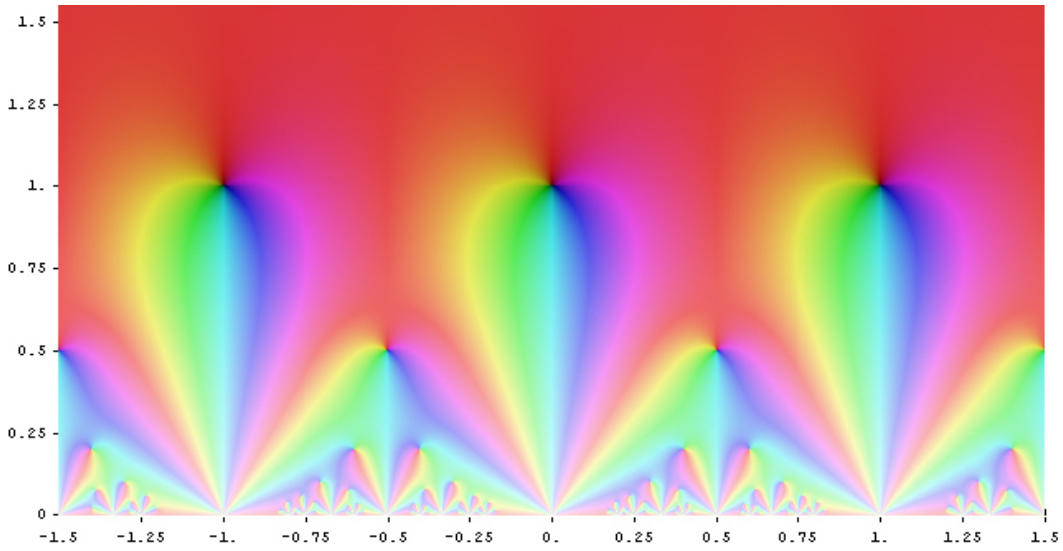
Introduction aux formes modulaires

Hanecart Valentin

2024



Sommaire

Notations

$\mathcal{H}$: ensemble des nombres complexes dont la partie imaginaire est strictement positive.

$\mathbb{P}_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$: droite projective complexe.

$\mathrm{SL}_2(\mathbb{R}) : \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \;\middle|\; ad - bc = 1 \right\}$.

$\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{-I_2; I_2\}$: groupe spécial linéaire projectif d'ordre 2 sur $\mathbb{R}$.

$\mathrm{SL}_2(\mathbb{Z}) : \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) \;\middle|\; ad - bc = 1 \right\}$.

$G = \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{-I_2; I_2\}$: groupe modulaire.

$\mathcal{D} = \left\{ z \in \mathcal{H} \;\middle|\; |z| \geq 1,\ |\mathrm{Re}(z)| \leq \dfrac{1}{2} \right\}$: domaine fondamental du groupe modulaire.

$\rho = e^{\frac{2i\pi}{3}}$

$L(\omega_1, \omega_2) = \left\{ m\omega_1 + n\omega_2,\ (m,n) \in \mathbb{Z}^2 \right\}$: $\mathbb{Z}$-réseau de $\mathbb{C}$ de $\mathbb{Z}$-base (ω_1, ω_2)

$\mathrm{Ind}_\gamma(z)$: indice du point affixe z par rapport au lacet γ.

$\mathrm{Res}(f, z)$: résidu de la fonction f au point d'affixe z.

$\wp$: fonction $\wp$ de Weierstrass.

$D(L) = g_4^3(L) - 27g_6^2(L)$: discriminant de la courbe elliptique d'équation $Y^2 = 4X^3 - g_4(L) - g_6(L)$.

$j(L) = (2\pi)^{12} \dfrac{1728 g_4^3}{D(L)}$: invariant modulaire de la courbe elliptique d'équation $Y^2 = 4X^3 - g_4(L)X - g_6(L)$.

$q = q(z) = e^{2i\pi z}$.

$\mathcal{D}(a, r) = \{z \in \mathbb{C} \mid |z - a| < r\}$: disque ouvert de centre a et de rayon r.

$\mathring{\mathcal{D}}(a, r) = \{z \in \mathbb{C} \mid 0 < |z - a| < r\}$: disque ouvert épointé de centre a et de rayon r.

M_k : $\mathbb{C}$-espace vectoriel des formes modulaires de poids k (et de niveau 1).

S_k : $\mathbb{C}$-espace vectoriel des formes paraboliques de poids k (et de niveau 1).

M_* : $\mathbb{C}$-algèbre graduée des formes modulaires (de niveau 1).

$\mathcal{R}$: ensemble des réseaux de $\mathbb{C}$.

M : ensemble des couples (ω_1, ω_2) d'éléments de $\mathbb{C}^*$ tels que $\mathrm{Im}\left(\dfrac{\omega_1}{\omega_2}\right) > 0$.

G_k : série d'Eisenstein de poids k non normalisée.

ζ : fonction ζ de Riemann.

$g_4 = 60G_4$.

$g_6 = 140G_6$.

$\Delta = \dfrac{1}{(2\pi)^{12}}\left(g_4^3 - 27g_6^2\right)$.

b_n : n-ième nombre de Bernoulli.

B_n : n-ième polynôme de Bernoulli.

$\sigma_k : n \longmapsto \displaystyle\sum_{\substack{d|n \\ d\geq 1}} d^k$.

E_k : série d'Eisenstein de poids k normalisée.

$v_p(f)$: plus petit entier naturel n tel que $\dfrac{f}{(z-p)^n}$ soit holomorphe et non nulle en p.

$j = \dfrac{1\ 728g_4^3}{\Delta}$: invariant modulaire.

T_n : n-ième opérateur de Hecke.

R_λ : opérateur d'homothétie par $\lambda \in \mathbb{C}^*$.

$\mathcal{P}$: ensemble des nombres premiers.

τ : fonction τ de Ramanujan.

$< \cdot ; \cdot >_{\mathcal{P}}$: produit scalaire de Petersson.

Γ : sous-groupe de congruence de $\mathrm{SL}_2(\mathbb{Z})$.

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ [N] \right\}.$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ [N] \right\}.$$

$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

$C(\Gamma)$: ensemble des pointes pour un sous-groupe de congruence Γ.

$M_k(\Gamma)$: $\mathbb{C}$-espace vectoriel des formes modulaires de poids k pour le sous-groupe de congruence Γ.

$S_k(\Gamma)$: $\mathbb{C}$-espace vectoriel des formes paraboliques de poids k pour le sous-groupe de congruence Γ.

$E_k(\Gamma)$: sous-espace d'Eisenstein de $M_k(\Gamma)$.

$M_*(\Gamma)$: $\mathbb{C}$-algèbre graduée des formes modulaires pour le sous-groupe de congruence Γ.

$v_p(N)$: valuation p-adique de N.

$\left(\frac{\cdot}{\cdot}\right)$: symbole de Legendre.

φ : fonction indicatrice d'Euler.

$\psi(N) = [\Gamma_0(N) : \Gamma_1(N)]$: indice de $\Gamma_1(N)$ dans $\Gamma_0(N)$.

$r(n,k)$: nombre de représentations de l'entier n en somme de k carrés.

$\theta(z,k)$: série génératrice des $r(n,k)$.

θ : fonction θ de Jacobi.

$\mathcal{S}(\mathbb{R})$: classe de Schwarz sur $\mathbb{R}$.

$\widehat{f}$: transformée de Fourier de f.

$D(f) = \dfrac{1}{2i\pi} f'$.

$\mathbb{G}_k$: série d'Eisenstein renormalisée de poids k.

ϑ_k : dérivée de Serre.

$\widetilde{M_*} = \mathbb{C}[G_2, G_4, G_6]$: anneau des formes quasimodulaires sur $\mathrm{SL}_2(\mathbb{Z})$.

$[\cdot,\cdot]_n$: n-ième crochet de Rankin-Cohen.

Introduction

En mathématiques, une forme modulaire est une fonction holomorphe sur le demi-plan de Poincaré satisfaisant à une certaine sorte d'équation fonctionnelle et de condition de croissance. La théorie des formes modulaires est par conséquent dans la lignée de l'analyse complexe mais l'importance principale de la théorie tient dans ses connexions avec le théorème de modularité (auparavant appelé conjecture de Taniyama-Weil ou conjecture de Shimura-Taniyama-Weil ou conjecture de Shimura-Taniyama) et la théorie des nombres.

En effet, la définition d'une forme modulaire pourrait donner l'impression que les formes modulaires occupent un coin sombre de l'analyse complexe, cependant ce n'est pas du tout le cas ! Les formes modulaires sont des objets très géométriques, arithmétiques et topologiques et qui possèdent un grand intérêt dans divers champs des mathématiques dont voici quelques exemples :

* **Dernier théorème de Fermat :**
  La preuve d'Andrew Wiles du dernier théorème de Fermat utilise de manière intensive les formes modulaires (cf. [8] pour plus de détails). Le travail d'Andrew Wiles et de ses collègues sur la modularité ont également étendu massivement les méthodes de calcul pour les courbes elliptiques sur $\mathbb{Q}$ (puisque beaucoup d'algorithmes pour les courbes elliptiques requièrent qu'elles soient modulaires).

* **Équations diophantiennes :**
  La preuve d'Andrew Wiles du dernier théorème de Fermat a mis à disposition un large éventail de nouvelles techniques pour résoudre certaines équations diophantiennes. Un tel travail repose essentiellement sur l'existence d'un accès à des tables ou à des logiciels pour le calcul des formulaires modulaires (Andrew Wiles n'avait pas besoin d'un ordinateur puisque les espaces pertinents de formes modulaires qui se posent dans sa preuve sont de dimension 0 !).

* **Conjecture de Birch et Swinnerton-Dyer :**
  Ce problème ouvert central en géométrie arithmétique relie les propriétés arithmétiques des courbes elliptiques (et des variétés abéliennes) à des valeurs spéciales de fonctions L. La plupart des résultats profonds vers cette conjecture utilisent largement des formes modulaires (par exemple les travaux de Victor Kolyvagin, Benedict Gross, Don Zagier et Kazuya Kato). En outre, les formes modulaires sont utilisées pour calculer et prouver les résultats sur les valeurs particulières de ces fonctions L.

* **Problème des nombres congruents :**
  Cet ancien problème ouvert est de déterminer quels entiers sont l'aire d'un triangle rectangle avec des côtés de longueurs rationnelles. Il existe une solution potentielle qui utilise intensivement des formes modulaires (de poids 1,5), cependant la solution est conditionnelle à l'exactitude de la conjecture de Birch et Swinnerton-Dyer (qui n'est pas encore connue)...

* **Construction de graphes de Ramanujan :**
  Les formes modulaires peuvent être utilisés pour construire des graphes d'expansion presque optimaux qui jouent un rôle important dans la théorie des réseaux de communication.

* **Cryptographie et théorie du codage :**
  Compter des points sur une courbe elliptique sur un corps fini est essentiel à la construction de cryptosystèmes

basés sur des courbes elliptiques et les formes modulaires sont pertinentes pour les algorithmes efficaces de comptage de points. Les courbes algébriques qui sont associées aux formes modulaires sont également utiles dans la construction et l'étude certains codes correcteurs d'erreurs.

* **Conjecture de Serre sur la modularité de représentations galoisiennes :**
  Jean-Pierre Serre conjectura et beaucoup de gens ont travaillé pour prouver que tout morphisme continu $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2(\mathbb{F}_q)$ (avec $\det\left(\rho\left(z \longmapsto \overline{z}\right)\right) = -1$) "provient" d'une forme modulaire. Plus précisément, pour presque tout nombre premier p, les coefficients a_p d'une forme modulaire $\sum a_n q^n$ sont congrus aux traces des éléments $\rho\left(\mathrm{Frob}_p\right)$ (où Frob_p sont certains éléments spéciaux du groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$).

* **Fonctions génératrices pour des partitions :**
  Les fonctions génératrices pour différents types de partitions d'un entier peut souvent être relié à des formes modulaires. Des théorèmes profonds sur les formes modulaires peuvent ainsi se traduire dans des résultats concernant les partitions d'entiers.

* **Réseaux :**
  Si $L \subseteq \mathbb{R}^n$ est un réseau unimodulaire pair (la matrice de base a pour déterminant ± 1 et pour tout $\lambda \in L$, on a $< \lambda; \lambda > \in 2\,\mathbb{Z}$), alors la fonction θ définie par

$$\theta_L(q) = \sum_{\lambda \in L} q^{<\lambda;\lambda>}$$

  est une forme modulaire de poids $\dfrac{n}{2}$. Le coefficient de q^m est le nombre de vecteurs du réseau dont la norme au carré vaut m. Ainsi, les théorèmes et les méthodes de calcul pour les formes modulaires se traduisent en théorèmes et méthodes de calcul pour les réseaux. Par exemple, le théorème 290 de Manjul Bhargava et Jonathan Hanke est un théorème sur les réseaux, qui affirme qu'une forme quadratique à valeur entière représente tous les entiers positifs si et seulement si elle représente les entiers jusqu'à 290 (il est prouvé en faisant de nombreux calculs (à la fois théoriques et avec un ordinateur) avec des formes modulaires).

Notre objectif ici sera de rendre compte de cette diversité en illustrant l'utilisation de plusieurs domaines des mathématiques afin d'obtenir des résultats tous aussi variés grâce à l'utilisation de formes modulaires. Nous tenterons également d'illustrer les propos avec une multitude d'exemples ainsi que l'utilisation de `PARI/GP` et `SAGE` pour vérifier nos résultats grâce à l'outil informatique.

Le contenu de ce projet sera divisé en cinq chapitres. Tout d'abord, le premier chapitre sera consacré à quelques préliminaires qui nous seront utiles pour la suite (notamment avec l'introduction du groupe modulaire ainsi que les fonctions et courbes elliptiques sur $\mathbb{C}$). Un deuxième chapitre servira d'introduction générale à la théorie des formes modulaires et nous y donnerons des premières applications. Dans un troisième chapitre nous parlerons des opérateurs de Hecke qui nous permettront de donner de nouvelles applications et de répondre à d'anciennes conjectures. Le quatrième chapitre sera dédié à la généralisation de la notion de forme modulaire et enfin un dernier chapitre rassemblera d'autres applications des formes modulaires.

Chapitre 1

Préliminaires

Le but de ce premier chapitre sera de donner des (r)appels sur les notions utiles afin aborder les chapitres qui suivent. On commencera dans un premier temps par la notion de groupe modulaire qui nous sera utile lorsque l'on parlera de formes modulaires, puis dans un deuxième temps nous parlerons de fonctions et courbes elliptiques sur $\mathbb{C}$ qui nous serons utiles lorsque nous aborderons notamment les fonctions réseaux, le discriminant et l'invariant modulaire.

I Le groupe modulaire

Commençons par le groupe modulaire en donnant quelques définitions puis les résultats essentiels à la compréhension du cours.

I.1 Définitions

On note $\mathcal{H}$ le demi-plan supérieur de $\mathbb{C}$ (autrement dit, l'ensemble des nombres complexes z tels que $\mathrm{Im}(z) > 0$) et $\mathbb{P}_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ la droite projective complexe.

On fait opérer $\mathrm{SL}_2(\mathbb{R})$ sur $\mathbb{P}_1(\mathbb{C})$ de la manière suivante : pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ et $z \in \mathbb{P}_1(\mathbb{C})$, on pose :

$$g.z = \frac{az+b}{cz+d}. \tag{1.1}$$

On rappelle que si $c = 0$, alors on pose $g.\infty = \infty$ et si $c \neq 0$, alors on pose $g.\infty = \dfrac{a}{c}$ et $g.\left(-\dfrac{d}{c}\right) = \infty$.

De plus, pour tout $z \in \mathcal{H}$, on a :

$$\mathrm{Im}(g.z) = \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}\right) = (ad-bc)\frac{\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0. \tag{1.2}$$

Ainsi, $\mathcal{H}$ est stable par l'action de $\mathrm{SL}_2(\mathbb{R})$ et on vérifie que cette action est bien une action de groupes.

On remarque que l'élément $-I_2 \in \mathrm{SL}_2(\mathbb{R})$ opère trivialement sur $\mathcal{H}$ au même titre que I_2 (et se sont les seuls). Pour rendre l'action précédente fidèle, on va plutôt considérer que c'est le groupe $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{-I_2; I_2\}$ qui opère sur $\mathcal{H}$.

On s'intéresse désormais au sous-groupe discret $\mathrm{SL}_2(\mathbb{Z})$ de $\mathrm{SL}_2(\mathbb{R})$.

Définition 1 : Groupe modulaire :
On appelle **groupe modulaire** le groupe $G = \mathrm{SL}_2(\mathbb{Z})/\{-I_2; I_2\}$ (image du groupe $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathrm{PSL}_2(\mathbb{R})$) et on le note $\mathrm{PSL}_2(\mathbb{Z})$.

Remarque :
Pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on se permettra un léger abus de notations en notant encore g son image dans le groupe modulaire G.

I.2 Domaine fondamental du groupe modulaire

On considère les matrices $S, T \in \mathrm{SL}_2(\mathbb{Z})$ définies par :

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

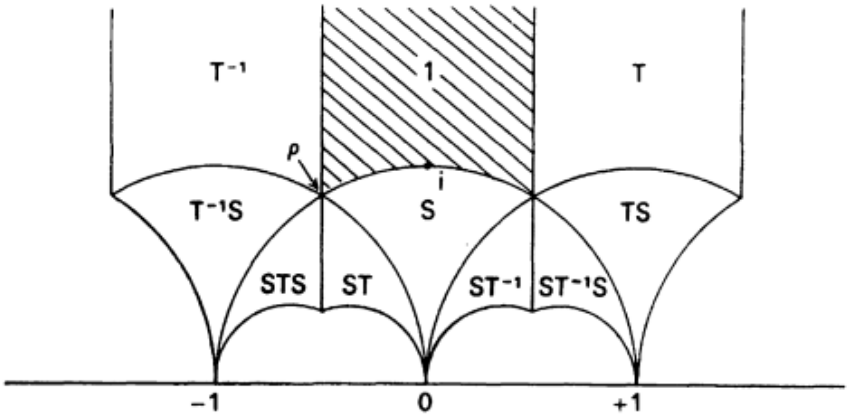
On remarque que l'on a les relations :

$$\left\{ \begin{array}{ll} S.z & = -\dfrac{1}{z} \\ S^2 & = I_2 \end{array} \right. \text{ et } \left\{ \begin{array}{ll} T.z & = z+1 \\ (ST)^3 & = I_2 \end{array} \right. . \tag{1.3}$$

On notera $\mathcal{D}$ le sous-ensemble de $\mathcal{H}$ formé des points z tels que $|z| \geq 1$ et $|\mathrm{Re}(z)| \leq \dfrac{1}{2}$.

La figure ci-dessous donne les transformations de $\mathcal{D}$ par les éléments de l'ensemble :

$$\{I_2; T; TS; ST^{-1}S; ST^{-1}; S; ST; STS; T^{-1}S; T^{-1}\}$$



Nous allons montrer que $\mathcal{D}$ est un **domaine fondamental** pour l'action de G sur le demi-plan $\mathcal{H}$. Plus précisément, on a le théorème suivant :

Théorème 1 :

- Pour tout $z \in \mathcal{H}$, il existe $g \in G$ tel que $g.z \in \mathcal{D}$.
- Si deux points distincts $z, z' \in \mathcal{D}$ sont congrus modulo G, alors on a :

$$\left(\mathrm{Re}(z) = \pm\frac{1}{2} \text{ et } z = z' \pm 1\right) \text{ ou bien } \left(|z| = 1 \text{ et } z' = -\frac{1}{z}\right).$$

- Pour $z \in \mathcal{D}$, on a $\mathrm{Stab}(z) = \{I_2\}$ sauf dans les trois cas suivants :
  - $z = i$, auquel cas $\mathrm{Stab}(z)$ est le groupe d'ordre 2 engendré par S.
  - $z = \rho = e^{\frac{2i\pi}{3}}$, auquel cas $\mathrm{Stab}(z)$ est le groupe d'ordre 3 engendré par ST.
  - $z = -\overline{\rho} = e^{\frac{i\pi}{3}}$, auquel cas $\mathrm{Stab}(z)$ est le groupe d'ordre 3 engendré par TS.

Preuve :

∗ Soient $z \in \mathcal{H}$ et $G' =< S, T >$ le sous-groupe de G engendré par S et T.
Si $g' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément de G', alors d'après (1.2) on a :

$$\mathrm{Im}(g.z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

Or, c et d sont des entiers et z est fixé, donc le nombre de couples $(c,d) \in \mathbb{Z}^2$ tels que $|cz+d|^2$ soit inférieur à un nombre donné est fini. Ainsi, il existe $g \in G'$ tel que $\mathrm{Im}(g.z)$ soit maximal.
De plus, il existe un entier relatif n tel que $T^n.(g.z)$ ait une partie réelle comprise entre $-\frac{1}{2}$ et $\frac{1}{2}$. Ainsi, l'élément $z' = T^n.(g.z)$ appartient à $\mathcal{D}$ puisque si l'on suppose que $|z'| < 1$, alors $-\frac{1}{z'}$ aurait une partie imaginaire strictement plus grande que celle de z', ce qui est contradictoire avec la définition de z'.
L'élément $g' = T^n.g \in G' \subseteq G$ est donc tel que $g'.z \in \mathcal{D}$.

∗ Soient $z \in \mathcal{D}$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ tels que $g.z \in \mathcal{D}$ (possible par le premier point puisque $\mathcal{D} \subseteq \mathcal{H}$).
Commençons par le cas où $\mathrm{Im}(g.z) \geq \mathrm{Im}(z)$ (c'est-à-dire $|cz+d| \leq 1$). Cela étant impossible pour $|c| \geq 2$ (car $z \in \mathcal{D}$), il nous reste à examiner les cas où $c = -1, 0$ et 1 :

— Si $c = 0$, alors on a $ad = \det(g) = 1$ et donc (quitte à changer g en $-g$) $a = d = 1$ et $g.z = z + b$. On a alors trois sous-cas :
- Si $|\mathrm{Re}(z)| \leq \frac{1}{2}$, alors $b = 0$ et $g = \pm I_2$.
- Si $\mathrm{Re}(z) = -\frac{1}{2}$, alors $b = 0$ ou 1 et $g = \pm I_2$ ou T.
- Si $\mathrm{Re}(z) = \frac{1}{2}$, alors $b = 0$ ou -1 et $g = \pm I_2$ ou T^{-1}.

— Si $c = 1$, alors $|z+d| \leq 1$ et donc $(d = 0)$, ou $(d = 1$ et $z = \rho)$ ou $(d = -1$ et $z = -\overline{\rho})$.
- Si $d = 0$, alors $b = -\det(g) = 1$, donc $g.z = a - \frac{1}{z}$. De plus, on a $|z| \leq 1$, donc comme $z \in \mathcal{D}$, on a $|z| = 1$ et $-\frac{1}{z}$ est le symétrique de z par rapport à l'axe des imaginaires purs. $g.z$ n'est donc dans $\mathcal{D}$ que si $(a = 0)$ ou $(z = \rho$ et $a = -1)$ ou $(z = -\overline{\rho}$ et $a = 1)$, d'où $g = S$ ou $(ST)^2$ ou TS.
- Si $d = 1$ et $z = \rho$, alors $a - b = \det(g) = 1$, donc $g.\rho = \frac{a\rho + (a-1)}{\rho + 1} = a + \rho$ qui n'est dans $\mathcal{D}$ que si $a = 0$ ou 1, c'est-à-dire $g = ST$ ou TST.
- Si $d = -1$ et $z = -\overline{\rho}$, alors on a de même que $g = (TS)^2$ ou $T^{-1}ST^{-1}$.

— Si $c = -1$, alors on se ramène au cas précédent en changeant g par $-g$, ce qui ne change pas $g.z$.

Finalement, si $\mathrm{Im}(g.z) < \mathrm{Im}(z) = \mathrm{Im}\left(g^{-1}.(g.z)\right)$, alors puisque z et $g.z$ sont dans $\mathcal{D}$, on applique le même raisonnement que ci-dessus à g^{-1}.

∗ Par ce qui précède, on a montré que $z \in \mathcal{D}$ on a $\mathrm{Stab}(z) = \{I_2\}$ et les cas où $z = i$, ρ et $-\overline{\rho}$ se déduisent des disjonctions de cas faites au point précédent.

■

Corollaire 1 :
La projection canonique $\pi : \mathcal{D} \longmapsto \mathcal{H}/G$ est surjective.
De plus, sa restriction à $\mathring{\mathcal{D}}$ est injective.

Preuve :
∗ Par le premier point du théorème 1, on obtient que pour tout $z \in \mathcal{H}$, il existe $g \in G$ tel que $g.z \in \mathcal{D}$. Autrement dit, le point $z' = g.z$ est congru à z modulo G, donc la projection canonique π est surjective.

∗ Par le deuxième point du théorème 1, deux points de $\mathring{\mathcal{D}}$ sont congrus modulo G si, et seulement si, ils sont égaux. Donc la restriction de π à $\mathring{\mathcal{D}}$ est injective.

■

Théorème 2 :
Le groupe G est engendré par S et T.

Preuve :
Soient $g \in G$ et $G' =< S, T >$ le sous-groupe de G engendré par S et T.
On choisit un point $z_0 \in \mathring{\mathcal{D}}$ (par exemple $2i$) et on pose $z = g.z_0$.
Par la preuve du premier point du théorème 1, il existe $g' \in G'$ tel que $g'.z \in \mathcal{D}$. Ainsi, les points z_0 et $g'.z = g'.(g.z_0) = (g'g).z_0$ de $\mathcal{D}$ sont congrus modulo G et puisque l'un d'eux est dans l'intérieur de $\mathcal{D}$ on en déduit par le corollaire 1 que ces points sont confondus et donc que $g'g = I_2$.

Finalement, on a $g = (g')^{-1} \in G'$ (car G' est un sous-groupe de G).

■

Remarques :

∗ On peut montrer qu'une présentation de G est donnée par $\langle S, T \mid S^2 = I_2,\ (ST)^3 = I_2 \rangle$.

∗ Dans `SAGE`, on peut calculer le groupe $\mathrm{SL}_2(\mathbb{Z})$ et ses générateurs de la manière suivante :

```
sage: G = SL(2,ZZ) ; G
Modular Group SL(2,Z)
sage: S,T = G.gens()
sage: S
[ 0 -1]
[ 1 0]
sage: T
[ 1 1]
[ 0 1]
```

II Fonctions elliptiques et courbes elliptiques sur $\mathbb{C}$

On donne désormais les outils de base sur les fonctions et courbes elliptiques sur $\mathbb{C}$ qui nous seront utiles lorsque nous aborderons notamment la forme parabolique Δ ainsi que l'invariant modulaire j.

II.1 Fonctions elliptiques

Historiquement, les fonctions elliptiques ont été inventées et étudiées par Gauss, Abel, Jacobi et Weierstrass. Grossièrement parlant, une fonction elliptique est une fonction définie sur le plan complexe qui est doublement périodique (périodique dans deux directions), elle peut ainsi être vue comme l'analogue d'une fonction trigonométrique (qui a une seule période).

II.1.1 Zéros et pôles

Nous introduisons ici les fonctions elliptiques en donnant leur définition ainsi que quelques propriétés fondamentales qui rendent ces fonctions remarquables.

Commençons par introduire la notion de réseau qui nous sera utile pour l'étude des fonctions elliptiques :

Définition 2 : Réseau sur un $\mathbb{R}$-espace vectoriel de dimension finie :
On considère V un $\mathbb{R}$-espace vectoriel de dimension finie.
On appelle **réseau de** V tout sous-groupe Γ de V vérifiant les conditions équivalentes suivantes :

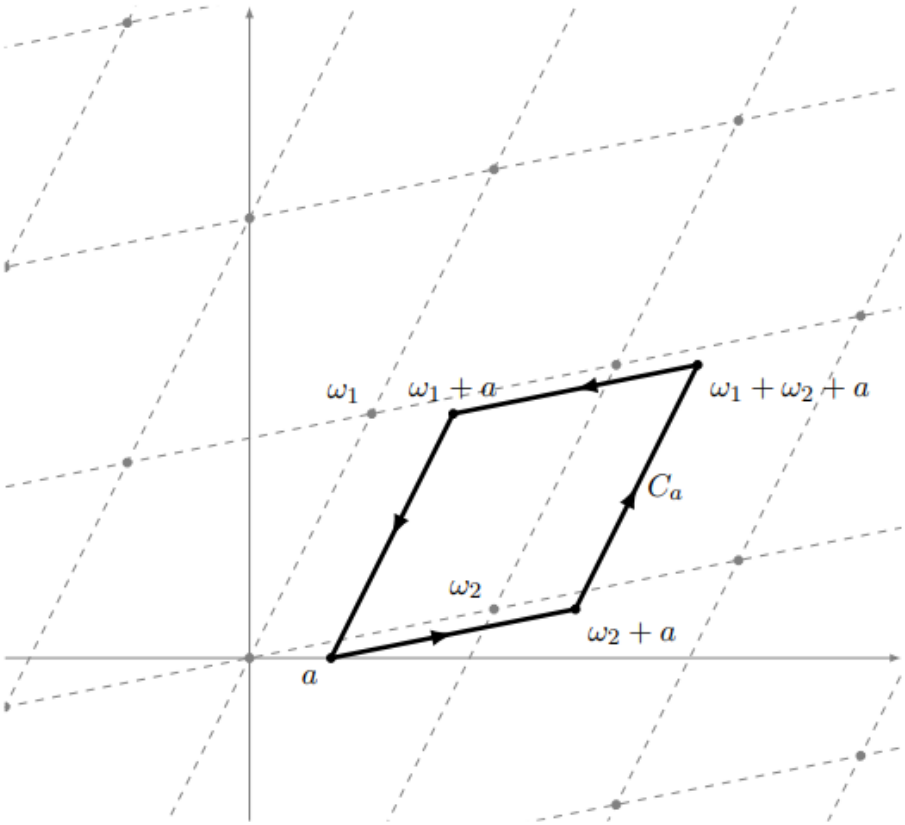
- Γ est discret et V/Γ est compact.
- Γ est discret et engendre le $\mathbb{R}$-espace vectoriel V.
- Il existe une $\mathbb{R}$-base $(e_1, ..., e_n)$ de V qui est une $\mathbb{Z}$-base de Γ (c'est-à-dire que $\Gamma = \mathbb{Z}e_1 \oplus ... \oplus \mathbb{Z}e_n$).

Dans toute la suite de cette partie, on considère ω_1 et ω_2 deux nombres complexes qui sont $\mathbb{R}$-indépendants (c'est-à-dire tels que $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$) et on supposera toujours que l'on a $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$ (et puisque $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right)$ est de signe opposé à $\mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right)$, l'hypothèse est alors toujours réalisable quitte à échanger les rôles de ω_1 et ω_2).

Définition 3 : Fonction elliptique :
On considère une fonction f méromorphe sur $\mathbb{C}$.
On dit que f est une **fonction elliptique** de périodes ω_1 et ω_2 lorsque pour tout $z \in \mathbb{C}$ qui n'est pas un pôle de f on a la relation :

$$f(z+\omega_1) = f(z) \text{ et } f(z+\omega_2) = f(z) \tag{1.4}$$

Remarque :
En posant $L(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \left\{m\omega_1 + n\omega_2,\ (m,n) \in \mathbb{Z}^2\right\}$, le réseau de $\mathbb{Z}$-base (ω_1, ω_2), la condition (1.4) est équivalente au fait que, pour tout $\omega \in L(\omega_1, \omega_2)$ on ait $f(z+\omega) = f(z)$.



Nous désignerons par C_a le contour formé de l'union des quatre segments

$$[a;\omega_2+a],\ [\omega_2+a;\omega_1+\omega_2+a],\ [\omega_1+\omega_2+a;\omega_1+a] \text{ et } [\omega_1+a;a]$$

et parcouru dans le sens trigonométrique (cf. figure ci-dessus).

Puisque f est une fonction méromorphe, ses zéros et ses pôles sont discrets (on supposera implicitement que f n'est pas la fonction nulle sinon il n'y a pas grand chose d'intéressant à dire...) et on peut alors toujours choisir a tel qu'aucun zéro ou pôle de f n'appartienne pas à C_a.

L'intérieur du contour C_a auquel on rajoute (à comprendre au sens de l'union) les segments $[a;\omega_2+a]$ et $[\omega_2+a;\omega_1+\omega_2+a]$ (que l'on notera D_a) forme un domaine fondamental de $\mathbb{C}$ pour le groupe $\mathcal{T}$ des translations de la forme $z\longmapsto z+\omega$ avec $\omega\in L(\omega_1,\omega_2)$ (c'est-à-dire que les images de D_a par l'action du groupe $\mathcal{T}$ forment une partition de $\mathbb{C}$) et donc en particulier que c'est un domaine contenant exactement un point par orbite du groupe $\mathcal{T}$ (c'est-à-dire que n'importe quel point de $\mathbb{C}$ peut être envoyé via un élément de $\mathcal{T}$ sur un point de D_a et deux points distincts dans l'intérieur de D_a ne peuvent pas être équivalents pour l'action de $\mathcal{T}$).

Proposition 1 :
Soit f une fonction elliptique sur le réseau $L(\omega_1,\omega_2)$ et non identiquement nulle.

- La somme des résidus de f en ses pôles dans D_a est égale à 0.
- Le nombre de zéros de f dans D_a est égal au nombre de pôles de f dans D_a (tous les deux comptés avec multiplicité) et cette quantité commune est appelée **ordre de la fonction elliptique** f.
- La somme des zéros et pôles de f (tous les deux comptés avec multiplicité) appartient à L.
- Si f est non constante, alors f est au moins d'ordre 2.

Preuve :
Soit f une fonction elliptique sur le réseau $L(\omega_1,\omega_2)$ et non identiquement nulle.

- D'une part, nous avons :

$$\begin{aligned}\int_{C_a} f(z)\mathrm{d}z &= \int_{[a;\omega_2+a]} f(z)\mathrm{d}z + \int_{[\omega_2+a;\omega_1+\omega_2+a]} f(z)\mathrm{d}z + \int_{[\omega_1+\omega_2+a;\omega_1+a]} f(z)\mathrm{d}z + \int_{[\omega_1+a;a]} f(z)\mathrm{d}z\\ &= \int_{[a;\omega_2+a]} f(z)\mathrm{d}z + \int_{[\omega_2+a;\omega_1+\omega_2+a]} f(z)\mathrm{d}z - \int_{[\omega_1+a;\omega_1+\omega_2+a]} f(z)\mathrm{d}z - \int_{[a;\omega_1+a]} f(z)\mathrm{d}z\\ &= \int_{[a;\omega_2+a]} f(z)\mathrm{d}z + \int_{[a;\omega_1+a]} f(z+\omega_2)\mathrm{d}z - \int_{[a;\omega_2+a]} f(z+\omega_1)\mathrm{d}z - \int_{[a;\omega_1+a]} f(z)\mathrm{d}z\\ &= \int_{[a;\omega_2+a]} \left(f(z)-f(z+\omega_1)\right)\mathrm{d}z + \int_{[a;\omega_1+a]} \left(f(z+\omega_2)-f(z)\right)\mathrm{d}z = 0\end{aligned}$$

  Or, par le théorème des résidus, on a aussi :

$$\int_{C_a} f(z)\mathrm{d}z = 2i\pi\sum_{k=1}^{n} \mathrm{Ind}_{C_a}(z_i)\,\mathrm{Res}(f,z_i) = 2i\pi\sum_{k=1}^{n}\mathrm{Res}(f,z_i)$$

  où les z_i sont les pôles de f. Donc la somme des résidus de f en ses pôles dans D_a est égale à 0.

- Posons la fonction g définie sur $\mathbb{C}$ privé des points où f s'annule ou a un pôle par $g(z)=\dfrac{f'(z)}{f(z)}$.
  La fonction g est alors une fonction elliptique et chaque période de f est une période de g. De plus, si f a un zéro d'ordre m en $\omega\in\mathbb{C}$, alors g a un pôle simple de résidu m en ω. De même, si f a un pôle d'ordre m en $\omega\in\mathbb{C}$, alors g a un pôle simple de résidu $-m$ en ω. Enfin, si $\omega\in\mathbb{C}$ n'est ni un zéro ni un pôle de f, alors g est holomorphe sur un voisinage de $\omega\in\mathbb{C}$.
  Il s'en suit que la somme des résidus de g au pôles de g dans D_a est égale à la somme des ordres des zéros de f dans D_a à laquelle on soustrait la somme des ordres des pôles de f dans D_a. Or, par le point précédent, la somme des résidus de g aux pôles de f dans D_a est égale à 0, donc le nombre de zéros de f dans D_a est égal au nombre de pôles de f dans D_a (comptés avec multiplicité).

∗ On considère la fonction $g : z \longmapsto z\dfrac{f'(z)}{f(z)}$ définie sur $\mathbb{C}$ privé des points où f s'annule ou a un pôle.
De même qu'au premier point, on a par le théorème des résidus que :

$$\frac{1}{2i\pi}\int_{C_a} z\frac{f'(z)}{f(z)}\mathrm{d}z = \sum_{i=1}^{r}\mathrm{Res}(g, z_i) = \sum_{i=1}^{r} z_i$$

avec les z_i qui sont les zéros et pôles de f comptés avec multiplicité.
De plus, on a par périodicité de f que :

$$\begin{aligned}\frac{1}{2i\pi}\left(\int_{[a;a+\omega_1]} z\frac{f'(z)}{f(z)}\mathrm{d}z - \int_{[a+\omega_2;a+\omega_1+\omega_2]} z\frac{f'(z)}{f(z)}\mathrm{d}z\right) &= \frac{1}{2i\pi}\int_a^{a+\omega_1}(z-(z-\omega_2))\frac{f'(z)}{f(z)}\mathrm{d}z \\ &= \frac{-\omega_2}{2i\pi}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}\mathrm{d}z\end{aligned}$$

En posant $u = f(z)$ et puisque f est ω_1-périodique, lorsque z parcourt $[a; a+\omega_1]$, u suit un contour fermé $C_{f,a}$ passant par $f(a)$, d'où :

$$\frac{1}{2i\pi}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}\mathrm{d}z = \int_{C_{f,a}}\frac{\mathrm{d}u}{u} = \mathrm{Ind}_{C_{f,a}}(0)$$

Ainsi, la différence des intégrales ci-dessus est égal à $-\omega_2\,\mathrm{Ind}_{C_{f,a}}(0)$ et on a la même chose avec les deux autres côtés de C_a, ce qui prouve le troisième point.

∗ Supposons que f est non constante et raisonnons par l'absurde en supposant que l'ordre de f est inférieur ou égal à 1 :
- Supposons tout d'abord que f soit d'ordre 1.
  f possède alors un unique pôle qui est simple (par le deuxième point). De plus, par le premier point, le résidu de f en ce pôle est égal à 0, ce qui est une contradiction car on obtient que l'ordre de f est nul.
- Désormais, si f est d'ordre 0, alors f n'a pas de pôles dans le domaine fondamental $\mathcal{D}_a$ et donc f n'a pas de pôles dans $\mathbb{C}$. Ainsi, f est une fonction entière et bornée sur $\mathbb{C}$ (puisqu'elle est continue sur le domaine fondamental $\mathcal{D}_a$ qui est compact). Par le théorème de Liouville, on en déduit que f est constante, ce qui est contradictoire avec l'hypothèse de départ.
  Finalement, pour f non constante, on a donc un ordre supérieur ou égal à 2.

■

Proposition 2 :

∗ Une fonction elliptique holomorphe (c'est-à-dire sans pôles) est constante.

∗ Une fonction elliptique avec aucun zéro est constante.

Preuve :

∗ Soit f une fonction elliptique holomorphe.
La fonction f n'a donc aucun pôle sur $\mathbb{C}$ et donc f est bornée sur $\mathbb{C}$ car elle l'est sur le domaine fondamental D_a qui est compact. Ainsi, par le théorème de Liouville, f est une fonction constante.

∗ Soit f une fonction elliptique avec aucun zéro.
Par le deuxième point de la proposition 1, f n'a alors aucun pôle sur $\mathbb{C}$ donc elle est holomorphe sur $\mathbb{C}$ et on a le résultat par le point précédent.

