Donc $A = 9C + 9D$ et $B = \frac{D-9}{4}C$. Comme $\det(\delta\sigma) = 9$, on a alors

$AD - BC = 9CD + 9D^2 - \frac{D-9}{4}C^2 = 9(D + C/2)^2 + \frac{-d}{4}C^2 = 9$. En particulier, comme d est premier avec 3, on a que 3 divise C. Comme de plus $d \equiv 1\ [4]$, on a $-d \geq 7$. On a alors $C = 0$ car $\frac{-d}{4}C^2 \leq 9$. Donc $D = 1$ ou $D = -1$.
On a alors $\sigma = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \delta^{-1}\begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}$ ou $\delta^{-1}\begin{pmatrix} -9 & 0 \\ 0 & -1 \end{pmatrix}$. On a forcément 9 divise a. Alors $a = 9$, $b = 1$. Comme $0 \leq c < b$, on a $c = 0$. Donc $\sigma = \sigma_0$, ce qui est absurde.

– Si $d \equiv 2, 3\ [4]$, on a $z_0 = \sqrt{d}$. De même, on a $A = 9D$ et $B = dC$. Donc $9D^2 - dC^2 = 9$.Comme $-d \geq 0$ et comme 3 ne divise pas $-d$, on a forcément $C = 0$, $D = 9$ ou -9. De même, on a $\sigma = \sigma_0$, ce qui est absurde.

On en déduit que $\gamma_2(z_0) \in \mathbb{Q}(j(3z_0), j(z_0/3))$. □

On pose $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(3z_0)$; c'est un ordre dans K. Il est facile de voir que $\mathcal{O}' := \mathbb{Z} + \mathbb{Z}(z_0/3)$ est un idéal fractionnaire propre de $\mathcal{O}$. On a remarqué dans la section 5.2 que $K(j(z_0)$ est le corps de classe de Hilbert de K et $\mathbb{Q}(j(3z_0)) = \mathbb{Q}(j(z_0/3))$ est le "ring class field" du $\mathcal{O}$. On ne définit pas le "ring class field" ici. On utilisera un corollaire de la théorie des corps de classes sans démonstration. On peut voir [3] pour les détails.

Proposition 5.15. *On utilise les notations précédentes. Alors l'extension* $K(j(z_0)) \hookrightarrow K(j(3z_0)) = K(j(z_0/3))$ *est de degré*

$$\frac{3}{[\mathcal{O}_K^* : \mathcal{O}^*]}(1 - \left(\frac{\mathcal{D}}{3}\right)\frac{1}{3})$$

ou $\mathcal{D}$ *est le discriminant de* $\mathcal{O}_K$, $\mathcal{O}_K^*$ *(resp.* $\mathcal{O}^*$*) est l'ensemble des éléments inversibles dans* $\mathcal{O}_K$ *(resp.* $\mathcal{O}$*) et* $\left(\frac{\mathcal{D}}{3}\right)$ *est le symbol de Legendre : il est égal à* 1 *si* 3 *ne divise pas* $\mathcal{D}$ *et* $\mathcal{D}$ *est congru à un carré modulo* 3 *; il est égal à* 0 *si* 3 *divise* $\mathcal{D}$ *; il est égal à* -1 *sinon.*

Enfin, on montre le théorème suivant :

Théorème 5.16. *Soit* K *et* z_0 *comme précédemment. Alors* $\gamma_2(z_0) \in Q(j(z_0))$.

Lemme 5.17. *L'extension* $\mathbb{Q}(j(z_0)) \hookrightarrow K(j(z_0))$ *est de degré* 2.

Démonstration On montre d'abord que $j(z_0 \in \mathbb{R}$. En effet, $q(z_0)$ est égal à $-e^{\pi\sqrt{-d}}$ si $d \equiv 1[4]$ et $e^{\sqrt{-d}}$ si $d \equiv 2, 3[4]$. Dans tout les cas, on a $q(z_0) \in \mathbb{R}$. Donc par l'expression du q-développement de j on a $j(z_0) \in \mathbb{R}$.

Maitenant comme l'extension $\mathbb{Q} \hookrightarrow K$ est de degré 2, on sait que le degré du $\mathbb{Q}(j(z_0)) \hookrightarrow K(j(z_0))$ est d'au plus 2. Mais comme $\mathbb{Q}(j(z_0)) \subset \mathbb{R}$

et $K(j(z_0)) \not\subseteq \mathbb{R}$, on sait alors que le degré n'est pas 1, donc qu'il est égal à 2 comme on veut. □

Démonstration du théorème 5.16
On a déja vu que $\gamma_2(z_0) \in \mathbb{Q}(j(3z_0), j(z_0/3)) \subset K(j(3z_0))$. De plus, par la proposition et le lemme précédents, on sait que le degré de $K(j(3z_0))$ sur $\mathbb{Q}(j(z_0))$ est $2\frac{3}{[\mathcal{O}_K^* : \mathcal{O}^*]}(1 - \left(\frac{\mathcal{D}}{3}\right)\frac{1}{3})$ qui divise $2(3 - \left(\frac{\mathcal{D}}{3}\right))$. Comme 3 ne divise pas d et donc ne divise pas $\mathcal{D}$, ce dernier nombre est égal à 2 ou 4. Ainsi le degré de $K(j(3z_0))$ sur $\mathbb{Q}(j(z_0))$ divise 8. En particulier, le degré de $\gamma_2(z_0)$ sur le corps $\mathbb{Q}(j(z_0))$ divise 8.

Comme $q(z_0) = e^{2\pi i z_0} \in \mathbb{R}$, par le q-développement de γ_2 on a $\gamma_2(z_0) \in \mathbb{R}$, et donc $\gamma_2(z_0)$ est la racine cubique réelle d'équation $X^3 - j(z_0)$. Donc le degré de $\gamma_2(z_0)$ sur le corps $\mathbb{Q}(j(z_0))$ est 1 ou 3. Mais ce degré divise 8, donc est égal à 1. On en déduit que $\gamma_2(z_0) \in \mathbb{Q}(j(z_0)$.