■

Remarque :
Pour alléger les notations, nous noterons désormais L le réseau $L(\omega_1, \omega_2)$.

II.1.2 La fonction $\wp$ de Weierstrass

Construisons désormais une fonction elliptique fondamentale à partir de laquelle les autres fonctions elliptiques pourront facilement s'en déduire.

Définition 4 : Fonction $\wp$ de Weierstrass :
On appelle **fonction $\wp$ de Weierstrass** la fonction définie par :

$$\forall z \in \mathbb{C}\backslash L,\ \wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Nous allons montrer ci-dessous que cette fonction est bien définie et que c'est une fonction elliptique. Commençons par les deux lemmes suivants qui nous serons utiles dans le théorème 3 :

Lemme 1 :
Soit $z = x + iy \in \mathbb{C}$.
Pour tous entiers naturels m et n, on a :

$$\frac{y^2}{x^2+y^2+1} \leq \frac{|mz+n|^2}{m^2+n^2} \leq x^2+y^2+1.$$

Preuve :
Soient $z = x + iy \in \mathbb{C}$ et $m, n \in \mathbb{N}$.

* La première inégalité est équivalente à :

$$\left((mx+n)^2 + m^2y^2\right)\left(x^2+y^2+1\right) - \left(m^2+n^2\right)y^2 \geq 0$$

Or, on remarque que le membre de gauche est égal à $(mx+n)^2 + \left(m\left(x^2+y^2\right)+nx\right)^2$ (qui est bien positif ou nul !), donc la première inégalité est vérifiée.

* De même, la deuxième inégalité est équivalente à :

$$\left(x^2+y^2+1\right)\left(m^2+n^2\right) - \left((mx+n)^2 + m^2y^2\right) \geq 0$$

Or, on remarque que le membre de gauche est égal à $(nx-m)^2 + n^2y^2$ (qui est bien positif ou nul !), donc la deuxième inégalité est également vérifiée.

■

Lemme 2 :
Soit $s \in \mathbb{C}$.
Si $\mathrm{Re}(s) > 2$, alors la série $\displaystyle\sum_{\omega \in L\backslash\{0\}} \frac{1}{\omega^s}$ converge absolument.

Preuve :
Soit $s \in \mathbb{C}$.
Puisque pour tout $\omega \in L(\omega_1, \omega_2)$ on a $||\omega|^{-s}| = |\omega|^{-\operatorname{Re}(s)}$, il suffit de se limiter au cas où s est réel.

Notons $z = \dfrac{\omega_1}{\omega_2} = x + iy \in \mathbb{C}$.
Par hypothèse sur $\dfrac{\omega_1}{\omega_2}$ on a $y \neq 0$ et par le lemme 1, on a :

$$|m\omega_1 + n\omega_2|^2 = |\omega_2|^2 |mz + n|^2 \geq A\left(m^2 + n^2\right) \geq A|m||n| \quad (\text{car } m^2 - |mn| + n^2 \geq 0)$$

où $A = |\omega_2|^2 \dfrac{y^2}{x^2 + y^2 + 1} > 0$. Ainsi :

$$\sum_{\omega \in L\setminus\{0\}} \frac{1}{|\omega|^s} \leq A^{-\frac{s}{2}} \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{|m^2+n^2|^{\frac{s}{2}}} \leq A^{-\frac{s}{2}} \left(\sum_{n\in\mathbb{Z}^*} \frac{1}{n^s} + \sum_{m\in\mathbb{Z}^*} \frac{1}{m^s} + \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(|m||n|)^{\frac{s}{2}}} \right)$$

Or la série $\displaystyle\sum_{m\in\mathbb{Z}^*} \frac{1}{m^s}$ converge pour $s > 1$ et la somme double ci-dessus est le carré de la série de Riemann $\displaystyle\sum_{m\in\mathbb{Z}^*} \frac{1}{|m|^{\frac{s}{2}}}$ qui converge pour $s > 2$.

Finalement, on en déduit que pour $\operatorname{Re}(s) > 2$, la série $\displaystyle\sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^s}$ converge absolument.

■

Le théorème suivant résume les propriétés basiques de la fonction $\wp$:

Théorème 3 :

- La fonction $\wp$ est une fonction elliptique paire d'ordre 2 avec des pôles en L d'ordre 2.
- Le développement en série de Laurent au voisinage de 0 est donné par :

$$\wp(z, L) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1) G_{2n+2}(L) z^{2n}, \text{ avec } G_k(L) = \sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^k}. \tag{1.5}$$

- La fonction $\wp$ satisfait l'équation différentielle $(y')^2 = 4y^3 - g_4(L)y - g_6(L)$ (avec $g_4(L) = 60G_4(L)$ et $g_6(L) = 140G_6(L)$).

Preuve :

- Montrons les différentes propriétés de $\wp$:
  - Montrons tout d'abord que $\wp$ est bien définie :
    À $z \in \mathbb{C}\setminus L$ fixé, on a par la deuxième inégalité triangulaire que $|z - \omega| \geq |\omega| - |z|$ et puisque L est discret, il n'y a qu'un nombre fini d'éléments $\omega \in L$ tels que $|\omega| \leq 2|z|$. Or, on peut exclure ce nombre fini de cas (ce qui ne change donc pas la nature de la série définissant $\wp$) et supposer que $|\omega| \geq 2|z|$ (c'est-à-dire que $|\omega| - |z| \geq |\omega| - \dfrac{|\omega|}{2} = \dfrac{|\omega|}{2}$). Ainsi :

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{\omega^2 - (z-\omega)^2}{\omega^2(z-\omega)^2}\right| = |z| \frac{|2\omega - z|}{|\omega|^2 |z-\omega|^2} \leq |z| \frac{2|\omega| + |z|}{|\omega|^2 \times \frac{|\omega|^2}{4}} \leq |z| \frac{\frac{5}{2}|\omega|}{\frac{|\omega|^4}{4}} \leq 10|z| \times \frac{1}{|\omega|^3}$$

    Ainsi, par le lemme 2, on en déduit que la série définissant $\wp$ converge absolument et même uniformément sur tout compact de $\mathbb{C}\setminus L$ et donc $\wp$ est bien définie et méromorphe.

— La fonction $\wp$ a clairement des pôles d'ordre 2 en les points de L de par sa définition.
— La fonction $\wp$ est une fonction paire. En effet, pour tout $z \in \mathbb{C}\setminus L$, on a :

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

— Par converge uniforme, on a pour tout $z \in \mathbb{C}\setminus L$:

$$\wp'(z,L) = -2\left(\frac{1}{z^3} + \sum_{\omega\in L\setminus\{0\}} \frac{1}{(z-\omega)^3}\right) = -2\sum_{\omega\in L} \frac{1}{(z-\omega)^3}$$

La fonction $\wp'$ est donc doublement périodique et méromorphe sur $\mathbb{C}\setminus L$, donc est une fonction elliptique.
Ainsi, pour tout $\omega \in L$, la fonction f_ω définie sur $\mathbb{C}\setminus L$ par $f_\omega(z) = \wp(z+\omega,L) - \wp(z,L)$ est de dérivée nulle et puisque $\mathbb{C}\setminus L$ est connexe, elle est constante.
Or, on sait que $\wp$ est une fonction paire et doublement périodique de période ω_1 et ω_2, donc en appliquant ce qui précède à f_{ω_1} et f_{ω_2}, on obtient pour $i \in \{1;2\}$ et en $z = -\dfrac{\omega_i}{2}$ que :

$$\wp(z+\omega_i,L) - \wp(z,L) = \wp\left(\frac{\omega_i}{2}\right) - \wp(-\frac{\omega_i}{2},L) = 0$$

Ainsi, $f_{\omega_1} = f_{\omega_2} = 0$ et donc $\wp$ est une fonction doublement périodique.

∗ Pour tout $\omega \in L\setminus\{0\}$ et tout $z \in \mathbb{C}\setminus L$ dans un voisinage de 0, on a :

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2}\frac{1}{\left(1-\frac{z}{\omega}\right)^2} = \frac{1}{\omega^2}\sum_{n=0}^{+\infty}(n+1)\left(\frac{z}{\omega}\right)^n = \sum_{n=0}^{+\infty}(n+1)\frac{z^n}{\omega^{n+2}}$$

Enfin, par convergence uniforme, on peut intervertir les ordres de sommation et on obtient sur un voisinage de 0 :

$$\wp(z,L) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(\left(\sum_{n=0}^{+\infty}(n+1)\frac{z^n}{\omega^{n+2}}\right) - \frac{1}{\omega^2}\right)$$
$$= \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(\sum_{n=1}^{+\infty}(n+1)\frac{z^n}{\omega^{n+2}}\right) = \frac{1}{z^2} + \sum_{n=0}^{+\infty}(n+1)z^n\left(\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^{n+2}}\right)$$
$$= \frac{1}{z^2} + \sum_{n=0}^{+\infty}(n+1)G_{n+2}(L)z^n$$

∗ Posons $g_4(L) = 60G_4(L)$ et $g_6(L) = 140G_6(L)$ et considérons également la fonction f définie sur $\mathbb{C}\setminus L$ par $f(z) = \left(\wp'(z,L)\right)^2 - \left(4\wp(z,L)^3 - g_4(L)\wp(z,L) - g_6(L)\right)$.
En utilisant le développement de Laurent trouvé au point précédent, on obtient que la fonction f est holomorphe et s'annule en $z = 0$ (en effet, les développements en série de Laurent de $\left(\wp'(z,L)\right)^2$ et $4\wp(z,L)^3 - g_4(L)\wp(z,L) - g_6(L)$ se compensent lorsque l'on regarde leur différence, de sorte que l'on obtient un développement en série entière dont le terme constant est nul).
De plus, la fonction f est une fonction elliptique puisque $\wp$ et $\wp'$ le sont et donc f s'annule sur L (car s'annule en 0). Enfin, les possibles pôles de f proviennent de ceux de $\wp$ et $\wp'$, c'est à dire que les possibles pôles sont les éléments de L et puisque f s'annule sur L on en conclut que f n'admet pas de pôle. Ainsi, f est une fonction entière et elle est bornée sur $\mathbb{C}$ (car elle l'est sur un domaine fondamental compact) donc par le théorème de Liouville elle est constante. Enfin on a $f = 0$ car f est nulle en 0.

■

Remarque :
En remplaçant f par $f - z$ pour tout $z \in \mathbb{C}$, on remarque que l'ordre de f et de $z \longmapsto f(z) - z$ est le même et donc f prend chaque valeur le même nombre de fois (compté avec multiplicité). En particulier, la fonction $\wp$ prend chaque valeur 2 fois sur un domaine fondamental.

Proposition 3 :

* La fonction $\wp$ satisfait l'équation différentielle $y'' = 6y^2 - \frac{1}{2}g_4(L)$.
* Pour tout entier pair $k \geq 8$, on a :

$$\frac{(k-6)(k-1)(k+1)}{6}G_k = \sum_{\substack{4 \leq j \leq k-4 \\ j \text{ pair}}} (j-1)(k-1-j)G_j G_{k-j}. \tag{1.6}$$

* En particulier, on a les relations explicites suivantes :

$$G_8 = \frac{3}{7}G_4^2,\ G_{10} = \frac{5}{11}G_4 G_6 \text{ et } G_{12} = \frac{18G_4^3 + 25G_6^2}{143}.$$

Preuve :

* On sait que la fonction $\wp$ est méromorphe sur $\mathbb{C}\setminus L$, on peut donc dériver la fonction $\wp$ deux fois et en reprenant l'équation différentielle vérifiée par $\wp$ dans le dernier point du théorème 3, on a :

$$2\wp''\wp' = 12\wp'\wp^2 - g_4(L)\wp'$$

  Et puisque $\wp'$ est non nulle, on obtient que $\wp$ est solution de l'équation différentielle $y'' = 6y^2 - \frac{1}{2}g_4(L)$.

* Afin d'obtenir la formule (1.6), il suffit de calculer les développement en série de Laurent de $\wp''$ et $6\wp^2 - \frac{1}{2}g_4(L)$ et d'identifier les coefficients.

* Reprenons l'égalité du point précédent avec quelques cas particuliers :
  — Pour $k = 8$, on obtient que :

$$\frac{(8-6)(8-1)(8+1)}{6}G_8 = (4-1)(8-1-4)G_4^2$$

  Soit $G_8 = \frac{6 \times 3 \times 3}{2 \times 7 \times 9}G_4^2 = \frac{3}{7}G_4^2$.
  — Pour $k = 10$, on a :

$$\frac{(10-6)(10-1)(10+1)}{6}G_{10} = (4-1)(10-1-4)G_4 G_6 + (6-1)(10-1-6)G_6 G_4$$

  Soit $G_{10} = \frac{30 \times 6}{4 \times 9 \times 11}G_4 G_6 = \frac{5}{11}$.
  — Finalement, on a de même pour $k = 12$:

$$\frac{(12-6)(12-1)(12+1)}{6}G_{12} = 42G_4 G_8 + 25G_6^2$$

  Soit, en utilisant la relation précédente entre G_4 et G_8 : $G_{12} = \frac{42 \times \frac{3}{7}G_4^3 + 26G_6^2}{143} = \frac{18G_4^2 + 25G_6^2}{143}$.

■

Corollaire 2 :

Posons $\omega_3 = \omega_1 + \omega_2$ et pour tout $i \in \{1;2;3\}$, $e_i = \wp\left(\frac{\omega_i}{2}, L\right)$.

* On a :
$$4X^3 - g_4(L)X - g_6(L) = 4\prod_{i=1}^{3}(X - e_i).$$
En particulier, les e_i sont les racines du polynôme $4X^3 - g_4(L)X - g_6(L)$ et elles sont distinctes.
* Pour $z_0 \notin L$, la fonction f définie sur $\mathbb{C}\setminus L$ par $f(z) = \wp(z, L) - \wp(z_0, L)$ possède exactement deux zéros en $z = \pm z_0$ (modulo l'addition par un élément de L) sauf lorsque $2z_0 \in L$, auquel cas on a un zéro double en $z = z_0$.

Preuve :

Posons $\omega_3 = \omega_1 + \omega_2$ et pour tout $i \in \{1;2;3\}$, $e_i = \wp\left(\frac{\omega_i}{2}, L\right)$.

* On sait que $\wp'$ est une fonction elliptique qui est de plus impaire (par la preuve du théorème 3). Ainsi, puisque $\frac{\omega_i}{2} \notin L$ et $\omega_i \in L$, on a :
$$\forall i \in \{1;2;3\},\ \wp'\left(\frac{\omega_i}{2}, L\right) = \wp'\left(-\frac{\omega_i}{2}, L\right) = -\wp'\left(\frac{\omega_i}{2}, L\right)$$
Donc pour tout $i \in \{1;2;3\}$, $\wp'\left(\frac{\omega_i}{2}, L\right) = 0$ et par l'équation différentielle vérifiée par $\wp$ dans le dernier point du théorème 3, on obtient que les e_i sont racines du polynôme $P = 4X^3 - g_4(L)X - g_6(L)$. Or, puisque $\deg(P) = 3$, on en déduit que se sont les seules et on a alors :
$$4X^3 - g_4(L)X - g_6(L) = 4\prod_{i=1}^{3}(X - e_i)$$
Enfin, pour $i \in \{1;2;3\}$, la fonction $z \longmapsto \wp(z, L) - e_i$ est une fonction elliptique d'ordre 2 et dont les deux zéros dans un parallélogramme fondamental sont $\pm\frac{\omega_i}{2}$ (car elle est paire). Ainsi, pour $j \neq i$, on a $e_j \neq e_i$, d'où les e_i tous distincts.

* Soit $z_0 \notin L$.
La fonction f définie sur $\mathbb{C}\setminus L$ par $f(z) = \wp(z, L) - \wp(z_0, L)$ est une fonction elliptique paire d'ordre 2 et il est clair que z_0 et $-z_0$ sont des zéros de f.
Ainsi, lorsque z_0 et $-z_0$ sont distincts (modulo l'addition par un élément de L), on a par la proposition 1 que se sont les seules racines de f (modulo l'addition par un élément de L) et que leur multiplicité est égale à 1.
Enfin, lorsque z_0 et $-z_0$ sont égaux modulo l'addition par un élément de L, on a que $2z_0 \in L$, c'est-à-dire que $z_0 = \frac{\omega_i}{2}$ modulo l'addition par un élément de L pour un certain i dans $\{1;2;3\}$ (puisque l'on a supposé que $z_0 \notin L$). On est alors ramené à la situation du premier point avec une racine double.

■

Remarque :

En particulier, on en déduit que le discriminant $D(L) = g_4^3(L) - 27g_6(L)^2$ est non nul puisque les racines de $4X^3 - g_4(L)X - g_6(L)$ sont distinctes.

Proposition 4 :

Toute fonction elliptique est une fonction rationnelle en $\wp$ et $\wp'$.
En d'autres termes, le corps des fonctions elliptiques est isomorphe à $\mathbb{C}[X,Y]/(Y^2 - (4X^3 - g_4(L)X - g_6(L)))$ (avec (X, Y) qui correspond à $(\wp, \wp')$).

Preuve :
Soit f une fonction elliptique.
Pour tout $z \in \mathbb{C} \setminus L$, il est possible d'écrire $f(z)$ sous la forme :

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

Ainsi f est une somme d'une fonction paire et d'une fonction impaire et qui sont toutes les deux elliptiques.
Or, on sait que $\wp$ est une fonction elliptique paire (par le théorème 3) et $\wp'$ est une fonction elliptique impaire (même technique que pour $\wp$), donc si f est une fonction elliptique impaire alors la fonction $\frac{f}{\wp'}$ est une fonction elliptique paire. Il suffit alors de prouver que toute fonction elliptique paire est une fonction rationnelle en $\wp$ et $\wp'$.

Supposons donc que f est une fonction elliptique paire.
Pour tout $z_0 \in \mathbb{C}$, on note $v_{z_0}(f)$ l'ordre de f en z_0 (qui est positif pour un zéro et négatif pour un pôle) et on pose :

$$w(z_0) = \begin{cases} 1 & \text{si } 2z_0 \notin L \\ 2 & \text{si } 2z_0 \in L \end{cases} .$$

Puisque f est paire, le raisonnement fait dans la preuve du corollaire précédent nous montre que $w(z_0)$ divise $v_{z_0}(f)$ (autrement dit, $v_{z_0}(f)$ est pair lorsque $2z_0 \in L$ et $z_0 \notin L$).

On introduit alors :

$$N(z) = \prod_{\substack{z_0 \text{ pôle de } f \\ z_0 \notin L}} (\wp(z, L) - \wp(z_0, L))^{\frac{v_{z_0}(f)}{w(z_0)}} \text{ et } D(z) = \prod_{\substack{z_0 \text{ pôle de } f \\ z_0 \notin L}} (\wp(z, L) - \wp(z_0, L))^{-\frac{v_{z_0}(f)}{w(z_0)}}.$$

Enfin, pour un entier a convenable (discuté plus loin dans la preuve), on pose :

$$g : \left| \begin{array}{ccc} \mathbb{C} \setminus L & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \wp(z, L)^{-a} \dfrac{N(z)}{D(z)} \end{array} \right. .$$

Montrons que pour a bien choisi, la fonction g a les mêmes zéros et pôles que f avec les mêmes multiplicités :

On a le résultat si $2z_0 \notin L$ et également si ($z_0 \notin L$ et $2z_0 \in L$) grâce aux propriétés de f et $\wp$ vues précédemment. De plus, puisque 0 est un pôle double de $\wp$, l'ordre de 0 dans $N(z)$ et $D(z)$ est pair et donc l'ordre de f en 0 est nécessairement pair (car f est une fonction paire et donc toutes les dérivées d'ordre impair de f (ou de $\frac{1}{f}$ dans le cas d'un pôle) sont nulles et ainsi la première dérivée non identiquement nulle est d'ordre pair).
On choisi alors a de telle sorte que l'ordre de g en 0 est le même que celui de f.

Finalement, la fonction $\frac{f}{g}$ est une fonction elliptique avec aucun zéro ou pôle, elle est donc constante. Il existe alors une constante $c \in \mathbb{C}$ telle que $f = cg \in \mathbb{C}(\wp, \wp')$.

■

L'ensemble de toutes les fonctions elliptiques de mêmes périodes fondamentales forme un corps commutatif. Plus précisément, étant donné un couple de périodes, toute fonction elliptique admettant ce couple de périodes peut être définie sur une certaine surface de Riemann : le tore complexe obtenu par recollement des couples de côtés opposés du parallélogramme fondamental. Les fonctions elliptiques sont alors les fonctions méromorphes sur ce tore. Par ailleurs, la fonction de Weierstrass associée à ce couple de périodes et sa dérivée paramètrent une certaine courbe complexe : une **courbe elliptique sur** $\mathbb{C}$.

II.2 Courbes elliptiques sur $\mathbb{C}$

Les courbes elliptiques sont intimement liées aux fonctions elliptiques. Elles sont également liées aux formes modulaires directement depuis leurs définitions quand elles sont considérées sur $\mathbb{C}$ (puis d'une manière plus profonde via leurs paramétrisation modulaire (dont l'existence a été conjecturée par Shimura-Taniyama-Weil et prouvée par André Weil et ses successeurs lorsqu'elles sont définies sur $\mathbb{Q}$)).

Si L est un réseau sur $\mathbb{C}$, alors le groupe quotient $\mathbb{C}/L$ a une topologie naturelle qui lui donne une structure de groupe de Lie compact, connexe et de dimension 1 sur $\mathbb{C}$. Topologiquement, ce groupe est alors un tore et donc en particulier il est de genre 1. Par définition, c'est une courbe elliptique sur $\mathbb{C}$ (et on peut montrer que réciproquement, tout groupe de Lie de ce type est de la forme $\mathbb{C}/L$ pour L un réseau de $\mathbb{C}$).

Proposition 5 :
L'application :

$$\Psi : \left| \begin{array}{ccc} \mathbb{C}/L & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ z & \longmapsto & \begin{cases} (\wp(z,L) : \wp'(z,L) : 1) & \text{si } z \notin L \\ (0:1:0) & \text{si } z \in L \end{cases} \end{array} \right.$$

est un isomorphisme de $\mathbb{C}/L$ vers la courbe algébrique projective dont l'équation affine est donnée par la formule $Y^2 = 4X^3 - g_4(L)X - g_6(L)$.

Preuve :

* Par le troisième point du théorème 3, on a que l'image de Ψ est bien contenue dans la courbe algébrique projective donc l'équation affine est $Y^2 = 4X^3 - g_4(L)X - g_6(L)$.

* Montrons que Ψ est surjective :
  Soit (x, y) un point appartenant à la courbe algébrique projective donc l'équation affine est donnée par $Y^2 = 4X^3 - g_4(L)X - g_6(L)$.
  La fonction $z \longmapsto \wp(z, L) - x$ est alors une fonction elliptique non constante, donc par la contraposée du deuxième point de la proposition 2, elle possède un zéro (disons en $z = a$). Il suit donc que $\wp'(a)^2 = y^2$ et en remplaçant a par $-a$ si nécessaire, on obtient que $\wp'(a) = y$. D'où $\Psi(a) = (x, y)$.

* Montrons que Ψ est injective :
  Soient $z_1, z_2 \in \mathbb{C}/L$ tels que $\Psi(z_1) = \Psi(z_2)$.
  Supposons tout d'abord que $2z_1 \notin L$.
  La fonction $z \longmapsto \wp(z, L) - \wp(z_1, L)$ est alors une fonction elliptique d'ordre 2 qui s'annule en z_1, $-z_1$ et z_2. Ainsi, deux de ces valeurs sont égales modulo l'addition par un élément de L et puisque l'on a supposé que $2z_1 \notin L$, on a alors $z_2 = \pm z_1$ (modulo d'addition par un élément de L). Finalement :

  $$\wp'(z_1, L) = \wp'(z_2, L) = \wp'(\pm z_1, L) = \pm\wp'(z_1, L)$$

  donne que z_2 est égal à z_1 modulo l'addition par un élément de L (notons que $\wp'(z_1, L) \neq 0$ d'après la preuve du corollaire 2).

  De même, si $2z_1 \in L$, alors $z \longmapsto \wp(z, L) - \wp(z_1, L)$ a une racine double en z_1 et s'annule aussi en z_2 et on conclut comme précédemment que z_2 est égal à z_1 modulo l'addition par un élément de L. Finalement, Ψ est bien injective.

■

Remarque :
Nous avons montré que l'application Ψ du théorème précédent est un isomorphisme de groupes mais en réalité, on a même un isomorphisme complexe analytique de groupes de Lie complexes (c'est-à-dire un isomorphisme de surfaces de Riemann qui est aussi un isomorphisme de groupes).

Une conséquence importante de cette proposition est que la fonction $\wp$ vérifie une formule d'addition :

Théorème 4 :
Soient $z_1, z_2 \in \mathbb{C}\backslash L$.
Si l'on pose :

$$a = \begin{cases} \dfrac{\wp'(z_2,L)-\wp'(z_1,L)}{\wp(z_2,L)-\wp(z_1,L)} & \text{si } z_2 \not\equiv z_1 \pmod{L} \\ \dfrac{\wp''(z_1,L)}{\wp'(z_1,L)} = \dfrac{6\wp^2(z_1,L)-\frac{g_4(L)}{2}}{\wp'(z_1,L)} & \text{si } z_2 \equiv z_1 \pmod{L} \end{cases}$$

alors on a les formules d'addition suivantes :

$$\wp(z_1+z_2,L) = \frac{a^2}{4} - \wp(z_1,L) - \wp(z_2,L) \text{ et } \wp'(z_1+z_2,L) = a(\wp(z_1,L)-\wp(z_1+z_2,L)) - \wp'(z_1,L)$$

Preuve :
Puisque $\mathbb{C}/L$ a une structure naturelle de groupe abélien, nous devons voir comment cette structure est envoyée sur une structure de groupes sur les paires $(\wp(z,L), \wp'(z,L))$ via l'isomorphisme de la proposition 5.

- Supposons tout d'abord que z_1 n'est pas égal à z_2 modulo l'addition par un élément de L.
  Si $\wp(z_2,L) = \wp(z_1,L)$, alors on sait que $\wp'(z_2,L) = -\wp'(z_1,L)$ et $z_1+z_2 \in L$. Donc les deux formes d'addition sont correctes puisque chaque terme de part et d'autre des égalités sont infinis.
  Si $\wp(z_2,L) \neq \wp(z_1,L)$, alors on peut trouver des nombres complexes a et b tels que :

  $$\wp'(z_1,L) = a\wp(z_1,L) + b \text{ et } \wp'(z_2,L) = a\wp(z_2,L) + b$$

  (une interprétation géométrique est que $y = ax + b$ est la droite passant par les points (affines) $(\wp(z_1,L), \wp'(z_1,L))$ et $(\wp(z_2,L), \wp'(z_2,L))$ sur la courbe elliptique $\mathbb{C}/L$).
  La fonction $\varphi : z \longmapsto \wp'(z,L) - (a\wp(z,L)+b)$ est une fonction elliptique ayant un pôle d'ordre exactement 3 (grâce à la définition de $\wp'$) et donc possède 3 zéros comptés avec multiplicité (par la proposition 1). Puisque l'on sait déjà que z_1 et z_2 sont deux zéros de φ, il existe un unique troisième zéro z_3 (possiblement égal à z_1 ou z_2) qui est racine de φ. De plus, par le troisième point de la proposition 1, on a $z_1+z_2+z_3 \in L$.
  Ainsi, $\wp'(z_3,L) = a\wp(z_3,L) + b$ et grâce à l'équation différentielle vérifiée par $\wp$, on a que :

  $$4X^3 - g_4(L)X - g_6(L) - (aX+b)^2 = 0$$

  a pour racines $\wp(z_i,L)$ pour $i \in \{1;2;3\}$ (comptés avec multiplicité). Ainsi, en écrivant :

  $$4X^3 - g_4(L)X - g_6(L) - (aX+b)^2 = 4(X-\wp(z_1,L))(X-\wp(z_2,L))(X-\wp(z_3,L))$$

  et en comparant le coefficient devant x^2, on a :

  $$\wp(z_1,L) + \wp(z_2,L) + \wp(z_3,L) = \frac{a^2}{4}.$$

  Si l'on décide de résoudre le système linéaire en a et b, on a :

  $$a = \frac{\wp'(z_2,L)-\wp'(z_1,L)}{\wp(z_2,L)-\wp(z_1,L)}$$

  et par parité, $\wp(z_3,L) = \wp(-z_1-z_2,L) = \wp(z_1+z_2,L)$. On a alors que :

  $$\wp(z_1+z_2,L) = \frac{a^2}{4} - \wp(z_1,L) - \wp(z_2,L)$$

  Enfin, pour $\wp'(z_1+z_2,L)$, on remarque que $b = \wp'(z_1,L) - a\wp(z_1,L)$ et ainsi :

  $$\wp'(z_3,L) = a\wp(z_3,L) + b = a(\wp(z_3,L)-\wp(z_1,L)) + \wp'(z_1,L).$$

  Or, puisque $\wp'$ est une fonction impaire, on a :

  $$\wp'(z_1+z_2,L) = -\wp'(z_3,L) = a(\wp(z_1,L)-\wp(z_3,L)) - \wp'(z_1,L) = a(\wp(z_1,L)-\wp(z_1+z_2,L)) - \wp'(z_1,L).$$

* Finalement, le cas où $z_1 = z_2$ modulo l'addition par un élément de L suit du premier point en faisant tendre z_2 vers z_1 et en utilisant l'équation différentielle vérifiée par $\wp$ dans le premier point de la proposition 3.

■

Remarque :
On redémontre ici en fait la loi de groupe sur des courbes elliptiques.

Revenons à nos courbes elliptiques :
On remarque que le discriminant du polynôme $4X^3 - g_4(L)X - g_6(L)$ est égal à

$$D(L) = g_4^3(L) - 27g_6^2(L)$$

Puisque la courbe $F(X,Y) = 0$ (avec $F(X,Y) = Y^2 - (4X^3 - g_4(L)X - g_6(L))$) est isomorphe à $\mathbb{C}/L$ (par le théorème 4), on en déduit qu'elle est non singulière (c'est-à-dire les dérivées partielles de F par rapport à X et Y ne s'annulent pas simultanément, ou encore que le polynôme $4X^3 - g_4(L)X - g_6(L)$ ne possède pas de racines multiples). Ainsi, $D(L)$ est non nul.
Or, on peut dire d'avantage. En effet, se donner un élément z de $\mathcal{H}$ nous permet de créer un réseau $L(1,z)$ de $\mathbb{Z}$-base $(1,z)$ et donc un quotient $\mathbb{C}/L(1,z)$. Or par la proposition 5, cela nous donne une courbe elliptique E_z à laquelle on peut associer un discriminant $D(z)$. Ainsi, par le paragraphe précédent, on en déduit que la fonction $z \longmapsto D(z)$ ne s'annule jamais sur $\mathcal{H}$.

Enfin, posons $j(L) = (2\pi)^{12}\dfrac{1728g_4^3(L)}{D(L)}$ (bien définie car $D(L)$ ne s'annule jamais).
Lorsque L est changé en un réseau λL via une homothétie (on parle alors de **réseaux homothétiques**), on a que $j(L)$ reste inchangé par homogénéité, donc la fonction $z \longmapsto j(z)$ (définie de la même manière que pour $\Delta(z)$) est invariante sous l'action de Γ :

$$\forall z \in \mathcal{H},\ \forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ j\left(\frac{az+b}{cz+d}\right) = j(z)$$

Comme les réseaux homothétiques correspondent à des courbes elliptiques isomorphes $\mathbb{C}/L$ et $\mathbb{C}/\lambda L$, cela signifie que $j(z)$ dépend uniquement de la classe d'isomorphisme de la courbe elliptique $\mathbb{C}/L$. Réciproquement, on peut montrer que si deux courbes elliptiques ont le même $j(z)$ (appelé **invariant modulaire**), alors elles sont isomorphes sur $\mathbb{C}$.
En effet, soient E et E' deux courbes elliptiques avec le même invariant modulaire j d'équations respectives :

$$E : y^2 = 4x^3 + Ax + B \text{ et } E' : \widetilde{y}^2 = 4\widetilde{x}^3 + A'\widetilde{x} + B'$$

Le fait que $j(E) = j'(E)$ donne :

$$\frac{A^3}{D(E)} = \frac{A'^3}{D(E')}$$

soit :

$$\frac{A^3}{A^3 - 27B^2} = \frac{A'^3}{A'^3 - 27B'^2}.$$

On a donc $A^3B'^2 = A'^3B^2$ et on cherche un isomorphisme de la forme $(x,y) \longmapsto \left(u^2x', u^3y'\right)$ en considérant trois cas :

* Si $A = 0$ (soit $j(E) = 0$), alors $B \neq 0$ puisque $D(E) \neq 0$ et donc $A' = 0$. On obtient alors l'isomorphisme voulu en posant $u = \left(\dfrac{B}{B'}\right)^{\frac{1}{6}}$.

* Si $B = 0$ (soit $j(E) = 1728$), alors $A \neq 0$ puisque $D(E) \neq 0$ et donc $A' = 0$. On obtient alors l'isomorphisme voulu en posant $u = \left(\dfrac{A}{A'}\right)^{\frac{1}{4}}$.

∗ Si $AB \neq 0$ (soit $j(E) \neq 0$ ou 1728), alors $A'B' \neq 0$ (puisque si l'un des deux est nul alors les deux seraient nuls et cela contredirait le fait que $D(E') \neq 0$). On obtient alors l'isomorphisme voulu en posant $u = \left(\frac{A}{A'}\right)^{\frac{1}{4}} = \left(\frac{B}{B'}\right)^{\frac{1}{6}}$.

Chapitre 2

Formes modulaires de niveau 1

Dans ce deuxième chapitre, nous allons commencer par définir les notions essentielles (fonction faiblement modulaire, fonction modulaire, forme modulaire, etc.) ainsi que les premières propriétés. Nous continuerons ensuite avec le lien entre les fonctions de réseaux et les fonctions modulaires avant de passer à des exemples de formes modulaires de niveau 1 via les séries d'Eisenstein et la forme parabolique Δ (appelée **discriminant**). Nous donnerons ensuite des exemples de q-développements qui nous permettrons par exemple de voir si une forme modulaire est parabolique ou non avant de finir ce chapitre par un résultat important qui est le théorème de structure des formes modulaires de niveau 1 ainsi qu'une dernière partie consacrée à la base de Miller.

I Définitions

Le but de cette première partie est de donner le vocabulaire de base nécessaire à l'introduction des formes modulaires.

Définition 1 : Fonction faiblement modulaire de poids k (et de niveau 1) :
On considère k un entier relatif.
On appelle **fonction faiblement modulaire de poids** k (de niveau 1) toute fonction f méromorphe sur le demi-plan $\mathcal{H}$ quelle que :

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right). \tag{2.1}$$

Exemple 1 :

- Les fonctions constantes sont faiblement modulaires et de poids 0 (et de niveau 1).
- La somme de deux fonctions faiblement modulaires de même poids k (et de niveau 1) est une fonction faiblement modulaire de poids k (et de niveau 1).
- Si f est g sont deux fonctions faiblement modulaires de poids respectifs k et ℓ (et de niveau 1), alors fg est une fonction faiblement modulaire de poids $k+\ell$ (et de niveau 1).
  En effet, on sait déjà que le produit fg est une fonction méromorphe sur le demi-plan supérieur $\mathcal{H}$ et de plus :

$$\begin{aligned} \forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ (fg)(z) &= f(z)g(z) \\ &= (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-\ell} g\left(\frac{az+b}{cz+d}\right) \\ &= (cz+d)^{-(k+\ell)}(fg)\left(\frac{az+b}{cz+d}\right) \end{aligned}$$

* Si f est une fonction faiblement modulaire de poids k (et de niveau 1) et qui ne s'annule pas, alors $\frac{1}{f}$ est une fonction faiblement modulaire de poids $-k$ (et de niveau 1).
  En effet, puisque f est méromorphe sur le demi-plan supérieur $\mathcal{H}$, il en est de même de $\frac{1}{f}$. De plus, on a la relation :

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ \left(\frac{1}{f}\right)(z) = \frac{1}{f(z)} = \frac{1}{(cz+d)^{-k}} \frac{1}{f\left(\frac{az+b}{cz+d}\right)} = (cz+d)^{-(-k)} \left(\frac{1}{f}\right)\left(\frac{az+b}{cz+d}\right)$$

* Il n'y a pas de fonction faiblement modulaire non nulle de poids impair (et de niveau 1).
  En effet, si l'on considère f une fonction faiblement modulaire de poids k impair (et de niveau 1), alors d'après la relation (2.1) appliquée avec la matrice $g = -I_2 \in \mathrm{SL}_2(\mathbb{Z})$ on a :

$$\forall z \in \mathcal{H},\ f(z) = (0 \times z - 1)^k f\left(\frac{-1 \times z + 0}{0 \times z - 1}\right) = (-1)^k f(z) = -f(z)$$

  Donc f est la fonction nulle.

Remarque :
Il ne paraît pas évident qu'il existe des fonctions faiblement modulaires pour tout poids pair $k \geq 2$ (mais c'est pourtant le cas comme on le verra par la suite !). Ceci explique que certains auteurs parlent directement de fonction faiblement modulaire de poids $2k$ (et de niveau 1).

Lorsque k est pair, la relation (2.1) a une interprétation plus conceptuelle. En effet, puisque le déterminant de g (vu comme élément de G) est égal à 1, on a :

$$\forall z \in \mathcal{H},\ \left(\frac{\mathrm{d}}{\mathrm{d}z} g.z\right)(z) = \frac{1}{(cz+d)^2}$$

Et donc on obtient :

$$\forall z \in \mathcal{H},\ f(g.z)\left(\mathrm{d}(g.z)\right)^{\frac{k}{2}} = f(z)(\mathrm{d}z)^{\frac{k}{2}}$$

Ainsi, la relation (2.1) dit simplement que la "forme différentielle de poids k" $f(z)(\mathrm{d}z)^{\frac{k}{2}}$ est fixe sous l'action de tout élément de G. Or, on sait que G est engendré par les matrices S et T (proposition 2 du chapitre 1), donc pour montrer qu'une fonction méromorphe f sur $\mathcal{H}$ est une fonction faiblement modulaire, il suffit qu'elle soit invariante par S et par T. D'où la proposition suivante :

Proposition 1 :
Soit f une fonction méromorphe sur $\mathcal{H}$.
Pour que f soit une fonction faiblement modulaire de poids k (et de niveau 1), il faut et il suffit que l'on ait les deux relations :

$$\forall z \in \mathcal{H},\ f(z+1) = f(z) \text{ et } f\left(-\frac{1}{z}\right) = z^k f(z)$$

Preuve :
Soit f une fonction méromorphe sur $\mathcal{H}$.

* Si f est une fonction faiblement modulaire de poids $k \in \mathbb{Z}$ (et de niveau 1), alors elle vérifie la relation (2.1) et donc en l'évaluant pour $g = S$ puis $g = T$ on obtient la relation voulue.

* Réciproquement, si f vérifie la relation donnée dans la proposition, alors puisque S et T engendrent le groupe modulaire on en déduit que f vérifie la relation (2.1).

■

Définition 2 : q-développement d'une fonction faiblement modulaire :
On considère une fonction faiblement modulaire f de poids k.
On appelle **q-développement de** f, lorsqu'il existe, une représentation de f de la forme :

$$\forall z \in \mathcal{H},\ f(z) = \sum_{n=m}^{+\infty} a_n e^{2i\pi nz} \text{ (avec } m \in \mathbb{Z})$$

En posant alors $q = q(z) = e^{2i\pi z}$ vu comme une fonction holomorphe sur $\mathbb{C}$ et $\dot{\mathcal{D}}$ le disque ouvert unité épointé (c'est-à-dire l'ensemble $\{z \in \mathbb{C} \mid 0 < |z| < 1\}$), on remarque que q définit une application de $\mathcal{H}$ dans $\dot{\mathcal{D}}$. En effet :

$$\forall z = x + iy \in \mathcal{H},\ |q(z)| = \left|e^{2i\pi z}\right| = e^{\mathrm{Re}(2i\pi z)} = e^{-2\pi y} < 1$$

Proposition 2 :
Soit f une fonction définie et holomorphe sur $\mathcal{H}$ et périodique de période 1.
Il existe une unique fonction F définie sur $\dot{\mathcal{D}}$ telle que $F(q(z)) = f(z)$.