□

Corollaire 5.18. *Soit K est un corps quadratique imaginaire de nombre de classes* 1. *Alors $j(\mathbb{C}/\mathcal{O}_K)$ est un cube d'un entier.*

Démonstration On pose z_0 et γ_2 comme précédemment. Par le corollaire **??** et le lemme précédent, $\gamma_2(z_0)$ est dans Q. Par ailleurs, $\gamma_2(z_0)$ est la racine cubique d'un entier, donc $\gamma_2(z_0)$ est un entier algébrique. Alors $\gamma_2(z_0)$ est un entier rationnel . Donc $j(\mathbb{C}/\mathcal{O}_K) = \gamma_2(z_0)^3$ est le cube d'un entier rationnel. □

6 Conclusion

Nous avons donc démontré les théorèmes suivants :

- Soit E une courbe elliptique à multiplication complexe. Alors $j(E)$ est un entier algébrique.
- Soit K un corps quadratique, $\mathcal{O}_K$ son anneau des entiers, et I un idéal fractionnaire non nul de $\mathcal{O}_K$. Alors $j(\mathbb{C}/I)$ est un nombre algébrique de degré au plus h_K.
- Soit K un corps quadratique imaginaire. Alors $j(\mathbb{C}/\mathcal{O}_K)$ est réel et la racine cubique réelle de $j(\mathbb{C}/\mathcal{O}_K)$ est dans $Q(j(\mathbb{C}/\mathcal{O}_K)$.

Par la théorie des courbes elliptiques, en utilisant la paramétrisation par la fonction j sur $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{C}$, et la théorie des fonctions modulaires pour arriver au q-développement de j et construire des polynômes annulant j, on établit donc un lien entre ces différents théorèmes et le nombre $e^{\pi\sqrt{163}}$.

Ainsi, en notant E la courbe elliptique isomorphe à $\mathbb{C}/(\mathbb{Z} + \frac{1+i\sqrt{163}}{2}\mathbb{Z})$, on a $j(E) \in \mathbb{Z}^3$ et $j(E) \simeq -e^{\pi\sqrt{163}} + 744 + 8 \times 10^{-13}$ par le q-développement de j.

Ceci explique pourquoi $e^{\pi\sqrt{163}}$ est un entier à 10^{-12} près et un cube à 744 près.

Cette jolie propriété connue depuis le dix-neuvième siècle a d'ailleurs fait l'objet d'un célèbre canular de Martin Gardner qui prétendit en guise de poisson d'Avril dans le journal de vulgarisation *Scientific American* que $e^{\pi\sqrt{163}}$ était effectivement un entier.

7 Annexe A : Compléments sur le nombre de classe

7.1 La formule des classes pour les corps quadratique

Les énoncés de cette section sont prouvés dans [2] ; il existe une formule plus générale pour tout corps de nombres.

On notera $\mathfrak{P}$ l'ensemble des entiers naturels premiers.

7.1.1 Décomposition d'idéaux

Soit $d \in \mathbb{Q}/\mathbb{Q}^{*2}$. On considère le corps $K = \mathbb{Q}[\sqrt{d}]$

$\mathcal{O}_K$ est un anneau de Dedekind ; ainsi tout idéal s'y décompose en produit fini d'idéaux premiers. Si $p \in \mathfrak{P}$, on a $p\mathcal{O}_K = \prod_{k=1}^{q} \mathfrak{P}_k^{e_k}$ où les $\mathfrak{P}_k$ sont des idéaux premiers non nuls, et les e_k des entiers.

On appelle degré de ramification de l'idéal $\mathfrak{P}_k$ l'entier e_k.

$\mathbb{Z}/p\mathbb{Z}$ et $\mathcal{O}_K/\mathfrak{P}_k$ sont des corps, et $\mathcal{O}_K/\mathfrak{P}_k$ est un $\mathbb{F}_p$-espace vectoriel, de dimension f_k, appelée degré résiduel de $\mathfrak{P}_k$.

Proposition 7.1. *On a avec ces notations*

$$\sum_{k=1}^{q} e_k f_k = [K : \mathbb{Q}] = 2.$$

On a donc les possibilités suivantes pour l'idéal (p), en notant I, J des idéaux premiers de $\mathcal{O}_K$:

$(p) = IJ$; (p) est alors décomposé.

$(p) = I^2$;(p) est alors ramifié.

$(p) = I$;(p) est alors inerte.

Définition 7.2. *Soit $p \in \mathfrak{P}$. On dit que d est résidu quadratique (respectivement non résidu quadratique) modulo p si $d \in \mathbb{F}_p^{*2}$ (respectivement $d \notin \mathbb{F}_p^2$). On note $(\frac{d}{p}) = 1$ (respectivement $(\frac{d}{p}) = -1$). On note $(\frac{d}{p}) = 0$ si $p|d$. Cette notation est le symbole de Legendre.*

Théorème 7.3. *On obtient les types des idéaux en fonctions de p, d :*

$p \neq 2$:
$(\frac{d}{p}) = 1 \Leftrightarrow$ (p) se décompose
$(\frac{d}{p}) = -1 \Leftrightarrow$ (p) est inerte
$p\|d \Leftrightarrow$ (p) se ramifie

$$\boxed{\begin{array}{c} p = 2 : \\ d \equiv 1\,[8] \Leftrightarrow \ (2) \text{ se décompose} \\ d \equiv 5\,[8] \Leftrightarrow \ (2) \text{ est inerte} \\ d \equiv 2,\,3\,[4] \Leftrightarrow \ (2) \text{ se ramifie} \end{array}}$$

7.1.2 Caractère quadratique de $\mathbb{Q}[\sqrt{d}]$

On note $\mathcal{D}$ le discriminant du corps $\mathbb{Q}[\sqrt{d}]$, et $P_{\mathcal{D}} = \{x \in \mathbb{Z} : \ x \wedge \mathcal{D} = 1\}$. On note $G_{\mathcal{D}}$ le groupe des éléments de $P_{\mathcal{D}}$ quotienté par la relation de congruence modulo $\mathcal{D}$.