Preuve :
Soit f une fonction définie et holomorphe sur $\mathcal{H}$ et périodique de période 1.

* Remarquons que l'application

$$q : \left| \begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & e^{2i\pi z} \end{array} \right.$$

est holomorphe sur $\mathcal{H}$, localement inversible et que son image $q(\mathcal{H})$ est contenue dans $\dot{\mathcal{D}}$. Il suffit donc de compléter le diagramme :

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{q} & \dot{\mathcal{D}} \\ & \searrow^{f} & \downarrow{\scriptstyle ?_F} \\ & & \mathbb{C} \end{array}$$

par une fonction holomorphe F.

* Pour construire F nous utilisons deux "cartes" recouvrant $\dot{\mathcal{D}}$ et nous construisons des inverses locaux de l'application q.
Les cartes sont :

$$\left\{ \begin{array}{ll} O_1 & = \{z \in \mathbb{C} \mid z \notin]-1; 0[\} \\ O_2 & = \{z \in \mathbb{C} \mid z \notin]0; 1[\} \end{array} \right. .$$

Dans O_1 nous choisissons pour inverse de q la fonction Ψ_1 définie par $\Psi_1(z) = \dfrac{1}{2i\pi}\log_1(z)$, avec $\log_1(z) = \log(|z|) + i\arg_1(z)$ (étant entendu que $\arg_1(z) \in]-\pi; \pi[$). De même, dans O_2 nous choisissons pour inverse de q la fonction Ψ_2 définie par $\Psi_2(z) = \dfrac{1}{2i\pi}\log_2(z)$, avec $\log_1(z) = \log(|z|) + i\arg_2(z)$ (étant entendu que $\arg_2(z) \in [0; 2\pi[$).

On voit donc que $\Psi_1 = \Psi_2$ sur $\mathcal{H} \cap \dot{\mathcal{D}}$, mais que $\Psi_2(z) = \Psi_1(z) + 1$ lorsque $\mathrm{Im}(z) < 0$. Mais puisque f est périodique et de période 1, on a :

$$\forall z \in \dot{\mathcal{D}},\ (f \circ \Psi_1)(z) = (f \circ \Psi_2)(z).$$

Donc $f \circ \Psi_1 = f \circ \Psi_2$ est la fonction F holomorphe que l'on cherchait.

■

Ainsi, si une fonction $f : \mathcal{H} \longrightarrow \mathbb{C}$ est 1-périodique, alors il existe une unique fonction $F : \dot{\mathcal{D}} \longrightarrow \mathbb{C}$ telle que pour tout $z \in \mathcal{H}$, $f(z) = F(q)$. De plus, f est une fonction holomorphe sur $\mathcal{H}$ si, et seulement si, F est une fonction holomorphe sur $\dot{\mathcal{D}}$. En effet, pour tout $z_0 \in \mathcal{H}$, l'application q induit une bijection biholomorphe entre le voisinage

ouvert $\left\{z \in \mathcal{H} \mid |\mathrm{Re}(z - z_0)| < \frac{1}{2}\right\}$ de z_0 dans $\mathcal{H}$ et le voisinage ouvert $\mathcal{D}\backslash\left\{\lambda e^{2i\pi z_0},\ \lambda \in \mathbb{R}^-\right\}$ (un inverse s'obtient alors en considérant une branche du logarithme complexe).

Ainsi, si f est holomorphe, alors il y a équivalence entre :
* $f(z)$ admet une limite quand $\mathrm{Im}(z) \to +\infty$.
* $|f(z)|$ est borné sur $\{z \in \mathcal{H} \mid \mathrm{Im}(z) > 1\}$.
* $|F(q)|$ est bornée au voisinage de $q = 0$.
* F se prolonge en une fonction holomorphe sur $\mathcal{D}$.
* F admet un développement en série entière en 0 de rayon de convergence supérieur ou égal à 1.

Par la proposition 1, toute fonction faiblement modulaire est 1-périodique donc il existe une fonction $F : \dot{\mathcal{D}} \longrightarrow \mathbb{C}$ telle que l'on ait $F \circ q = f$. Cependant, il est possible qu'elle ne soit pas prolongeable en 0 en une fonction méromorphe (respectivement holomorphe) en 0... Lorsqu'elle l'est, nous dirons que f est **méromorphe à l'infini** (respectivement **holomorphe à l'infini**). Cela signifie que F admet un développement de Laurent sur un voisinage de l'origine de la forme :

$$F(q) = \sum_{n=m}^{+\infty} a_n q^n,\ m \in \mathbb{Z}$$

Remarque :
La relation ci-dessus est aussi appelée **q-développement de f à l'infini**.

Nous pouvons maintenant aborder les notions de fonction modulaire et de forme modulaire :

Définition 3 : Fonction/forme modulaire de poids k (et de niveau 1) :
On appelle :
* **fonction modulaire de poids** k (et de niveau 1) toute fonction faiblement modulaire de poids k (et de niveau 1) qui est méromorphe à l'infini.
* **forme modulaire de poids** k (et de niveau 1) toute fonction faiblement modulaire de poids k (et de niveau 1) qui est holomorphe sur $\mathcal{H}$ et à l'infini.

Remarque :
Lorsque f est holomorphe à l'infini, on pose $f(\infty) = F(0)$: c'est la **valeur de f à l'infini**.

Ainsi, si f est une forme modulaire de poids k (et de niveau 1), alors elle est holomorphe sur $\mathcal{H}$ et donc admet un développement en série entière de la forme :

$$f(z) = \sum_{n=0}^{+\infty} a_n q^n = \sum_{n=0}^{+\infty} a_n e^{2i\pi nz} \tag{2.2}$$

qui converge pour $|q| < 1$ (c'est-à-dire $\mathrm{Im}(z) > 0$) et qui vérifie l'identité :

$$\forall z \in \mathcal{H},\ f\left(-\frac{1}{z}\right) = z^k f(z)$$

Définition 4 : Forme parabolique de poids k (et de niveau 1) :
On appelle **forme parabolique de poids** k (et de niveau 1) toute forme modulaire de poids k (et de niveau 1) qui s'annule à l'infini.

Remarques :
* En anglais on parle de *cusp-form* et en allemand de *Spitzenform*.
* Puisque $e^{2i\pi z} \underset{\mathrm{Im}(z)\to+\infty}{\longrightarrow} 0$, on a $f(\infty) = F(0) = a_0$. Ainsi une forme modulaire de poids k (et de niveau 1) est parabolique lorsque l'on a $a_0 = 0$ (ce critère peut être très pratique à utiliser car il est facile de voir si une forme modulaire est parabolique ou non une fois que l'on possède son q-développement).

Proposition 3 :
Soit $k \in \mathbb{N}$.
L'ensemble des formes modulaires de poids k (et de niveau 1) (noté M_k) est un $\mathbb{C}$-espace vectoriel et l'ensemble des formes parabolique (noté S_k) en est un sous-espace vectoriel.

Preuve :

* On a clairement que toute combinaison linéaire de fonctions faiblement modulaires de poids k (et de niveau 1) est faiblement modulaire de poids k (et de niveau 1).
  De plus, toute combinaison linéaire de fonctions holomorphes sur $\mathcal{H}$ est holomorphe sur $\mathcal{H}$, il nous reste donc à traiter le cas du point à l'infini. Or par la relation (2.2), on a un développement en série entière sur tout le disque $\mathcal{D}(0,1)$, donc toute combinaison linéaire de fonctions dans M_k est holomorphe à l'infini.

* De plus, l'ensemble des formes paraboliques est égal au noyau de l'application :

$$\varphi : \left| \begin{array}{ccc} M_k & \longrightarrow & \mathbb{C} \\ f : z \longmapsto \displaystyle\sum_{n=0}^{+\infty} a_n q^n & \longmapsto & a_0 \end{array} \right.$$

  qui est une application linéaire de M_k dans $\mathbb{C}$, donc S_k est un sous-espace vectoriel de $\mathbb{C}$.

■

Remarque :
On a donc montré que M_k est un $\mathbb{C}$-espace vectoriel, mais d'après les points 3 et 4 de l'exemple 1 on a même que M_k est une $\mathbb{C}$-algèbre (et même que l'ensemble $M_* = \bigoplus_{k \in \mathbb{Z}} M_k$ des formes modulaires (de niveau 1) est une $\mathbb{C}$-algèbre graduée par le poids !).

II Fonctions de réseaux et fonctions modulaires

Le but de cette partie et de faire le lien entre la notion de réseau et les fonctions modulaires. Ce lien nous sera notamment utile lorsque nous introduirons les séries d'Eisenstein.

Considérons $\mathcal{R}$ l'ensemble des réseaux de $\mathbb{C}$ (où $\mathbb{C}$ est vu comme un $\mathbb{R}$-espace vectoriel d'après la définition 2 du chapitre 1) et notons M l'ensemble des couples (ω_1, ω_2) d'éléments de $\mathbb{C}^*$ tels que $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$. À un tel couple on associe le réseau $\Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ de $\mathbb{Z}$-base (ω_1, ω_2). On obtient ainsi une application $\varphi : M \longrightarrow \mathcal{R}$ qui est surjective (par ce qui précède et quitte à prendre $-\omega_1$ au lieu de ω_1).

On considère $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $(\omega_1, \omega_2) \in M$ puis l'on pose :

$$\omega_1' = a\omega_1 + b\omega_2 \text{ et } \omega_2' = c\omega_1 + d\omega_2.$$

La famille (ω_1', ω_2') est encore une base de $\Gamma(\omega_1, \omega_2)$. De plus, si l'on pose $z = \dfrac{\omega_1}{\omega_2}$ et $z' = \dfrac{\omega_1'}{\omega_2'}$, on a alors :

$$z' = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d} = \frac{az + b}{cz + d} = g.z$$

On en conclut donc que $\mathrm{Im}\,(z') > 0$ (par (1.2)) et donc que (ω_1', ω_2') appartient à M. Ainsi, on obtient finalement que le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit sur l'ensemble M.

Proposition 4 :
Pour que deux éléments de M définissent le même réseau, il faut et il suffit qu'ils soient congrus modulo $\mathrm{SL}_2(\mathbb{Z})$.

Preuve :

* Nous venons de voir que si deux éléments de M sont congrus, alors ils définissent le même réseau.

* Réciproquement, soient (ω_1, ω_2) et (ω_1', ω_2') deux éléments de M définissant le même réseau.
Il existe alors une matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ de déterminant ± 1 qui transforme la première base en la seconde. Or, en posant $z = \dfrac{\omega_1}{\omega_2}$ et $z' = \dfrac{\omega_1'}{\omega_2'}$ comme précédemment on a :

$$\mathrm{Im}(z') = \mathrm{Im}(g.z) = \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}\right) = (ad-bc)\frac{\mathrm{Im}(z)}{|cz+d|^2} = \det(g)\frac{\mathrm{Im}(z)}{|cz+d|^2}$$

Cependant $\mathrm{Im}(z)$ et $\mathrm{Im}(z')$ sont de même signe, donc $\det(g) = 1$ et ainsi $g \in \mathrm{SL}_2(\mathbb{Z})$.

■

Ainsi, on peut identifier l'ensemble $\mathcal{R}$ des réseaux de $\mathbb{C}$ avec le quotient de M par l'action de $\mathrm{SL}_2(\mathbb{Z})$.

Faisons maintenant opérer $\mathbb{C}^*$ sur $\mathcal{R}$ (respectivement sur M) via l'application $\Gamma \longmapsto \lambda\Gamma$ (respectivement $(\omega_1, \omega_2) \longmapsto (\lambda\omega_1, \lambda\omega_2)$). Le quotient $M/\mathbb{C}^*$ s'identifie à $\mathcal{H}$ par $(\omega_1, \omega_2) \longmapsto z = \dfrac{\omega_1}{\omega_2}$ et cette identification transforme l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur M en celle de $G = \mathrm{SL}_2(\mathbb{Z})/\{-I_2; I_2\}$ sur $\mathcal{H}$. On obtient alors la proposition suivante :

Proposition 5 :
L'application $(\omega_1, \omega_2) \longmapsto \dfrac{\omega_1}{\omega_2}$ induit par passage au quotient une bijection de $\mathcal{R}/\mathbb{C}^*$ sur $\mathcal{H}/G$.

Remarques :
* Ainsi, un élément de $\mathcal{H}/G$ peut être identifié à un réseau de $\mathbb{C}$ (défini à homothétie près).
* Associons à un réseau Γ de $\mathbb{C}$ la courbe elliptique $E_\Gamma = \mathbb{C}/\Gamma$. On peut de plus montrer que deux réseaux Γ et Γ' définissent des courbes elliptiques isomorphes si, et seulement si, ils sont homothétiques. Cela nous donne une troisième description de $\mathcal{H}/G \cong \mathcal{R}/\mathbb{C}^*$: c'est l'ensemble des classes d'isomorphisme de courbes elliptiques sur $\mathbb{C}$.

Passons maintenant au lien avec les fonctions modulaires :

Définition 5 : Fonction de réseaux de poids k (et de niveau 1) :
On considère F une fonction sur $\mathcal{R}$ et à valeurs complexes et $k \in \mathbb{Z}$.
On dit que F est une **fonction de réseaux de poids** k (et de niveau 1) lorsque l'on a :

$$\forall \Gamma \in \mathcal{R},\ \forall \lambda \in \mathbb{C}^*,\ F(\lambda\Gamma) = \lambda^{-k} F(\Gamma) \tag{2.3}$$

Remarque :
La relation (2.3) signifie que la fonction F est homogène de degré $-k$.

En considérant F une telle fonction, $(\omega_1, \omega_2) \in M$ et en notant $F(\omega_1, \omega_2)$ la valeur de F sur le réseau $\Gamma(\omega_1, \omega_2)$ on obtient que (2.3) se traduit par :

$$\forall \lambda \in \mathbb{C}^*,\ F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k} F(\omega_1, \omega_2) \tag{2.4}$$

De plus, $F(\omega_1, \omega_2)$ est invariante par l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur M (par la proposition 4).

La formule (2.4) montre que le produit $\omega_2^k F(\omega_1, \omega_2)$ ne dépend que de $z = \dfrac{\omega_1}{\omega_2}$. Il existe donc une fonction f sur $\mathcal{H}$ telle que :

$$F(\omega_1, \omega_2) = \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right) \tag{2.5}$$

En écrivant que F est invariante par $\mathrm{SL}_2(\mathbb{Z})$, on voit que f satisfait à l'identité :

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

Inversement, si f vérifie la relation (2.1), alors la formule (2.5) lui associe une fonction F sur $\mathcal{R}$ qui est de poids k (et de niveau 1). On peut ainsi identifier les fonctions modulaires de poids k (et de niveau 1) à certaines fonctions de réseaux de poids k (et de niveau 1).

III Exemples de formes modulaires de niveau 1

Dans cette partie nous nous intéressons à des exemples de formes modulaires de niveau 1 en introduisant en premier lieu les séries d'Eisenstein puis en revenant sur le discriminant Δ (introduit dans la partie II.2 du chapitre 1) qui est une forme parabolique de poids 12. Ces exemples sont essentiels car nous énoncerons un peu plus loin un théorème de structure qui nous donne que toute forme modulaire de niveau 1 est polynomiale en les séries d'Eisenstein.

III.1 Les séries d'Eisenstein

Définition 6 : Série d'Eisenstein de poids k non normalisée :
On considère k un entier naturel pair supérieur ou égal à 4.
On appelle **série d'Eisenstein de poids k non normalisée** la fonction définie sur le demi-plan complexe supérieur étendu $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ par :

$$\forall z \in \mathcal{H}^*,\ G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k}$$

Puisque l'ensemble $\left\{n + mz,\ (n,m) \in \mathbb{Z}^2\right\}$ correspond au réseau $L = \mathbb{Z} \oplus \mathbb{Z}\, z$, on en déduit par le lemme 2 du chapitre 1 que la série d'Eisenstein est bien définie pour $k > 2$ (c'est-à-dire $k \geq 3$).

Ainsi, pour un entier naturel $k \geq 3$ et un réseau Γ de $\mathbb{C}$, la série :

$$G_k(\Gamma) = \sum_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \frac{1}{\gamma^k}$$

est absolument convergente (en vertu du lemme 2 du chapitre 1) et donc convergente. De même que précédemment, on peut considérer G_k comme une fonction sur M donnée par :

$$G_k(\omega_1, \omega_2) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^k}$$

La fonction sur $\mathcal{H}$ correspondant à G_k (par le procédé explicité dans la partie précédente) est encore notée G_k et d'après la relation précédente et (2.4), on a :

$$\forall z \in \mathcal{H},\ G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k}$$

Proposition 6 :
Soit k un entier naturel supérieur ou égal à 4.
La fonction G_k est une forme modulaire de poids k (et de niveau 1).

Preuve :

* Par ce qui précède, on obtient que la fonction G_k est bien définie.

* Pour tout $z \in \mathcal{H}$, on a :

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

où nous avons utilisé dans la dernière égalité le fait que l'application $(m,n) \longmapsto (m, n+m)$ est une bijection de $\mathbb{Z}^2$ dans $\mathbb{Z}^2$.
De même, on a pour tout $z \in \mathcal{H}$:

$$G_k\left(-\frac{1}{z}\right) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{\left(-\frac{m}{z}+n\right)^k} = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{z^k}{(-m+nz)^k} = z^k \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^k} = z^k G_k(z)$$

où nous avons utilisé dans l'avant-dernière égalité le fait que l'application $(m,n) \longmapsto (n,-m)$ est une bijection de $\mathbb{Z}^2$ dans $\mathbb{Z}^2$. Ainsi, les séries d'Eisenstein sont des fonctions faiblement modulaires de poids k (et de niveau 1).

* Montrons que G_k est partout holomorphe :
Supposons tout d'abord que z appartienne au domaine fondamental $\mathcal{D}$. On a alors :

$$|mz+n|^2 = m^2 z\overline{z} + 2mn\,\mathrm{Re}(z) + n^2 \geq m^2 - mn + n^2 = |m\rho - n|^2 \quad \left(\text{avec } \rho = e^{\frac{2i\pi}{3}}\right).$$

Or par le lemme 2 du chapitre 1, la série $\displaystyle\sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{|m\rho-n|^2}$ est convergente, donc la série $G_k(z)$ converge normalement sur $\mathcal{D}$ et donc aussi dans chacune des transformées $g\mathcal{D}$ de $\mathcal{D}$ par G (en appliquant le résultat précédent à $G_k\left(g^{-1}z\right)$ pour $g \in G$). Or, ceux-ci forment un recouvrement de $\mathcal{H}$, donc G_k est holomorphe sur $\mathcal{H}$.
Il nous reste à montrer que G_k est holomorphe à l'infini (et à trouver sa valeur en ce point) : cela revient à prouver que G_k a une limite pour $\mathrm{Im}(z) \to \infty$. En effet, le problème à l'infini peut se ramener à un problème en 0 avec le q-développement. Or, on sait déjà que G_k est holomorphe sur le disque unité épointé, donc la continuité en 0 (c'est-à-dire la limite éventuelle en ce point) permettra de conclure quant à l'holomorphie de f en se point.
Par le même argument que précédemment, on peut supposer que z appartient à $\mathcal{D}$ (quitte à faire agir G). La fonction $z \longmapsto \dfrac{1}{(mz+n)^k}$ tend vers $\dfrac{1}{n^k}$ ou 0 lorsque $\mathrm{Im}(z)$ tend vers $+\infty$ selon que $m = 0$ ou non. Par convergence uniforme de G_k sur $\mathcal{D}$, on peut intervertir limite et sommation et l'on obtient que :

$$\lim_{\mathrm{Im}(z)\to+\infty} G_k(z) = \sum_{n\in\mathbb{Z}^*} \frac{1}{n^k} = 2\sum_{n=1}^{+\infty} \frac{1}{n^k} = 2\zeta(k).$$

■

Exemple 2 :
Les séries d'Eisenstein de poids les plus bas sont G_4 et G_6 qui sont respectivement de poids 4 et 6.

Remarque :
Nous donnerons un peu plus loin le q-développement des fonctions G_k.

III.2 La forme parabolique Δ

Dans toute cette sous-partie, on considère L un réseau de $\mathbb{C}$.

Il est commode, à cause de la théorie des courbes elliptiques (cf. II du chapitre 1), de remplacer les séries d'Eisenstein $G_4(L)$ et $G_6(L)$ par les multiples suivants :

Définition 7 : $g_4(L)$ et $g_6(L)$:
On définit $g_4(L)$ et $g_6(L)$ sur un réseau L comme étant :

$$g_4(L) = 60G_4(L) \text{ et } g_6(L) = 140G_6(L). \tag{2.6}$$

On obtient alors à l'infini que :

$$g_4(\infty) = 120\zeta(4) = \frac{4\pi^4}{3} \text{ et } g_6(\infty) = 280\zeta(6) = \frac{8\pi^6}{27}.$$

On introduit alors la fonction suivante :

Définition 8 : Discriminant :
On appelle **discriminant** la fonction Δ définie sur $\mathcal{R}$ par :

$$\Delta(L) = \frac{D(L)}{(2\pi)^{12}} = \frac{1}{(2\pi)^{12}}\left(g_4^3(L) - 27g_6^2(L)\right). \tag{2.7}$$

Remarques :

* De même que pour le discriminant d'une courbe elliptique et l'invariant modulaire (cf. II.2 du chapitre 1), on définit la fonction $z \longmapsto \Delta(z)$.
* Le facteur $\frac{1}{(2\pi)^{12}}$ qui apparaît dans la définition de Δ peut sembler artificiel mais sera en réalité utile plus tard pour normaliser le q-développement.

On obtient alors que Δ est une forme modulaire de poids $4 \times 3 = 12$ (et de niveau 1) et qui de plus vérifie $\Delta(\infty) = \frac{1}{(2\pi)^{12}}\left(g_4(\infty)^3 - 27g_6(\infty)^2\right) = \frac{64}{27} - \frac{64}{27} = 0$. Ainsi, Δ est une forme parabolique de poids 12. De plus, Δ ne s'annule jamais sur $\mathcal{H}$ car la courbe elliptique $E = \mathbb{C}/(z\mathbb{Z} + \mathbb{Z})$ est de discriminant $D(E)$ non nul (cf. II.2 du chapitre 1).

IV Exemples de q-développements

IV.1 Nombres de Bernoulli

On définit la fonction :

$$f : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \displaystyle\sum_{n=0}^{+\infty} \frac{z^n}{(n+1)!} \end{array} \right.$$

qui vérifie pour tout $z \in \mathbb{C}^*$, $f(z) = \frac{e^z - 1}{z}$.
Puisque $f(0) = 1 \neq 0$, on sait que la fonction $\frac{1}{f}$ est développable en série entière sur un disque épointé $\dot{\mathcal{D}}(0, r)$ pour un certain $r > 0$. Ainsi, il existe une suite $(b_n)_{n\in\mathbb{N}}$ telle que :

$$\forall z \in \mathcal{D}(0,r)\backslash\{0\},\ \frac{z}{e^z - 1} = \sum_{n=0}^{+\infty} \frac{b_n}{n!} z^n$$

Cela nous conduit à la définition suivante :

Définition 9 : Nombres de Bernoulli :
Les termes de la suite $(b_n)_{n\in\mathbb{N}}$ ci-dessus sont appelés les **nombres de Bernoulli**.

Pour tout $x \in \mathbb{C}$, grâce au produit de Cauchy des développements en série entière des fonctions $z \longmapsto \dfrac{z}{e^z-1}$ et $z \longmapsto e^{xz}$, la fonction $z \longmapsto \dfrac{ze^{xz}}{e^z-1}$ est développable en série entière sur un disque $\dot{\mathcal{D}}(0,r)$ épointé pour un certain $r > 0$. On obtient alors la définition suivante :

Définition 10 : Polynômes de Bernoulli :
On considère $x \in \mathbb{C}$.
On appelle $(B_n(x))_{n\in\mathbb{N}}$ la suite des **polynômes de Bernoulli** définie de sorte que :

$$\forall x \in \mathbb{C},\ \forall z \in \mathcal{D}(0,r)\backslash\{0\},\ \frac{ze^{xz}}{e^z-1} = \sum_{n=0}^{+\infty} \frac{B_n(x)}{n!} z^n$$

Ces nombres et polynômes vérifient les propriétés suivantes (dont les démonstrations découlent des propriétés de la fonction $(z,x) \longmapsto \dfrac{ze^{xz}}{e^z-1}$ et du fait que l'on peut dériver terme à terme une série entière sur son disque de convergence) :

Proposition 7 :
On a les propriétés suivantes :
* $\forall n \in \mathbb{N},\ B_n(1-x) = (-1)^n B_n(x)$.
* $\forall n \in \mathbb{N}^*,\ B_n(x+1) - B_n(x) = nx^{n-1}$.
* $\forall n \in \mathbb{N}^*,\ \displaystyle\int_0^1 B_n(t)\mathrm{d}t = 0$.
* $\forall n \in \mathbb{N}^*,\ B_n' = nB_{n-1}$.
* $\forall n \in \mathbb{N}\backslash\{0;1\},\ B_n(0) = B_n(1)$.
* $\forall n \in \mathbb{N}^*,\ b_{2n+1} = 0$.

De plus, par produit de Cauchy et unicité du développement en série entière, on a également le résultat suivant :

Proposition 8 :
Pour tout $n \in \mathbb{N}$, on a :

$$\forall x \in \mathbb{C},\ B_n(x) = \sum_{k=0}^{n} \binom{n}{k} b_{n-k} x^k \text{ et } b_n \in \mathbb{Q}$$

Remarque :
Les nombres de Bernoulli interviennent dans d'autres domaines des mathématiques, notamment via la formule d'Euler-Maclaurin qui donne par exemple le résultat suivant :

$$H_n = \sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \frac{1}{252n^6} + \frac{1}{240n^8} - \frac{1}{132n^{10}} + O\left(\frac{1}{n^{13}}\right)$$

Proposition 9 :
Pour tout entier naturel non nul k, on a :

$$\zeta(2k) = \frac{(-1)^{k+1} b_{2k}}{2(2k)!} (2\pi)^{2k}$$

Pour une démonstration des trois propositions précédentes, on pourra consulter [2] (pages 319 à 321).

Remarques :

* Ainsi, on retrouve le fait que $\zeta(2) = \dfrac{\pi^2}{6}$, $\zeta(4) = \dfrac{\pi^4}{90}$ et $\zeta(6) = \dfrac{\pi^6}{945}$ (résultats que l'on peut obtenir via les séries de Fourier) mais on obtient également que par exemple :

$$\zeta(8) = \frac{\pi^8}{9\ 450},\ \zeta(10) = \frac{\pi^{10}}{93\ 555},\ \zeta(12) = \frac{691\pi^{12}}{638\ 512\ 875} \text{ et } \zeta(14) = \frac{2\pi^{14}}{18\ 243\ 225}.$$

De plus, en utilisant le fait que $\zeta(2k) \underset{k\to+\infty}{\longrightarrow} 1$ on a l'équivalent :

$$b_{2k} \underset{k\to+\infty}{\sim} (-1)^{k+1}\frac{2(2k)!}{(2\pi)^{2k}} \underset{k\to+\infty}{\sim} (-1)^{k+1}\frac{4\sqrt{\pi}k^{\frac{2k+1}{2}}}{(e\pi)^{2k}}$$

* On ne connaît presque rien des $\zeta(2k+1)$... Le nombre $\zeta(3) \approx 1,202$ est irrationnel d'après Roger Apéry (1978) et on l'appelle la **constante d'Apéry**. Hormis cela on ne connaît actuellement pas d'autre nombre irrationnel parmi les valeurs de la fonction ζ aux entiers impairs (le lecteur intéressé pourra consulter [14]).
* Les nombres de Bernoulli jouent un rôle important dans des parties aussi diverses des mathématiques que l'analyse, la théorie des nombres et la topologie différentielle. Citons par exemple l'étonnant théorème de Von Staudt :

Si pour tout $n \in \mathbb{N}^*$, s_n désigne la somme des inverses des nombres premiers p tels que $p-1$ divise $2n$, alors $s_n + b_{2n}$ est un entier.

Exemple 3 :

Le développement en série entière de la fonction $z \longmapsto \dfrac{z}{e^z-1}$ donne :

$$\frac{z}{e^z-1} = 1 - \frac{z}{2} + \frac{z^2}{12} - \frac{z^4}{720} + \frac{z^6}{30\ 240} - \frac{z^8}{1\ 209\ 600} + ...$$

On obtient alors les premiers nombres de Bernoulli suivants :

$$b_0 = 1,\ b_1 = -\frac{1}{2},\ b_2 = \frac{1}{6},\ b_4 = -\frac{1}{30},\ b_6 = \frac{1}{42},\ b_8 = \frac{-1}{30},\ b_{10} = \frac{5}{66},\ b_{12} = -\frac{691}{2\ 730},\ b_{14} = \frac{7}{6},\ b_{16} = -\frac{3\ 617}{510}$$

$$b_{18} = \frac{43\ 867}{798},\ b_{20} = -\frac{174\ 611}{330},\ b_{22} = \frac{854\ 513}{138},\ b_{24} = -\frac{236\ 364\ 091}{2\ 730},\ b_{26} = \frac{8\ 553\ 103}{6}$$

IV.2 q-développements des fonctions G_k

On rappelle que toute fonction f qui est une forme modulaire de poids k (et de niveau 1) peut être écrite comme une série formelle de puissances de $q = q(z) = e^{2i\pi z}$ et que cette expression est appelée q-développement de f. Nous allons donc ici déterminer le q-développement des séries d'Eisenstein G_k.

Définition 11 : Fonction σ_t :

Pour tout entier naturel t et tout entier naturel strictement positif n, on définit la **fonction** σ_t par :

$$\sigma_t : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \displaystyle\sum_{\substack{d|n \\ d\geq 1}} d^t \end{array} \right.$$

Ainsi, $\sigma_t(n)$ est la somme des puissances t-ième des diviseurs positifs de n.

On notera $d(n) = \sigma_0(n)$ (nombre de diviseurs positifs de n) et $\sigma(n) = \sigma_1(n)$ (somme des diviseurs positifs de n).

Exemple 4 :

* Pour tout $t \in \mathbb{N}$ et tout nombre premier p, on a $\sigma_t(p) = 1 + p^t$.
* Pour le nombre $n = 69$, ses diviseurs positifs sont $1, 3, 23$ et 69, donc :

$$d(69) = 4,\ \sigma(69) = 1 + 3 + 23 + 69 = 96 \text{ et } \sigma_2(n) = 1 + 3^2 + 23^2 + 69^2 = 10 + 529 + 4761 = 5300$$

Proposition 10 :
Pour tout entier naturel pair $k \geq 4$:

$$\forall z \in \mathcal{H}^*,\ G_k(z) = 2\zeta(k) + 2\frac{(2i\pi)^k}{(k-1)!}\sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n \tag{2.8}$$

Preuve :
Partons de la formule :

$$\forall z \in \mathcal{H},\ \pi\cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{+\infty}\left(\frac{1}{z+n} + \frac{1}{z-n}\right)$$

dont on pourra trouver une démonstration dans [2] (pages 273 et 274).
On a par ailleurs que pour tout $z \in \mathcal{H}$:

$$\pi\cot(\pi z) = \pi\frac{\cos(\pi z)}{\sin(\pi z)} = i\pi\frac{q+1}{q-1} = i\pi\left(\frac{-q+1-2}{1-q}\right) = i\pi\left(1 - \frac{2}{1-q}\right) = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi\sum_{n=0}^{+\infty}q^n$$

On a alors :

$$\forall z \in \mathcal{H},\ \frac{1}{z} + \sum_{n=1}^{+\infty}\left(\frac{1}{z+n} + \frac{1}{z-n}\right) = i\pi - 2i\pi\sum_{n=0}^{+\infty}q^n$$

Par dérivations successives (possible car la série de droite est une série entière sur le disque unité ouvert), on a alors pour tout entier naturel k supérieur ou égal à 2 :

$$\forall z \in \mathcal{H},\ \sum_{n=-\infty}^{+\infty}\frac{1}{(n+z)^k} = \frac{1}{(k-1)!}(-2i\pi)^k\sum_{n=1}^{+\infty}n^{k-1}q^n$$

En appliquant l'égalité précédente à nz au lieu de z, on a donc pour tout entier naturel $k \geq 4$:

$$\forall z \in \mathcal{H},\ G_k(z) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}}\frac{1}{(m+nz)^k} = 2\zeta(k) + 2\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\frac{1}{(m+nz)^k} = 2\zeta(k) + 2\frac{(-2i\pi)^k}{(k-1)!}\sum_{n=1}^{+\infty}\sum_{a=1}^{+\infty}a^{k-1}q^{an}$$

Enfin, en intervertissant les deux sommes et en posant le changement de variables bijectif de $\mathbb{N}^* \times \mathbb{N}^*$ dans $\mathbb{N}^* \times a\mathbb{N}^*$ défini par $(a, n) \longmapsto (a, an)$, on obtient que :

$$\begin{aligned}\forall z \in \mathcal{H},\ G_k(z) &= 2\zeta(k) + 2\frac{(2i\pi)^k}{(k-1)!}\sum_{a=1}^{+\infty}\sum_{n=1}^{+\infty}a^{k-1}q^{an} = 2\zeta(k) + 2\frac{(2i\pi)^k}{(k-1)!}\sum_{a=1}^{+\infty}\sum_{m\in a\mathbb{N}^*}a^{k-1}q^m\\ &= 2\zeta(k) + 2\frac{(2i\pi)^k}{(k-1)!}\sum_{m=1}^{+\infty}\sum_{\substack{a|m\\a\geq 1}}a^{k-1}q^m = 2\zeta(k) + 2\frac{(2i\pi)^k}{(k-1)!}\sum_{m=1}^{+\infty}\sigma_{k-1}(m)q^m\end{aligned}$$

Enfin, pour le cas du point à l'infini, on remarque que le q-développement de G_k est défini sur le disque épointé $\mathring{\mathcal{D}}(0,1)$ et lorsque $\mathrm{Im}(z)$ tend vers $+\infty$, on a pour tout $n \in \mathbb{N}^*$ que $|q^n|$ tend vers 0 donc $G_k(z)$ tend vers $2\zeta(k)$ par convergence uniforme.

■

On conclut cette partie avec les séries d'Eisenstein normalisées :

Définition 12 : Série d'Eisenstein normalisée de poids k :
On considère k un entier naturel supérieur ou égal à 4.
On appelle **série d'Eisenstein normalisée de poids** k la fonction définie sur $\mathcal{H}$ par :

$$E_k : z \longmapsto \frac{(k-1)!}{2(2i\pi)^k} G_k(z)$$

On obtient alors que le q-développement de E_k est donné par :

$$E_k(z) = -\frac{b_k}{2k} + q + \sum_{n=2}^{+\infty} \sigma_{k-1}(n) q^n$$

En particulier, E_k n'est pas une forme parabolique puisque b_k est non nul pour tout entier naturel $k \geq 4$.

Exemple 5 :
On donne ci-dessous le début des q-développements des premières séries d'Eisenstein normalisées :

$$\begin{aligned}
E_4(z) &= \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6 + \cdots \\
E_6(z) &= \frac{-1}{504} + q + 33q^2 + 244q^3 + 1\ 057q^4 + \cdots \\
E_8(z) &= \frac{1}{480} + q + 129q^2 + 2\ 188q^3 + \cdots \\
E_{10}(z) &= \frac{-1}{264} + q + 513q^2 + \ldots \\
E_{12}(z) &= \frac{691}{65\ 520} + q + 2\ 049q^2 + \ldots
\end{aligned}$$

Remarque :
Les séries d'Eisenstein normalisées sont telles que le coefficient devant q dans le q-développement est 1, mais souvent dans la littérature la normalisation est faite pour que le coefficient constant vaille 1. On préfère ici normaliser le terme devant q car on peut par exemple relier cela avec des propriétés du n-ième opérateur de Hecke (cf. III du chapitre 3).

Donnons une première application des formes modulaires :

Proposition 11 :
On a la relation :

$$\sum_{n=1}^{+\infty} \frac{n^5}{e^{2\pi n} - 1} = \frac{1}{504}.$$

Preuve :
On sait que E_6 est une forme modulaire de poids 6, on a donc en particulier :

$$\forall z \in \mathcal{H},\ E_6\left(-\frac{1}{z}\right) = z^6 E_6(z).$$

En $z = i$ on a alors que

$$E_6\left(-\frac{1}{i}\right) = E_6(i) = i^6 E_6(i) = -E_6(i)$$

donc $E_6(i) = 0$. Or en examinant le q-développement de E_6 et en l'évaluant en $z = i$, on a :

$$E_6(i) = \frac{-1}{504} + \sum_{n=1}^{+\infty} \sigma_5(n) e^{-2\pi n} = \frac{-1}{504} + \sum_{n=1}^{+\infty} \frac{n^5 e^{-2\pi n}}{1 - e^{-2\pi n}} = \frac{-1}{504} + \sum_{n=1}^{+\infty} \frac{n^5}{e^{2\pi n} - 1}.$$

Finalement, on obtient le résultat voulu en comparant les deux valeurs de $E_6(i)$ obtenues.

■

IV.3 Ordre de grandeur des coefficients des formes modulaires

Dans toute cette sous-partie, on considère une fonction f telle que :

$$\forall z \in \mathcal{H}^*,\ f(z) = \sum_{n=0}^{+\infty} a_n q^n,\ \text{où } q = q(z) = e^{2i\pi z}$$

et qui est une forme modulaire de poids pair k (avec $k \geq 4$). On souhaite s'intéresser à la croissance de ses coefficients a_n lorsque n tend vers $+\infty$.

Proposition 12 :
Soit $n \in \mathbb{N}^*$.
Si l'on a $f = G_k$, alors on a $a_n = O\left(n^{k-1}\right)$.
Plus précisément, il existe deux constantes $A, B > 0$ (indépendantes de n mais qui dépendent de k) telles que :

$$An^{k-1} \leq |a_n| \leq Bn^{k-1}$$

Preuve :
D'une part, la proposition 10 montre qu'il existe une constante $A > 0$ telle que $|a_n| = A\sigma_{n-1}$. Ainsi :

$$|a_n| = A\sigma_{k-1}(n) \geq An^{k-1}$$

D'autre part, on a :

$$\frac{|a_n|}{n^{k-1}} = A\frac{\sigma_{k-1}(n)}{n^{k-1}} = A\sum_{\substack{d|n \\ d\geq 1}} \left(\frac{d}{n}\right)^{k-1} = A\sum_{\substack{d|n \\ d\geq 1}} \frac{1}{\left(\frac{n}{d}\right)^{k-1}}$$

Enfin, en posant le changement de variables bijectif de $n\,\mathbb{N}^*$ dans $n\,\mathbb{N}^*$ défini par $m = \dfrac{n}{d}$ on obtient que :

$$\frac{|a_n|}{n^{k-1}} = \sum_{\substack{m|n \\ m\geq 1}} \frac{1}{m^{k-1}} \leq A\sum_{m=1}^{+\infty} \frac{1}{m^{k-1}} = A\zeta(k-1)$$

En posant alors $B = A\zeta(k-1) > 0$ on a le résultat.

■

Théorème 1 : Théorème de Hecke :
Si f est une forme parabolique, alors pour tout $n \in \mathbb{N}^*$, on a $a_n = O\left(n^{\frac{k}{2}}\right)$.