On introduit le symbole de Jacobi, extension du symbole de Legendre à des entiers n impairs non premiers. Si la décomposition de $n \in \mathbb{N}$ impair en produit de facteurs premiers s'écrit $n = \prod_{i=1}^{q} p_i^{a_i}$, alors, pour tout $x \in \mathbb{Z}$, on note $(\frac{x}{n}) = \prod_{i=1}^{q} (\frac{x}{p_i})^{a_i}$.

On peut alors définir le **caractère quadratique** de $\mathbb{Q}[\sqrt{d}]$:

$$\chi : \left\{ \begin{array}{c} P_{\mathcal{D}} \to \{-1, 1\} \\ x \mapsto \left\{ \begin{array}{l} (\frac{x}{|d|}) \text{ si } d \equiv 1\,[4] \\ (-1)^{\frac{x-1}{2}} (\frac{x}{|d|}) \text{ si } d \equiv 3\,[4] \\ (-1)^{\frac{x^2-1}{8} + \frac{x-1}{2}\frac{d'-1}{2}} (\frac{x}{|d|}) \text{ si } d \equiv 2\,[4]\,;\ d = 2d' \end{array} \right. \end{array} \right.$$

Proposition 7.4. *$\chi(x)$ dépend uniquement de la classe de x modulo $\mathcal{D}$; χ induit un homomorphisme de $G_{\mathcal{D}}$ sur $\{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.*

Remarque On peut poser $\chi(x) = 0$ pour $x \in \mathbb{Z} \setminus P_{\mathcal{D}}$.

Théorème 7.5. *On a pour $p \in \mathfrak{P}$*

$$\boxed{\begin{array}{c} \chi(p) = 1 \Leftrightarrow \ (p) \text{ se décompose} \\ \chi(p) = -1 \Leftrightarrow \ (p) \text{ est inerte} \\ \chi(p) = 0 \Leftrightarrow \ (p) \text{ se ramifie} \end{array}}$$

7.1.3 Formule des classes

On note h le nombre de classes d'idéaux de $\mathbb{Q}[\sqrt{d}]$.

Théorème 7.6. *Si $\mathcal{D} < -4$, alors*

$$\boxed{h = \frac{-1}{|\mathcal{D}|} \sum_{x=1,\, x \in P_{\mathcal{D}}}^{|\mathcal{D}|-1} \chi(x)x}$$

Proposition 7.7. *On a pour $p \in \mathfrak{P}$:*

$$\forall x \in \mathbb{F}_p,\ x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$$

Pour $d = -163$, on a $\mathcal{D} = -163$.
Ainsi, $|\mathcal{D}|$ est premier.
$d \equiv 1\ [4]$, donc $\forall x \in P_{\mathcal{D}}, \chi(x) = (\frac{x}{163})$.
$x \in \mathbb{F}_{163}^{*2} \Leftrightarrow x^{81} \equiv\ 1[163]$
$x \notin \mathbb{F}_{163}^{2} \Leftrightarrow x^{81} \equiv\ -1[163]$
On peut aussi calculer à la main les carrés de $\mathbb{F}_{163}$ pour pouvoir obtenir les valeurs de χ.
Puis $h = \frac{-1}{163} \sum_{x=1}^{162} \chi(x)x$.

On obtient $\boxed{h = 1}$.

Théorème 7.8. *L'anneau des entiers de $\mathbb{Q}[\sqrt{-163}]$ est principal.*

7.2 Finitude du groupe des classes d'un corps de nombres

On montre dans cette section que pour tout corps de nombre K, son nombre de classe h_K est fini.

La preuve est celle donnée dans [12]. Elle consiste à montrer que le nombre d'idéaux de $\mathcal{O}_K$ de norme bornée par un certain réel M_K déterminé par K est fini, puis à prouver que toute classe d'idéaux contient un idéal de norme inférieure à M_K.

7.2.1 Quelques calculs sur les réseaux

Définition 7.9. *On appelle* réseau *de $\mathbb{R}^n$ tout sous groupe discret L de rang n de $\mathbb{R}^n$. C'est un $\mathbb{Z}$-module engendré par une base de $\mathbb{R}^n$.*

Etant donnée une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de L, $P = \{a_1e_1 + \ldots + a_ne_n | a_i \in \mathbb{R},\ 0 \leq a_i < 1\}$ est appelé un domaine fondamental de L.

Le volume $v(L)$ d'un réseau est la mesure de Lebesgue sur $\mathbb{R}^n$ d'un domaine fondamental P.

Exemple 7.10. *L'anneau des entiers d'un corps de nombres, ainsi que ses idéaux, sont des réseaux de* $\mathbb{R}^n$.

Démonstration On montre que $v(L)$ ne dépend pas de la base choisie et donc du domaine fondamental associé. Si $(f_i)_{1\leq i\leq n}$ est une deuxième base de L, avec A la matrice de changement de base, on a, avec des notations explicites, $\lambda(P_{f_i}) = |det(A)|\lambda(P_{(e_i)}$; or $det(A)$ est nécessairement inversible dans $\mathbb{Z}$ car A l'est, d'où $|det(A)| = 1$. □

Exemple 7.11. *On va calculer* $v(\mathcal{O}_K)$ *pour* $K = \mathbb{Q}[\sqrt{d}]$ *avec* $d \in \mathcal{A} \cap -\mathbb{N}$.