Preuve :
Puisque f est parabolique, on peut mettre q en facteur dans le q-développement de f, d'où :

$$\forall z \in \mathcal{H},\ |f(z)| \underset{q\to 0}{=} O(q) = O\left(e^{-2\pi \operatorname{Im}(z)}\right) \tag{2.9}$$

Posons φ définie sur $\mathcal{H}$ par $\varphi(z) = |f(z)|\operatorname{Im}(z)^{\frac{k}{2}} = |f(x+iy)|y^{\frac{k}{2}}$, où $z = x + iy$.
Les formules (2.1) et (1.2) montrent que φ est invariante par le groupe modulaire G. De plus, φ est continue sur le domaine fondamental $\mathcal{D}$ et la relation (2.9) montre que φ tend vers 0 quand $\operatorname{Im}(z)$ tend vers $+\infty$. On en conclut que φ est bornée sur $\mathcal{D}$ donc sur $\mathcal{H}$ et donc il existe une constante $M > 0$ telle que :

$$\forall z \in \mathcal{H},\ |f(z)| \leq My^{-\frac{k}{2}} \tag{2.10}$$

Soit $n \in \mathbb{N}^*$.
Fixons désormais $y > 0$ et faisons varier x entre 0 et 1.
Le point $q = e^{2i\pi(x+iy)}$ décrit un cercle $\mathcal{C}_y$ de centre 0 et par la formule de Cauchy, on a :

$$\forall n \in \mathbb{N}^*,\ a_n = \frac{1}{2i\pi}\int_{\mathcal{C}_y} f(z)q^{-n-1}\mathrm{d}q = \int_0^1 f(x+iy)q^{-n}\mathrm{d}x$$

En utilisant (2.10), on en tire :

$$|a_n| \leq My^{-\frac{k}{2}} e^{2\pi ny}$$

Cette égalité étant valable pour tout $y > 0$, on prend alors $y = \frac{1}{n}$ on a $|a_n| \leq e^{2\pi} M n^{\frac{k}{2}}$, d'où $a_n = O\left(n^{\frac{k}{2}}\right)$.

■

Remarque :

L'exposant $\frac{k}{2}$ du théorème de Hecke peut être amélioré. En effet, pour tout $\varepsilon > 0$ on a : $a_n = O\left(n^{\frac{k}{2}-\frac{1}{4}+\varepsilon}\right)$. On conjecture même que $\frac{k}{2}$ peut être remplacé par $\frac{k}{2} - \frac{1}{2} + \varepsilon$, ou encore que $a_n = O\left(n^{\frac{k}{2}-\frac{1}{2}} d(n)\right)$.

V Théorème de structure des formes modulaires de niveau 1

On continue ce chapitre par une avant-dernière partie consacrée au théorème de structure des formes modulaires de niveau 1 en étudiant d'abord les zéros et les pôles d'une fonction modulaire puis en donnant à la fin quelques applications de ce théorème.

V.1 Les zéros et les pôles d'une fonction modulaire

Soient f une fonction méromorphe sur $\mathcal{H}$ non identiquement nulle et p un point de $\mathcal{H}$.

Nous appellerons **ordre de f en p**, et nous noterons $v_p(f)$, le plus petit entier naturel n tel que $\frac{f}{(z-p)^n}$ soit holomorphe et non nulle en p.

Lorsque f est une fonction fonction modulaire de poids k (et de niveau 1), l'identité :

$$\forall z \in \mathcal{H},\ f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

montre que pour $g \in G$, on a $v_p(f) = v_{g.p}(f)$. En d'autres termes, $v_p(f)$ ne dépend que de l'image de p dans le quotient $\mathcal{H}/G$. On peut également définir $v_\infty(f)$ comme l'ordre en $q = 0$ de la fonction $F(q)$ associée à f. Enfin, nous noterons e_p l'ordre du stabilisateur du point p (on a alors par le théorème 1 du chapitre 1 que $e_p = 2$ si p est congru à i modulo G, $e_p = 3$ si p est congru à ρ modulo G et $e_p = 1$ sinon).

Théorème 2 : Formule de valence :
Soit f une fonction modulaire de poids k (et de niveau 1) non identiquement nulle.
On a la relation (appelée **formule de valence**) :

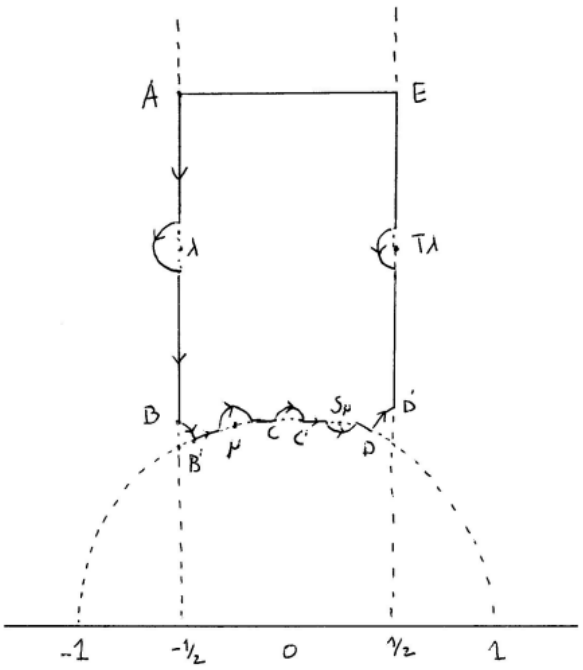
$$v_\infty(f) + \sum_{p \in \mathcal{H}/G} \frac{1}{e_p} v_p(f) = \frac{k}{12} \tag{2.11}$$

Preuve :
Soit f une fonction modulaire de poids k (et de niveau 1) non identiquement nulle.

- Rappelons que l'orbite sous l'action de G de tout zéro de f rencontre le domaine $\mathcal{D}$. Pour r un réel strictement positif, posons $\Omega_r = \{z \in \mathcal{H} \text{ tq } \mathrm{Im}(z) > r\}$. La fonction F associée à f étant méromorphe en 0, il existe $r > 0$ tel que f n'admet pas de zéro dans Ω_r.
  La partie $\mathcal{D}$ privée de Ω_r étant compacte (car fermée et bornée), la fonction méromorphe f n'y admet qu'un nombre fini de zéros (qui sont isolés). Cela montre que le nombre d'orbites sous l'action de G contenant un zéro de f est fini, et donc que la somme apparaissant dans la formule a tous ses termes nuls sauf au plus un nombre fini d'entre eux (la formule a donc bien un sens).

∗ Considérons le contour $\mathcal{C}$ indiqué par la figure ci-dessous.

Sur cette figure, les zéros éventuels de f qui sont dans $\partial\mathcal{D}\backslash\{i;\rho;-\overline{\rho}\}$ et de partie réelle $-\dfrac{1}{2}$ (respectivement de module 1) sont notés λ (respectivement μ). En particulier, ce contour ne contient aucun zéro de f. On suppose que chaque portion de cercle dessinée est de rayon suffisamment petit de sorte que le disque bordé ne contienne que le point indiqué pour éventuel zéro (c'est-à-dire $i, \rho, -\overline{\rho}$, l'un des λ, $\lambda+1$, ou l'un des μ, $\dfrac{-1}{\mu}$). Enfin, on suppose que le chemin γ_{EA} (joignant E à A dans le sens trigonométrique) est de partie imaginaire r suffisamment grande de sorte qu'aucun zéro de f ne soit de partie imaginaire strictement plus grande que r (l'existence d'un tel contour est justifiée par le paragraphe précédent).



∗ Le théorème des résidus appliqué à la fonction $\dfrac{f'}{f}$ nous donne que :

$$\frac{1}{2i\pi}\int_{\mathcal{C}}\frac{f'(z)}{f(z)}\mathrm{d}z=\sum_{\substack{p\in\mathcal{H}/G\\ p\neq i,\rho}} v_p(f).$$

Examinons maintenant les contributions des diverses portions du contour :

Les fonctions f et f' étant invariantes sous l'action de $T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, on a alors :

$$\int_{\gamma_{AB}}\frac{f'(z)}{f(z)}\mathrm{d}z=\int_{T.\gamma_{AB}}\frac{f'(z)}{f(z)}\mathrm{d}z=\int_{\gamma_{ED'}}\frac{f'(z)}{f(z)}\mathrm{d}z=-\int_{\gamma_{D'E}}\frac{f'(z)}{f(z)}\mathrm{d}z.$$

De plus, le chemin $\omega : t\longmapsto e^{2i\pi\gamma_{EA}(t)}$ est un cercle de centre 0 dans le disque unité ouvert faisant un tour dans le sens indirect. On a alors par un changement de variables que :

$$\frac{1}{2i\pi}\int_{\gamma_{EA}}\frac{f'(z)}{f(z)}\mathrm{d}z=\frac{1}{2i\pi}\int_{\omega}\frac{F'(q)}{F(q)}\mathrm{d}q.$$

Et par le théorème des résidus appliqué à F (sachant que par hypothèse 0 est le seul zéro éventuel de F dans le disque bordé par ω) :

$$\frac{1}{2i\pi}\int_{\gamma_{EA}}\frac{f'(z)}{f(z)}\mathrm{d}z=\frac{1}{2i\pi}\int_{\omega}\frac{F'(q)}{F(q)}\mathrm{d}q=-v_\infty(f).$$

De plus, puisque f est une fonction modulaire non nulle de poids k, on a pour tout z où $\frac{f'}{f}$ est bien définie que :

$$\frac{f'(z)}{f(z)} = -\frac{k}{z} + \frac{(f\circ S)'(z)}{(f\circ S)(z)}$$

de sorte que :

$$\frac{1}{2i\pi}\int_{\gamma_{B'C}} \frac{f'(z)}{f(z)}\mathrm{d}z = \frac{-1}{2i\pi}\int_{\gamma_{B'C}} \frac{k}{z}\mathrm{d}z + \frac{1}{2i\pi}\int_{\gamma_{B'C}} \frac{(f\circ S)'(z)}{(f\circ S)(z)}\mathrm{d}z = \frac{-1}{2i\pi}\int_{\gamma_{B'C}} \frac{k}{z}\mathrm{d}z + \frac{1}{2i\pi}\int_{S.\gamma_{B'C}} \frac{f'(z)}{f(z)}\mathrm{d}z$$

où $S.\gamma_{B'C} = \gamma_{DC'}$.

Or, lorsque B' tend vers ρ, C tend vers i et les portions de cercles autour des points notés μ sont de rayon tendant vers 0, l'intégrale $\frac{1}{i}\int_{\gamma_{B'C}} \frac{\mathrm{d}z}{z}$ tends vers l'angle orienté défini par ρ, 0 et i, c'est-à-dire $-\left(\frac{2\pi}{3} - \frac{2\pi}{4}\right) = -\frac{\pi}{6}$.

De même, lorsque B et B' tendent vers ρ alors l'intégrale $\frac{1}{i}\int_{\gamma_{BB'}} \frac{f'(z)}{f(z)}\mathrm{d}z$ tend vers l'angle orienté $\widehat{B\rho B'} = -\frac{\pi}{3}$ multiplié par $v_p(f)$.

Enfin, lorsque C et C' tendent vers i alors l'intégrale $\frac{1}{i}\int_{\gamma_{CC'}} \frac{f'(z)}{f(z)}\mathrm{d}z$ tend vers $-\pi v_i(f)$.

En mettant bout à bout toutes ses égalités, on a alors :

$$v_\infty(f) + \sum_{p\in\mathcal{H}/G} \frac{1}{e_p} v_p(f) = \frac{k}{12}$$

■

Remarque :
La formule de valence peut aussi s'écrire sous la forme :

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p\in\mathcal{H}/G \\ p\neq i,\rho}} v_p(f) = \frac{k}{12} \tag{2.12}$$

V.2 Énoncé et preuve du théorème de structure des formes modulaires de niveau 1

Lemme 1 :
Soit k un entier naturel pair supérieur ou égal à 4.
On a $M_k = S_k \oplus \mathbb{C}G_k$ et la suite suivante est exacte :

$$0 \longrightarrow S_k \xrightarrow{\iota} M_k \xrightarrow{\iota_\infty} \mathbb{C} \longrightarrow 0$$

où ι est l'injection canonique de S_k dans M_k et ι_∞ la forme linéaire qui à f associe $f(\infty)$

Preuve :
Soit k un entier naturel pair supérieur ou égal à 4.

- Montrons que la suite est exacte :
  L'injection canonique ι de S_k dans M_k est injective. De plus, la forme linéaire i_∞ est non nulle puisque l'espace M_k contient la série d'Eisenstein G_k et $G_k(\infty) = 2\zeta(k) \neq 0$, donc par le théorème du rang, i_∞ est surjective.

∗ De plus, puisque S_k est le noyau de la forme linéaire (non nulle) ι_∞, on en déduit qu'il est de co-dimension 1 et comme $\iota_\infty(G_k) \neq 0$, on a $M_k = S_k \oplus \mathbb{C}G_k$.

■

Corollaire 1 :
Soient k un entier naturel pair supérieur ou égal à 4 et f une forme modulaire de poids k (et de niveau 1).
Si f n'est pas une forme parabolique, alors pour tout $n \in \mathbb{N}^*$, $a_n = O\left(n^{k-1}\right)$.

Preuve :
Soit $f \in M_k \backslash S_k$.
Écrivons f sous la forme $f = \sum_{n=0}^{+\infty} a_n q^n = \lambda G_k + h$ avec $\lambda \neq 0$ et h parabolique (possible par le lemme 1). On peut alors appliquer la proposition 12 à G_k et le théorème de Hecke (théorème 1) à h pour conclure que pour tout $n \in \mathbb{N}^*$, $a_n = O\left(n^{k-1}\right)$.

■

Proposition 13 :
Soit $k \in \mathbb{Z}$.
Pour $k < 0$ et $k = 2$, on a $M_k = \{0\}$.

Preuve :
Soit $k \in \mathbb{Z}$.
Raisonnons par l'absurde en supposant qu'il existe $f \in M_k$ non nulle pour $k < 0$ ou $k = 2$.
Par la formule de valence, on a alors :

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p \in \mathcal{H}/G \\ p \neq i, \rho}} v_p(f) = \frac{k}{12} \leq \frac{1}{6} \tag{2.13}$$

Or chaque quantité du membre de gauche est positive ou nulle (par définition) et ce même membre est non nul car f est non nulle. Ainsi, en notant respectivement :

$$n_1 = v_\infty(f),\ n_2 = v_i(f),\ n_3 = v_\rho(f) \text{ et } n_4 = \sum_{\substack{p \in \mathcal{H}/G \\ p \neq i, \rho}} v_p(f)$$

on obtient que la relation (2.13) est équivalente à :

$$12n_1 + 6n_2 + 4n_4 + 12n_4 = k \leq 2$$

Or cette équation n'a pas de solution dans $(\mathbb{N}^*)^4$ pour $k < 0$ ni pour $k = 2$), d'où une contradiction.

■

Théorème 3 :
Soit $k \in \mathbb{Z}$.
La multiplication par Δ induit un isomorphisme de $\mathbb{C}$-espaces vectoriels de M_{k-12} dans S_k.

Preuve :
Soit $k \in \mathbb{Z}$.

∗ La fonction Δ ne s'annule jamais (cf. III.2) et puisque Δ est une forme modulaire de poids 12, la multiplication par Δ induit une application $\mathbb{C}$-linéaire injective de M_{k-12} dans M_k. Or, pour tout $f \in M_{k-12}$, on a $f(\infty)\Delta(\infty) = f(\infty) \times 0 = 0$, donc en réalité on a une application de M_{k-12} dans S_k.

∗ Pour montrer que la multiplication par Δ est surjective, montrons que si $f \in S_k$, alors on a $\dfrac{f}{\Delta} \in M_{k-12}$. On sait que Δ est de poids 12 et que $v_\infty(\Delta) \geq 1$ (car forme parabolique), donc la formule de valence implique que Δ a un zéro simple en ∞ et ne s'annule pas sur $\mathcal{H}^*$. Ainsi, si $f \in S_k$ et que l'on pose $g = \dfrac{f}{\Delta}$, alors g est holomorphe, satisfait la formule (2.1) et est de poids $k-12$, d'où $g \in M_{k-12}$.

■

Corollaire 2 :
Pour $k = 0, 4, 6, 8, 10$ et 14, le $\mathbb{C}$-espace vectoriel M_k est de dimension 1 de bases respectives $(z \longmapsto 1)$, (G_4), (G_6), (G_8), (G_{10}) et (G_{14}) et on a $S_k = \{0\}$.

Preuve :

∗ Pour $k = 0$:
Par le lemme 1, on a que $M_0/S_0 \cong \mathrm{Im}(i_\infty)$, donc $\dim \mathbb{C}(M_0/S_0) = \dim_{\mathbb{C}}(M_0) - \dim_{\mathbb{C}}(S_0) = 0$ ou 1. Or, toute fonction constante sur $\mathcal{H}$ est une forme modulaire de poids 0, donc $\dim_{\mathbb{C}}(M_0) = 1$ et admet pour base $(z \longmapsto 1)$. Enfin, on a $S_0 \subsetneq M_0$ (car la fonction constante égale à 1 appartient à M_0 mais pas S_0), d'où $S_0 = \{0\}$.

∗ Pour $k \in \{4; 6; 8; 10\}$, on a $k - 12 < 0$ et donc $S_k = \{0\}$ car on a $M_{k-12} \cong S_k$ (par le théorème 3) et $M_{k-12} = \{0\}$ (par la proposition 13). Ainsi, on a $M_k = S_k \oplus \mathbb{C}G_k \cong \mathbb{C}G_k$ (par le lemme 1). Or, on a G_4, G_6, G_8 et G_{10} qui appartiennent respectivement à M_4, M_6, M_8 et M_{10} et sont non nulles, donc M_k est de dimension 1 et de base respective (G_4), (G_6), (G_8), (G_{10}).

∗ Pour $k = 14$:
On a par le théorème 3 que $S_{14} \cong M_{14-12} = M_2$, donc S_{14} a une dimension nulle en tant que $\mathbb{C}$-espace vectoriel (par la proposition 13) et puisque G_{14} existe et est une forme modulaire non nulle de poids 14 (et de niveau 1), on a $M_{14} \cong \mathbb{C}G_{14}$ (par le lemme 1).

■

Corollaire 3 :
On a la relation :

$$\dim_{\mathbb{C}}(M_k) = \begin{cases} 0 & \text{si } k \text{ est impair ou strictement négatif} \\ \left\lfloor \dfrac{k}{12} \right\rfloor & \text{si } k > 0 \text{ et } k \equiv 2\ [12] \\ \left\lfloor \dfrac{k}{12} \right\rfloor + 1 & \text{sinon} \end{cases}$$

Preuve :

∗ D'après l'exemple 1 et la proposition 13, on a la relation pour k impair, k strictement négatif ainsi que $k = 2$.

∗ D'après le corollaire 2, on a les deux autres relations pour $k \in [\![0; 11]\!] \backslash \{2\}$.

∗ Pour les autres cas, il suffit de constater que $M_k = S_k \oplus \mathbb{C}G_k$ (par le lemme 1) et que $S_k \cong M_{k-12}$ (par le théorème 3). Ainsi, on a $M_k \cong M_{k-12} \oplus \mathbb{C}G_k$ et donc :

$$\dim_{\mathbb{C}}(M_{k+12}) = \dim_{\mathbb{C}}(M_k) + 1$$

Finalement, pour $k > 0$ et $k \equiv 2\ [12]$ on a :

$$\dim_{\mathbb{C}}(M_{k+12}) = \dim_{\mathbb{C}}(M_k) + 1 = \left\lfloor \frac{k}{12} \right\rfloor + 1 = \left\lfloor \frac{k}{12} + \frac{12}{12} \right\rfloor = \left\lfloor \frac{k+12}{12} \right\rfloor$$

Et sinon :

$$\dim_{\mathbb{C}}(M_{k+12}) = \dim_{\mathbb{C}}(M_k) + 1 = \left(\left\lfloor \frac{k}{12} \right\rfloor + 1 \right) + 1 = \left(\left\lfloor \frac{k}{12} + \frac{12}{12} \right\rfloor \right) + 1 = \left\lfloor \frac{k+12}{12} \right\rfloor + 1$$

■

On résume les résultats précédents dans le tableau ci-dessous :

k	0	2	4	6	8	10	12	14	16	18	20	22	24	26	$\cdots$	k	$\cdots$	$k+12$	$\cdots$
$\dim_{\mathbb{C}}(M_k)$	1	0	1	1	1	1	2	1	2	2	2	2	3	2	$\cdots$	d	$\cdots$	$d+1$	$\cdots$
$\dim_{\mathbb{C}}(S_k)$	0	0	0	0	0	0	1	0	1	1	1	1	2	1	$\cdots$	$d-1$	$\cdots$	d	$\cdots$

Le théorème suivant est une conséquente très pratique du fait que les espaces des formes modulaires sont de dimension finie

Théorème 4 :
Soient k un entier naturel et f une forme modulaire de poids k (et de niveau 1) dont le q-développement est donné par $\sum_{n=0}^{+\infty} a_n q^n$.
Si on a, pour tout $i \in \left[\!\left[0; \left\lfloor \frac{k}{12} \right\rfloor\right]\!\right]$, $a_i = 0$, alors f est nulle.

Preuve :
Soient k un entier naturel et f une forme modulaire de poids k (et de niveau 1) dont le q-développement est donné par $\sum_{n=0}^{+\infty} a_n q^n$.
Raisonnons par l'absurde en supposant que f est non identiquement nulle.
Par hypothèse, on a alors :

$$v_\infty(f) \geq \left\lfloor \frac{k}{12} \right\rfloor + 1 > \left\lfloor \frac{k}{12} \right\rfloor$$

On a alors que le terme de gauche dans la formule de valence (théorème 2) est strictement plus grand que $\left\lfloor \frac{k}{12} \right\rfloor$, ce qui est contradictoire.

Finalement, on en déduit que f est identiquement nulle.

■

Remarque :
On retrouve ici un cas particulier des bornes de Sturm.

Corollaire 4 :
Soient $k \in \mathbb{N}$ et f, g deux formes modulaires de poids k (et de niveau 1) dont les q-développements sont donnés respectivement par $\sum_{n=0}^{+\infty} a_n q^n$ et $\sum_{n=0}^{+\infty} b_n q^n$.
Si on a, pour tout $i \in \left[\!\left[0; \left\lfloor \frac{k}{12} \right\rfloor\right]\!\right]$, $a_i = b_i$, alors $f = g$.

Preuve :
Soient $k \in \mathbb{N}$ et f, g deux formes modulaires de poids k (et de niveau 1) dont les q-développements sont donnés respectivement par $\sum_{n=0}^{+\infty} a_n q^n$ et $\sum_{n=0}^{+\infty} b_n q^n$.
En considérant la forme modulaire de poids k (et de niveau 1) $f - g$, on a alors que les coefficients c_i de son q-développement sont nuls pour tout $i \in \left[\!\left[0; \left\lfloor \frac{k}{12} \right\rfloor\right]\!\right]$. Donc par le théorème 4, on en déduit que $f - g$ est identiquement nulle.

Finalement, on obtient que $f = g$.

■

Théorème 5 :
Soit k un entier naturel pair.
L'espace vectoriel M_k admet pour base la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$.

Preuve :
Soit k un entier naturel pair.

* Montrons par récurrence forte que la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ engendre M_k :
  - Initialisation :
    Les cas où $k \leq 10$ et $k = 14$ ont été traités précédemment dans la proposition 13 et le corollaire 2 (en particulier pour $k = 0$ on a $a = b = 0$ et la base correspondante est $(z \longmapsto 1)$). Ceci nous donne donc l'initialisation.
  - Hérédité :
    On considère k un entier naturel pair et on suppose que la propriété est vraie pour tout entier naturel $n \leq k$.
    Choisissons une paire (a, b) d'entiers naturels non nuls tels que $4a + 6b = k$.
    La forme modulaire $g = G_4^a G_6^b$ n'est pas une forme parabolique puisque :

$$g(\infty) = G_4^a(\infty) G_6^b(\infty) = (2\zeta(4))^a (2\zeta(6))^b = \frac{2^{a+b}\pi^{4a+6b}}{90^a \times 945^b} = \frac{2^{a+b}\pi^k}{90^a \times 945^b} \neq 0.$$

    Ainsi, pour $f \in M_k$ fixé, il existe $\alpha \in \mathbb{C}$ tel que $f - \alpha g \in S_k$ (concrètement on peut prendre le scalaire $\alpha = \frac{f(\infty)}{g(\infty)}$) et donc par le théorème 3, il existe une forme modulaire $h \in M_{k-12}$ tel que $f - \alpha g = \Delta h$.
    Or, par hypothèse de récurrence, on a

$$M_{k-12} = \text{Vect}\left(G_4^{a'} G_6^{b'},\ a', b' \geq 0,\ 4a' + 6b' = k - 12\right)$$

    et

$$S_{12} = \text{Vect}\left(G_4^{a''} G_6^{b''},\ a'', b'' \geq 0,\ 4a'' + 6b'' = 12\right).$$

    Ainsi, on a

$$\Delta h \in \text{Vect}\left(G_4^{a'+a''} G_6^{b'+b''},\ a' + a'', b' + b'' \geq 0),\ 4(a' + a'') + 6(b' + b'') = k - 12 + 12 = k\right).$$

    Finalement, la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ engendre M_k, d'où l'hérédité.

  Ainsi, on a montré par récurrence que la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ engendre M_k.

* Montrons par récurrence forte que la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ est libre sur M_k :
  - Initialisation :
    Les cas où $k \leq 10$ et $k = 14$ ont été traités précédemment dans la proposition 13 et le corollaire 2 (en particulier pour $k = 0$ on a $a = b = 0$ et la base correspondante est $(z \longmapsto 1)$). Ceci nous donne donc l'initialisation.

— Hérédité :
On considère k un entier naturel pair et on suppose que la propriété est vraie pour tout entier naturel $n \leq k$.
Considérons une relation de dépendance linéaire de la forme

$$\sum_{\substack{4a+6b=k \\ a,b\geq 0}} \lambda_{a,b} G_4^a G_6^b = 0.$$

Or, si k est un multiple de 4, alors on a la relation :

$$\forall z \in \mathcal{H},\ \lambda_{a,0} G_4^a(z) = 0$$

En particulier en $z = i$, on a $\lambda_{a,0} = 0$ puisque $G_4(i) \neq 0$ (en effet, par l'exemple 5 on a l'expression de E_4 et pour $z = i$ on a $q = e^{-2\pi}$). On a donc montré par contraposition que si $\lambda_{a,b} \neq 0$, alors on a $b \neq 0$.
Ainsi, soit tous les $\lambda_{a,b}$ sont nuls, soit on a $k \geq 6$. Or on a le résultat voulu dans le premier cas et si l'on est dans le second, alors on peut alors simplifier la relation de dépendance linéaire par G_6 (l'anneau des fonctions holomorphes sur $\mathcal{H}$ étant intègre) et par l'hypothèse de récurrence on peut alors conclure que tous les $\lambda_{a,b}$ sont nuls.
Finalement, la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ est libre sur M_k, d'où l'hérédité.

Ainsi, on a montré par récurrence que la famille $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ est libre sur M_k.

Finalement, $\{G_4^a G_6^b,\ a, b \geq 0,\ 4a + 6b = k\}$ est à la fois une famille libre et génératrice de M_k, donc est une base de M_k.

■

Remarque :
Reprenons M_* l'algèbre graduée par le poids des formes modulaires et posons $\varepsilon : \mathbb{C}[X, Y] \longrightarrow M_*$ le morphisme de $\mathbb{C}$-algèbres qui envoie X sur G_4 et Y sur G_6.
Le théorème 5 équivaut à dire que ε est en fait un isomorphisme de $\mathbb{C}$-algèbres et on peut alors identifier M_* à l'algèbre des polynômes $\mathbb{C}[X, Y]$ (autrement dit, les fonctions G_4 et G_6 sont algébriquement indépendantes sur $\mathbb{C}$).

V.3 Quelques applications

V.3.1 Obtention de base et de relations arithmétiques

Grâce au théorème 5, il est possible de trouver une base explicite de M_k (et elle est donnée par le théorème) !

Exemple 6 :
Cherchons une base de l'espace vectoriel M_{24} :
On sait que sa dimension est 3 et une base est donnée par $\left(G_4^6, G_4^3 G_6^2, G_6^4\right)$. Pour plus de simplicité dans les calculs, on préfère choisir les série d'Eisenstein normalisées pour obtenir la base $\left(E_4^6, E_4^3 E_6^2, E_6^4\right)$ dont les débuts des q-développements sont :

$$E_4^6 = \frac{1}{191\ 102\ 976\ 000\ 000} + \frac{1}{132\ 710\ 400\ 000} q + \frac{203}{44\ 236\ 800\ 000} q^2 + ...$$

$$E_4^3 E_6^2 = \frac{1}{3\ 511\ 517\ 184\ 000} - \frac{1}{12\ 192\ 768\ 000} q + \frac{377}{4\ 064\ 256\ 000} q^2 + ...$$

$$E_6^4 = \frac{1}{64\ 524\ 128\ 256} - \frac{1}{32\ 006\ 016} q + \frac{241}{10\ 668\ 672} q^2 + ...$$

De plus, le corollaire 3 nous donne la dimension des $\mathbb{C}$-espaces vectoriels M_k, il est alors possible d'obtenir des relations entre les éléments de cet espace ! En effet, notons $d = \dim_{\mathbb{C}}(M_k)$ et supposons avoir une famille de ℓ formes modulaires dans M_k avec $\ell > d$. Par la théorie de la dimension en algèbre linéaire, cette famille est liée sur $\mathbb{C}$.

Ainsi, on peut écrire une relation linéaire non triviale entre ces formes modulaires (les coefficients s'obtenant grâce aux premiers coefficients des q-développements) et par unicité du q-développement, on peut identifier ces mêmes coefficients et obtenir une identité arithmétique.

Exemple 7 :
On sait que l'espace M_8 est de dimension 1 et qu'il contient les formes modulaires non identiquement nulles E_4^2 et E_8. Il existe alors une constante $\alpha \in \mathbb{C}$ telle que $E_8 = \alpha E_4^2$. En comparant le premier coefficient de chacun des deux q-développements, on obtient que :

$$\frac{1}{480} = \alpha \left(\frac{1}{240}\right)^2 = \frac{\alpha}{57\ 600} \text{ soit } \alpha = \frac{57\ 600}{480} = 120.$$

En identifiant alors les coefficients des deux q-développements, on obtient après simplification :

$$\forall n \in \mathbb{N}^*,\ \sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

On obtient alors que pour tout $n \in \mathbb{N}^*,\ \sigma_7(n) \equiv \sigma_3(n)\ [120]$ et en particulier, pour tout nombre premier p, on a $p^7 \equiv p^3\ [120]$.

Exemple 8 :
On sait que l'espace M_{10} est de dimension 1 et qu'il contient les formes modulaires non identiquement nulles E_4E_6 et E_{10}. Il existe alors une constante $\alpha \in \mathbb{C}$ telle que $E_{10} = \alpha E_4 E_6$. En comparant le premier coefficient de chacun des deux q-développements, on obtient que :

$$\frac{-1}{264} = \alpha \times \frac{1}{240} \times \frac{-1}{504} = \frac{-\alpha}{120\ 960} \text{ soit } \alpha = \frac{120\ 960}{264} = \frac{5\ 040}{11}.$$

De plus, pour tout $z \in \mathcal{H}$, on a :

$$\begin{aligned} E_4(z)E_6(z) &= \left(\frac{1}{240} + \sum_{n=1}^{+\infty} \sigma_3(n)q^n\right)\left(\frac{-1}{504} + \sum_{n=1}^{+\infty} \sigma_5(n)q^n\right) \\ &= \frac{-1}{120\ 960} + \sum_{n=1}^{+\infty} \frac{\sigma_5(n)}{240} q^n + \sum_{n=1}^{+\infty} \frac{-\sigma_3(n)}{504} q^n + \sum_{n=1}^{+\infty} \left(\sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m)\right) q^n \\ &= \frac{-1}{120\ 960} + \sum_{n=1}^{+\infty} \left(\frac{\sigma_5(n)}{240} - \frac{\sigma_3(n)}{504} + \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m)\right) q^n. \end{aligned}$$

En identifiant les coefficients des deux q-développements, on a alors :

$$\begin{aligned} \forall n \in \mathbb{N}^*,\ \sigma_9(n) &= \frac{5\ 040}{11}\left(\frac{\sigma_5(n)}{240} - \frac{\sigma_3(n)}{504} + \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m)\right) \\ &= \frac{21}{11}\sigma_5(n) - \frac{10}{11}\sigma_3(n) + \frac{5\ 040}{11} \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m). \end{aligned}$$

On a alors :

$$\forall n \in \mathbb{N}^*,\ 11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5\ 040 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m).$$

On obtient alors en particulier que pour tout $n \in \mathbb{N}^*,\ 11\sigma_9(n) \equiv 21\sigma_5(n) - 10\sigma_3(n)\ [5\ 040]$ et ainsi pour tout nombre premier p, on a $11p^9 \equiv 21p^5 - 10p^3\ [5\ 040]$.

Remarque :
Par le théorème 5, on a même que chaque E_k peut s'exprimer comme polynôme par rapport à E_4 et E_6.

V.3.2 L'invariant modulaire

On rappelle que si l'on considère une courbe elliptique non singulière sur $\mathbb{P}^1(\mathbb{C})$ dont la forme de Weierstrass est $Y^2 = 4X^3 - g_4(L)X - g_6(L)$, alors son discriminant est $D(L) = g_4^3(L) - 27g_6^2(L) \neq 0$ et que

$$\Delta(L) = \frac{D(L)}{(2\pi)^{12}} = \frac{g_4^3(L) - 27g_6^2(L)}{(2\pi)^{12}} = 8\ 000E_4^3(L) - 147E_6^2(L).$$

Définition 13 : Invariant modulaire :
On considère L un réseau de $\mathbb{C}$.
On appelle **invariant modulaire** la fonction $j : \mathcal{R} \longrightarrow \mathbb{C}$ définie par $j(L) = \dfrac{1\ 728g_4^3(L)}{\Delta(L)} = \dfrac{13\ 824\ 000E_4^3(L)}{\Delta(L)}$.

Par le même procédé que pour D et Δ, on peut considérer j comme une fonction sur les réseaux (c'est la définition) mais également comme fonction définie sur $\mathcal{H}$ (cf. II.2 du chapitre 1).

Proposition 14 :

* La fonction j est une fonction modulaire de poids 0.
* La fonction j est holomorphe sur $\mathcal{H}$ et a un pôle simple à l'infini.
* Elle définit par passage au quotient une bijection de $\mathcal{H}/G$ sur $\mathbb{C}$.

Preuve :

* Les fonctions g_4^3 et Δ sont des formes modulaires de poids 12 et Δ ne s'annule jamais sur $\mathcal{H}$, donc j est bien définie et est une forme modulaire de poids 0.

* La fonction Δ ne s'annule jamais sur $\mathcal{H}$ donc j est holomorphe sur $\mathcal{H}$ en tant que quotient de deux fonctions holomorphes sur $\mathcal{H}$ dont le dénominateur ne s'annule jamais. De plus, g_4 est non nulle à l'infini alors que Δ a un zéro simple (par le théorème 3) à l'infini, donc j possède un pôle simple à l'infini.

* Pour obtenir le dernier point, il faut voir que, si $\lambda \in \mathbb{C}$, la forme modulaire $f_\lambda = 1728g_4^3 - \lambda\Delta$ a un zéro et un seul modulo G (puisque $j(z) = \infty$ si, et seulement si, z est équivalent au point à l'infini modulo G grâce au point précédent). Pour cela, on applique la formule (2.13) avec $f = f_\lambda$ et $k = 12$.
Les seules décompositions de $k = 12$ sous la forme $12n_1 + 6n_2 + 4n_3$ avec $n_1, n_2, n_3 \in \mathbb{N}^*$ correspondent $(1, 0, 0)$, $(0, 2, 0)$ et $(0, 0, 3)$. Cela entraîne bien que f_λ s'annule en un point et un seul de $\mathcal{H}/G$.

■

Remarque :
Autrement dit, la fonction j est une application surjective qui donne une bijection entre les classes d'isomorphismes des courbes elliptiques sur $\mathbb{C}$ et les nombres complexes.

Proposition 15 :
Soit f une fonction méromorphe sur $\mathcal{H}$.
Les assertions suivantes sont équivalentes :

* f est une fonction modulaire de poids 0.
* f est le quotient de deux formes modulaires de même poids.
* f est une fonction rationnelle de j.

Preuve :
Pour montrer la proposition, il suffit de montrer que si f est une fonction modulaire de poids 0, alors f est une fonction rationnelle de j (en effet, les implications *iii)* $\Longrightarrow$ *ii)* $\Longrightarrow$ *i)* sont immédiates).

Soit f une fonction modulaire de poids 0.
Puisque j a pour image $\mathbb{C}$ tout entier (par le troisième point de la proposition 14), après multiplication (si

nécessaire) de f par un polynôme en j, on peut supposer que f est holomorphe sur $\mathcal{H}$. De plus, comme Δ s'annule à l'infini, il existe un entier $n \in \mathbb{N}$ tel que $g = \Delta^n f$ soit holomorphe à l'infini. La fonction g est alors une forme modulaire de poids $12n$ et d'après le théorème 5 on peut l'écrire comme combinaison linéaire des $G_4^a G_6^b$ avec a et b des entiers naturels non nuls tels que $4a + 6b = 12n$. Par linéarité, on est ramené au cas où $g = G_4^a G_6^b$,c'est-à-dire $f = \dfrac{G_4^a G_6^b}{\Delta^n}$.

Or, la relation $4a + 6b = 12n$ (soit $2a + 3b = 6n$) montre que $p = \dfrac{a}{3}$ et $q = \dfrac{b}{2}$ sont des entiers (par le lemme de Gauss) et on a alors $f = \dfrac{G_4^{3p} G_6^{2q}}{\Delta^{p+q}}$. On est donc ramené à voir que $\dfrac{G_4^3}{\Delta}$ et $\dfrac{G_6^2}{\Delta}$ sont des fonctions rationnelles en j, ce qui est bien le cas puisque :

$$\frac{G_4^3}{\Delta} = \frac{1}{1\ 728 \times 60^3} j$$

et

$$\frac{G_6^2}{\Delta} = \frac{1}{140^2} \times \frac{g_6^2}{\Delta} = \frac{1}{140^2} \times \frac{g_4^3 - (2\pi)^{12}\Delta}{27\Delta} = \frac{1}{140^2 \times 27} \times \left(\frac{j}{1\ 728} - (2\pi)^{12} \right) = \frac{j - (2\pi)^{12} \times 1\ 728}{24 \times 1\ 728 \times 140^2}.$$

■

Remarque :
Le coefficient $1728 = 2^6 \times 3^3$ a été introduit pour que j ait un résidu égal à 1 à l'infini.

V.3.3 Le q-développement de Δ

Rappelons que l'on a :

$$\forall z \in \mathcal{H}^*,\ \Delta(z) = \frac{D(z)}{(2\pi)^{12}} = \frac{g_4^3(z) - 27 g_6^2(z)}{(2\pi)^{12}} = 8\ 000 E_4^3(z) - 147 E_6^2(z).$$

Théorème 6 : Formule du produit de Jacobi pour Δ :
Pour tout $z \in \mathcal{H}^*$, on a :

$$\Delta(z) = q \prod_{n=1}^{+\infty} (1 - q^n)^{24}$$

Preuve :
Considérons la fonction :

$$F : \left| \begin{array}{ccc} \mathcal{H}^* & \longrightarrow & \mathbb{C} \\ z & \longmapsto & q \displaystyle\prod_{n=1}^{+\infty} (1 - q^n)^{24} \end{array} \right.$$

La fonction F est bien définie car pour tout $z \in \mathcal{H}^*$ on a l'équivalence :

$$F(z) \text{ existe} \iff q \prod_{n \in \mathbb{N}^*} (1 - q^n)^{24} \text{ converge} \iff \prod_{n \in \mathbb{N}^*} (1 - q^n)^{24} \text{ converge}$$
$$\iff \sum_{n \in \mathbb{N}^*} \ln\left((1 - q^n)^{24} \right) \text{ converge} \iff \sum_{n \in \mathbb{N}^*} \ln(1 - q^n) \text{ converge}$$

Or, on a $\ln(1 - q^n) \underset{n \to +\infty}{\sim} q^n$ et puisque $|q| < 1$ on en déduit la convergence absolue de la série $\displaystyle\sum_{n \in \mathbb{N}^*} q^n$. Ainsi la série $\displaystyle\sum_{n \in \mathbb{N}^*} \ln(1 - q^n)$ converge et donc F est bien définie.

Pour montrer le résultat, il nous suffit de montrer F est une forme modulaire de poids 12. En effet, le fait que le q-développement de F ait un terme constant nul montrera que F est parabolique et puisque S_{12} est de dimension 1 (par le corollaire 3) on aura que Δ et F sont proportionnelles et puisque le coefficient devant q dans les deux q-développements est égal à 1, on aura même l'égalité entre Δ et F.

Or on sait déjà que F est holomorphe sur $\mathcal{H}^*$. En effet, en posant $f_n : z \longmapsto (1-q^n)^{24}$, on a que la série $\sum_{n\geq 1} |f_n|$ converge uniformément sur tout compact de $\mathcal{H}$ (car elle converge même normalement sur tout compact de $\mathcal{H}$) et donc F est holomorphe sur $\mathcal{H}$ (et son q-développement nous donne l'holomorphie à l'infini).

Il nous suffit donc de montrer que F est une fonction faiblement modulaire et comme on sait déjà que Δ est 1-périodique (car q l'est grâce à l'exponentielle complexe), donc il nous suffit même d'après la proposition 1 de montrer que :

$$\forall z \in \mathcal{H},\ F\left(-\frac{1}{z}\right) = z^{12}F(z). \tag{2.14}$$

Notons que la fonction F ne s'annule pas sur $\mathcal{H}$ et on peut donc poser la fonction g définie sur $\mathcal{H}$ par

$$g(z) = \frac{F\left(-\frac{1}{z}\right)}{z^{12}F(z)}.$$

On veut alors montrer que g est constante et égale à 1. Pour cela, il suffit de montrer que g est constante puisque l'on a $g(i) = 1$. Notons aussi que la dérivée logarithmique de g s'exprime facilement à partir de celle de Δ :

$$\forall z \in \mathcal{H},\ \frac{g'(z)}{g(z)} = \frac{\Delta'\left(-\frac{1}{z}\right)}{z^2\Delta\left(-\frac{1}{z}\right)} - \frac{12}{z} - \frac{\Delta'(z)}{\Delta(z)}$$

et en utilisant le développement en série entière de la fonction $x \longmapsto \dfrac{1}{1-x}$, on a :

$$\frac{\Delta'(z)}{\Delta(z)} = 2i\pi\left(1 - 24\sum_{n=1}^{+\infty}\frac{nq^n}{1-q^n}\right) = 2i\pi\left(1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right).$$

Pour simplifier un peu les formules, on notera $\sum'$ pour signifier que l'on fait la somme sur les paires $(c,d) \in \mathbb{Z}^2\setminus\{(0,0)\}$ (afin que la division par $cz+d$ ait un sens).

On va voir que l'on peut définir pour $z \in \mathcal{H}$:

$$G_2(z) = \sum_{c\in\mathbb{Z}}\left(\sum_{d\in\mathbb{Z}}{}'\frac{1}{(cz+d)^2}\right)$$

en tant que série convergente (mais pas absolument convergente !) et que l'on a

$$G_2(z) = \frac{\pi^2}{3}\left(1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right)$$

ce qui fait que l'annulation de $\dfrac{g'}{g}$ revient finalement à montrer que :

$$\forall z \in \mathcal{H},\ G_2\left(-\frac{1}{z}\right) = z^2G_2(z) - 2i\pi z. \tag{2.15}$$

Pour montrer le théorème, il nous suffit donc de montrer la relation (2.15) En reprenant le début de la preuve de la proposition 10 on a que pour tout $c \in \mathbb{Z}^*$:

$$\forall z \in \mathcal{H},\ \sum_{d=-\infty}^{+\infty}\frac{1}{(cz+d)^2} = -4\pi^2\sum_{d=1}^{+\infty}dq^{|c|d}.$$

D'autre part, on a :

$$\sum_{c=-\infty}^{+\infty}\sum_{d=1}^{+\infty}nq^{|c|n} = 2\sum_{c=1}^{+\infty}\sum_{d=1}^{+\infty}nq^{cn} = 2\sum_{n=1}^{+\infty}\sigma_1(n)q^n$$

toute série manipulée ci-dessus étant convergente. Cela nous montre alors que :

$$\forall z \in \mathcal{H},\ G_2(z) = \sum_{d\in\mathbb{Z}^*} \frac{1}{d^2} + \sum_{c\in\mathbb{Z}^*}\sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^2} = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{+\infty} \sigma_1(n) q^n = \frac{\pi^2}{3}\left(1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right)$$

Montrons enfin la relation (2.15) :

On "régularise" G_2 en remarquant que pour tout $c \in \mathbb{Z}^*$ on a $\displaystyle\sum_{d=-\infty}^{+\infty} \frac{1}{(cz+d)(cz+d+1)} = 0$ car c'est une série télescopique grâce à la formule :

$$\forall z \in \mathcal{H},\ \forall (c,d) \in \mathbb{Z}^2\backslash\{(0,0)\},\ \frac{1}{(cz+d)(cz+d+1)} = \frac{1}{cz+d} - \frac{1}{cz+d+1}.$$

Donc :

$$\begin{aligned}\forall z \in \mathcal{H},\ G_2(z) &= \sum_{d\in\mathbb{Z}^*}\frac{1}{d^2} + \sum_{c\in\mathbb{Z}^*}\left(\sum_{d\in\mathbb{Z}}{}' \frac{1}{(cz+d)^2} - \sum_{d\in\mathbb{Z}}{}' \frac{1}{(cz+d)(cz+d+1)}\right)\\ &= \sum_{d\in\mathbb{Z}^*}\frac{1}{d^2} + \sum_{c\in\mathbb{Z}^*}\sum_{d\in\mathbb{Z}}{}' \frac{1}{(cz+d)^2(cz+d+1)} = \sum_{d\in\mathbb{Z}^*}\frac{1}{d^2} + \sum_{d\in\mathbb{Z}}\sum_{c\in\mathbb{Z}^*}{}' \frac{1}{(cz+d)^2(cz+d+1)}\end{aligned}$$

la dernière interversion étant justifiée par la convergence absolue de la somme.

Ensuite, on a :

$$\begin{aligned}\forall z \in \mathcal{H},\ \frac{1}{z^2}G_2\left(-\frac{1}{z}\right) &= \sum_{c\in\mathbb{Z}}\left(\sum_{d\in\mathbb{Z}}{}' \frac{1}{(dz-c)^2}\right) = \sum_{c\in\mathbb{Z}}\left(\sum_{d\in\mathbb{Z}}{}' \frac{1}{(dz+c)^2}\right)\\ &= \sum_{c\in\mathbb{Z}^*}\frac{1}{c^2} + \sum_{d\in\mathbb{Z}}\sum_{c\in\mathbb{Z}^*}{}' \frac{1}{(cz+d)^2}\end{aligned}$$

On a alors en utilisant la même identité qu'au tout début de la preuve de la proposition 10 (appelée **identité d'Euler**), on a :

$$\begin{aligned}\forall z \in \mathcal{H},\ \frac{1}{z^2}G_2\left(-\frac{1}{z}\right) - G_2(z) &= \sum_{d\in\mathbb{Z}}\left(\sum_{c\in\mathbb{Z}^*}{}'\left(\frac{1}{(cz+d)^2} - \frac{1}{(cz+d)^2(cz+d+1)}\right)\right)\\ &= \sum_{d\in\mathbb{Z}}\sum_{c\in\mathbb{Z}^*}{}' \frac{1}{(cz+d)(cz+d+1)} = \lim_{N\to+\infty}\sum_{d=-N}^{N-1}\left(\sum_{c\in\mathbb{Z}^*}{}'\left(\frac{1}{cz+d} - \frac{1}{cz+d+1}\right)\right)\\ &= \lim_{N\to+\infty}\sum_{c\in\mathbb{Z}^*}{}'\left(\frac{1}{cz-N} - \frac{1}{cz+N}\right) = \lim_{N\to+\infty} -\frac{2}{z}\sum_{c=1}^{+\infty}\left(\frac{1}{\frac{N}{z}-c} + \frac{1}{\frac{N}{z}+c}\right)\\ &= \lim_{N\to+\infty} -\frac{2}{z}\left(\pi\cot\left(\frac{\pi N}{z}\right) - \frac{z}{N}\right) = \lim_{N\to+\infty} -\frac{2i\pi}{z}\frac{e^{i\pi\frac{N}{z}}+1}{e^{i\pi\frac{N}{z}}-1}\\ &= \lim_{N\to+\infty} -\frac{2i\pi}{z}\left(1 - \frac{2}{e^{i\pi\frac{N}{z}}-1}\right) = -\frac{2i\pi}{z}\end{aligned}$$

On a ainsi démontré la relation (2.15), ce qui permet de conclure grâce aux remarques préliminaires.

■

Remarque :

L'expression $1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n$ dans la preuve précédente ressemble drôlement au q-développement d'une hypothétique série d'Eisenstein G_2, qui n'existe pas vraiment en tant que forme modulaire... De plus, notons que cette fonction G_2 est nettement plus délicate que les G_4, G_6, etc. à cause de l'absence de convergence absolue des séries utilisées.

Grâce à cette expression de Δ, on obtient les premiers termes de son q-développement :

$$\forall z \in \mathcal{H}^*,\ \Delta(z) = q - 24q^2 + 252q^3 - 1\ 472q^4 + ...$$

Nous étudierons plus en détail les coefficients du q-développement de la forme parabolique Δ dans le chapitre suivant.

On peut alors obtenir le début du q-développement de j dans un voisinage de 0 assez petit :

$$j(z) = \frac{1}{q} + 744 + 196\ 884q + 21\ 473\ 760q^2 + ... = \frac{1}{q} + 744 + \sum_{n=1}^{+\infty} c(n)q^n$$

et on retrouve le fait que j a un pôle simple à l'infini de résidu égal à 1.

Remarques :

* Les coefficients $c(n)$ sont des entiers et jouissent de remarquables propriétés de divisibilité (grâce au fait qu'ils proviennent des coefficients du q-développement de Δ qui eux-mêmes vérifient des relations arithmétiques très intéressantes), par exemple :

$$\begin{aligned}
n \equiv 0\ [2^a] &\implies c(n) \equiv 0\ \left[2^{3a+8}\right] \\
n \equiv 0\ [3^a] &\implies c(n) \equiv 0\ \left[3^{2a+3}\right] \\
n \equiv 0\ [5^a] &\implies c(n) \equiv 0\ \left[5^{a+1}\right] \\
n \equiv 0\ [7^a] &\implies c(n) \equiv 0\ [7^a] \\
n \equiv 0\ [11^a] &\implies c(n) \equiv 0\ [11^a]
\end{aligned}$$

* Hans Petersson (et plus tard Hans Rademacher de manière indépendante) a montré la formule asymptotique :

$$c(n) \underset{n\to+\infty}{\sim} \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{\frac{3}{4}}}$$

* Dans la preuve précédente, on a montré que $\dfrac{\Delta'}{\Delta} = -48i\pi G_2$, donc en utilisant les q-développements, on obtient par unicité des coefficients que :

$$\forall n \in \mathbb{N}^*,\ \tau(n) = \frac{-24}{n-1}\sum_{k=1}^{n-1}\tau(k)\sigma_1(n-k)$$

VI Base de Miller

Dans cette dernière partie on donne une autre base que celle donnée par le théorème 5 qui nous sera utile pour donner la matrice des opérateurs de Hecke dans le prochain chapitre.

Lemme 2 : Lemme de Miller :
Soient $k \in \mathbb{N}$ et $d = \dim_{\mathbb{C}}(S_k)$.
L'espace S_k admet une base $(f_1, ..., f_d)$ telle que, en notant $a_i(f_j)$ le i-ième coefficient du q-développement de la forme parabolique f_j, on ait :

$$\forall i, j \in [\![1; d]\!],\ a_i(f_j) = \delta_{i,j}$$

De plus, chaque f_j appartient à $\mathbb{Z}[[q]]$.

Preuve :
Soient $k \in \mathbb{N}$ et $d = \dim_{\mathbb{C}}(S_k)$.
Pour tous $i, j \in [\![1; d]\!]$, on note $a_i(f_j)$ le i-ième coefficient du q-développement de la forme parabolique f_j.

Puisque $b_4 = \dfrac{-1}{30}$ et $b_6 = \dfrac{1}{42}$, on pose :

$$F_4 = -\frac{8}{b_4}E_4 = 1 + 240q + 2\ 160q^2 + 6\ 720q^3 + 17\ 520q^4 + ...$$

et

$$F_6 = \frac{-12}{b_6}E_6 = 1 - 504q - 16\ 632q^2 - 122\ 976q^3 - 532\ 728q^4 + ...$$

On remarque alors que F_4 et F_6 ont des coefficients constants égaux à 1 dans leur q-développements et appartiennent à $\mathbb{Z}[[q]]$ (par la définition de E_k et la renormalisation associée).

Choisissons désormais des entiers $a, b \geq 0$ tels que $4a + 6b \leq 14$ et $4a + 6b \equiv k\ [12]$ et posons :

$$\forall j \in [\![1; d]\!],\ g_j = \Delta^j F_6^{2(d-j)+b} F_4^a = \left(\frac{\Delta}{F_6^2}\right)^j F_6^{2d+b} F_4^a.$$

Puisque le coefficient constant du q-développement de Δ est nul et que le coefficient devant q dans son q-développement est égal à 1, on obtient que le premier coefficient non nul du q-développement d'un g_j est le coefficient devant q^j dans son q-développement et il vaut $1 \times 1 \times 1 = 1$. On a donc :

$$\forall j \in [\![1; d]\!],\ \forall i \in [\![1; j-1]\!],\ a_i(g_j) = \delta_{i,j}.$$

Ainsi, les g_j sont linéairement indépendants sur $\mathbb{C}$ et donc forment une base de S_k. De plus, puisque Δ, F_4 et F_6 appartiennent à $Z[[q]]$, il en est de même des g_j.

Finalement, on obtient les formes modulaires f_j à partir des g_j en appliquant la méthode d'élimination de Gauss et elles appartiennent encore à $\mathbb{Z}[[q]]$ car à chaque fois que l'on nettoie une colonne on utilise les g_j dont le coefficient constant est égal à 1 (donc aucun dénominateur est introduit).

■

Remarque :
La démonstration précédente fait apparaître la base duale de S_k via les applications $a_i : f_j \longmapsto \delta_{i,j}$.

Définition 14 : Base de Miller :
On considère $k \in \mathbb{N}$ et $d = \dim_{\mathbb{C}}(S_k)$.
La base $(f_1, ..., f_d)$ de S_k du lemme précédent est appelée **base de Miller de** S_k.

Remarque :
La base du lemme de Miller est "canonique" puisqu'il s'agit de la forme échelonnée réduite d'une base de S_k. De plus, l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ des éléments des bases de Miller sont exactement les formes modulaires de niveau 1 avec des q-développements dans $\mathbb{Z}[[q]]$.

Nous étendons désormais la base de Miller à l'espace M_k en prenant un multiple de G_k dont le terme constant de son q-développement vaut 1 et en soustrayant les f_i de la base de Miller de S_k de sorte à ce que les coefficients devant q, q^2, ..., q^d dans le q-développement résultant sont 0. L'élément supplémentaire obtenu est alors noté f_0.

Exemple 9 :
Cherchons la base de Miller de l'espace S_{24}.
On sait que $d = \dim_{\mathbb{C}} S_{24} = 2$ et puisque $k \equiv 0$ [12], on pose $a = b = 0$. On trouve alors :

$$g_1 = \Delta F_6^2 = q - 1\ 032q^2 + 245\ 196q^3 + 10\ 965\ 568q^4 + 60\ 177\ 390q^5 - ...$$

et

$$g_2 = \Delta^2 = q^2 - 48q^3 + 1\ 080q^4 - 15\ 040q^5 + ...$$

On pose alors :

$$\begin{cases} f_2 = & g_2 \\ f_1 = & g_1 + 1\ 032g_2 = q + 195\ 660q^2 + 12\ 080\ 128q^4 + 44\ 656\ 110q^5 - ... \end{cases}$$

La base de Miller de S_{24} est alors (f_1, f_2).

Exemple 10 :
Cherchons la base de Miller de l'espace M_{36}.
On sait que $d = \dim_{\mathbb{C}} S_{36} = 3$ (par le corollaire 3) et puisque $k \equiv 0$ [12], on pose $a = b = 0$. Suivant le même principe que l'exemple précédent, on a alors :

$$\begin{array}{lllll} f_1 = & q+ & & 57\ 093\ 088q^4+ & 37\ 927\ 345\ 230q^5 + ... \\ f_2 = & & q^2+ & 194\ 184q^4+ & 7\ 442\ 432q^5 + ... \\ f_3 = & & q^3- & 72q^4+ & 2\ 484q^5 + ... \end{array}$$

On peut alors trouver $f_0 = 1 + 6\ 218\ 175\ 600q^4 + 15\ 281\ 788\ 354\ 560q^5$ et ainsi la base (f_0, f_1, f_2, f_3) est la base de Miller de M_{36}.

Remarques :

* Pour écrire $f \in M_k$ comme un polynôme en E_4 et E_6, c'est une perte de temps de calculer la base de Miller. À la place, on peut utiliser la base échelonnée (mais pas réduite !) $\left(\Delta^j F_6^{2(d-j)+b} F_4^a\right)_{j \in [\![0;d]\!]}$ et d'identifier les coefficients du q-développement de q^0 jusqu'à q^d.
* Il est possible d'obtenir la base de Miller via `SAGE` grâce à la commande `victor_miller_basis` :

```
sage: victor_miller_basis(28,5)
[
1 + 15590400*q^3 + 36957286800*q^4 + O(q^5),
q + 151740*q^3 + 61032448*q^4 + O(q^5),
q^2 + 192*q^3 - 8280*q^4 + O(q^5),
]
```

Chapitre 3

Opérateurs de Hecke et applications

Dans ce troisième chapitre, nous introduisons les opérateurs de Hecke (tout d'abord sur les réseaux puis sur les formes modulaires). Nous commencerons par donner quelques définitions et propriétés sur ces opérateurs afin de s'intéresser dans un deuxième temps à leur action sur les formes modulaires. Dans une troisième partie nous parlerons des vecteurs propres des opérateurs de Hecke et nous investirons ces résultats dans une quatrième partie en montrant que les séries d'Eisenstein sont des vecteurs propres des opérateurs de Hecke puis en donnant des résultats sur les coefficients du q-développement de la forme modulaire Δ. Finalement, nous terminerons ce chapitre par quelques compléments avec l'introduction du produit scalaire de Petersson, quelques propriétés d'intégralité et enfin en parlant rapidement de la conjecture de Ramanujan-Petersson.

I Définition et premières propriétés

I.1 Notion de correspondance sur un ensemble

Nous commençons par introduire la notion de correspondance sur un ensemble qui nous sera utile pour définir les opérateurs de Hecke.

On considère E un ensemble non vide et X_E le groupe abélien libre engendré par E.

Définition 1 : Correspondance sur un ensemble :
On appelle **correspondance sur** E (à coefficients entiers) tout endomorphisme T de X_E.

Remarque :
On peut se donner T par ses valeurs sur les éléments x de E :

$$\forall x \in E,\ T(x) = \sum_{y \in E} n_y(x) y \tag{3.1}$$

avec les $n_y(x)$ qui sont des éléments de $\mathbb{Z}$ et presque tous nuls.

I.2 Définition des T_n

Considérons désormais $\mathcal{R}$ l'ensemble des réseaux de $\mathbb{C}$ et n un entier naturel non nul.

Définition 2 : Opérateur de Hecke (pour un réseau) :
On considère $n \in \mathbb{N}^*$.
On note T_n la correspondance sur $\mathcal{R}$ qui transforme un réseau en la somme (dans $X_{\mathcal{R}}$) de ses sous-réseaux d'indice n et on l'appelle n**-ième opérateur de Hecke**.

On a alors :

$$\forall \Gamma \in \mathcal{R},\ T_n([\Gamma]) = \sum_{\substack{\Gamma' \subset \Gamma \\ [\Gamma:\Gamma']=n}} [\Gamma']. \tag{3.2}$$

Remarques :

* La notation "$[\Gamma]$" est introduite pour appuyer le fait que dans la formule (3.2) on a une somme formelle.
* La somme du deuxième membre est finie. En effet, la condition $((\Gamma' \subseteq \Gamma)$ et $([\Gamma : \Gamma'] = n))$ est équivalente à la condition $n\Gamma \subseteq \Gamma' \subseteq \Gamma$ (on remarque cela en constatant que pour tout $\gamma \in \Gamma$, $n\overline{\gamma} = \overline{n\gamma} = \overline{0}$ d'où $n\gamma \in \Gamma'$). Or, cette dernière condition est équivalente à Γ' est un sous-groupe de $\Gamma/n\Gamma$ et on a $\Gamma = a\,\mathbb{Z} \oplus b\,\mathbb{Z}$ (comme c'est un réseau de $\mathbb{C}$) et donc $\Gamma/n\Gamma \cong \mathbb{Z}/n\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z}$. Ainsi, le nombre d'indices dans la somme est égal au nombre de sous-groupes de $\Gamma/n\Gamma = (\mathbb{Z}/n\mathbb{Z})^2$.

Nous utiliserons également les opérateurs d'homothétie R_λ définis pour $\lambda \in \mathbb{C}^*$ par :

$$R_\lambda : \left| \begin{array}{ccc} \mathcal{R} & \longrightarrow & \mathcal{R} \\ [\Gamma] & \longmapsto & [\lambda\Gamma] \end{array} \right.$$

Remarque :

On peut composer les correspondances T_n et R_λ entre elles, puisqu'elles sont toutes les deux des endomorphismes du groupe abélien $X_{\mathcal{R}}$.

Proposition 1 :

Les correspondances T_n et R_λ vérifient les identités :

* $\forall \lambda, \mu \in \mathbb{C}^*,\ R_\lambda \circ R_\mu = R_{\lambda\mu}$.
* $\forall n \in \mathbb{N}^*,\ \forall \lambda \in \mathbb{C}^*,\ R_\lambda \circ T_n = T_n \circ R_\lambda$.
* Si m, n sont deux entiers naturels non nuls et premiers entre eux, alors $T_m \circ T_n = T_{mn}$.
* $\forall p \in \mathcal{P},\ \forall n \in \mathbb{N}^*,\ T_p \circ T_{p^n} = T_{p^{n+1}} + pR_p \circ T_{p^{n-1}}$.

Preuve :

* Soient $\lambda, \mu \in \mathbb{C}^*$.
  Pour tout $\Gamma \in \mathcal{R}$, on a :

$$(R_\lambda \circ R_\mu)([\Gamma]) = R_\lambda(R_\mu([\Gamma])) = R_\lambda([\mu\Gamma]) = [(\lambda\mu)\Gamma] = R_{\lambda\mu}([\Gamma]).$$

  D'où $R_\lambda \circ R_\mu = R_{\lambda\mu}$.

* Soient $n \in \mathbb{N}^*$ et $\lambda \in \mathbb{C}^*$.
  Pour tout $\Gamma \in \mathcal{R}$, on a :

$$T_n \circ R_\lambda([\Gamma]) = T_n([\lambda\Gamma]) = \sum_{\substack{\Gamma' \subseteq \lambda\Gamma \\ [\lambda\Gamma : \Gamma'] = n}} [\Gamma']$$

  D'autre part :

$$R_\lambda \circ T_n([\Gamma]) = R_\lambda \left(\sum_{\substack{\Gamma' \subseteq \Gamma \\ [\Gamma : \Gamma'] = n}} [\Gamma'] \right) = \sum_{\substack{\Gamma' \subseteq \Gamma \\ [\Gamma : \Gamma'] = n}} [\lambda\Gamma']$$

  Or, en posant $\Gamma'' = \lambda\Gamma$, on obtient que les réseaux Γ' et Γ'' sont homothétiques, donc $[\Gamma : \Gamma'] = [\lambda\Gamma : \lambda\Gamma'] = [\lambda\Gamma : \Gamma'']$. Ainsi, on a :

$$R_\lambda \circ T_n([\Gamma]) = \sum_{\substack{\Gamma'' \subseteq \lambda\Gamma \\ [\lambda\Gamma : \Gamma''] = n}} [\Gamma''].$$

  D'où $R_\lambda \circ T_n = T_n \circ R_\lambda$.

* Soient m, n deux entiers naturels non nuls et premiers entre eux.
  Ce point de la proposition est équivalent à l'assertion suivante :
  Si Γ'' est un sous-réseau d'un réseau Γ d'indice mn, alors il existe un unique sous-réseau Γ' de Γ contenant Γ'' tel que $[\Gamma : \Gamma'] = n$ et $[\Gamma' : \Gamma''] = m$.

Or, la véracité cette assertion résulte du fait que le groupe Γ/Γ'', qui est un groupe abélien fini d'ordre mn, se décompose de façon unique en somme directe d'un groupe d'ordre m et d'un groupe d'ordre n (ce qui est assuré par le théorème des restes chinois).

∗ Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.
Pour tout $\Gamma \in \mathcal{R}$, on a $(T_p \circ T_{p^n})([\Gamma]) = \sum_{(\Gamma'',\Gamma')} [\Gamma'']$, la somme portant sur les couples (Γ'', Γ') avec Γ'' d'indice p dans Γ' et Γ' d'indice p^n dans Γ (en particulier, Γ'' est d'indice p^{n+1} dans Γ).

Soit Γ'' un sous-réseau quelconque d'indice p^{n+1} dans Γ. On est dans un, et un seul, des cas suivants :

— $\Gamma'' \subseteq p\Gamma$ (c'est-à-dire $\frac{1}{p}\Gamma'' \subseteq \Gamma$). Dans ce cas, il y a exactement $p+1$ sous groupes Γ' de Γ'' dans lequel Γ'' est d'indice p : ces sous-groupes sont en bijection avec les droites sur le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\frac{1}{p}\Gamma''/\Gamma'' \cong (\mathbb{Z}/p\mathbb{Z})^2$.

— $\Gamma'' \subsetneq p\Gamma$. Dans ce cas, on a $\Gamma/\Gamma'' \cong \mathbb{Z}/(p^{n+1})\mathbb{Z}$, et il y a donc un unique sous-groupe Γ' de Γ dans lequel Γ'' est d'indice p.

On a donc :

$$(T_p \circ T_{p^n})([\Gamma]) = (p+1) \sum_{\substack{\Gamma'' \subseteq p\Gamma \\ [\Gamma:\Gamma'']=p^{n+1}}} [\Gamma''] + \sum_{\substack{\Gamma'' \subsetneq p\Gamma \\ [\Gamma:\Gamma'']=p^{n+1}}} [\Gamma''] = p \sum_{\substack{\Gamma'' \subseteq p\Gamma \\ [\Gamma:\Gamma'']=p^{n+1}}} [\Gamma''] + \sum_{\substack{\Gamma'' \subseteq \Gamma \\ [\Gamma:\Gamma'']=p^{n+1}}} [\Gamma'']$$

Enfin, si Γ'' est dans $p\Gamma$, alors il est d'indice p^{n+1} dans Γ si, et seulement si, il est d'indice p^{n-1} dans $p\Gamma$.
Ainsi, on a démontré, après réécriture des sommes, que :

$$T_p \circ T_{p^n} = T_{p^{n+1}} + pR_p \circ T_{p^{n-1}}$$

■

Remarque :
D'après le deuxième point de la proposition précédente, le quatrième point de cette propriété est équivalent à :

$$\forall p \in \mathcal{P},\ \forall n \in \mathbb{N}^*,\ T_p \circ T_{p^n} = T_{p^{n+1}} + pT_{p^{n-1}} \circ R_p$$

Corollaire 1 :
Soit $n \in \mathbb{N}^*$.
Les T_{p^n} sont des polynômes en T_p et R_p.

Preuve :
Soit $p \in \mathcal{P}$.
Montrons par récurrence double sur $n \in \mathbb{N}^*$ que T_{p^n} est un polynôme en T_p et R_p.

∗ Initialisation :
Pour $n = 1$, on a directement que $T_{p^1} = T_p$, donc c'est bien un polynôme en T_p et R_p.
Pour $n = 2$, grâce à la dernière relation de la proposition 1, on a $T_{p^2} = T_p \circ T_p - pT_p \circ R_p$ (qui est également bien un polynôme en T_p et R_p).
L'initialisation est donc bien vérifiée.

∗ Hérédité :
Supposons que pour un $n \in \mathbb{N}^*$ donné on ait $T_{p^{n-1}}$ et T_{p^n} qui soient un polynôme en T_p et R_p. Montrons que $T_{p^{n+1}}$ en est également un :
Par la dernière relation de la proposition 1, on a :

$$T_{p^{n+1}} = T_{p^n} \circ T_p - pT_{p^{n-1}} \circ R_p \tag{3.3}$$

Or, par hypothèse, $T_{p^{n-1}}$ et T_{p^n} sont des polynômes en T_p et R_p, donc $T_{p^{n+1}}$ aussi par la relation (3.3). Ainsi la propriété est bien héréditaire.

Finalement, on a donc démontré la propriété par récurrence double sur $n \in \mathbb{N}^*$.

■

Corollaire 2 :
L'algèbre engendrée par les R_λ et les T_p est commutative et elle contient tous les opérateurs de Hecke T_n.

Preuve :

* L'algèbre engendré par les R_λ et T_p contient tous les opérateurs de Hecke T_n (avec $n \in \mathbb{N}^*$) d'après le troisième point de la proposition 1 et le corollaire 1.

* De plus, cette même algèbre est commutative puisque les R_λ commutent entre eux, les T_n commutent entre eux et enfin les R_λ et T_n commutent également entre eux (d'après les trois premiers points de la proposition 1).

■

I.3 Action des T_n sur les fonctions de poids k

On considère une fonction F de poids k sur l'ensemble des réseaux (cf. II du chapitre 2).

Par définition, on a :

$$\forall \lambda \in \mathbb{C}^*,\ R_\lambda(F) = \lambda^{-k} F$$

De plus, pour tout entier naturel $n \geq 1$, par le deuxième point de la proposition 1, on a :

$$\forall \lambda \in \mathbb{C}^*,\ R_\lambda(T_n(F)) = T_n(R_\lambda(F)) = \lambda^{-k} T_n(F)$$

c'est-à-dire que $T_n(F)$ est aussi de poids k.

De plus, les deux derniers points de la même proposition nous donnent que :

$$\forall m, n \in \mathbb{N}^*,\ (\mathrm{PGCD}(m,n) = 1) \implies ((T_m \circ T_n)(F) = T_{mn}(F)) \tag{3.4}$$

$$\forall p \in \mathcal{P},\ \forall n \in \mathbb{N}^*,\ (T_p \circ T_{p^n})(F) = T_{p^{n+1}}(F) + p^{1-k} T_{p^{n-1}}(F) \tag{3.5}$$

I.4 Un lemme matriciel

On considère Γ un réseau de $\mathbb{C}$ de base (ω_1, ω_2), n un entier naturel non nul et on note :

$$X_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) \mid a \geq 1,\ ad = n,\ 0 \leq b < d \right\}$$

Le lemme suivant nous donne un moyen de construire tous les sous-réseaux de Γ d'indice n :

Lemme 1 :
Soit Γ_σ le sous-réseau de Γ ayant pour base (ω_1', ω_2') avec $\omega_1' = a\omega_1 + b\omega_2$ et $\omega_2' = d\omega_2$.
L'application $\Psi : \sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \longmapsto \Gamma_\sigma$ est une bijection de X_n sur l'ensemble $\Gamma(n)$ des sous-réseaux d'indice n de Γ.

Preuve :
Soit Γ_σ le sous-réseau de Γ ayant pour base (ω_1', ω_2') avec $\omega_1' = a\omega_1 + b\omega_2$ et $\omega_2' = d\omega_2$.
Considérons l'application $\Psi : \sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \longmapsto \Gamma_\sigma$ de X_n sur l'ensemble $\Gamma(n)$ des sous-réseaux d'indice n de Γ.

* Le fait que Ψ est bien définie provient du fait que $ad = n$.

* Réciproquement, considérons $\Gamma' \in \Gamma(n)$ et posons :

$$Y_1 = \Gamma / (\Gamma' + \mathbb{Z}\,\omega_2) \text{ et } Y_2 = \mathbb{Z}\,\omega_2 / (\Gamma' \cap \mathbb{Z}\,\omega_2).$$

Le groupe Y_1 est cyclique (car monogène et fini) et engendré par l'image de ω_1. En effet :
— Tout élément $y \in Y_1$ s'écrit de la forme $\overline{m\omega_1 + n\omega_2}$ et comme on effectue le quotient par $\Gamma' + \mathbb{Z}\,\omega_2$, on a :
$$y = \overline{m\omega_1 + n\omega_2} = \overline{m\omega_1} = m\overline{\omega_1}$$
et donc $\overline{\omega_1}$ engednre Y_1.
— De plus, on a $[\Gamma : \Gamma'] = n$, donc $n\Gamma \subseteq \Gamma' \subseteq \Gamma$. Et puisque $n\omega_1 \in n\Gamma \subseteq \Gamma'$, on a $n\overline{\omega_1} = \overline{0}$ et donc $o(\overline{\omega_1})$ divise n (donc en particulier est fini).

De même, le groupe Y_2 est cyclique et engendré par l'image de ω_2. En effet :
— Par définition de Y_2, on a directement que $\overline{\omega_2}$ engendre Y_2.
— De plus, on a $n\omega_2 \in n\Gamma \subseteq \Gamma'$ et $n\omega_2 \in \mathbb{Z}\,\omega_2$, donc $n\omega_2 \in \Gamma' \cap \mathbb{Z}\,\omega_2$ et ainsi $n\overline{\omega_2} = \overline{0}$. Donc $o(\overline{\omega_2})$ divise n (donc en particulier est fini).

Notons respectivement a et d l'ordre de $\overline{\omega_1}$ dans Y_1 et $\overline{\omega_2}$ dans Y_2.
On a la suite exacte :
$$0 \longrightarrow Y_2 \xrightarrow{\iota} \Gamma/\Gamma' \xrightarrow{\pi} Y_1 \longrightarrow 0$$

En effet, on a le diagramme
$$\begin{array}{ccc} \Gamma & \xrightarrow{p} & \Gamma/(\Gamma' + \mathbb{Z}\,\omega_2) \\ \downarrow{\scriptstyle \widetilde{p}} & \nearrow_{\pi} & \\ \Gamma/\Gamma' & & \end{array}$$

Or, on a $\ker(p) = \Gamma' + \mathbb{Z}\,\omega_2$ et $\Gamma' \subseteq \mathrm{Ker}(f)$. Finalement, comme p est surjective, on a par le théorème de factorisation que π l'est également. De même, on a le diagramme
$$\begin{array}{ccccc} \mathbb{Z}\,\omega_2 & \xrightarrow{i} & \Gamma & \twoheadrightarrow & \Gamma/\Gamma' \\ \downarrow{\scriptstyle p} & & \nearrow_{\iota} & & \\ \mathbb{Z}\,\omega_2/(\Gamma' \cap \mathbb{Z}\,\omega_2) & & & & \end{array}$$

Et par le théorème de factorisation, on obtient que ι est injective. Enfin, $\pi \circ \iota$ est nul par définition de Y_1 et Y_2. On peut ainsi dire par cardinalité que $ad = n$.

De plus, en posant $\omega_2' = d\omega_2$, on a $\omega_2' \in \Gamma'$ (car dans le groupe quotient Y_2 on a $d\overline{\omega_2} = 0$ donc $\overline{\omega_2'} = 0$ et ainsi $\omega_2' \in \Gamma' \cap \mathbb{Z}\,\omega_2 \subseteq \Gamma'$).

D'autre part, il existe $\omega_1' \in \Gamma'$ tel que $\omega_1' \equiv a\omega_1\ [\omega_2]$ (car $\overline{a\omega_1} = \overline{0}$ dans Y_1 c'est-à-dire $a\omega_1 \in \Gamma' + \mathbb{Z}\,\omega_2$). De plus (ω_1', ω_2') forme une base de Γ' (car $\mathbb{Z}\,\omega_1' \oplus \mathbb{Z}\,\omega_2'$ est d'indice $ad = n$ dans Γ, et il est contenu dans Γ' qui est lui-même d'indice n dans Γ d'où $\mathbb{Z}\,\omega_1' \oplus \mathbb{Z}\,\omega_2' = \Gamma'$) et on peut écrire ω_1' sous la forme

$$\omega_1' = a\omega_1 + b\omega_2,\ b \in \mathbb{Z}$$

avec b déterminé de façon unique modulo d.

Donc si l'on impose que $b \in [\![0; d-1]\!]$, alors ω_1' est déterminé de manière unique et la matrice $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ appartient à X_n.

* Par les deux points précédents, les applications suivantes sont bien définies :

$$\Psi : \left| \begin{array}{ccc} X_n & \longrightarrow & \Gamma(n) \\ \sigma & \longmapsto & \Gamma_\sigma \end{array} \right. \quad \text{et} \quad \Phi : \left| \begin{array}{ccc} \Gamma(n) & \longrightarrow & X_n \\ \Gamma' & \longmapsto & \sigma(\Gamma') \end{array} \right. .$$

De plus, par la définition de Γ_σ et le déroulement du deuxième point, on en déduit que les applications Ψ et Φ sont inverses l'une de l'autre. Ainsi, la fonction Ψ est bien bijective.

■

Exemple 1 :

Si p est un nombre premier, alors X_p se compose de la matrice $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ ainsi que des p matrices de la forme $\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$, avec $b \in [\![0; p-1]\!]$.

II L'action des T_n sur les formes modulaires

Dans toute cette partie, on considère k un entier naturel et f une fonction faiblement modulaire de poids k.

Comme on l'a vu dans la partie II du chapitre 1 (plus précisément avec la relation (2.4)), on peut faire correspondre avec f une fonction F de poids k sur $\mathcal{R}$ telle que :

$$\forall \lambda \in \mathbb{C}^*,\ F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k} F(\omega_1, \omega_2) \tag{3.6}$$

Définition 3 : Opérateur de Hecke (pour une fonction faiblement modulaire) :

On définit T_n, toujours appelé **opérateur de Hecke**, comme la fonction définie sur l'ensemble des fonctions faiblement modulaires et on pose $T_n(f) = n^{k-1} T_n(F)$ (ou F est associée à f comme ci-dessus).

Remarque :

Le coefficient n^{k-1} permettra d'avoir des formules "sans dénominateur" par la suite.

On a alors par définition :

$$\forall z \in \mathcal{H},\ T_n(f)(z) = n^{k-1} T_n(F(\Gamma(z, 1))) \tag{3.7}$$

soit, grâce au lemme 1 :

$$\forall z \in \mathcal{H},\ T_n(f)(z) = n^{k-1} \sum_{\substack{a \geq 1,\ ad = n \\ 0 \leq b < d}} d^{-k} f\left(\frac{az + b}{d}\right). \tag{3.8}$$

Proposition 2 :

* Pour tout $n \in \mathbb{N}^*$, la fonction $T_n(f)$ est faiblement modulaire et de poids k.
  De plus, si f est holomorphe sur $\mathcal{H}$, alors $T_n(f)$ l'est également.

* Pour tous entiers naturels non nuls m, n premiers entre eux, on a :

$$(T_m \circ T_n)(f) = T_{mn}(f)$$

* Pour tout entier naturel $n \geq 1$ et tout nombre premier p, on a :

$$(T_p \circ T_{p^n})(f) = T_{p^{n+1}}(f) + p^{k-1} T_{p^{n-1}}(f)$$

Preuve :

* Pour tout $n \in \mathbb{N}^*$, d'après la relation (3.8), on obtient que $T_n(f)$ est méromorphe sur $\mathcal{H}$.
De plus, $T_n(f)$ est 1-périodique car f l'est et en faisant correspondre f au réseau F on a par la relation (3.6) que :
$$F\left(\Gamma\left(-\frac{1}{z},1\right)\right) = z^{-k}F(\Gamma(-1,z)) = z^{-k}F(\Gamma(z,1)).$$
Donc par la relation (3.7), on a :
$$\forall z \in \mathcal{H},\ T_n(f)\left(-\frac{1}{z}\right) = n^{k-1}T_n\left(F\left(\Gamma\left(-\frac{1}{z},1\right)\right)\right) = z^{-k}\left(n^{k-1}T_n(F(\Gamma(z,1))\right) = z^{-k}T_n(f)(z)$$
Donc par la proposition 1 du chapitre 2, on en déduit que $T_n(f)$ est faiblement modulaire et de poids k.
De plus, si f est holomorphe sur $\mathcal{H}$, alors toujours par la relation (3.8), on obtient que $T_n(f)$ est méromorphe sur $\mathcal{H}$.

* Soient m et n des entiers naturels premiers entre eux.
Par la formule (3.7) et la relation (3.4), on obtient directement que $(T_m \circ T_n)(f) = T_{mn}(f)$.