Si $d \equiv 2, 3\,[4]$, *une* $\mathbb{Z}$*-base de* $\mathcal{O}_K$ *réseau de* $\mathbb{R}^2 \simeq \mathbb{C}$ *est* $(1, 0)$, $(0, \sqrt{-d})$. *D'où* $v(\mathcal{O}_K) = \sqrt{-d} = \frac{1}{2}\sqrt{\mathcal{D}}$.

Si $d \equiv 1\,[4]$, *une* $\mathbb{Z}$*-base de* $\mathcal{O}_K$ *réseau de* $\mathbb{R}^2 \simeq \mathbb{C}$ *est* $(1, 0)$, $(\frac{1}{2}, \frac{\sqrt{-d}}{2})$. *D'où* $v(\mathcal{O}_K) = \frac{1}{2}\sqrt{-d} = \frac{1}{2}\sqrt{\mathcal{D}}$.

Donc si $d < 0$, $v(\mathcal{O}_K) = \frac{1}{2}\sqrt{\mathcal{D}}$.

Si I *est un idéal de* $\mathcal{O}_K$, *alors* I *est un réseau et un domaine fondamental de* I *correspond à* $N(I)$ *domaines fondamentaux de* $\mathcal{O}_K$ *par définition de la norme. Donc* $v(I) = \frac{1}{2}\sqrt{\mathcal{D}}N(I)$.

Théorème 7.12. *(Minkowski) Soit* L *un réseau de* $\mathbb{R}^n$ *et* S *un sous-ensemble intègrable de* $\mathbb{R}^n$ *tels que* $\lambda(S) > v(L)$. *Alors il existe* $x, y \in S$ *tels que* $x \neq y$ *et* $x - y \in H$.

Démonstration Soit $e = (e_1, \ldots, e_n)$ une $\mathbb{Z}$-base de L . On note $P_e = \{a_1e_1 + \ldots + a_ne_n | a_i \in \mathbb{R},\ 0 \leq a_i < 1\}$.

Alors $S = \bigsqcup_{h\in L} S \cap (h + P_e)$ car P_e est un domaine fondamental. Puis $\lambda(S) = \sum_{h\in L} \lambda(S \cap (h + P_e))$.

La mesure de Lebesgue est invariante par translation, donc pour tout $h \in L$, $\lambda(S \cap (h + P_e) = \lambda((-h + S) \cap P_e)$. Si les ensembles $(-h + S) \cap P_e$ étaient deux à deux disjoints, on aurait

$$\lambda(S) = \sum_{h\in L} \lambda(S \cap (h + P_e)) = \sum_{h\in L} \lambda((-h + S) \cap P_e) \leq \lambda(P_e) = v(L)$$

ce qui est contradictoire.

Donc il existe $h \neq h' \in L$ tels que $(-h+S)\cap(-h'+S) \neq$, donc $x, y \in S$ tels que $x - y = h' - h \in L \setminus \{0\}$.

□

Corollaire 7.13. *Si S est de plus symétrique par rapport à 0, convexe, et que $\lambda(S) > 2^n v(L)$, alors $S \cap L$ n'est pas réduit à $\{0\}$. Si S est de plus compact, on peut se contenter de l'inégalité $\lambda(S) \geq 2^n v(L)$.*

Démonstration Dans le premier cas, on considère $S' = \frac{1}{2}S$, qui est intégrable de mesure de Lebesgue strictement supérieure à $v(L)$. On applique le théorème précédent : il existe $x \neq y$ dans S' tels que $x - y \in L$. Alors $2x$ et $2y$ sont dans S ; comme S est symétrique et convexe, $\frac{1}{2}(2x - 2y) \in S \setminus \{0\}$; c'est aussi un élément de L.

Si S est compact avec $\lambda(S) \geq 2^n v(L)$, en posant $H = L \setminus 0$, ce qui précède appliqué à $(1 + \epsilon)S$ donne $\forall \epsilon > 0$, $H \cap (1 + \epsilon)S \neq \emptyset$. Or cette intersection est compacte et discrète, donc finie.

Par ailleurs, $\forall \epsilon_1 > \epsilon_2 > 0$, $H \cap (1 + \epsilon_2)S \subset H \cap (1 + \epsilon_1)S$. On en déduit que $\bigcap_{\epsilon>0} H \cap (1 + \epsilon)S = H \cap \bigcap_{\epsilon>0}(1 + \epsilon)S = H \cap S$ est non-vide. En effet, dans le cas contraire, comme c'est une intersection infinie d'ensembles finis emboîtés, il existerait $\epsilon_0 > 0$ tel que $\forall \epsilon < \epsilon_0$, $H \cap (1 + \epsilon)S = \emptyset$.

□

7.2.2 Le Théorème de finitude du groupe des classes

Définition 7.14. *Soient A, B deux anneaux tels que B soit un A-module de rang n.*

La trace de $x \in B$ relativement à B et A, notée $Tr_{A/B}(x)$, est la trace de l'endomorphisme de multiplication par x sur B.

La norme de $x \in B$ relativement à B et A, notée $N_{A/B}(x)$, est le déterminant de l'endomorphisme de multiplication par x sur B.

Définition 7.15. *Soit K un corps de nombres d'anneau des entiers $\mathcal{O}_K$. Soit I un idéal de $\mathcal{O}_K$. On appelle norme de I la quantité $N(I) = card(\mathcal{O}_K/I)$.*

Remarque Cette quantité est bien définie, car pour tout $x \in I, x \neq 0$, $\mathcal{O}_K/I$ est à isomorphisme près un quotient de $\mathcal{O}_K/(x)$, qui est de norme finie par ce qui précéde.

Remarque Pour les idéaux principaux, cette définition se confond avec celle de la norme du générateur.

Proposition 7.16. *La norme est multiplicative.*

Définition 7.17. *Si $\mathcal{B} = (e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, on appelle discriminant de $\mathcal{B}$ le nombre $D(\mathcal{B}) = \det\left(Tr(e_i e_j)\right)_{1 \leq i,j \leq n}$.*

Définition 7.18. *On appelle discriminant d'un corps de nombres K la valeur commune, notée $\mathcal{D}$, des discriminants des $\mathbb{Z}$-bases de $\mathcal{O}_K$. Si $\mathcal{B} = (e_1, \dots, e_n)$ est une telle base, on a $\mathcal{D} = D(\mathcal{B}) = \begin{vmatrix} Tr(e_1e_1) & \cdots & Tr(e_1e_n) \\ \vdots & \ddots & \vdots \\ Tr(e_ne_1) & \cdots & Tr(e_ne_n) \end{vmatrix}$.*

Proposition 7.19. *Pour tout corps de nombres K, $\mathcal{O}_K$ est de Dedekind. En particulier, $\mathcal{O}_K$ a la propriété de factorisation unique en produit d'idéaux premiers.*

Démonstration On peut voir par exemple [12]. □

Proposition 7.20. *Soit K un corps de nombres de degré n. Alors il existe n plongements $\tau : K \to \mathbb{C}$.*

Il en existe r, notés $\rho_1, \dots, \rho_r$ tels que $\rho_i(K) \subset \mathbb{R}$, et $2s$, notés $\sigma_1, \bar{\sigma_1}, \dots, \sigma_s, \bar{\sigma_s}$ tels que leur image n'est pas dans $\mathbb{R}$, où $\bar{}$ dénote la conjugaison complexe.

On a $n = r + 2s$.

Démonstration $\mathbb{C}$ est une cloture algèbrique de $\mathbb{Q}$, et $\mathbb{Q} \hookrightarrow K$ est séparable, donc $[K : \mathbb{Q}]_s = [K : \mathbb{Q}] = n$.

□

On fixe les notations de cette proposition.

Définition 7.21. *Le plongement canonique Π d'un corps de nombres K est l'application*

$$\Pi : \begin{cases} K \to \mathbb{R}^r \times \mathbb{C}^s \\ x \mapsto (\rho_1(x), \dots \rho_r(x), \sigma_1(x), \dots, \sigma_s(x)) \end{cases}$$

Exemple 7.22. *Soit $d \in \mathcal{A} \cap \mathbb{N}$. On pose $K = \mathbb{Q}[\sqrt{d}]$. Alors $\Pi(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^2$. Si $d \equiv 2, 3[4]$, il est de $\mathbb{Z}$-base (par exemple) $(1, 1)$, $(\sqrt{d}, -\sqrt{d})$. Donc $v(\Pi(\mathcal{O}_K)) = 2\sqrt{d} = \sqrt{\mathcal{D}}$. Si $d \equiv 1\ [4]$, il est de $\mathbb{Z}$-base (par exemple) $(1, 1)$, $(\frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2})$. Donc $v(\Pi(\mathcal{O}_K)) = \sqrt{d} = \sqrt{\mathcal{D}}$.*

De même que pour $d < 0$, si on prend I un idéal de $\mathcal{O}_K$, $\Pi(I)$ est un réseau de $\mathbb{R}^2$ de volume $v(\Pi(I)) = \sqrt{\mathcal{D}}N(I)$.

Proposition 7.23. *Soit K un corps de nombres, et I un idéal de $\mathcal{O}_K$. Alors $\Pi(\mathcal{O}_K)$ et $\Pi(I)$ sont des réseaux de $\mathbb{R}^n$ de volumes respectifs $\frac{1}{2^s}\sqrt{|\mathcal{D}|}$ et $\frac{1}{2^s}\sqrt{|\mathcal{D}|}N(I)$.*

Démonstration Si $B = (x_1, \dots, x_n)$ est une $\mathbb{Q}$-base de K, alors un calcul simple donne le discriminant de B, en notant τ_i les plongements $K \hookrightarrow \mathbb{C}$: $D(B) = det(\tau_i(x_j)_{1\leq i,j\leq n})^2$.

Or $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n. On en fixe une base $(e_1, \dots, e_n)$. Les coordonnées dans la base canonique de R^n de $\Pi(e_i)$ sont

$$(\rho_1(e_i), \dots, \rho_r(e_i), \mathrm{Re}(\sigma_1(e_i)), \mathrm{Im}(\sigma_1(e_i)), \dots, \mathrm{Re}(\sigma_s(e_i)), \mathrm{Im}(\sigma_s(e_i))).$$

On en déduit le déterminant D dont les colonnes sont les coordonnées dans $\mathbb{R}^n$ des $\Pi(e_i)$: on obtient $D = \frac{1}{(2i)^s} det(\tau_j(x_i)) = \frac{1}{(2i)^s}\sqrt{\mathcal{D}}$, qui est non nul ; donc $\Pi(\mathcal{O}_K)$ est bien un $\mathbb{Z}$-module libre de rang n, donc un réseau, et son volume est $v(\Pi(\mathcal{O}_K)) = |D| = \frac{1}{2^s}\sqrt{|\mathcal{D}|}$.

En appliquant le même raisonnement à I, on obtient que $\Pi(I)$ est un réseau de $\mathbb{R}^n$. Un domaine fondamental de I correspond à $N(I)$ domaines fondamentaux de $\mathcal{O}_K$ par définition de la norme. Donc $v(I) = \frac{1}{2^s}\sqrt{\mathcal{D}}N(I)$. □

Proposition 7.24. *Soit K un corps de nombres. On note $\mathcal{D}$ le discriminant de K, $\Pi : K \to \mathbb{C}^s \times \mathbb{R}^r$ son plongement canonique. En conservant les notations de la partie précédente, toute classe d'idéaux de K contient un idéal I tel que $N(I) \leq (\frac{4}{\pi})^s \frac{n!}{n}\sqrt{|\mathcal{D}|}$.*

Démonstration Il suffit de montrer que pour tout idéal I de $\mathcal{O}_K$, il existe $x \in I$ tel que $|N_{\mathbb{Q}/K}(x)| \leq (\frac{4}{\pi})^s \frac{n!}{n}\sqrt{|\mathcal{D}|}N(I)$. En effet, si on choisit alors une classe d'idéaux $\mathcal{C}$ et un idéal $J \in \mathcal{C}$, alors on peut considérer son inverse J'. J' est un idéal fractionnaire ; quitte à multiplier J par un idéal principal, on peut supposer J' entier. Si on choisit $x \in J'$ tel que $|N_{\mathbb{Q}/K}(x)| \leq (\frac{4}{\pi})^s \frac{n!}{n}\sqrt{|\mathcal{D}|}N(J')$, alors $I = xJ$ convient. On a bien $I \in \mathcal{C}$.