* Soient $n \in \mathbb{N}$ et $p \in \mathcal{P}$.
Par la formule (3.7) et la relation (3.5), on obtient directement que :
$$(T_p \circ T_{p^n})(f) = T_{p^{n+1}}(f) + p^{k-1}T_{p^{n-1}}(f).$$

■

Remarque :
La $\mathbb{C}$-algèbre engendrée par la famille $(T_n)_{n\in\mathbb{N}^*}$ est donc commutative et on l'appelle **algèbre de Hecke**.

Étudions maintenant le comportement des $T_n(f)$ à l'infini :
On suppose désormais que f est une fonction modulaire (c'est-à-dire méromorphe à l'infini) et on note :
$$f(z) = \sum_{m\in\mathbb{Z}} c(m)q^m$$
le q-développement de f.

Proposition 3 :
Soit n un entier naturel non nul.
La fonction $T_n(f)$ est une fonction modulaire de poids k et on a :
$$\forall z \in \mathcal{H}^*,\ T_n(f)(z) = \sum_{m\in\mathbb{Z}} \gamma(m)q^m,\ \text{avec } \gamma(m) = \sum_{\substack{a\,|\,\mathrm{PGCD}(m,n)\\ a\geq 1}} a^{k-1}c\left(\frac{mn}{a^2}\right)$$

Preuve :
Soit n un entier naturel non nul.

* Par la proposition 2, on sait déjà que $T_n(f)$ est une fonction modulaire de poids k.

* Par la formule (3.8), on en déduit que $T_n(f)$ est méromorphe à l'infini (par somme finie de fonctions méromorphes à l'infini).

* Par définition de $T_n(f)$, on a :

$$T_n(f)(z) = n^{k-1} \sum_{\substack{a\geq 1,\ ad=n \\ 0\leq 0\leq b<d}} d^{-k} f\left(\frac{az+b}{d}\right) = n^{k-1} \sum_{\substack{a\geq 1,\ ad=n \\ 0\leq b<d}} d^{-k} \left(\sum_{m\in\mathbb{Z}} c(m) e^{2i\pi \frac{az+b}{d} m}\right)$$

Or :

$$\sum_{0\leq b<d} e^{2i\pi \frac{bm}{d}} = \begin{cases} d & \text{si } d|m \\ \dfrac{1-\left(e^{2i\pi\frac{m}{d}}\right)^d}{1-e^{2i\pi\frac{m}{d}}} = 0 & \text{si } d\nmid m \end{cases}$$

On peut donc écrire, en posant $m' = \dfrac{m}{d}$:

$$T_n(f)(z) = n^{k-1} \sum_{\substack{a\geq 1,\ ad=n \\ m'\in\mathbb{Z}}} d^{-k+1} c(m'd) q^{am'}.$$

Soit, en posant $\mu = am'$:

$$T_n(f)(z) = n^{k-1} \sum_{\mu\in\mathbb{Z}} q^\mu \left(\sum_{ad=n,\ a\geq 1} d^{1-k} c\left(\frac{\mu d}{a}\right)\right) = \sum_{\mu\in\mathbb{Z}} q^\mu \left(\sum_{\substack{a|\,\mathrm{PGCD}(m,n) \\ a\geq 1}} \left(\frac{n}{d}\right)^{k-1} c\left(\frac{\mu d}{a}\right)\right)$$

$$= \sum_{\mu\in\mathbb{Z}} \left(\sum_{\substack{a|\,\mathrm{PGCD}(\mu,n) \\ a\geq 1}} a^{k-1} c\left(\frac{\mu n}{a^2}\right)\right) q^\mu$$

Or, puisque f est méromorphe à l'infini, il existe un entier $N \geq 0$ tel que pour tout entier relatif $m \leq -N$ on ait $c(m) = 0$. Ainsi, les $c\left(\dfrac{mn}{a^2}\right)$ sont nuls pour $\mu \leq -nN$. Ainsi, $T_n(f)$ est également méromorphe à l'infini et puisqu'elle est faiblement modulaire d'après la proposition 2, on en déduit que c'est une fonction modulaire.

Finalement, le fait que ses coefficients dans son q-développement sont ceux annoncés résulte du calcul ci-dessus.

■

Corollaire 3 :
Soit n un entier naturel non nul.
On a $\gamma(0) = \sigma_{k-1}(n)c(0)$ et $\gamma(1) = c(n)$.

Preuve :
Soit n un entier naturel non nul.
En utilisant l'expression des coefficients du q-développement de $T_n(f)$ donné dans la proposition 3, on obtient que :

$$\gamma(0) = \sum_{\substack{a|\,\mathrm{PGCD}(n,0)\\ a\geq 1}} a^{k-1}c\left(0\right) = c(0)\sum_{a|n,\ a\geq 1} a^{k-1} = \sigma_{k-1}(n)c(0).$$

Et de même :

$$\gamma(1) = \sum_{\substack{a|\,\mathrm{PGCD}(n,1)\\ a\geq 1}} a^{k-1}c\left(\frac{n}{a^2}\right) = 1^{k-1}c\left(\frac{n}{1^2}\right) = c(n).$$

■

Corollaire 4 :
Soient $p \in \mathcal{P}$ et $m \in \mathbb{Z}$.
On a la relation :

$$\gamma(m) = \begin{cases} c(pm) & \text{si } m \not\equiv 0\ [p] \\ c(pm) + p^{k-1}c\left(\dfrac{m}{p}\right) & \text{si } m \equiv 0\ [p] \end{cases}$$

Preuve :
Soient $p \in \mathcal{P}$ et $m \in \mathbb{Z}$.

* Si m n'est pas divisible par p, alors $\mathrm{PGCD}(p, m) = 1$ et par l'expression des coefficients du q-développement de $T_n(f)$ donné dans la proposition 3, on a :

$$\gamma(m) = 1^{k-1}c\left(\frac{mp}{1^2}\right) = c(mp)$$

* De même, si m est divisible par p, alors $\mathrm{PGCD}(p, m) = p$ et on a :

$$\gamma(m) = 1^{k-1}c\left(\frac{mp}{1^2}\right) + p^{k-1}c\left(\frac{mp}{p^2}\right) = c(mp) + p^{k-1}c\left(\frac{m}{p}\right)$$

■

Corollaire 5 :
Soit $n \in \mathbb{N}$.
Si f est une forme modulaire (respectivement une forme parabolique) de poids k, alors $T_n(f)$ aussi.

Preuve :
Soit $n \in \mathbb{N}$.

* Si f est une forme modulaire, alors elle est holomorphe à l'infini et donc $c(m)$ est nul pour m strictement négatif. Or, d'après les coefficients du q-développement de $T_n(f)$ (cf. proposition 3), cela implique que les $c\left(\dfrac{\mu d}{a}\right)$ sont nuls également pour $\mu \geq 0$, donc $T_n(f)$ admet un développement en série entière au voisinage de 0 donc est holomorphe en ce point et donc à l'infini.

* Si f est une forme parabolique, alors $c(0) = 0$ et donc par le corollaire 3 on a que $\gamma(0) = \sigma_{k-1}(n)c(0) = 0$. Ainsi, $T_n(f)$ est une forme parabolique (car on sait déjà qu'elle est modulaire par le point précédent).

■

Ainsi, les T_n opèrent sur les espaces M_k et S_k et d'après ce qu'on a vu plus haut, les opérateurs ainsi définis commutent entre eux et vérifient les identités :

$$T_m \circ T_n = T_{mn}, \text{ avec } \text{PGCD}(m,n) = 1 \tag{3.9}$$

$$T_p \circ T_{p^n} = T_{p^{n+1}} + p^{k-1} T_{p^{n-1}}, \text{ avec } p \in \mathcal{P} \text{ et } n \geq 1 \tag{3.10}$$

Remarque :
En fait, on a même que tout élément inclus dans l'algèbre engendrée par les R_λ et les T_p (avec $\lambda \in \mathbb{C}^*$ et $p \in \mathcal{P}$) agit respectivement sur M_k et S_k et les laissent stables.

Exemple 2 :
On rappelle que l'on a (cf. exemple 5 du chapitre 2) :

$$\forall z \in \mathcal{H}^*, \ E_4(z) = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6.$$

En utilisant la formule donnée en proposition 3, on obtient :

$$\forall z \in \mathcal{H}^*, \ T_2(E_4)(z) = \left(\frac{1}{240} + 2^3 \times \frac{1}{240}\right) + 9q + \left(73 + 2^3 \times 1\right) q^2 + ...$$

Or, par le corollaire 5, on sait que T_2 préserve M_4 et puisque M_4 est de dimension 1, on a alors que T_2 agit simplement comme étant la multiplication par un scalaire et en comparant les coefficients constants des deux q-développements, on obtient que $T_2(E_4) = 9E_4$.

Plus généralement, pour tout nombre premier p, on obtient en examinant les coefficients constants que :

$$T_p(E_4) = \left(1 + p^3\right) E_4.$$

Remarque :
En fait, pour tout $n \in \mathbb{N}^*$ et tout entier naturel pair $k \geq 4$ on a $T_n(E_k) = \sigma_{k-1}(n) E_k$ (cf. proposition 4).

III Vecteurs propres des opérateurs de Hecke

Considérons dans toute cette partie $f : z \longmapsto \sum_{n=0}^{+\infty} c(n) q^n$ une forme modulaire de poids k (avec $k > 0$) non identiquement nulle.

Supposons que pour tout $n \in \mathbb{N}^*$, f soit vecteur propre des T_n, c'est-à-dire :

$$\forall n \in \mathbb{N}^*, \ \exists \lambda_n \in \mathbb{C} \text{ tq } T_n(f) = \lambda_n f. \tag{3.11}$$

Théorème 1 :

- Le coefficient $c(1)$ de q dans le q-développement de f est non nul.
- Si f est normalisée de telle sorte que $c(1) = 1$, alors on a que pour tout $n \in \mathbb{N}^*$, $c(n) = \lambda_n$.

Preuve :

- D'après le corollaire 3, le coefficient devant q dans le q-développement de $T_n(f)$ est $c(n)$ et d'après la relation (3.11) c'est aussi $\lambda_n c(1)$. On a donc :

  $$\forall n \in \mathbb{N}^*, \ c(n) = \lambda(n) c_1 \tag{3.12}$$

  Or, si $c(1) = 0$, alors tous les $c(n)$ seraient nuls et donc f serait constante, ce qui contredit $k > 0$. On en déduit donc que $c(1) \neq 0$.
- Si f est normalisée de telle sorte que $c(1) = 1$, alors d'après (3.12), on a que pour tout $n \in \mathbb{N}^*$, $c(n) = \lambda_n$.

■

Corollaire 6 :
Deux formes modulaires de même poids $\ell > 0$ qui sont vecteurs propres des T_n associés aux mêmes valeurs propres λ_n, et qui sont normalisées, coïncident sur $\mathcal{H}^*$.

Preuve :
Soient g et h deux formes modulaires de même poids $\ell > 0$ qui sont vecteurs propres des T_n associés aux mêmes valeurs propres λ_n, et qui sont normalisées.

On a alors par le théorème 1 que g et h ont les mêmes coefficients dans leur q-développement hormis éventuellement le terme constant. Or, si les termes constants des q-développement de g et h sont différents, alors $g - h$ est une forme modulaire constante mais de poids $\ell > 0$, ce qui est contradictoire.

Finalement, on a donc $g = h$ sur $\mathcal{H}^*$.

■

Corollaire 7 :
Si f est normalisée de telle sorte que $c(1) = 1$, alors on a :

$$\forall m, n \in \mathbb{N},\ (\text{PGCD}(m,n) = 1) \implies (c(m)c(n) = c(mn)). \tag{3.13}$$

$$\forall p \in \mathcal{P},\ \forall n \in \mathbb{N}^*,\ c(p)c(p^n) = c(p^{n+1}) + p^{k-1}c(p^{n-1}). \tag{3.14}$$

Preuve :
Supposons que f est normalisée de telle sorte que $c(1) = 1$.
Par les relations (3.9) et (3.10), on obtient que les valeurs propres λ_n vérifient les mêmes identités que les T_n.
Or, d'après le théorème 1, on a $\lambda_n = c(n)$, d'où le résultat.

■

Les formules (3.13) et (3.14) peuvent se traduire analytiquement de la manière suivante :

Considérons la série de Dirichlet définie par les $c(n)$:

$$\Psi_f(s) = \sum_{n=1}^{+\infty} \frac{c(n)}{n^s}. \tag{3.15}$$

Par le corollaire 1, on sait que cette série converge pour $\text{Re}(s) > k$. Nous allons monter également que Ψ_f admet un développement en produit eulérien grâce au lemme suivant :

Lemme 2 :
Soit f une fonction multiplicative et bornée.
La série de Dirichlet $\displaystyle\sum_{n\geq 1} \frac{f(n)}{n^s}$ converge absolument pour $\text{Re}(s) > 1$ et sa somme dans ce domaine est égale au produit infini convergent :

$$\prod_{p\in\mathcal{P}} \left(\sum_{m=0}^{+\infty} f(p^m) p^{-ms} \right).$$

Preuve :
Soit f une fonction multiplicative et bornée.
Puisque f est bornée, on a par la convergence de la série des $\dfrac{1}{n^s}$ que la série de Dirichlet converge absolument lorsque $\text{Re}(s) > 1$.

Soient S_k l'ensemble des k premiers nombres premiers et $\mathbb{N}(k)$ l'ensemble des entiers naturels non nuls dont tous les facteurs premiers appartiennent à S_k.
Par multiplicativité de f, on a l'égalité :

$$\sum_{n\in\mathbb{N}(k)} \frac{f(n)}{n^s} = \prod_{p\in S_k} \left(\sum_{m=0}^{+\infty} f(p^m) p^{-ms} \right).$$

Or, quand k tend vers $+\infty$, la membre de gauche converge et tend vers $\sum_{n=1}^{+\infty} \frac{f(s)}{n^s}$, d'où la convergence du second membre et l'égalité voulue.

■

Donnons à présent le développement eulérien de Ψ_f :

Corollaire 8 :
Pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > k$, on a :

$$\Psi_f(s) = \prod_{p\in\mathcal{P}} \frac{1}{1 - c(p)p^{-s} + p^{k-1-2s}}. \tag{3.16}$$

Preuve :
D'après le corollaire 7, la fonction $n \longmapsto c(n)$ est multiplicative et donc par le lemme 2, $\Psi_f(s)$ est le produit des $\sum_{n=0}^{+\infty} c(p^n)p^{-ns}$.
Or, en posant $T = p^{-s}$, on est ramené à prouver l'identité :

$$\sum_{n=0}^{+\infty} c(p^n)T^n = \frac{1}{\Psi_{f,p}(T)}, \text{ avec } \Psi_{f,p}(T) = 1 - c(p)T + p^{k-1}T^2. \tag{3.17}$$

De plus, en regardant la série :

$$\Psi(T) = \left(\sum_{n=0}^{+\infty} c(p^n)T^n \right) \left(1 - c(p)T + p^{k-1}T^2\right).$$

on se rend compte que le coefficient de T dans Ψ est $c(p) - c(p) = 0$ et pour tout $n \in \mathbb{N}^*$, on a par calcul direct et d'après (3.14) que le coefficient de T^{n+1} est :

$$c(p^{n+1}) - c(p)c(p^n) + p^{k-1}c(p^{n-1}) = 0.$$

Finalement, la série $\Psi(T)$ est donc réduite à son terme constant qui vaut $c(1) = 1$, d'où (3.16).

■

Remarques :

* Inversement, les relations (3.15) et (3.16) entraînent (3.13) et (3.14).
* Hecke a montré que Ψ_f se prolonge analytiquement en une fonction méromorphe sur tout le plan complexe (et même holomorphe si f est une forme parabolique) et que la fonction $X_f : s \longmapsto (2\pi)^{-s}\Gamma(s)\Psi_f(s)$ vérifie l'équation fonctionnelle :
$$X_f(s) = (-1)^{\frac{k}{2}} X_f(k-s).$$
Hecke a également démontré une réciproque : toute série de Dirichlet Ψ qui vérifie une équation fonctionnelle de ce type, ainsi que certaines hypothèses de régularité et de croissance, provient d'une forme modulaire f de poids k. De plus, f est une fonction propre normalisée des T_n si, et seulement si, Ψ est un produit eulérien du type (3.16).

IV Exemples

On donne ici quelques applications de ce qui précède, notamment avec la détermination de valeurs propres et vecteurs propres des opérateurs des Hecke ainsi que des identités arithmétiques avec la fonction τ de Ramanujan.

IV.1 Séries d'Eisenstein

Dans toute cette sous-partie, on considère k un entier naturel pair supérieur ou égal à 4.

Proposition 4 :
La série d'Eisenstein G_k est vecteur propre des T_n, les valeurs propres correspondantes sont les $\sigma_{k-1}(n)$ et le vecteur propre normalisée est E_k.
De plus, la série de Dirichlet correspondante est $s \longmapsto \zeta(s)\zeta(s-k+1)$.

Preuve :

* Commençons par prouver que G_k est vecteur propre des T_n :
Par la relation (3.9), il suffit de montrer que G_k est vecteur propre pour les T_p avec $p \in \mathcal{P}$.
Considérons G_k comme une fonction sur l'ensemble $\mathcal{R}$ avec :

$$G_k(\Gamma) = \sum_{\gamma \in \Gamma \backslash \{0\}} \frac{1}{\gamma^k}.$$

On a alors :

$$T_p(G_k(\Gamma)) = \sum_{\substack{\Gamma' \subseteq \Gamma \\ [\Gamma:\Gamma']=p}} \left(\sum_{\gamma \in \Gamma' \backslash \{0\}} \frac{1}{\gamma^k} \right).$$

Soit $\gamma \in \Gamma$.
Si $\gamma \in p\Gamma$, alors γ appartient à chacun des $p+1$ sous-réseaux de Γ d'indice p. Ainsi, sa contribution dans $T_p(G_k(\Gamma))$ est $\dfrac{p+1}{\gamma^k}$.
Sinon, $\gamma \in \Gamma \backslash p\Gamma$ et donc γ n'appartient qu'à un seul sous-réseau d'indice p et sa contribution est $\dfrac{1}{\gamma^k}$.
Finalement, en utilisant le fait que $G_k(p\Gamma) = p^{-k} G_k(\Gamma)$, on a donc :

$$T_p(G_k(\Gamma)) = G_k(\Gamma) + p \sum_{\gamma \in p\Gamma} \frac{1}{\gamma^k} = G_k(\Gamma) + pG_k(p\Gamma) = \left(1 + p^{1-k}\right) G_k(\Gamma).$$

Ceci nous montre donc que G_k (considérée comme fonction sur $\mathcal{R}$) est un vecteur propre de T_p associé à la valeur propre $1 + p^{1-k}$ et donc que G_k (considérée comme forme modulaire) est un vecteur propre de T_p associé à la valeur propre $p^{k-1}(1 + p^{1-k}) = \sigma_{k-1}(p)$.

* On a alors par le q-développement de G_k que le vecteur propre normalisé associé à G_k est E_k et donc que les valeurs propres des T_n sont les $\sigma_{k-1}(n)$.

* Enfin, pour tout complexe s tel que $\mathrm{Re}(s) > 1$, on a :

$$\sum_{n=1}^{+\infty} \frac{\sigma_{k-1}(n)}{n^s} = \sum_{a=1}^{+\infty} \sum_{d=1}^{+\infty} \frac{a^{k-1}}{a^s d^s} = \left(\sum_{d=1}^{+\infty} \frac{1}{d^s} \right) \left(\sum_{a=1}^{+\infty} \frac{1}{a^{s+1-k}} \right) = \zeta(s)\zeta(s-k+1).$$

■

Remarque :
Une autre manière de d'interpréter ce résultat est que tous les opérateurs de Hecke respectent la décomposition $M_k = S_k \oplus \mathbb{C}\, G_k = S_k \oplus \mathbb{C}\, E_k$ et donc les E_k sont vecteurs propres de tous les T_n.

IV.2 La fonction Δ

Proposition 5 :
La fonction Δ est un vecteur propre des T_n associé à la valeur propre égale au n-ième coefficient du q-développement de Δ et le vecteur propre normalisé est égal à Δ.

Preuve :
On sait que Δ est une forme parabolique non nulle de poids 12 (et de niveau 1) et que le $\mathbb{C}$-espace vectoriel S_{12} est de dimension 1 (par le corollaire 3 du chapitre 2) et que T_n le laisse stable (par la proposition 4).

Ainsi, Δ est vecteur propre des T_n et c'est également le vecteur propre normalisé car le coefficient devant q dans son q-développement est égal à 1 et on a par le théorème 1 que la valeur propre associée à Δ pour T_n est égale au n-ième coefficient du q-développement de Δ.

■

Nous noterons désormais le q-développement de Δ par $\Delta(z) = \sum_{n=1}^{+\infty} \tau(n) q^n$ (le coefficient constant est nul puisque l'on a montré que Δ est une forme parabolique).

Corollaire 9 :
Soient $p \in \mathcal{P}$ et $m, n \in \mathbb{N}^*$.

* Si $\text{PGCD}(m, n) = 1$, alors $\tau(n)\tau(m) = \tau(nm)$.
* $\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$

Preuve :
On sait que Δ est une forme parabolique de poids 12 (et de niveau 1), que les $\tau(n)$ sont les coefficients de son q-développement et que $\tau(1) = 1$, donc par le corollaire 7, on a les deux relations voulues.

■

Remarques :

* Ce résultat fut conjecturé par Ramanujan en 1916 et démontré par Mordell en 1917 en utilisant les propriétés précédentes des opérateurs des Hecke pour les formes modulaires.
* On a des résultats analogues chaque fois que l'espace S_k est de dimension 1 (ce qui se produit lorsque l'on a $k = 12, 16, 18, 20$ et 22 et avec pour bases respectives Δ, ΔG_4, ΔG_6, ΔG_8 et ΔG_{10}).

IV.3 La fonction τ de Ramanujan

Définition 4 : Fonction τ de Ramanujan :
On appelle **fonction τ de Ramanujan** la fonction définie sur $\mathbb{N}^*$ et qui à n associe le n-ième coefficient du q-développement de la forme parabolique Δ.

Exemple 3 :
On donne ci-dessous quelques valeurs de τ :

$$\tau(1) = 1,\ \tau(2) = -24,\ \tau(3) = 252,\ \tau(4) = -1\,472,\ \tau(5) = 4\,830,\ \tau(6) = -6\,048,\ \tau(7) = -16\,744,\ \tau(8) = 84\,480$$

$$\tau(9) = -113\,643,\ \tau(10) = -115\,920,\ \tau(11) = 534\,612 \text{ et } \tau(12) = -370\,944$$

Remarque :
En réalité, par la formule du produit de Jacobi, on a que τ est une fonction à valeurs dans $\mathbb{Z}$ (comme on peut le conjecturer dans l'exemple ci-dessus).

Le corollaire 9 nous a déjà donné deux résultats sur la fonction τ de Ramanujan. Nous en rajoutons un ci-dessous :

Proposition 6 :
On a $\tau(n) = O(n^6)$.

Preuve :
Les $\tau(n)$ sont les coefficients du q-développement de la forme parabolique Δ de poids 12 (et de niveau 1), donc par le théorème 1 du chapitre 2, on a que $\tau(n) = O(n^6)$.

■

De même qu'avec les relations (3.13) et (3.14), on peut traduire analytiquement les propriétés du corollaire 9 en disant que la série de Dirichlet $L_\tau : s \longmapsto \sum_{n=1}^{+\infty} \frac{\tau(n)}{n^s}$ admet le développement Eulérien suivant :

$$L_\tau(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}}.$$

De plus, d'après Hecke, la fonction L_τ se prolonge en une fonction entière dans tout le plan complexe et la fonction $s \longmapsto (2\pi)^{-s}\Gamma(s)L_\tau(s)$ est invariante par $s \longmapsto 12 - s$.

Finalement, nous terminons cette partie en donnant divers résultats de congruence vérifiés par les $\tau(n)$.

Théorème 2 :
Pour tout $n \in \mathbb{N}^*$, on a $\tau(n) \equiv \sigma_{11}(n)$ [691].

Preuve :
On sait que $\dim_{\mathbb{C}}(S_{12}) = 1$ et que $\Delta \in S_{12}$ est non identiquement nulle, donc $S_{12} = \mathbb{C}\,\Delta$. De plus, on a $E_{12}, E_6^2 \in M_{12}$ et grâce à leurs termes constants, on obtient que

$$65\ 520E_{12} - 691 \times (504)^2 E_6^2 \in S_{12}.$$

Il existe alors $\alpha \in \mathbb{C}$ tel que $65\ 520E_{12} - 691 \times (504)^2 E_6^2 = \alpha\Delta$. Or, en comparant les coefficients des q-développements devant le terme q, on a :

$$65\ 520 - 691 \times (504)^2 \times \frac{-2}{504} = \alpha$$

soit :

$$\alpha = 65\ 520 + 691 \times 504 \times 2 = 762\ 048.$$

En comparant les coefficients des q-développements de E_{12}, E_6^2 et Δ, on obtient :

$$\forall n \in \mathbb{N}^*,\ 65\ 520\sigma_{11}(n) \equiv \alpha\tau(n)\ [691].$$

Or, pour $n = 1$ on a alors $\alpha \equiv 65\ 520 \equiv 566$ [691], qui est inversible dans $\mathbb{Z}/691\,\mathbb{Z}$ (car $\mathrm{PGCD}(566, 691) = 1$), d'où en simplifiant :

$$\forall n \in \mathbb{N}^*,\ \sigma_{11}(n) \equiv \tau(n)\ [691].$$

■

Remarque :
Suivant le même principe, on peut montrer que :

$$\forall n \in \mathbb{N}^*,\ \tau(n) \equiv n^2\sigma_7(n)\ \left[3^3\right] \text{ et } \tau(n) \equiv n\sigma_3(n)\ [7].$$

(et il existe également d'autres congruences intéressantes modulo 2^{12}, $3^6, 5^3$ et 23 par exemple).

Enfin, donnons trois résultats dont le premier (connu sous le nom de conjecture de Ramanujan) a été démontré par Deligne en 1969 comme conséquence de sa preuve des conjectures de Weil pour les variétés algébriques sur les corps finis :

Proposition 7 :
Pour tout nombre premier p, $|\tau(p)| \leq 2p^{\frac{11}{2}}$.

Le deuxième qui est encore un problème ouvert (connu sous le nom de conjecture de non-annulation) et qui fut conjecturée par Lehmer en 1947 :

Conjecture 1 : Conjecture de non-annulation :
Pour tout $n \in \mathbb{N}^*$, $\tau(n) \neq 0$.

Ce résultat a été expérimentalement vérifié pour tout entier $n \leq 816\ 212\ 624\ 008\ 487\ 344\ 127\ 999$ (cf. [6] pour plus de détails).

Enfin, le dernier résultat est la conjecture de Sato–Tate. Cette conjecture affirme l'équirépartition des valeurs $\frac{\tau(p)}{p^{\frac{11}{2}}}$ lorsque p varie parmi les nombres premiers pour la mesure de Sato–Tate. Autrement dit, pour tous nombres réels a, b tels que $-2 < a < b < 2$, on a :

$$\lim_{x \to +\infty} \frac{\text{Card}\left(\left\{p \in \mathcal{P} \mid p < x \text{ et } ap^{\frac{11}{2}} < \tau(p) < bp^{\frac{11}{2}}\right\}\right)}{\text{Card}(\{p \in \mathcal{P} | p < x\})} = \frac{1}{\pi} \int_a^b \sqrt{1 - \frac{x^2}{4}} \mathrm{d}x.$$

V Calcul des opérateurs de Hecke

Dans toute cette partie, on considère k et n des entiers naturels non nuls.

L'algorithme suivant nous permet d'obtenir la matrice des T_n dans la base de Miller de M_k :

* Calculer $d = \dim_{\mathbb{C}}(M_k) - 1$ grâce au corollaire 3 du chapitre 2.
* Trouver la base de Miller $(f_0, ..., f_d)$ de M_k modulo q^{dn+1} grâce au lemme 2 du chapitre 2.
* Pour tout $i \in [\![0; d]\!]$, calculer $T_n(f_i)$ en utilisant la proposition 3.
* Les éléments $T_n(f_i)$ modulo q^{d+1} détermine des combinaisons linéaires de $f_0, ..., f_d$ modulo q^d. Ces combinaisons linéaires sont faciles à obtenir une fois les $T_n(f_i)$ calculés modulo q^{d+1} (puisque la base composée des f_i est échelonnée). Les combinaisons linéaires sont juste les coefficients des séries $T_n(f_i)$ de q^0 jusqu'à q^d inclus.
* La matrice de T_n agissant à droite sur la base $(f_0, ..., f_d)$ est la matrice dont les lignes sont les combinaisons linéaires trouvées à l'étape précédente (c'est-à-dire dont les lignes sont les coefficients de $T_n(f_i)$).

En effet, la proposition 3 nous donne que le d-ième coefficient du q-développement de $T_n(f)$ implique seulement $c(dn)$ ainsi que d'autres coefficients d'indices plus petits dans le q-développement de f. Ainsi, il nous faut seulement calculer le q-développement de f modulo q^{dn+1} pour calculer l'opérateur de Hecke $T_n(f)$ modulo q^{d+1}. Enfin, l'unicité donnée dans la quatrième étape résulte du fait que l'on travaille avec une base (d'après la proposition 2 du chapitre 2).

Exemple 4 :

Donnons la matrice de l'opérateur de Hecke T_2 dans la base de Miller de M_{12} grâce à l'algorithme ci-dessus :

* On a $d = \dim_{\mathbb{C}}(M_k) - 1 = 2 - 1 = 1$.

* On calcule les coefficients des q-développement des éléments de la base de Miller jusqu'à $q^{1\times 2+1} = q^3$ exclus et par la preuve du lemme 2 du chapitre 2, on a :

$$F_4 = 1 + 240q + 2\ 160q^2 + ... \text{ et } F_6 = 1 - 504q - 16\ 632q^2 + ...$$

Donc M_{12} a pour base (F_4^3, Δ) avec :

$$F_4^3 = 1 + 720q + 179\ 280q^2 + ... \text{ et } \Delta = q - 24q^2 + ...$$

Ainsi, en soustrayant 720Δ à F_4^3, on trouve que la base de Miller de M_{12} est (f_0, f_1) avec :

$$f_0 = 1 + 196\ 560q^2 + ... \text{ et } f_1 = q - 24q^2 + ...$$

* Nous lisons directement que :

$$T_2(f_0) = 2\ 049 f_0 + 196\ 560 f_1 \text{ et } T_2(f_1) = 0f_0 + (-24)f_1.$$

* La matrice de T_2 dans la base de Miller (f_0, f_1) de M_{12} est donc :

$$\begin{pmatrix} 2\ 049 & 196\ 560 \\ 0 & -24 \end{pmatrix}.$$

On notera que le polynôme caractéristique de T_2 est $(X - 2\ 049)(X + 24)$ et que $2\ 049 = 1 + 2^{11}$ est la somme des puissances 11-ièmes des diviseurs positifs de 2.

Exemple 5 :

* Donnons la matrice de l'opérateur de Hecke T_2 dans la base de Miller de M_{32} :
Après calculs, on trouve :

$$\begin{aligned} f_0 &= 1 + 2\ 611\ 200q^3 + 19\ 524\ 758\ 400q^4 + ... \\ f_1 &= q + 50\ 220q^3 + 87\ 866\ 368q^4 + ... \\ f_2 &= q^2 + 432q^3 + 39\ 960q^4 + ... \end{aligned}$$

La matrice de T_2 dans la base (f_0, f_1, f_2) est alors :

$$\begin{pmatrix} 2\ 147\ 483\ 649 & 0 & 19\ 524\ 758\ 400 \\ 0 & 0 & 2\ 235\ 350\ 016 \\ 0 & 1 & 39\ 960 \end{pmatrix}.$$

Enfin, cette matrice a pour polynôme caractéristique :

$$\chi_{T_2, M_{32}} = (X - 2\ 147\ 483\ 649)\left(X^2 - 39\ 960X - 2\ 235\ 350\ 016\right)$$

et on remarque que $X - 2\ 147\ 483\ 649$ et $X^2 - 39\ 960X - 2\ 235\ 350\ 016$ sont des polynômes irréductibles.

* De même, la matrice de l'opérateur de Hecke T_2 dans la base de Miller de M_{36} est donnée par :

$$\begin{pmatrix} 34\ 359\ 738\ 369 & 0 & 6\ 218\ 175\ 600 & 9\ 026\ 867\ 482\ 214\ 400 \\ 0 & 0 & 34\ 416\ 831\ 456 & 5\ 681\ 332\ 472\ 832 \\ 0 & 1 & 194\ 184 & -197\ 264\ 484 \\ 0 & 0 & -72 & -54\ 528 \end{pmatrix}.$$

De plus, son polynôme caractéristique est :

$$\chi_{T_2,M_{36}} = (X - 34\ 359\ 738\ 369)\left(X^3 - 139\ 656X^2 - 59\ 208\ 339\ 456X - 1\ 467\ 625\ 047\ 588\ 864\right)$$

où le facteur de degré 3 est irréductible.

On conclut cette partie par un problème ouvert sur les opérateurs de Hecke agissant sur les formes modulaires de niveau 1 : ce problème généralise notre observation faite sur le polynôme caractéristique de T_2 sur M_{12} et M_{36}, c'est-à-dire qu'il se factorise en un produit de polynômes de degré 1 et d'au plus un facteur irréductible.

Il est possible d'utiliser `SAGE` pour obtenir une base sous forme échelonnée du $\mathbb{C}$-espace vectoriel des formes modulaires de poids quelconque et de niveau 1 :

```
sage: M = ModularForms(1,36, prec = 6).echelon_form()
sage: M.basis()
[
1 + 6218175600*q^4 + 15281788354560*q^5 + O(q^6),
q + 57093088*q^4 + 37927345230*q^5 + O(q^6),
q^2 + 194184*q^4 + 7442432*q^5 + O(q^6),
q^3 - 72*q^4 + 2484*q^5 + O(q^6)
]
```

Conjecture 2 : Conjecture de Maeda :
Soit $k \in \mathbb{N}$.
Le polynôme caractéristique de T_2 sur S_k est irréductible.

Remarque :
Kevin Buzzard observa que dans quelques cas spécifiques, le groupe de Galois du polynôme caractéristique de T_2 est isomorphe au groupe symétrique tout entier (on pourra consulter [15] pour plus de détails).

VI Compléments

VI.1 Le produit scalaire de Petersson

On considère f et g deux formes paraboliques de poids $k > 0$.

Définition 5 : Mesure hyperbolique $\mathrm{d}\mu$:
On considère $z = x + iy \in \mathcal{H}$.
On défini sur $\mathcal{H}$ la **mesure hyperbolique** par $\mathrm{d}\mu(z) = \dfrac{\mathrm{d}x\mathrm{d}y}{y^2}$.

Proposition 8 :
La mesure hyperbolique est invariante par l'action de $\mathrm{SL}_2(\mathbb{Z})$.

Preuve :
Soient $A \subseteq \mathcal{H}$ un borélien et $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.
En posant, pour tout $z \in \mathcal{H}$, $T(z) = \dfrac{az+b}{cz+d}$, on a :

$$\mathrm{Im}(T(z)) = \frac{y}{|cz+d|^2} \text{ et } T'(z) = \frac{1}{(cz+d)^2}$$

Ainsi, on a :

$$\mu(T(A)) = \int_{T(A)} \frac{\mathrm{d}u\mathrm{d}v}{v^2} = \int_A |T'(z)|^2 \frac{|cz+d|^4}{y^2}\mathrm{d}x\mathrm{d}y = \int_A \frac{\mathrm{d}x\mathrm{d}y}{y^2} = \mu(A)$$

■

Définition 6 : Produit scalaire de Petersson :
L'application :

$$< \cdot;\cdot >_{\mathcal{P}} : (f,g) \longmapsto \int_{\mathcal{D}} f(z)\overline{g(z)}\,\mathrm{Im}(z)^{k-2}\mathrm{d}z$$

est un produit scalaire hermitien sur S_k appelé **produit scalaire de Petersson**.

Montrons que l'application ci-dessus est bien définie :

Lemme 3 :
La fonction $z \longmapsto f(z)\overline{g(z)}\,\mathrm{Im}(z)^k$ est invariante par l'action de $\mathrm{SL}_2(\mathbb{Z})$.

Preuve :
Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.
Comme f et g sont des fonctions faiblement modulaires (car sont des formes modulaires), on a :

$$f(\gamma.z)\overline{g(\gamma.z)}\,\mathrm{Im}(\gamma.z)^k = (cz+d)^k f(z)\overline{(cz+d)^k g(z)}\frac{y^k}{|cz+d|^{2k}} = f(z)g(z)\,\mathrm{Im}(z)^k$$

■

Proposition 9 :
Le produit scalaire de Petersson est bien défini.

Preuve :
Pour prouver que le produit scalaire de Petersson est bien défini, il nous suffit de regarder ce qu'il se passe lorsque $\mathrm{Im}(z) \to +\infty$.
Or, puisque f et g sont des formes paraboliques, on obtient lorsque $\mathrm{Im}(z) \to +\infty$ que $f(z)g(z) = O\left(e^{-4\pi\,\mathrm{Im}(z)}\right)$ et donc par comparaison, l'intégrale est bien définie.

■

Remarque :
En regardant la preuve précédente, on se rend compte que le produit scalaire de Petersson est en réalité bien défini lorsqu'au moins l'une des deux fonctions f et g est parabolique.

On vérifie par le calcul que $< \cdot;\cdot >_{\mathcal{P}}$ est bien un produit scalaire hermitien sur S_k. Or, puisque M_k est un $\mathbb{C}$-espace vectoriel de dimension finie (par le corollaire 3 du chapitre 2) et que S_k en est un sous-espace vectoriel, il est également de dimension finie. Et puisqu'il est muni d'un produit scalaire, on en déduit que S_k est un espace de Hilbert.

De plus, pour tout $n \in \mathbb{N}^*$, on peut montrer que $< T_n(f); g >_{\mathcal{P}} = < f; T_n(g) >_{\mathcal{P}}$, ce qui signifie que les T_n sont des opérateurs hermitiens par rapport à $< \cdot;\cdot >_{\mathcal{P}}$ (donc en particulier diagonalisable et avec des valeurs propres réelles). De plus, les T_n commutent entre-eux donc il existe une base orthogonale de S_k formée de vecteurs propres des T_n (par le théorème spectral des opérateurs auto-adjoints).

Remarque :
Le théorème spectral des opérateurs auto-adjoints nous permet même d'en dire un peu plus ! En effet, les $\mathbb{C}$-espaces vectoriels S_k sont de dimension finie donc de Hilbert et les opérateurs de Hecke $T_n : S_k \longrightarrow S_k$ sont linéaires (par la relation (3.8)) et donc continues. En posant alors

$$m = \inf_{\|f\|\leq 1} < T_n(f); f >_{\mathcal{P}} \text{ et } M = \sup_{\|f\|\leq 1} < T_n(f); f >_{\mathcal{P}}$$

on obtient que le spectre de T_n est inclus dans $[-m; M]$ et que m et M sont des éléments du spectre.

Enfin, puisque f est une forme parabolique, elle admet un q-développement avec $a_0 = 0$. On peut alors définir, pour tout $m \in \mathbb{N}$, une forme linéaire :

$$\Phi_m^k : \left| \begin{array}{ccc} S_k & \longrightarrow & \mathbb{C} \\ f = \sum_{n=1}^{+\infty} a_n q^n & \longmapsto & a_m \end{array} \right.$$

et par le théorème de représentation des formes linéaires de Riesz, on en déduit qu'il existe une unique forme parabolique $P_m^k \in S_k$ telle que :

$$< f; P_m^k >_{\mathcal{P}} = \Phi_m^k(f) = a_m.$$

Une forme parabolique vérifiant la propriété ci-dessus est alors appelée **série de Poincaré**.

VI.2 Propriétés d'intégralité

Notons $M_{k,\mathbb{Z}}$ l'ensemble des formes modulaires f de poids k dont les coefficients $c(n)$ de son q-développement sont entiers.