On montre donc que pour tout idéal I de $\mathcal{O}_K$, il existe $x \in I$ tel que $|N_{\mathbb{Q}/K}(x)| \leq (\frac{4}{\pi})^s \frac{n!}{n}\sqrt{|\mathcal{D}|}N(I)$. On choisit un tel idéal I.

Soit $t > 0$. Alors $B_t = \{x = (y_i, z_j) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i=1}^r y_i + 2\sum_{j=1}^s z_j \leq t\}$.

C'est un ensemble compact, convexe, symètrique par rapport à 0 et de mesure $\lambda(B_t) = 2^r(\frac{\pi}{2})^s \frac{t^n}{n!}$. Ce volume se calcule en utilisant une double récurrence sur r et s et une intégration par "tranches" d'incrémentation en r ou s. On pourra voir [12, pg 79,80] pour le détail du calcul.

On pose $t = (\frac{2^{n-r}}{\pi^s} n!\sqrt{|\mathcal{D}|}N(I))^{\frac{1}{n}}$ de manière à avoir $\lambda(B_t) = v(\Pi(I))$.

D'après 7.13, il existe $x \in I$, $x \neq 0$ tel que $\Pi(x) \in B_t$.

Alors $|N(x)| = \prod_{l=1}^n |\tau_l(x)| = \prod_{i=1}^r |\rho_i(x)| \prod_{j=1}^s |\sigma_j(x)|^2$. On en déduit par l'inégalité arithmético-géométrique (qui donne $m_g \leq m_a$, pour un ensemble fini de n réels positifs de moyennes arithmétique et géomtrique m_a

et m_g) :

$$|N(x)| \leq \left(\frac{1}{n} \sum_{i=1}^{r} |\rho_i(x)| + \frac{2}{n} \sum_{j=1}^{s} |\sigma_j(x)| \right)^n \leq \frac{t^n}{n!} = \frac{2^{n-r}}{\pi^s} \sqrt{|\mathcal{D}|} N(I)$$

Ce qui conclut car $n = 2s + r$.

□

Théorème 7.25. *(Théorème de Dirichlet) Pour tout corps de nombre K, h_K est fini.*

Démonstration On note $\mathcal{D}$ le discriminant de K, $\Pi : K \to \mathbb{C}^s \times \mathbb{R}^r$ son plongement canonique.

Soit $q \in \mathbb{N}$, soit I un idéal de $\mathcal{O}_K$ de norme q. Alors par définition $q = card(\mathcal{O}_K/I)$. $\mathcal{O}_K/I$ est un groupe abélien additif de la forme $\mathbb{Z}/c_1\mathbb{Z} \times \cdots \mathbb{Z}/c_p\mathbb{Z}$, avec $c_1 \cdots c_p = q$ par le théorème de Lagrange ; on en déduit $q \in I$. Donc $(q) \subset I$. Or $N(q) = card(A/(q))$ est fini ; le nombre d'idéaux contenant (q) est donc fini.

On en déduit que pour tout $M \in \mathbb{R}_+$, il n'existe qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme inférieure à M.

On pose $M_K = (\frac{4}{\pi})^s \frac{n!}{n} \sqrt{|\mathcal{D}|}$. Il suffit pour conclure de montrer que pour toute classe d'idéaux, il existe un représentant de la classe de norme majorée par M_K, ce qui est vrai par 7.24.

□

8 Annexe B : Compléments sur j et Δ

8.1 Jungendtraum de Kronecker

Soient K un corps des nombres fixé et L une extension finie de K. On dit que l'extension $K \hookrightarrow L$ est **abélienne** si elle est Galoisienne de groupe de Galois abélien.

Définition 8.1. *On note K^{ab}* ***l'extension abélienne maximale*** *de K. C'est la composée de toutes les extensions abéliennes finies de K.*

On s'intéresse à la détermination de ce corps K^{ab}. Plus précisément, notant $\mathcal{E}(K)$ l'ensemble des extensions abéliennes de K, on veut en trouver une *base de voisinages*, c'est-à-dire un sous-ensemble $\mathcal{B}$ de $\mathcal{E}$ tel que tous les éléments de $\mathcal{E}(K)$ soient inclus dans un élément de $\mathcal{B}$.

La théorie des corps de classes permet de résoudre ce problème dans le cas $K = \mathbb{Q}$. On note dans ce qui suit $\zeta_n = e^{2\pi i/n}$ pour tout n entier positif.

Théorème 8.2. *(Kronecker-Weber) Soit L une extension abélienne de Q. Alors il existe un entier positif n, tel que $L \subset \mathbb{Q}(\zeta_n)$. De plus, le corps $\mathbb{Q}^{ab}$ est engendré sur $\mathbb{Q}$ par les racines de l'unité.*

$\mathbb{Q}^{ab}$ est en fait engendré par les valeurs sur $\mathbb{Q}$ de la fonction $z \mapsto e^{2\pi iz}$. On note e cette fonction.

Kronecker s'est intéressé à ce résultat et s'est en particulier posé la question suivante :

Jungendtraum de Kronecker Pour K un corps de nombre quelconque, l'extension $K \hookrightarrow K^{ab}$ est-elle engendrée par les valeurs d'une fonction transcendante sur K ?

C'est le rêve de jeunesse ("Jugendtraum") de Kronecker. Ce problème n'est pas encore résolu dans le cas général ; il l'est pour les corps quadratiques imaginaires. En effet, dans ces cas, la fonction j convient.

Fixons K un corps quadratique imaginaire. Par la théorie des corps de classes, on sait que K^{ab} est le composé des "ring class field" de tous les ordres de K et $\mathbb{Q}^{ab}$. On a remarqué dans la section 5.2 que pour $\mathcal{O}$ un ordre de K, $K(j(\mathcal{O}))$ est exactement le "ring class field" de $\mathcal{O}$.

Par ailleurs, soit z un élément de $K \cap \mathcal{H}$. Le réseau $\mathbb{Z} + \mathbb{Z}z$ est un idéal fractionnaire propre d'un ordre de K par le théorème 5.5. Alors $K(j(z)) = K(j(\mathcal{O}))$ est le "ring class field" de $\mathcal{O}$.

Donc le corps K^{ab} est engendré par les valeurs de j sur $K \cap \mathcal{H}$ et $\mathbb{Q}^{ab}$. De plus, $\{\mathbb{Q}(j(\mathcal{O})) \cdot K(\zeta_n) : \mathcal{O}$ est un ordre de K, $n \in \mathbb{N}^*\}$ est une *base de voisinages* de $\mathcal{E}(K)$. On dit la partie $\{\mathbb{Q}(\zeta_n)\}$ est **cyclotomique** et la partie $\{K(j(\mathcal{O}))\}$ est **anti-cyclotomique**. Il est facile de voir que les $j(\Lambda)$ pour un réseau Λ de K engendrent aussi la partie anti-cyclotomique.

On a des correspondances suivantes :

Le corps $\mathbb{Q}$	Le corps K
La fonction transcendante e	La fonction transcendante j
$e(\mathcal{O}_{\mathbb{Q}}) \in \mathbb{Z}$	$j(\mathcal{O}_K \cap \mathcal{H}) \in \mathbb{Z}$
$f_n(X) := X^n - 1$ $= \prod_{i=1}^{n}(X - \zeta_n^i) \in \mathbb{Z}[X]$	$F_n(Y, X) \in \mathbb{Z}[X, Y]$ avec $F_n(j, X) = \prod_{M \in S_n}(X - j \circ M)$
$\phi_n(X) \in \mathbb{Z}[X]$ $\phi_n(X) = \prod_{i=1, ppcm(i,n)=1}^{n}(X - \zeta_n^i)$	$\Phi_m(Y, X) \in \mathbb{Z}[X, Y]$ $\Phi_m(j, X) = \prod_{\sigma \in T_n}(X - j \circ \sigma)$
$f_n(X) = \prod_{d\|n} \phi_d(X)$	$F_n(Y, X) = \prod_{d^2\|n} \Phi(Y, X)$
Le polynôme cyclotomique ϕ_n est irréductible	$\Phi(Y, X)$ est irréductible par rapport à X
$E_{\mathbb{R}/\mathbb{Q}} = \{$Réseaux de $\mathbb{R}$ dans $\mathbb{Q}\}$	$E_{\mathbb{C}/K} = \{$Réseaux de $\mathbb{C}$ dans $K\}$
$Q^{ab} = \mathbb{Q}(e(E_{\mathbb{R}/\mathbb{Q}}))$	$K^{ab} = \mathbb{Q}^{ab} \cdot K(j(E_{\mathbb{C}/K}))$

Les réseaux de $\mathbb{R}$ dans $\mathbb{Q}$ sont simplement les groupes de la forme $\mathbb{Z}q$ avec $q \in \mathbb{Q}$

.

8.2 Les coefficients du q-développement de j et Δ

8.2.1 Les coefficients du q-développement de j

On a vu que le q-développement de j est $q^{-1} + \sum_{n=0} a_n q^n$ avec les a_n entiers. Peterson ([11]) montre que $a_n \sim e^{4\pi\sqrt{n}}/(\sqrt{2}n^{3/4})$ quand $n \to \infty$ en utilisant la méthode du cercle de Hardy, Ramanujan et Littlewood.

Des propriétés de congruences sur les coefficients ont également été démontrées :

Théorème 8.3. *Soient k et n deux entiers positifs. Les coefficients du q-développement de j vérifient :*

$$c(2^k n) \equiv 0 \mod 2^{3k+8}$$

$$c(3^k n) \equiv 0 \mod 3^{2k+3}$$

$$c(5^k n) \equiv 0 \mod 5^{k+1}$$
$$c(7^k n) \equiv 0 \mod 7^k$$
$$c(11^k n) \equiv 0 \mod 11^k$$

Pour les détails, on pourra voir [8], [9].

Les coefficients des q-développements d'autres fonctions modulaires commes g_2 et g_3 présentent aussi un grand intérêt ; on pourra voir à ce sujet [1],[7].

8.2.2 L'opérateurs de Hecke et application sur les coefficients du q-développement de Δ

Les coefficients du q-développement de Δ sont aussi très importants ; on les appelle les nombres de Ramanujan et les note $\tau(n)$.

Dans la section 3.2, on a vu que $\Delta(z) = q + \sum_{n\geq 1} \tau(n) q^n$. Donc Δ s'annule en ∞. Or on a vu que c'est une fonction modulaire de poids 12 holomorphe sur $\mathcal{H}$; on appelle **forme parabolique** une telle fonction (modulaire holomorphe sur $\mathcal{H}$ est s'annulant en ∞).