On peut prouver qu'il existe une $\mathbb{Z}$-base de $M_{k,\mathbb{Z}}$ qui est une $\mathbb{C}$-base de M_k. En effet, considérons un entier $N > \dfrac{k}{12}$ ainsi que l'application linéaire $u : M_k \longrightarrow \mathbb{C}^{N+1}$ définie par $u(f) = (a_n(f))_{n \in [\![0;N]\!]}$.
L'application u est alors injective car si l'on a f non identiquement nulle dans $\mathrm{Ker}(u)$, alors $v_\infty(f) > \dfrac{k}{12}$, ce qui contredit la formule de valence (théorème 2 du chapitre 2). En particulier, l'ensemble $M_{k,\mathbb{Z}}$ se plonge dans $\mathbb{Z}^{N+1}$: il est donc libre et de type fini sur $\mathbb{Z}$. Or, comme toute famille $\mathbb{Z}$-libre dans $\mathbb{Z}^r$ est $\mathbb{C}$-libre dans $\mathbb{C}^r$, toute famille $\mathbb{Z}$-libre de $M_{k,\mathbb{Z}}$ est $\mathbb{C}$-libre dans M_k (il suffit d'appliquer u). Ainsi le $\mathbb{Z}$-rang de $M_{k,\mathbb{Z}}$ est inférieur ou égal à $\dim_{\mathbb{C}}(M_k)$. Enfin, comme les formes modulaires du type $E_4^r E_6^s$ appartiennent à $M_{4r+6s,\mathbb{Z}}$, on peut alors conclure par le théorème 5 du chapitre 2.

De plus, par la proposition 3, on a que $M_{k,\mathbb{Z}}$ est stable par tous les T_n. Donc puisque $M_{k,\mathbb{Z}}$ admet une $\mathbb{Z}$-base qui est également une $\mathbb{C}$-base de M_k, on en déduit que les matrices des T_n dans cette base sont à coefficients entiers et ainsi les coefficients du polynôme caractéristique des T_n sont des entiers (signalons au passage qu'il existe une formule explicite donnant la trace des T_n). En particulier, les valeurs propres des T_n en plus d'être réelles (par la sous-partie précédente), sont des entiers algébriques.

VI.3 Le conjecture de Ramanujan-Petersson

Soient $f = \sum_{c=1}^{+\infty} c(n) q^n$ une forme parabolique de poids k qui est une fonction propre normalisée des T_n (donc $c(1) = 1$) et $\Psi_{f,p}(T) = 1 - c(p)T + p^{k-1}T^2$ (avec $p \in \mathcal{P}$) le polynôme défini dans la relation (3.17).

Le polynôme $\Psi_{f,p}(T)$ peut s'écrire :

$$\Psi_{f,p}(T) = (1 - \alpha_p T)(1 - \alpha'_p T)$$

avec $\alpha_p + \alpha'_p = c(p)$ et $\alpha_p \alpha'_p = p^{k-1}$ (par les relations coefficients-racines).

La conjecture de Ramanujan-Petersson consiste à dire que α_p et α'_p sont imaginaires conjugués, ce qui peut aussi s'exprimer en disant que :

$$|\alpha_p| = |\alpha'_p| = p^{\frac{k-1}{2}}.$$

Soit :

$$|c(p)| \leq 2p^{\frac{k-1}{2}}.$$

Ou encore :

$$\forall n \in \mathbb{N}^*,\ |c(n)| \leq n^{\frac{k-1}{2}} \sigma_0(n).$$

Remarques :

* Pour $k = 6$, on retrouve la conjecture de Ramanujan (donc la conjecture de Ramanujan-Petersson est plus générale que la conjecture de Ramanujan).
* Ces conjectures peuvent être ramenées aux conjectures générales de Weil sur les variétés algébriques sur les corps finis.

Chapitre 4

Formes modulaires de niveau quelconque

Le but de ce chapitre sera d'étendre la notion de forme modulaire en la généralisant avec un niveau quelconque puis en donnant quelques formules de dimension de sous-espaces remarquables dans des cas particuliers.

I Formes modulaires de niveau quelconque

Dans cette partie, nous commençons par donner une généralisation de la notion de forme modulaire via la notion de forme modulaire de niveau quelconque avant de donner quelques remarques sur les sous-groupes de congruence.

I.1 Définitions

Définition 1 : Sous-groupe de congruence :
On appelle **sous-groupe de congruence de** $\mathrm{SL}_2(\mathbb{Z})$ tout sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ contenant le noyau de la projection canonique $\pi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ (noté $\Gamma(N)$) pour un entier naturel N donné.
De plus, le plus petit entier naturel N précédent est appelé **niveau de** Γ.

Les sous-groupes de congruence les plus importants que nous utiliserons seront :

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ [N] \right\} \text{ et } \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ [N] \right\}$$

où " $*$ " signifie "n'importe quel élément".

Proposition 1 :
$\Gamma_0(N)$ et $\Gamma_1(N)$ sont deux sous-groupes de $\mathrm{SL}_2(\mathbb{Z})$ d'indice fini et ont tous les deux un niveau N.

Preuve :

- $\Gamma_1(N)$ est l'image réciproque du sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ généré par $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, donc est un sous-groupe du groupe $\mathrm{SL}_2(\mathbb{Z})$.
  De plus, le groupe $\Gamma_1(N)$ contient le noyau de la projection canonique $\pi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et puisque ce noyau est d'indice fini (puisque le quotient est contenu dans $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ par le premier théorème d'isomorphisme) on en déduit que $\Gamma_1(N)$ est d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$.
  Enfin, le niveau de $\Gamma_1(N)$ est au plus N puisqu'il contient $\Gamma(N)$ et ne peut pas être plus grand car $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ appartient à $\Gamma_1(N)$.
- De même qu'au point précédent on démontre que $\Gamma_0(N)$ est bien un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$, qu'il est d'indice fini et que son niveau est N également.

■

Remarque :
On a $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1) = \Gamma(1)$.
En effet, puisque le groupe $\mathrm{SL}_2(\mathbb{Z}/1\mathbb{Z})$ est le groupe trivial, la projection canonique envoie tout élément de $\mathrm{SL}_2(\mathbb{Z})$ sur l'élément neutre, d'où $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$. Or, on a également $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1) \subseteq \Gamma_1(1) \subseteq \Gamma_0(1) \subseteq \mathrm{SL}_2(\mathbb{Z})$, d'où le résultat.

Considérons un entier relatif k et définissons **l'action de poids k à droite de** $\mathrm{GL}_2(\mathbb{Q})$ sur l'ensemble des fonctions $f : \mathcal{H} \longrightarrow \mathbb{C}$:
Pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$, on pose :

$$\forall z \in \mathcal{H},\ \left(f^{[\gamma]_k}\right)(z) = \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma.z). \tag{4.1}$$

La formule (4.1) définie une action à droite de $\mathrm{GL}_2(\mathbb{Z})$ sur l'ensemble des fonctions $f : \mathcal{H} \longrightarrow \mathbb{C}$.
En particulier, pour tous $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbb{Z})$, on a :

$$f^{[\gamma_1\gamma_2]_k} = \left(f^{[\gamma_1]_k}\right)^{[\gamma_2]_k}.$$

Définition 2 : Fonction faiblement modulaire de poids k pour un sous-groupe de congruence :
On considère Γ un sous-groupe de congruence et k un entier relatif.
On appelle **fonction faiblement modulaire de poids k pour** Γ toute fonction méromorphe $f : \mathcal{H} \longrightarrow \mathbb{C}$ telle que pour tout $\gamma \in \Gamma$, $f^{[\gamma]_k} = f$.

Un objet central dans la théorie des formes modulaires est **l'ensemble des pointes de** $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.
Un élément $\gamma \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathbb{P}^1(\mathbb{Q})$ par :

$$\gamma.z = \begin{cases} \dfrac{az+b}{cz+d} & \text{si } z \neq \infty \\ \dfrac{a}{c} & \text{si } z = \infty. \end{cases}$$

Notons également que si le dénominateur $cz+d$ ou c est nul, alors $\gamma.z = \infty \in \mathbb{P}^1(\mathbb{Q})$.

L'ensemble des pointes pour un sous-groupe de congruence Γ est l'ensemble $C(\Gamma)$ des Γ-orbites de $\mathbb{P}^1(\mathbb{Q})$ (et nous identifierons souvent les éléments de $C(\Gamma)$ avec un représentant de l'orbite considérée).

Lemme 1 :
Pour tous $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, il existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma.\alpha = \beta$.

Preuve :
Soient $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$.

* Si $\alpha, \beta \in \mathbb{Q}$, alors écrivons α sous la forme $\alpha = \dfrac{p}{q} \in \mathbb{Q}$ avec p et q premiers entre eux. Par l'algorithme d'Euclide, il existe alors $x, y \in \mathbb{Z}$ tels que $px + qy = 1$. En posant $\gamma_\alpha = \begin{pmatrix} p & -y \\ q & x \end{pmatrix}$ on a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et $\gamma_\alpha(\infty) = \alpha$ et en posant également γ_∞ l'application identité sur $\mathbb{P}^1(\mathbb{Q})$ et γ_β (construite comme γ_α) qui envoie ∞ sur β, on obtient que $\gamma_\beta \circ \gamma_\alpha^{-1}$ envoie α sur β.

* Si $\alpha = \infty$ et $\beta \in \mathbb{Q}$, alors écrivons $\beta = \dfrac{p}{q}$ avec p et q premiers entre eux. Par l'algorithme d'Euclide, il existe alors $x, y \in \mathbb{Z}$ tels que $px + qy = 1$. En posant $\gamma_\alpha = \begin{pmatrix} p & -y \\ q & x \end{pmatrix}$ on a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et $\gamma_\alpha(\infty) = \beta$.

* Enfin, si $\alpha = \beta = \infty$, alors on prend $\gamma = I_2 \in \mathrm{SL}_2(\mathbb{Z})$ et on a $\gamma(\alpha) = \beta$.

■

Remarque :
Le lemme précédent nous dit que l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q})$ est transitive. Il nous donne par exemple que pour $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, il y a une unique orbite et donc $C(\mathrm{SL}_2(\mathbb{Z})) = \{\overline{\infty}\}$.

Proposition 2 :
Pour tout sous-groupe de congruence Γ, l'ensemble $C(\Gamma)$ est fini.

Preuve :
Soit Γ un sous-groupe de congruence.
Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est l'union disjointe de ses classes (à droite par exemple) modulo Γ et par le lemme 1 on sait que l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q})$ est transitive. Ainsi :

$$\mathbb{P}^1(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Z}).0 = \left(\bigsqcup_{i=1}^{m} \Gamma\gamma_i\right).0 = \bigsqcup_{i=1}^{m} \left(\Gamma\left(\gamma_i.0\right)\right)$$

avec $m = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ et les γ_i des représentants des différentes orbites.

Ainsi, chacun des éléments de cette union est une orbite, l'union vaut tout l'ensemble de départ donc on les a toutes et il y en a donc au plus m.

■

Afin de donner du sens à l'holomorphie pour une fonction faiblement modulaire f pour un sous-groupe de congruence Γ quelconque en tout $\alpha \in \mathbb{Q}$, on donne le lemme suivant :

Lemme 2 :
Soient $k \in \mathbb{Z}$, Γ un sous-groupe de congruence et $f : \mathcal{H} \longrightarrow \mathbb{C}$ une fonction faiblement modulaire de poids k pour Γ.
Pour $\delta \in \mathrm{SL}_2(\mathbb{Z})$, $f^{[\delta]_k}$ est une fonction faiblement modulaire pour $\delta^{-1}\Gamma\delta$.

Preuve :
Soient $k \in \mathbb{Z}$, Γ un sous-groupe de congruence et $f : \mathcal{H} \longrightarrow \mathbb{C}$ une fonction faiblement modulaire de poids k pour Γ.
Soit $s = \delta^{-1}\gamma\delta \in \delta^{-1}\Gamma\delta$.

$$\left(f^{[\delta]_k}\right)^{[s]_k} = f^{[\delta s]_k} = f^{[\delta\delta^{-1}\gamma\delta]_k} = f^{[\gamma\delta]_k} = f^{[\delta]_k}$$

d'où le fait que $f^{[\delta]_k}$ est une fonction faiblement modulaire pour $\delta^{-1}\Gamma\delta$.

■

Considérons une fonction faiblement modulaire f de poids k pour un sous-groupe de congruence Γ et $\alpha \in \mathbb{Q}$. Dans le chapitre 2, nous avons construit le q-développement d'une fonction faiblement modulaire f de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ en utilisant le fait que cette fonction était 1-périodique (ce qui traduit le fait que $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$). Cependant, il y a des sous-groupes de congruence Γ tels que $T \notin \Gamma$. De plus, même si l'on considère les formes modulaires pour $\Gamma_1(N)$ où on a $T \in \Gamma_1(N)$ pour tout $N \in \mathbb{N}$, nous aurons toujours à considérer les q-développements à l'infini pour des formes modulaires sur $\delta^{-1}\Gamma_1(N)\delta$ qui ne contient pas forcément T !

Heureusement, on a $T^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N)$, donc un sous-groupe de congruence de niveau N contient T^N. Ainsi, nous avons $f(z + H) = f(H)$ pour un certain entier positif H (par exemple $H = N$ fonctionne mais il peut y avoir des choix plus petits). Le choix du plus petit $H > 0$ tel que $\begin{pmatrix} 1 & H \\ 0 & 1 \end{pmatrix} \in \delta^{-1}\Gamma\delta$ avec $\delta(\infty) = \alpha$ est appelé **l'épaisseur de la pointe α relativement au sous-groupe de congruence Γ**.

Lorsque f est méromorphe à l'infini, on obtient le q-développement :

$$\forall z \in \mathcal{H}^*,\ f(z) = \sum_{n=m}^{+\infty} a_n q^{\frac{n}{H}} \quad (\text{avec } m \in \mathbb{Z}) \tag{4.2}$$

et on dit que f est holomorphe à l'infini lorsque $m \geq 0$ dans (4.2).

Que peut-on dire des autres pointes $\alpha \in \mathbb{P}^1(\mathbb{Q})$? Par le lemme 1, il existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma(\infty) = \alpha$. On dit alors que f est **holomorphe** en la pointe α lorsque la fonction faiblement modulaire $f^{[\gamma]_k}$ est holomorphe à l'infini.

Définition 3 : Forme modulaire de poids k pour un sous-groupe de congruence :
On considère $k \in \mathbb{Z}$ et Γ un sous-groupe de congruence.
On appelle **forme modulaire de poids k pour Γ** toute fonction faiblement modulaire de poids k pour Γ qui est holomorphe sur $\mathcal{H}^*$ (c'est-à-dire que pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f^{[\gamma]_k}$ est holomorphe à l'infini).

Lemme 3 :
Si une fonction faiblement modulaire f est holomorphe sur un ensemble de représentants de $C(\Gamma)$, alors elle est holomorphe en tout élément de $\mathbb{P}^1(\mathbb{Q})$.

Preuve :
Soit f une fonction holomorphe et faiblement modulaire sur un ensemble $(c_1, ..., c_n)$ de représentants de $C(\Gamma)$.
Soit $\alpha \in \mathbb{P}^1(\mathbb{Q})$.
Il existe alors $\gamma \in \Gamma$ et $i \in [\![1; n]\!]$ tels que $\gamma(\alpha) = c_i$. Par hypothèse, f est holomorphe en c_i et donc pour $\delta \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\delta(\infty) = c_i$, on a $f^{[\delta]_k}$ est holomorphe en ∞.
Enfin, puisque f est une fonction faiblement modulaire pour Γ, on a :

$$f^{[\delta]_k} = \left(f^{[\gamma]_k}\right)^{[\delta]_k} = f^{[\gamma\delta]_k}.$$

Or, $\gamma(\delta(\infty)) = \gamma(c_i) = \alpha$ donc l'égalité ci-dessus implique que f est holomorphe en α.

■

Proposition 3 :
Soient f et g deux fonctions faiblement modulaires pour un sous-groupe de congruence Γ avec f non identiquement nulle.

- Le produit fg est une fonction faiblement modulaire pour Γ.
- $\dfrac{1}{f}$ est une fonction faiblement modulaire pour Γ.
- Si f et g sont des fonctions modulaires, alors fg est une fonction modulaire pour Γ.
- Si f et g sont des formes modulaires, alors fg est une forme modulaire pour Γ.

Preuve :

- Le produit fg est une fonction méromorphe sur $\mathcal{H}$ (car f et g le sont) et pour tout $\gamma \in \Gamma$ on a :

$$(fg)^{[\delta]_{k+j}} = \frac{1}{(cz+d)^{k+j}}\,(fg \circ \gamma) = \frac{1}{(cz+d)^k}(f \circ \gamma)\frac{1}{(cz+d)^j}(g \circ \gamma) = fg.$$

- La fonction $\dfrac{1}{f}$ est méromorphe sur $\mathcal{H}$ (car f l'est) et pour tout $\gamma \in \Gamma$ on a :

$$\frac{1}{f} = \frac{1}{(cz+d)^{-k}(f \circ \gamma)} = (cz+d)^k \left(\frac{1}{f} \circ \gamma\right) = \left(\frac{1}{f}\right)^{[\gamma]_{-k}}.$$

∗ Soient f et g deux fonctions modulaires.
Comme précédemment, on obtient que fg est une fonction méromorphe sur $\mathcal{H}$. De plus, en écrivant

$$f = \sum_{n=m}^{+\infty} a_n q^n \text{ et } g = \sum_{n=m'}^{+\infty} b_n q^n$$

les q-développements de f et g au voisinage d'une pointe $\alpha \in \mathbb{P}^1(\mathbb{Q})$, on obtient que leur produit formel est égal au q-développement de fg. Or le produit de deux séries de Laurent est encore une série de Laurent dont le disque de convergence est inclus dans l'intersection des disques de convergence. Ainsi fg a un développement en série de Laurent en tout $\alpha \in \mathbb{P}^1(\mathbb{Q})$ et donc en toute pointe.

∗ Nous sommes exactement dans le même cas qu'au dessus, mais puisque f et g sont des formes modulaires, on a $m, m' \geq 0$ et donc la fonction fg est une fonction holomorphe en chaque pointe de $\mathbb{P}^1(\mathbb{Q})$.

■

Remarque :
Si f est une fonction faiblement modulaire de poids impair k pour $\Gamma_0(N)$ pour un certain N, alors f est nulle. En effet, on a $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(N)$ et pour tout $z \in \mathcal{H}$:

$$f(z) = (-1)^{-k} f(\gamma(z)) = -f(z)$$

I.2 Remarques sur les sous-groupes de congruence

Tout sous-groupe de congruence est d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$ (puisque $\Gamma(N)$ l'est). Qu'en est-il de la réciproque : tout sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ est-il un sous-groupe de congruence ?

On peut s'interroger sur la même question mais en remplaçant $\mathrm{SL}_2(\mathbb{Z})$ par d'autres groupes similaires. Si p est un nombre premier, on peut alors montrer que tout sous-groupe d'indice fini de $\mathrm{SL}_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ est un sous-groupe de congruence (c'est-à-dire contient le noyau d'une réduction modulo un entier premier avec p). De même, pour tout $n \in \mathbb{N}\backslash\{0;1;2\}$, tout sous-groupe d'indice fini de $\mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe de congruence. Cependant, il existe des sous-groupes d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ qui ne sont pas des sous-groupes de congruence (il existe même un algorithme qui permet de décider si certains sous-groupes d'indice fini sont des sous-groupes de congruence et donne un exemple de sous-groupe d'indice 12 qui n'est pas un sous-groupe de congruence).

Il est également possible de calculer de l'épaisseur d'une pointe. En effet, considérons Γ un sous-groupe de congruence de niveau N et supposons que $\alpha \in C(\Gamma)$ est une pointe et choisissons $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma(\infty) = \alpha$. L'algorithme suivant nous permet de calculer l'épaisseur h de α pour $\Gamma = \Gamma_0(N)$ ou $\Gamma_1(N)$:

∗ Utiliser l'algorithme d'Euclide étendu pour trouver $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma(\infty) = \alpha$ comme suit :
  — Si $\alpha = \infty$, alors $\gamma = I_2$;
  — Sinon, écrire $\alpha = \dfrac{a}{b}$ et trouver c et d dans $\mathbb{Z}$ tels que $ad - bc = 1$ et poser $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

∗ Calculer dans $\mathcal{M}_2(\mathbb{Z}[x])$:

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1}.$$

∗ Les conditions de congruence définissant Γ donnent quatre congruences linéaires en x qui imposent des conditions. En utilisant des techniques de théorie des nombres ou de dénombrement, trouver le plus petit entier positif h qui vérifie simultanément les quatre congruences.

Exemple 1 :

* Supposons que $\alpha = 0$ et $\Gamma = \Gamma_0(N)$ ou $\Gamma_1(N)$.
  En posant $\gamma = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$ on obtient que $\gamma(\infty) = \alpha$ et de plus, la condition de congruence est :

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ [N].$$

  Ainsi, le plus petit entier positif solution de la congruence ci-dessus est $H = N$, donc l'épaisseur de 0 est N.

* Supposons que $N = pq$ avec p et q deux nombres premiers distincts et posant $\alpha = \dfrac{1}{p}$.
  En posant $\gamma = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$ on obtient que $\gamma(\infty) = \alpha$ et de plus, la condition de congruence pour $\Gamma_0(pq)$ est :

$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 - px & x \\ -p^2 x & px + 1 \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ [pq].$$

  Or, puisque $p^2 x \equiv 0 \ [pq]$, on obtient que le plus petit entier positif solution de la congruence ci-dessus est $x = q$. Ainsi, $\dfrac{1}{p}$ est d'épaisseur q et par symétrie, $\dfrac{1}{q}$ est d'épaisseur p.

Remarque :
Pour $\Gamma_0(N)$, une fois que la valeur inférieure gauche est congrue à 0 modulo N et que le discriminant est 1, la coprimalité des deux autres congruences est automatique. Il y a donc une congruence à résoudre dans le cas de $\Gamma_0(N)$. De même, il y a deux congruences dans le cas de $\Gamma_1(N)$.

II Formules de dimension

Lorsque l'on travaille avec des espaces de formes modulaires, il est très pratique de disposer d'une formule nous donnant la dimension des espaces en jeu afin de s'assurer qu'une famille libre ou génératrice est une base de cet espace (et ces mêmes formules peuvent nous permettre d'améliorer l'efficacité de certains algorithmes car on peut les utiliser pour déterminer la rang de certaines matrices sans avoir à calculer explicitement ces matrices).

On donne dans cette partie des formules pour calculer la dimension de $S_k(\Gamma_0(N))$ et $S_k(\Gamma_1(N))$ mais sans en donner une démonstration (on pourra en trouver une preuve dans [13] (chapitre 3), [16] (chapitre 2) et [17] (chapitre 2)). On introduit également $E_k(\Gamma_0(N))$ (respectivement $E_k(\Gamma_1(N))$) comme étant un supplémentaire de $S_k(\Gamma_0(N))$ (respectivement $S_k(\Gamma_1(N))$) dans $M_k(\Gamma_0(N))$ (respectivement $M_k(\Gamma_1(N))$) que l'on appelle **sous-espace d'Eisenstein**.

Dans toute cette partie, on considère N un entier naturel non nul et p un nombre premier.

II.1 Formes modulaires pour $\Gamma_0(N)$

Posons :

$$\mu_0(N) = \prod_{\substack{p\in\mathcal{P}\\ p|N}} \left(p^{v_p(N)} + p^{v_p(N)-1}\right);$$

$$\mu_{0,2}(N) = \begin{cases} 0 & \text{si } 4|N \\ \displaystyle\prod_{\substack{p\in\mathcal{P}\\ p|N}} \left(1+\left(\frac{-4}{p}\right)\right) & \text{sinon} \end{cases};$$

$$\mu_{0,3}(N) = \begin{cases} 0 & \text{si } 2|N \text{ ou } 9|N \\ \displaystyle\prod_{\substack{p\in\mathcal{P}\\ p|N}} \left(1+\left(\frac{-3}{p}\right)\right) & \text{sinon} \end{cases};$$

$$c_0(N) = \sum_{\substack{d|N\\ d\geq 1}} \varphi\left(\text{PGCD}\left(d, \frac{N}{d}\right)\right)$$

$$\text{et } g_0(N) = 1 + \frac{\mu_0(N)}{12} - \frac{\mu_{0,2}(N)}{4} - \frac{\mu_{0,3}(N)}{3} - \frac{c_0(N)}{2}.$$

Proposition 4 :
On a $\dim_{\mathbb{C}}\left(S_2\left(\Gamma_0(N)\right)\right) = g_0(N)$ et pour tout entier naturel $k \geq 4$ pair :

$$\dim_{\mathbb{C}}\left(S_k\left(\Gamma_0(N)\right)\right) = (k-1)(g_0(N)-1) + \left(\frac{k}{2}-1\right)c_0(N) + \mu_{0,2}(N)\left\lfloor\frac{k}{4}\right\rfloor + \mu_{0,3}\left\lfloor\frac{k}{3}\right\rfloor.$$

De plus, la dimension du sous-espace d'Eisenstein est :

$$\dim_{\mathbb{C}}\left(E_k(\Gamma_0(N))\right) = \begin{cases} c_0(N) & \text{si } k \neq 2 \\ c_0(N)-1 & \text{si } k = 2. \end{cases}$$

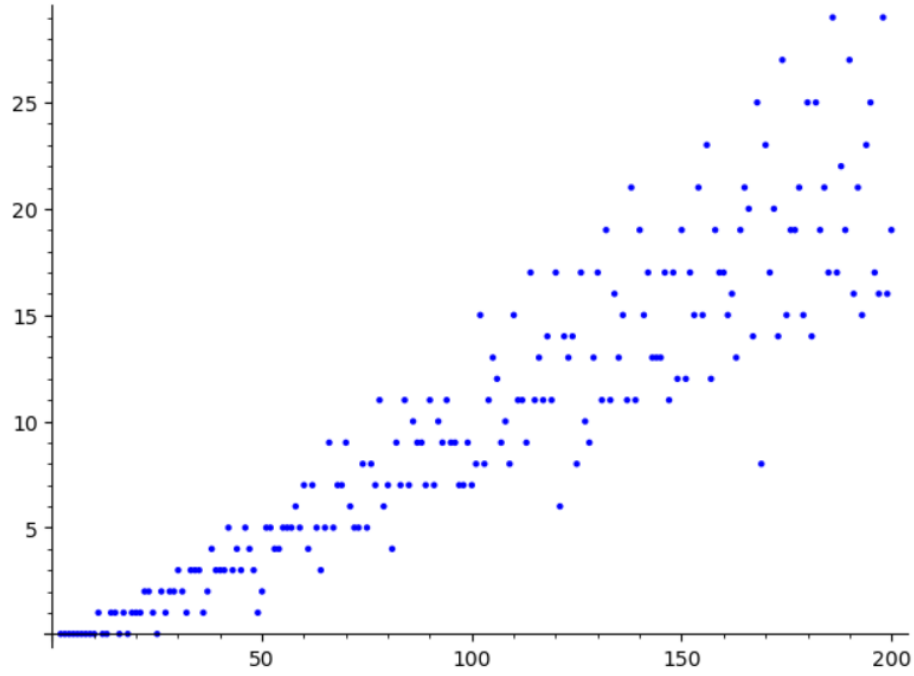
On donne ci-dessous une table de la dimension de $S_k(\Gamma_0(N))$ pour quelques valeurs de N et k :

N	$S_2(\Gamma_0(N))$	$S_4(\Gamma_0(N))$	$S_6(\Gamma_0(N))$	$S_{24}(\Gamma_0(N))$
1	0	0	0	2
10	0	3	5	33
11	1	2	4	22
100	7	36	66	336
389	32	97	161	747
1 000	131	430	730	3 430
2 007	221	806	1 346	6 206
100 000	14 801	44 800	74 800	344 800

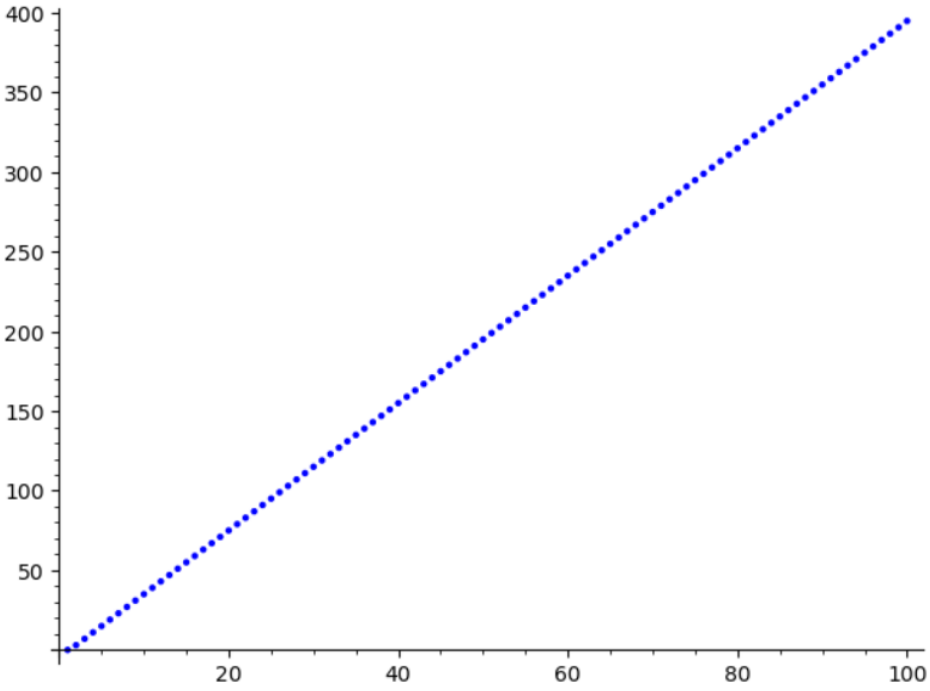
Remarque :
Il est possible d'obtenir les dimensions des espaces $S_k(\Gamma_0(N))$, $E_k(\Gamma_0(N))$ et $M_k(\Gamma_0(N))$ grâce aux commandes respectives `dimension_cusp_forms`, `dimension_eis`, et `dimension_modular_forms`. On obtient par exemple :

```
sage: dimension_cusp_forms(Gamma0(2007),2)
sage: 221
sage: dimension_eis(Gamma0(2007),2)
sage: 7
sage: dimension_modular_forms(Gamma0(2007),2)
sage: 228
```

On donne ci-dessous le graphique de la fonction $N \longmapsto \dim_{\mathbb{C}} \left(S_2\left(\Gamma_0(N)\right)\right)$:



On donne également le graphique de la fonction $k \longmapsto S_{2k}(\Gamma_0(12))$:



II.2 Formes modulaires pour $\Gamma_1(N)$

Cette sous-partie ressemblera assez fidèlement à la précédente mais en remplaçant $\Gamma_0(N)$ par $\Gamma_1(N)$.

en écrivant $\psi(N) = [\Gamma_0(N) : \Gamma_1(N)]$, on pose :

$$\mu_1(N) = \begin{cases} \mu_0(N) & \text{si } N \in \{1;2\} \\ \dfrac{\psi(N)\mu_0(N)}{2} & \text{sinon} \end{cases} ;$$

$$\mu_{1,2}(N) = \begin{cases} 0 & \text{si } N \geq 4 \\ \mu_{0,2}(N) & \text{sinon} \end{cases} ;$$

$$\mu_{1,3}(N) = \begin{cases} 0 & \text{si } N \geq 4 \\ \mu_{0,3}(N) & \text{sinon} \end{cases} ;$$

$$c_1(N) = \begin{cases} c_0(N) & \text{si } N \in \{1;2\} \\ 3 & \text{si } N = 4 \\ \displaystyle\sum_{\substack{d|N \\ d\geq 1}} \frac{\psi(d)\psi\left(\frac{N}{d}\right)}{2} & \text{sinon} \end{cases}$$

$$\text{et } g_1(N) = 1 + \frac{\mu_1(N)}{12} - \frac{\mu_{1,2}(N)}{4} - \frac{\mu_{1,3}(N)}{3} - \frac{c_1(N)}{2}.$$

Proposition 5 :

* On a $\dim_{\mathbb{C}}\left(S_2\left(\Gamma_1(N)\right)\right) = g_1(N)$.

* Si $N \geq 2$, alors $\Gamma_0(N) = \Gamma_1(N)$, donc $\dim_{\mathbb{C}}(S_k(\Gamma_1(N))) = \dim_{\mathbb{C}}(S_k(\Gamma_0(N)))$.

* Si $k \geq 3$ et $N \geq 3$, alors en posant

$$a = (k-1)(g_1(N)-1) + \left(\frac{k}{2} - 1\right) c_1(N)$$

on a :

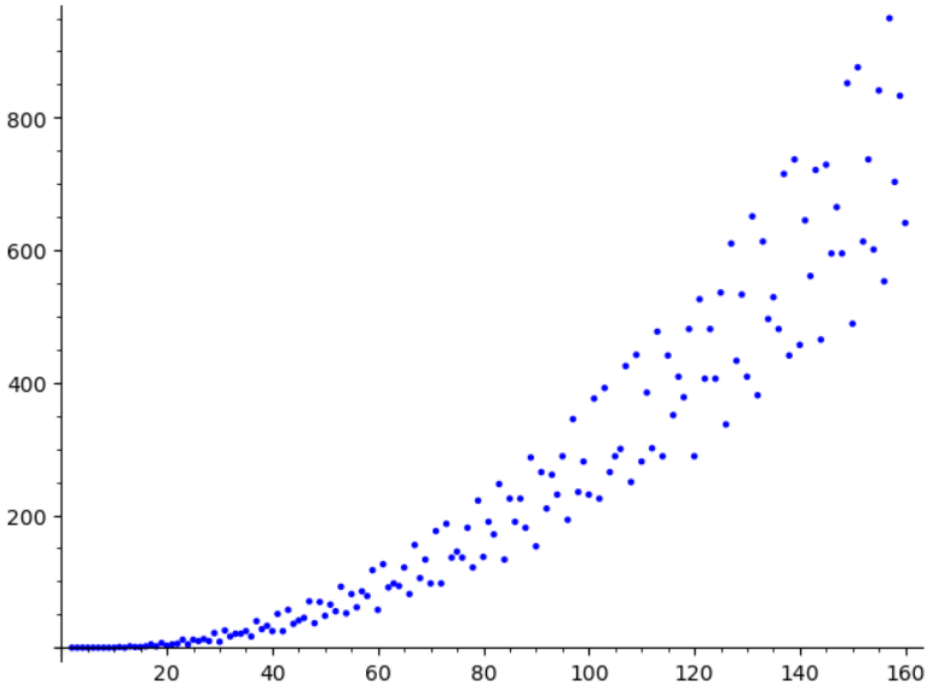
$$\dim_{\mathbb{C}}\left(S_k\left(\Gamma_1(N)\right)\right) = \begin{cases} a + \dfrac{1}{2} & \text{si } N = 4 \text{ et } 2 \nmid k \\ a + \left\lfloor \dfrac{k}{3} \right\rfloor & \text{si } N = 3 \\ a & \text{sinon.} \end{cases}$$

De plus, la dimension du sous-espace d'Eisenstein est :

$$\dim_{\mathbb{C}}\left(E_k(\Gamma_0(N))\right) = \begin{cases} c_1(N) & \text{si } k \neq 2 \\ c_1(N) - 1 & \text{si } k = 2. \end{cases}$$

Remarque :
Puisque $M_k(\Gamma_1(N)) = S_k(\Gamma_1(N)) \oplus E_k(\Gamma_1(N))$, les formules de la proposition 5 conduisent à une formule pour la dimension de $M_k(\Gamma_1(N))$.

On donne ci-dessous le graphique de la fonction $N \longmapsto \dim_{\mathbb{C}} (S_2(\Gamma_1(N)))$:



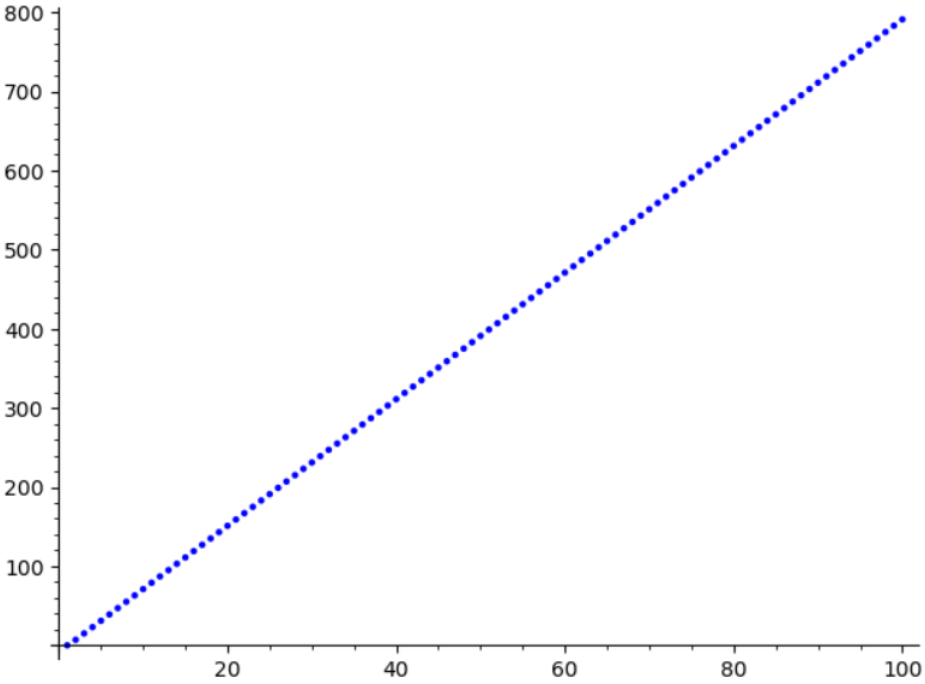
La table suivante contient la dimension de $S_k(\Gamma_1(N))$ pour quelques valeurs de N et k :

N	$S_2(\Gamma_1(N))$	$S_3(\Gamma_1(N))$	$S_4(\Gamma_1(N))$	$S_{24}(\Gamma_1(N))$
1	0	0	0	2
10	0	2	5	65
11	1	5	10	110
100	231	530	830	6 830
389	6 112	12 416	18 721	144 821
1 000	28 921	58 920	88 920	688 920
2 007	147 409	296 592	445 776	3 429 456
100 000	299 792 001	599 792 000	899 792 000	6 899 792 000

On peut également obtenir les dimensions de $M_k(\Gamma_1(N))$, $S_k(\Gamma_1(N))$ et $E_k(\Gamma_1(N))$ avec `SAGE` avec les mêmes commandes que précédemment. Par exemple :

```
sage: dimension_cusp_forms(Gamma1(2007),2)
sage: 147409
sage: dimension_eis(Gamma1(2007),2)
sage: 3551
sage: dimension_modular_forms(Gamma1(2007),2)
sage: 150960
```

On donne finalement le graphique de la fonction $k \longmapsto S_{2k}(\Gamma_1(12))$:



On remarquera que pour des petites valeurs de N, le graphique de cette fonction est très semblable à son analogue pour $S_{2k}(\Gamma_0(12))$ en termes de régularité et la croissance de la dimension semble être deux fois plus rapide $S_{2k}(\Gamma_1(12))$ que pour $S_{2k}(\Gamma_0(12))$.

Chapitre 5

Quelques applications

Dans ce dernier chapitre, on donne de nouvelles applications des formes modulaires en s'intéressant tout d'abord à la série d'Eisenstein de poids 2 qui nous permettra d'obtenir de nouvelles relations et qui nous sera utile dans la partie suivante consacrée à la fonction θ de Jacobi et qui permet d'exprimer des résultats sur le nombre de représentations d'un entier sous forme d'une somme de carrés. Dans une troisième partie on s'intéresse aux formes modulaires et aux opérateurs différentiels ainsi qu'au crochet de Rankin-Cohen qui nous permet d'obtenir d'autres identités arithmétiques. Enfin, on conclut ce chapitre par une dernière partie sur le dernier théorème de Fermat.

I Série d'Eisenstein de poids 2

Dans cette partie, nous allons étudier un peu plus en détail la série d'Eisenstein de poids 2 qui est apparue lors de la preuve de la formule du produit de Jacobi pour Δ (théorème 6 du chapitre 2).