En utilisant les opérateurs de Hecke, on peut montrer que τ est multiplicative :

Proposition 8.4.
- *Soient m et n deux entiers positifs premiers entre eux, alors $\tau(mn) = \tau(n)\tau(m)$.*
- *Soient p un entier premier et l un entier positif, alors $\tau(p^{l+1}) = \tau(p^l)\tau(p) - p^{2k-1}\tau(p^{l-1})$.*

Cette proposition a été conjecturée par Ramanujan et démontrée par Mordell.

Suivent quelques mots sur les opérateurs de Hecke.

On fixe $2k$ un entier pair positif dans la suite.

Définition 8.5. *Soient n un entier positif, f un fonction parabolique de poids $2k$ et z un nombre dans $\mathcal{H}$. On définit une fonction F_f sur l'ensemble des réseaux de $\mathbb{C}$ par $F_f(\mathbb{Z}z_1 + \mathbb{Z}z_2) := z_2^{-2k} f(z_1/z_2)$. Il est facile de voir que F_f ne dépend pas le choix de la base de Λ sur $\mathbb{Z}$.*

Et on définit ***le*** n^{ieme} ***opérateur de Hecke*** *par*

$$(T(n)f)(z) := \sum_{\Lambda' \subset \mathbb{Z}+\mathbb{Z}z, [\mathbb{Z}+\mathbb{Z}z:\Lambda']=n} F_f(\Lambda') = n^{2k-1} \sum_{M \in S_n} f \circ M$$

On rappelle que S_n est l'ensemble des matrices de la forme $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$ tel que $ad = n, 0 \leq b < d$.

Il n'est pas difficile de voir que :

Théorème 8.6.
- *Soient m et n deux entiers positifs premier entre eux, alors $T(mn) = T(n)T(m)$.*
- *Soient p un entier premier et l un entier positif, alors $T(p^{l+1}) = T(p^l)T(p) - p^{2k-1}T(p^{l-1})$.*

En effet, l'opérateur de Hecke envoit une forme parabolique de poids $2k$ sur une forme parabolique de poids $2k$:

Proposition 8.7. *Soient f une forme parabolique de poids $2k$ et n un entier, alors $T(n)f$ est aussi une forme parabolique de poids $2k$.*

Cette proposition vient du fait que l'application de $\{f$: fonctions modulaires de poids $2k\}$ dans $\{F$: fonctions sur les réseaux tel que $F(\lambda\Lambda) = \lambda^{-2k}F(\Lambda)$ pour tout les réseaux Λ et complexes $\lambda\}$ définie par $f \mapsto F_f$ est bijective.

Par le théorème 3.2, on peut en déduire que toutes les formes paraboliques de poids 12 sont multiples de Δ. La démonstration fonctionne comme celle montrant que toutes les fonctions modulaires de poids 0 holomorphes sur $\mathcal{H}$ sont dans $\mathbb{C}[j]$. En particulier, Δ est une fonction propre pour tous les T_n. En calculant le coefficient initial du q-développement, on a $T(n)\Delta = \tau_n\Delta$. A l'aide du théorème 8.6, on en déduit la proposition 8.4.

8.2.3 Bornes des coefficients du q-développement de Δ

Ramanujan a conjecturé que $\tau_p \leq 2p^{11/2}$ pour tout $p \in \mathcal{P}$. Deligne a indiqué que la conjecture de Weil implique cette conjecture de Ramanujan, et il a ensuite donné une démonstration de la conjecture de Weil par la théorie de cohomology d'étale. La démonstration pour la conjecture de Weil inclus les travaux remarquables de Grothendieck et Serre, elle est très importante dans la théorie moderne de la geométrie algébrique.

Théorème 8.8. *(Deligne) Pour tout les $n \in \mathbb{N}$, $|\tau(n)| \leq \sigma_0(n)n^{1/2}$ où σ_0 est le nombre de diviseurs de n. On remarque que si n est premier, alors $\sigma_0(n) = 2$.*

On pourra voir [4], [5].

Plus généralement, on a une conjecture pour tous les formes paraboliques :

Conjecture 8.9. *(Ramanujan-Petersson) Soit $f = \sum_{n\geq 1} c_n q^n$ une forme parabolique de poids k où $k \geq 1$ est un entier, alors pour tout $\epsilon > 0$, il existe un nombre C_ϵ, tel que $|a_n| \leq C_\epsilon n^{(k-1)/2+\epsilon}$ pour tout entier positif n.*

Deligne et Serre ont prouvé cette conjecture pour tous les $k \geq 2$. C'est une conséquence de la conjecture de Weil.

Références

[1] T Apostol. *Modular Functions and Dirichlet Series in Number Theory.* Number 41 in GTM. Springer, 1970.

[2] Zenon Borevitch and Igor Chafarevitch. *Théorie des nombres.* Gauthier-Villars, 1967.

[3] David A. Cox. *Primes of the Form $x^2 + ny^2$.* John Wiley & Sons, 1989.

[4] P Deligne. Formes modulaires et représentations l-adiques. In *Séminaire Bourbaki, 21e année, 1968/69*, number 179 in Lecture Notes in Mathematics, pages 139–172. Springer, 1971.

[5] P Deligne. La conjecture de Weil I. *Publications Mathématiques IHES*, (43) :273–307, 1974.

[6] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Springer, 1993.

[7] Serge Lang. *Elliptic Functions.* Number 112 in GTM. Springer, 1987.

[8] J Lehner. Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. *American Journal of Mathematics*, (71) :136–148, 1949.

[9] J Lehner. Further congruence properties for the Fourier coefficients of the modular invariant $j(\tau)$. *American Journal of Mathematics*, (71) :373–386, 1949.

[10] James Milne. *Elliptic Curves.* BookSurge Publishers, 2006.

[11] H Petersson. Uber die Entwicklungskoeffzienten der automorphen formen. *Acta Mathematica*, (58) :169–215, 1932.

[12] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, 2003.

[13] R Schertz. Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_2, γ_3. *Journal für die reine und angewandte Mathematik*, (286/287) :pg 46–74, 1976.

[14] Joseph Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer, 1994.