Définition 1 : Série d'Eisenstein de poids 2 :
On appelle **série d'Einsenstein de poids 2** la série G_2 définie sur $\mathcal{H}$ par :

$$G_2(z) = \sum_{c\in\mathbb{Z}} \left({\sum_{d\in\mathbb{Z}}}' \frac{1}{(cz+d)^2} \right).$$

où la sommation porte sur les paires $(c,d) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ (afin que la division par $cz+d$ ait un sens).

L'inconvénient de cette série est qu'elle converge mais pas absolument et donc sa manipulation est plus délicate que les séries d'Eisenstein G_4, G_6 ou G_8 par exemple... Cependant, nous avons tout de même réussi à monter que l'on a :

$$\forall z \in \mathcal{H},\ G_2(z) = \frac{\pi^2}{3}\left(1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right) = 2\zeta(2) - 8\pi^2\sum_{n=1}^{+\infty}\sigma_1(n)q^n. \tag{5.1}$$

ainsi que la relation :

$$\forall z \in \mathcal{H},\ G_2\left(-\frac{1}{z}\right) = z^2 G_2(z) - 2i\pi z. \tag{5.2}$$

Remarque :
On remarquera que le q-développement de G_2 prolonge la formule générale pour le q-développement de G_k (cf. proposition 10 du chapitre 2) au cas $k = 2$.

Dans la même veine que pour les séries d'Eisenstein, on introduit une normalisation :

Définition 2 : Série d'Eisenstein normalisée de poids 2 :
On appelle **série d'Eisenstein normalisée de poids 2** la fonction définie sur $\mathcal{H}$ par :

$$E_2 : z \longmapsto \frac{-1}{8\pi^2}G_2(z).$$

On obtient alors :

$$E_2(z) = \frac{-2\zeta(2)}{8\pi^2} + \sum_{n=1}^{+\infty} \sigma_1(n) q^n = \frac{-1}{24} + \sum_{n=1}^{+\infty} \sigma_1(n) q^n. \tag{5.3}$$

La série G_2 (et donc également E_2) n'est pas une forme modulaire de poids 2 et de niveau 1 ! En effet, on peut le constater via l'expression (5.2) ou bien grâce à la proposition 13.

Proposition 1 :
Pour tout $z \in \mathcal{H}$, on a :

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) - \frac{z}{4i\pi}.$$

En particulier, on a $E_2(i) = -\frac{1}{8\pi}$.

Preuve :
Soit $z \in \mathcal{H}$.
En utilisant la relation (5.2) et en multipliant de chaque côtés par $\frac{-1}{8\pi^2}$, on obtient :

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{2i\pi z}{8\pi^2} = z^2 E_2(z) + \frac{iz}{4\pi} = z^2 E_2(z) - \frac{z}{4i\pi}.$$

En particulier, en $z = i$ on a alors :

$$E_2\left(-\frac{1}{i}\right) = E_2(i) = i^2 E_2(i) - \frac{i}{4i\pi} = -E_2(i) - \frac{1}{4\pi}.$$

C'est-à-dire :

$$E_2(i) = -\frac{1}{2} \times \frac{1}{4\pi} = -\frac{1}{8\pi}.$$

■

Corollaire 1 :
On a la relation :

$$\sum_{n=1}^{+\infty} \frac{n}{e^{2\pi n} - 1} = \frac{1}{24} - \frac{1}{8\pi}.$$

Preuve :
Par la proposition 1, on sait que $E_2(i) = -\frac{1}{8\pi}$.
Or on a également le q-développement de E_2 en $z = i$ par la relation (5.3) :

$$E_2(i) = \frac{-1}{24} + \sum_{n=1}^{+\infty} \sigma_1(n) e^{-2\pi n} = \frac{-1}{24} + \sum_{n=1}^{+\infty} \frac{n e^{-2\pi n}}{1 - e^{-2\pi n}} = \frac{-1}{24} + \sum_{n=1}^{+\infty} \frac{n}{e^{2\pi n} - 1}.$$

D'où, en comparant les résultats obtenus :

$$\sum_{n=1}^{+\infty} \frac{n}{e^{2\pi n} - 1} = \frac{1}{24} - \frac{1}{8\pi}.$$

■

Nous allons désormais étudier plus en détail la fonction G_2.
On sait grâce à la preuve de la formule du produit de Jacobi pour Δ que :

$$\forall z \in \mathcal{H},\ G_2(z) = \sum_{d\in\mathbb{Z}^*} \frac{1}{d^2} + \sum_{c\in\mathbb{Z}^*} \sum_{d=-\infty}^{+\infty} \frac{1}{(cz+d)^2}$$

qui s'écrit aussi :

$$\forall z \in \mathcal{H},\ G_2(z) = 2\sum_{d=1}^{+\infty} \frac{1}{d^2} + 2\sum_{c=1}^{+\infty} \sum_{d\in\mathbb{Z}} \frac{1}{(cz+d)^2}.$$

Pour déterminer le comportement de cette fonction sous l'action de $\mathrm{SL}_2(\mathbb{Z})$, on introduit une déformation pour un $\varepsilon > 0$ fixé :

$$\forall z \in \mathcal{H},\ G_2^\varepsilon(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^2|mz+n|^{2\varepsilon}}.$$

On définit également sur $\mathcal{H}$ la fonction $G_2^\star : z \longmapsto \lim\limits_{\varepsilon\to 0^+} G_2^\varepsilon(z)$ (l'existence de cette limite est donnée par un résultat de continuité sous la somme pour $\varepsilon > -\dfrac{1}{2}$, suivant le même principe que les raisonnements qui vont suivre).

Par le même argument que la proposition 6 du chapitre 2, on obtient :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ G_2^\varepsilon\left(\frac{az+b}{cz+d}\right) = (cz+d)^2|cz+d|^{2\varepsilon} G_2^\varepsilon(z). \tag{5.4}$$

On a alors par passage à la limite :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ G_2^\star\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_2^\star(z). \tag{5.5}$$

On pose, pour $\varepsilon > -\dfrac{1}{2}$:

$$\forall z \in \mathcal{H},\ I_\varepsilon(z) = \int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{(z+t)^2|z+t|^{2\varepsilon}}.$$

Ainsi :

$$\forall z \in \mathcal{H},\ G_2^\varepsilon(z) - 2\sum_{c=1}^{+\infty} I_\varepsilon(cz) = 2\sum_{d=1}^{+\infty} \frac{1}{d^{2(1+\varepsilon)}} + 2\sum_{c=1}^{+\infty} \sum_{d=-\infty}^{+\infty} \underbrace{\left[\frac{1}{(cz+d)^2|cz+d|^{2\varepsilon}} - \int_d^{d+1} \frac{\mathrm{d}t}{(cz+t)^2|cz+t|^{2\varepsilon}}\right]}_{=O(|cz+d|^{-3-2\varepsilon})}.$$

Montrons que le membre de droite est une quantité continue par rapport à $\varepsilon > -\dfrac{1}{2}$:
Pour $c > 0$, $z \in \mathcal{H}$ et $d \in \mathbb{Z}$, l'application :

$$J_{c,d,z} : \varepsilon \longmapsto \int_d^{d+1} \frac{\mathrm{d}t}{(cz+t)^2|cz+t|^{2\varepsilon}}$$

est continue (car l'intégration se fait sur un segment et l'intégrande est continue sur ce même segment). Ainsi, le terme ci-dessus entre crochets, que l'on note $f_z((c,d),\varepsilon)$, est une fonction mesurable telle que pour tout $(c,d) \in \mathbb{Z}^2$, la fonction $\varepsilon \longmapsto f_z((c,d),\varepsilon)$ est continue.

De plus, pour $z \in \mathcal{H}$ fixé et $\varepsilon_0 \in \left]\varepsilon; -\dfrac{1}{2}\right[$, il n'y a qu'un nombre fini de couples $(c,d) \in \mathbb{Z}^2$ tels que $|cz+d| < 1$, donc :

$$|f_z((c,d),\varepsilon)| = O\left(|cz+d|^{-3-2\varepsilon_0}\right).$$

On a donc continuité sous la somme, et un raisonnement identique donne la continuité par rapport à ε de la première somme (sur $d > 0$).

Le membre de droite étant continu par rapport à $\varepsilon > -\frac{1}{2}$, il admet une limite fini en $\varepsilon = 0$ et celle-ci est donnée en remplaçant ε par 0 dans l'expression. On obtient alors :

$$\forall z \in \mathcal{H},\ G_2^\star(z) - 2\lim_{\varepsilon\to 0^+}\sum_{c=1}^{+\infty} I_\varepsilon(cz) = 2\sum_{d=1}^{+\infty}\frac{1}{d^2} + 2\sum_{c=1}^{+\infty}\sum_{d=-\infty}^{+\infty}\left[\frac{1}{(cz+d)^2} - \int_d^{d+1}\frac{\mathrm{d}t}{(cz+t)^2}\right].$$

Or, on a :

$$\sum_{c=1}^{+\infty}\left(\sum_{d=-\infty}^{+\infty}\left(\int_d^{d+1}\frac{\mathrm{d}t}{(cz+t)^2}\right)\right) = \sum_{c=1}^{+\infty}\left(\underbrace{\int_{-\infty}^{+\infty}\frac{\mathrm{d}t}{(cz+t)^2}}_{=0}\right) = 0.$$

D'où :

$$\forall z \in \mathcal{H},\ G_2^\star(z) - 2\lim_{\varepsilon\to 0^+}\sum_{c=1}^{+\infty} I_\varepsilon(cz) = G_2(z).$$

Par ailleurs, pour tous $x, y \in \mathbb{R}$ on a :

$$I_\varepsilon(x+iy) = \int_{-\infty}^{+\infty}\frac{\mathrm{d}t}{(x+t+iy)^2\left((x+t)^2+y^2\right)^\varepsilon} = \int_{-\infty}^{+\infty}\frac{\mathrm{d}u}{(u+iy)^2(u^2+y^2)^\varepsilon} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}}$$

où

$$I(\varepsilon) = \int_{-\infty}^{+\infty}(u+i)^{-2}(u^2+1)^{-\varepsilon}\mathrm{d}u.$$

On a donc :

$$\forall z \in \mathcal{H},\ \sum_{c=1}^{+\infty} I_\varepsilon(cz) = \sum_{c=1}^{+\infty}\frac{I(\varepsilon)}{c^{1+2\varepsilon}y^{1+2\varepsilon}} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}}\zeta(1+2\varepsilon)$$

et puisque I est une fonction de classe $\mathcal{C}^1$ telle que $I(0) = 0$, $I'(0) = -\pi$ et $\zeta(1+2\varepsilon) = \frac{1}{2\varepsilon} + O(1)$ on obtient :

$$\lim_{\varepsilon\to 0^+}\frac{I(\varepsilon)}{y^{1+2\varepsilon}}\zeta(1+2\varepsilon) = -\frac{\pi}{2y}.$$

Finalement, on trouve que :

$$\forall z \in \mathcal{H},\ G_2^\star(z) = G_2(z) - \frac{\pi}{y}. \tag{5.6}$$

Remarque :
On obtient en particulier que $G_2^\star$ n'est pas holomorphe à l'infini à cause de la présence du terme $\frac{\pi}{y}$!

Proposition 2 :
On a la relation :

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \forall z \in \mathcal{H},\ G_2^{[\gamma]_2}(z) = G_2(z) - \frac{2i\pi c}{cz+d}$$

Preuve :
Soit $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.
On vérifie par le calcul que pour tout $z = x + iy \in \mathcal{H}$, on a :

$$\frac{1}{\mathrm{Im}(\gamma.z)} = \frac{|cz+d|^2}{y} = \frac{(cz+d)^2}{\mathrm{Im}(z)} - 2ic(cz+d)$$

soit :

$$\frac{\pi}{(cz+d)^2\,\mathrm{Im}(\gamma.z)} = \frac{\pi}{\mathrm{Im}(z)} - \frac{2i\pi c}{cz+d}.$$

Ainsi, pour tout $z \in \mathcal{H}$, on a par les relations (5.5) et (5.6) que :

$$G_2^{[\gamma]_2}(z) = (cz+d)^{-2} G_2(\gamma.z) = (cz+d)^{-2} G_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-2}\left(G_2^\star\left(\frac{az+b}{cz+d}\right) + \frac{\pi}{\operatorname{Im}(\gamma.z)}\right)$$
$$= G_2^\star(z) + \frac{\pi}{(cz+d)^2 \operatorname{Im}(\gamma.z)} = \left(G_2(z) - \frac{\pi}{\operatorname{Im}(z)}\right) + \left(\frac{\pi}{\operatorname{Im}(z)} - \frac{2i\pi c}{cz+d}\right) = G_2(z) - \frac{2i\pi c}{(cz+d)}$$

■

On donne le lemme suivant dont la démonstration est admise (mais le lecteur intéressé pourra en trouver une preuve dans l'exercice 1.2.6 de [13]) et qui nous sera utile pour la proposition qui suit.

Lemme 1 :
Soient $f : \mathcal{H} \longrightarrow \mathbb{C}$ et Γ un sous-groupe de congrunce de $\mathrm{SL}_2(\mathbb{Z})$ de niveau N.
Si l'on a :

- f holomorphe sur $\mathcal{H}$.
- Pour tout $\gamma \in \Gamma$, on a $f^{[\gamma]_k} = f$.
- f admet un q-développement du type $f(z) = \sum_{n=n_0}^{+\infty} a_n q^{\frac{n}{N}}$ avec $n_0 \geq 0$ et $a_n = O\left(n^r\right)$ pour $r > 0$.

alors f est une forme modulaire de poids k pour le groupe de congruence Γ de niveau N.

Proposition 3 :
Pour tout $N \in \mathbb{N}^*$, la fonction $G_{2,N}$ définie sur $\mathcal{H}$ par $G_{2,N}(z) = G_2(z) - NG_2(Nz)$ définit une forme modulaire appartenant à $M_2(\Gamma_0(N))$.

Preuve :
Soient $N \in \mathbb{N}^*$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.
Pour tout $z \in \mathcal{H}$, on a la relation :

$$N(\gamma.z) = N\left(\frac{az+b}{cz+d}\right) = \frac{Naz+Nb}{cz+d} = \frac{a(Nz)+bN}{\frac{c}{N}(Nz)+d} = \underbrace{\begin{pmatrix} a & bN \\ \frac{c}{N} & d \end{pmatrix}}_{=\gamma'}.(Nz).$$

Or comme $\gamma \in \Gamma_0(N)$, on a $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. Donc par la proposition 2 :

$$\begin{aligned} G_{2,N}^{[\gamma]_2}(z) &= G_2(z) - \frac{2i\pi c}{cz+d} - N(cz+d)^{-2} G_2(N(\gamma.z)) \\ &= G_2(z) - \frac{2i\pi c}{cz+d} - N(cz+d)^{-2}\left(\frac{c}{N}Nz+d\right)^2 G_2(Nz) + \frac{2i\pi N\frac{c}{N}}{\frac{c}{N}Nz+d} \\ &= G_2(z) - \frac{2i\pi c}{cz+d} - NG_2(Nz) + \frac{2i\pi c}{cz+d} \\ &= G_2(z) - NG_2(Nz) \\ &= G_{2,N}(z) \end{aligned}$$

La fonction $G_{2,N}$ est holomorphe sur $\mathcal{H}$ et à l'infini (grâce au q-développement de G_2) et les coefficients du q-développement sont majorés (à une constante multiplicative près) par $\sigma(n) = O\left(n^2\right)$, donc par le lemme 1 on a $G_{2,N} \in M_2(\Gamma_0(4))$.

■

II Fonction thêta

Si Q est une forme quadratique définie positive à coefficients entiers en m variables, alors on peut y associer une forme modulaire de poids $\frac{m}{2}$ (m ici peut être impair mais nous ne parlerons pas de formes modulaires de poids non entier) appelée **fonction thêta de** Q et dont le n-ième coefficient de son q-développement (pour $n \geq 0$) est le nombre de représentations de l'entier n par Q. Il s'agit d'une des principales constructions de formes modulaires et l'une des sources les plus importantes d'applications de la théorie.

Nous n'étudierons ici que la fonction thêta à une variable, ce cas est le plus classique et remonte à Jacobi mais possède déjà beaucoup d'applications. C'est également la base de la théorie générale car toute forme quadratique peut-être diagonalisée sur $\mathbb{Q}$ (c'est-à-dire qu'en passant à un sous-réseau approprié elle devient somme directe de m formes quadratiques d'une seule variable).

II.1 La fonction θ de Jacobi

Notons

$$r(n,k) = \text{Card}\left(\left\{ v = (v_1, ..., v_k) \in \mathbb{Z}^k \;\middle|\; n = \sum_{i=1}^{k} v_i^2 \right\}\right)$$

le nombre de représentations de l'entier n en somme de k carrés (en prenant en compte l'ordre des termes).

Exemple 1 :

* On a par exemple :

$$5 = 0^2 + 0^2 + 1^2 + 2^2 = 0^2 + 0^2 + (-1)^2 + 2^2 = 0^2 + 0^2 + 1^2 + (-2)^2 = (-1)^2 + 0^2 + 0^2 + 2^2 = \cdots$$

  En fait, on peut montrer que $r(5,4) = 48$.

* De même, on a :

$$91 = 0^2 + 1^2 + 3^2 + 9^2 = 4^2 + 5^2 + 5^2 + 5^2 = 1^2 + 4^2 + 5^2 + 7^2 = \cdots$$

  On peut également montrer que $r(91,4) = 896$.

La première remarque que l'on peut faire est que si l'on a une relation du type $i + j = k$, alors on peut montrer par des arguments combinatoires que l'on a

$$r(n,k) = \sum_{\ell=0}^{n} r(\ell, i) r(n-\ell, j). \tag{5.7}$$

Cela ressemble énormément à la règle $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ pour obtenir les coefficients du produit de Cauchy de deux séries entières

$$\left(\sum_{k=0}^{+\infty} a_k z^k\right)\left(\sum_{i=0}^{+\infty} b_i z^i\right) = \sum_{j=0}^{+\infty} c_j z^j.$$

On considère alors la "série génératrice des $r(n,k)$", c'est-à-dire la série définie sur $\mathcal{H}$ par :

$$\theta(z,k) = \sum_{n=0}^{+\infty} r(n,k) q^n$$

Proposition 4 :
Pour tout $k \in \mathbb{N}$, la série $\theta(z,k)$ est absolument convergente sur $\mathcal{H}$.

Preuve :
Soient $z \in \mathcal{H}$ et $k \in N$.
Pour $n \in \mathbb{N}$, lorsque l'on a une décomposition du type $n = v_1^2 + ...v_k^2$, on peut grossièrement majorer chaque v_i par $\sqrt{n}$ et donc on peut également majorer $r(n,k)$ par $\sqrt{n}^k$ (noter qu'ici l'ordre des termes a été pris en compte). Ainsi, on a :

$$\forall n \in \mathbb{N},\ |r(n,k)q^n| \leq \sqrt{n}^k e^{-2n\pi \operatorname{Im}(z)}$$

Or, comme $z \in \mathcal{H}$, on a $\operatorname{Im}(z) > 0$ et donc $\sqrt{n}^k e^{-2n\pi \operatorname{Im}(z)} \underset{n\to+\infty}{=} o\left(\frac{1}{n^2}\right)$. Ainsi, par comparaison de fonctions positives, on en déduit que la série $\theta(z,k)$ converge absolument sur $\mathcal{H}$.

■

Proposition 5 :
Pour tous $k_1, k_2 \in \mathbb{N}$ et pour tout $z \in \mathcal{H}$, on a :

$$\theta(z,k_1)\theta(z,k_2) = \theta(z,k_1+k_2).$$

Preuve :
Soient $k_1, k_2 \in \mathbb{N}$ et $z \in \mathcal{H}$.
Par la proposition 4, les séries $\theta(n,k_1)$ et $\theta(n,k_2)$ sont absolument convergentes sur $\mathcal{H}$, on peut donc faire leur produit de Cauchy :

$$\theta_1(z,k_1)\theta_2(z,k_2) = \left(\sum_{i=0}^{+\infty} r(i,k_1)q^i\right)\left(\sum_{j=0}^{+\infty} r(j,k_2)q^j\right) = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} r(k,k_1)r(n-k,k_2)\right)q^n$$

Or par la relation (5.7), on a

$$\sum_{k=0}^{n} r(k,k_1)r(n-k,k_2) = r(n,k_1+k_2).$$

D'où :

$$\theta_1(z,k_1)\theta_2(z,k_2) = \left(\sum_{n=0}^{+\infty} r(n,k_1+k_2)q^n\right) = \theta(z,k_1+k_2)$$

■

Remarque :
De plus, puisque $z \longmapsto \theta(z,k)$ est une fonction en q est que q est 1-périodique, on obtient également pour $k > 0$ fixé et $z \in \mathcal{H}$ que $\theta(z+1,k) = \theta(z,k)$.

Définition 3 : Fonction θ de Jacobi :
On appelle **fonction θ de Jacobi** la fonction définie sur $\mathcal{H}$ par

$$\theta(z) = \theta(z,1) = \sum_{n=0}^{+\infty} r(n,1)q^n = \sum_{n\in\mathbb{Z}} q^{n^2}.$$

En effet, on remarque que $r(n,1) = 2$ si n est un carré et 0 sinon. On a alors :

$$\forall z \in \mathcal{H},\ \theta(z) = \sum_{m^2\in\mathbb{N}} 2q^{m^2} = \sum_{n\in\mathbb{Z}} q^{n^2}.$$

On remarque également que cette expression ressemble à un des deux membres de la formule sommatoire de Poisson dont on rappelle l'énoncé ci-dessous pour des fonctions dans la classe de Schwarz $\mathcal{S}(\mathbb{R})$:

Proposition 6 : Formule sommatoire de Poisson :
Soit $f \in \mathcal{S}(\mathbb{R})$.
On a la relation

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n), \text{ où } \widehat{f}(n) = \int_{\mathbb{R}} f(t)e^{-2i\pi nt}\mathrm{d}t.$$

Lemme 2 :
Soit $b \in \mathbb{R}_+^*$.

La transformée de Fourier de la fonction f définie sur $\mathbb{R}$ par $f(x) = e^{-bx^2}$ est donnée par $\widehat{f}(\xi) = \sqrt{\frac{\pi}{b}}e^{-\frac{\xi^2}{4b}}$.

Preuve :
Soit $b \in \mathbb{R}_+^*$.
On considère l'application :

$$f : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ (x,\xi) & \longmapsto & e^{-bx^2}e^{-ix\xi} \end{array} \right.$$

* L'application $x \longmapsto f(x,\xi)$ est intégrable car $\displaystyle\int_{\mathbb{R}} e^{-bx^2}\mathrm{d}x = \sqrt{\frac{\pi}{b}}$ (intégrale de Gauss).
* L'application $\xi \longmapsto f(x,\xi)$ est dérivable sur $\mathbb{R}$.
* Pour tout $(x,\xi) \in \mathbb{R}^2$, on a $\left|\dfrac{\partial f}{\partial \xi}(x,\xi)\right| = \left|-ixe^{-bx^2}e^{-ix\xi}\right| \leq \left|xe^{-bx^2}\right| = o\left(\dfrac{1}{x^2}\right)$ (majoration indépendante de ξ).

Donc par le théorème de dérivation sous le signe intégrale, on obtient :

$$\forall \xi \in \mathbb{R},\ \widehat{f}'(\xi) = -\int_{\mathbb{R}} e^{-bx^2} \times ixe^{-ix\xi}\mathrm{d}x$$

On a donc pour tout $\xi \in \mathbb{R}^2$, on a :

$$\begin{aligned}\widehat{f}'(\xi) &= \frac{i}{2b}\int_{\mathbb{R}} -2bxe^{-bx^2}e^{-ix\xi}\mathrm{d}x \underset{I.P.P.}{=} \frac{i}{2b}\left[e^{-bx^2}e^{-ix\xi}\right]_{-\infty}^{+\infty} + \frac{i}{2b}\int_{\mathbb{R}} e^{-bx^2}i\xi e^{-ix\xi}\mathrm{d}x \\ &= 0 + \frac{-\xi}{2b}\int_{\mathbb{R}} e^{-bx^2}e^{-ix\xi}\mathrm{d}x = \frac{-\xi}{2b}\widehat{f}(\xi)\end{aligned}$$

Ainsi, l'application $\widehat{f}$ est solution du problème de Cauchy suivant :

$$(PC) : \left\{ \begin{array}{l} y'(t) + \dfrac{t}{2b}y(t) = 0 \\ y(0) = \sqrt{\dfrac{\pi}{b}} \end{array} \right.$$

Finalement, on donc bien $\widehat{f}(\xi) = \sqrt{\frac{\pi}{b}}e^{-\frac{\xi^2}{4b}}$.

■

Proposition 7 :
Pour tout $z \in \mathcal{H}$, on a :

$$\theta\left(-\frac{1}{4z}\right) = \sqrt{-2iz}\theta(z)$$

où $\sqrt{-2iz} = e^{\frac{1}{2}\operatorname{Log}(-2iz)}$ avec Log la détermination principale du logarithme.

Preuve :
Soit $y > 0$.
Considérons les fonctions f et g définies sur $\mathbb{R}$ respectivement par $f(t) = e^{-\pi t^2}$ et $g(t) = f\left(\sqrt{y}t\right) = e^{-\pi t^2 y}$.
La fonction g appartient à $\mathcal{S}(\mathbb{R})$ car elle est clairement de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ (car composée de fonctions de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$) et g et ses dérivées sont à décroissance rapide par les croissances comparées. On a alors par la formule sommatoire de Poisson et les règles de calcul sur les transformées de Fourier que :

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = \frac{1}{\sqrt{y}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{y}}.$$

En posant $z = \dfrac{iy}{2}$, on a alors :

$$\theta\left(\frac{-1}{4z}\right) = \sqrt{-2iz}\theta(z)$$

avec $\sqrt{-2iz} = e^{\frac{1}{2}\operatorname{Log}(-2iz)}$ et Log la détermination principale du logarithme (possible ici car $2iz \in \mathcal{H}$).

Or cette relation est vraie sur $i\,\mathbb{R}_+^*$ qui admet un point d'accumulation dans $\mathcal{H}$ (qui est un ouvert connexe de $\mathbb{C}$) et les deux fonctions dans cette même relation sont holomorphes, donc par le principe du prolongement analytique, on obtient :

$$\forall z \in \mathcal{H},\ \theta\left(\frac{-1}{4z}\right) = \sqrt{-2iz}\theta(z).$$

■

Or cette règle de transformation n'est pas satisfaisante pour notre étude car l'homographie $z \longmapsto \dfrac{-1}{4z}$ est représentée par la matrice $\begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix}$ qui n'appartient pas à $\mathrm{SL}_2(\mathbb{Z})$... Cependant, la matrice :

$$\begin{pmatrix} 0 & \frac{1}{4} \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$$

qui correspond l'homographie $z \longmapsto \dfrac{1}{4z+1}$ appartient bien à $\mathrm{SL}_2(\mathbb{Z})$. En appliquant alors les transformations successives correspondantes, on obtient :

$$\begin{aligned}\forall z \in \mathcal{H},\ \theta\left(\frac{z}{4z+1}\right) &= \theta\left(-\frac{1}{4\left(\frac{-1}{4z}-1\right)}\right) = \sqrt{2i\left(\frac{1}{4z}+1\right)}\theta\left(\frac{-1}{4z}-1\right) \\ &= \sqrt{2i\left(\frac{1}{4z}+1\right)}\theta\left(\frac{-1}{4z}\right) = \sqrt{2i\left(\frac{1}{4z}+1\right)(-2iz)}\theta(z) = \sqrt{4z+1}\theta(z).\end{aligned}$$

En utilisant la proposition 5, on a pour tout $z \in \mathcal{H}$ que $\theta(z,4) = \theta(z)^4$ et on obtient alors la formule :

$$\theta\left(\frac{z}{4z+1}, 4\right) = (4z+1)^2\theta(z,4). \tag{5.8}$$

De même, on obtient que :

$$\forall \gamma \in \left\{\pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \pm\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}\right\},\ \forall z \in \mathcal{H},\ \theta(\gamma.z, 4) = (cz+d)^2\theta(z,4).$$

Ainsi, θ^4 est une forme faiblement modulaire de poids 2 pour le groupe :

$$\Gamma = \left\langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \right\rangle.$$

On a clairement que Γ est inclus dans $\Gamma_0(4)$ (par définition). Montrons algorithmiquement l'inclusion réciproque : Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$ et notons

$$A = \begin{pmatrix} 1 & 0 \\ 4 & 0 \end{pmatrix}, \ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Raisonnons par disjonction de cas :

* Si $c = 0$, alors on a $\gamma \in \left\{-T^{-b}; -T^b; T^{-b}; T^b\right\} \subseteq \Gamma$.

* Sinon, on remarque que :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & an+b \\ c & nc+d \end{pmatrix}$$

donc on peut se ramener, avec une matrice de Γ, à une matrice telle que $|d'| < \dfrac{|c'|}{2}$ (l'inégalité est stricte car $4 \mid c'$ et $2 \nmid d'$). Ensuite, on remarque que :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4n & 1 \end{pmatrix} = \begin{pmatrix} a+4bn & b \\ c+4nd & d \end{pmatrix}$$

donc on peut se ramener, avec une matrice de Γ, à une matrice telle que $|c'| < |d'|$. En itérant ce procédé, la quantité $\max(|c'|, 2|d'|)$ diminue, donc le processus termine (car partie non vide et minorée de $\mathbb{N}$) et cela montre $\Gamma_0(4) \subseteq \Gamma$.

Proposition 8 :
On a $\theta^4 \in M_2(\Gamma_0(4))$.

Preuve :
Il nous faut montrer que θ^4 est une fonction faiblement modulaire de poids 2 pour le sous-groupe de congruence $\Gamma_0(4)$ et qu'elle est holomorphe en chaque pointe. Or, en utilisant `SAGE`, on obtient qu'il y a trois pointes et elles sont données par 0, $\dfrac{1}{2}$ et l'infini.

* Par ce qui précède, on sait déjà que θ^4 est une fonction faiblement modulaire de poids 2 pour le sous-groupe de congruence $\Gamma_0(4)$.

* θ^4 est clairement holomorphe à l'infini (d'après son q-développement).

* De plus, on a :

$$\forall z \in \mathcal{H}, \ \theta\left(\frac{-1}{4z}\right) = \sqrt{-2iz}\theta(z).$$

Donc $\theta(z) \underset{z\to 0}{=} O\left(|z|^{-\frac{1}{2}}\right)$ et on a également :

$$\left(\theta^4\right)^{[S]_2} = z^2\theta\left(-\frac{1}{z}\right)^4 \underset{z\to+\infty}{=} O(1).$$

Ainsi, θ est holomorphe en la pointe 0.

* Finalement, pour montrer que θ est holomorphe en la pointe $\dfrac{1}{2}$, on remarque d'abord que :

$$\theta\left(z - \frac{1}{2}\right) = \sum_{n\in\mathbb{Z}} q^{n^2}(-1)^{n^2} = \sum_{n\in\mathbb{Z}} q^{4n^2} - \sum_{n\in\mathbb{Z}} q^{(2n+1)^2} = \theta(4z) - (\theta(z) - \theta(4z)) = 2\theta(4z) - \theta(z).$$

On en déduit avec $\gamma = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ que $\gamma(\infty) = \frac{1}{2}$ et

$$\begin{aligned}\forall z \in \mathcal{H},\ \left(\theta^4\right)^{[\gamma]_2}(z) &= (2z+1)^2\theta\left(\frac{z}{4z+1}\right)^4 = (2z+1)^2\left(2i\left(\frac{1}{2}+\frac{1}{4z}\right)\right)^2\theta\left(-\frac{1}{2}-\frac{1}{4z}\right)^4 \\ &= (2z+1)^2\left(2i\left(\frac{1}{2}+\frac{1}{4z}\right)\right)^2\left(2\theta\left(-\frac{1}{8z}-\theta\left(-\frac{1}{4z}\right)\right)\right) \underset{z\to+\infty}{=} O\left(|z|^2\left(|z|^{-\frac{1}{2}}\right)^4\right) \\ &\underset{z\to+\infty}{=} O(1).\end{aligned}$$

donc θ^4 est bien holomorphe en la pointe $\frac{1}{2}$.

On a ainsi vérifié que θ^4 est holomorphe à l'infini, en 0 et en $\frac{1}{2}$, qui sont les trois pointes non $\Gamma_0(4)$-équivalentes. Or, il y a trois pointes pour $\Gamma_0(4)$, donc on a bien $\theta^4 \in M_2(\Gamma_0(4))$.

■

Remarque :
De manière plus générale, on peut montrer que $\theta^{2k} \in M_k(\Gamma_0(4))$.

II.2 Somme de quatre carrés

Dans cette sous-partie, on s'intéresse à la quantité $r(n,4)$ et plus précisément, on veut montrer qu'elle est non nulle pour tout entier naturel non nul n.

Théorème 1 : Théorème des quatre carré de Lagrange (1770) :
Tout entier naturel peut s'exprimer comme la somme de quatre carrés d'entiers.

Preuve :
Introduisons les fonctions définies sur $\mathcal{H}$ par :

$$G_{2,2} : z \longmapsto -\frac{\pi^2}{3}\left(1+24\sum_{n=1}^{+\infty}\left(\sum_{\substack{d|n,\ d>0 \\ 2\nmid d}} d\right)q^n\right) \text{ et } G_{2,4} : z \longmapsto -\pi^2\left(1+8\sum_{n=1}^{+\infty}\left(\sum_{\substack{d|n,\ d>0 \\ 4\nmid d}} d\right)q^n\right).$$

On a que $G_{2,2}, G_{2,4} \in M_2(\Gamma_0(4))$ par la proposition 3 (en effet, on a $G_{2,2} \in M_2(\Gamma_0(2))$ et $M_2(\Gamma_0(2)) \subset M_2(\Gamma_0(4))$ car $2 \mid 4$). Or par la proposition 4 du chapitre 4, on a $\dim_{\mathbb{C}} M_2(\Gamma_0(4)) = 2$ et la famille $(G_{2,2}, G_{2,4})$ est une famille libre (en examinant les deux premiers termes de leurs q-développements respectifs), donc c'est une base de $M_2(\Gamma_0(4))$.

Ainsi, par la proposition 8 il existe $a, b \in \mathbb{C}$ tels que $\theta^4 = aG_{2,2} + bG_{2,4}$. Or, les débuts des q-développements sont :

$$\begin{aligned}\theta^4(z) = \theta(z,4) &= 1+8q+\ldots \\ -\frac{3}{\pi^2}G_{2,2}(z) &= 1+24q+\ldots \\ -\frac{1}{\pi^2}G_{2,4}(z) &= 1+8q+\ldots\end{aligned}$$

Finalement, on trouve que $\theta^4 = -\frac{1}{\pi^2}G_{2,4}$ et en identifiant les coefficients des q-développements, on trouve que :

$$\forall n \in \mathbb{N}^*,\ r(n,4) = 8\sum_{\substack{d|n,\ d>0 \\ 4\nmid d}} d > 0.$$

■

Remarque :
En particulier, si 4 ne divise pas n, alors $r(n,4) = 8\sigma_1(n)$.

Tout le travail fait ici peut se décliner de la même manière pour obtenir des résultats sur la somme de deux, six ou encore huit carrés, il suffit de garder la même logique mais en modifiant les formes modulaires introduites.

III Formes modulaires et opérateurs différentiels

Le point de départ de cette partie est de constater que la dérivée d'une forme modulaire n'est pas une forme modulaire, mais presque ! Plus précisément, si f est une forme modulaire de poids k et de niveau 1 dont le q-développement est donné par $\sum_{n=0}^{+\infty} a_n q^n$, alors en posant comme dérivée la fonction $D(f)$ définie par

$$\forall z \in \mathcal{H},\ D(f)(z) = \frac{1}{2i\pi} f'(z) = \sum_{n=1}^{+\infty} n a_n q^n$$

on obtient en dérivant la relation (2.1) que :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ D(f)\left(\frac{az+b}{cz+d}\right) = (cz+d)^{k+2} D(f)(z) + \frac{k}{2i\pi} c(cz+d)^{k+1} f(z). \tag{5.9}$$

Si nous avions seulement le premier terme, alors $D(f)$ serait une forme modulaire de poids $k+2$ et de niveau 1. La présence d'un second terme, loin d'être un problème, rend la théorie plus riche. Pour y faire face, nous pouvons :

* Modifier l'opérateur D pour qu'il préserve la modularité.
* Faire des combinaisons de dérivées de formes modulaires pour conserver la modularité.
* Modifier la définition de forme modulaire pour y inclure les fonctions vérifiant la relation (5.9).
* Dériver par rapport à une fonction t qui est une forme modulaire de la variable t plutôt que par rapport à z directement.

Nous allons ici nous concentrer sur les deux premiers point précédents en les traitant chacun dans les deux sous-parties ci-dessous. Pour plus de détail, le lecteur pourra se référer à [9] (partie 5 du chapitre 1).

III.1 Dérivées de formes modulaires

Définition 4 : Série d'Eisenstein renormalisée de poids k :
On considère k un entier naturel supérieur ou égal à 2.
On appelle **série d'Eisenstein renormalisée de poids** k la fonction définie sur $\mathcal{H}$ par :

$$\mathbb{G}_k : z \longmapsto \frac{1}{2\zeta(k)} G_k(z)$$

Exemple 2 :
On donne ci-dessous le début des q-développements des premières séries d'Eisenstein renormalisées :

$$\begin{aligned}
\mathbb{G}_2(z) &= 1 - 24q - 72q^2 - \cdots \\
\mathbb{G}_4(z) &= 1 + 240q + 2\ 160q^2 + \cdots \\
\mathbb{G}_6(z) &= 1 - 504q - 16\ 632q^2 - \cdots \\
\mathbb{G}_8(z) &= 1 + 480q + 61\ 920q^2 + \cdots
\end{aligned}$$

Remarque :
Contrairement aux séries E_k où la normalisation a été faite de sorte à ce que les valeurs propres se comportent bien avec les opérateurs de Hecke, ici on normalise afin que le coefficient constant fasse 1 dans le but d'avoir des formules plus simples.

Comme nous l'avons dit, la première approche est de modifier l'opérateur D pour qu'il préserve la modularité. Une manière de faire est d'introduire une nouvelle dérivée. En effet, en posant pour tout $f \in M_k$ l'opérateur

$$\vartheta_k : f \longmapsto D(f) - \frac{k}{12}\mathbb{G}_2 f$$

(qui est appelé parfois **dérivée de Serre**), on obtient que $\vartheta_f(f) \in M_{k+2}$.

Une première conséquence est la suivante :
En introduisant l'anneau $\widetilde{M_*} = M_*[E_2] = \mathbb{C}[E_2, E_4, E_6] = \mathbb{C}[\mathbb{G}_2, \mathbb{G}_4, \mathbb{G}_6]$ appelé **anneau des formes quasimodulaires sur** $\mathrm{SL}_2(\mathbb{Z})$, on obtient la proposition suivante :

Proposition 9 :
L'anneau $\widetilde{M_*}$ est stable par dérivation.
Plus précisément, on a :

$$D(\mathbb{G}_2) = \frac{\mathbb{G}_2^2 - \mathbb{G}_4}{12},\ D(\mathbb{G}_4) = \frac{\mathbb{G}_2\mathbb{G}_4 - \mathbb{G}_6}{3} \text{ et } D(\mathbb{G}_6) = \frac{\mathbb{G}_2\mathbb{G}_6 - \mathbb{G}_4^2}{2}. \tag{5.10}$$

Preuve :

* $\vartheta_4(\mathbb{G}_4)$ et $\vartheta_6(\mathbb{G}_6)$ sont des formes modulaires de poids respectifs 6 et 8 et de niveau 1. Par le théorème 5 du chapitre 2, on en déduit qu'elles sont respectivement proportionnelles à $\mathbb{G}_6$ et $\mathbb{G}_4^2$. Or, en examinant les premiers termes des q-développements, on obtient que :

  $$\vartheta_4(\mathbb{G}_4) = -\frac{1}{3}\mathbb{G}_6 \text{ et } \vartheta_6(\mathbb{G}_6) = -\frac{1}{2}\mathbb{G}_4^2$$

  Ainsi, grâce à la définition de la dérivée de Serre, on obtient que :

  $$D(\mathbb{G}_4) = \frac{\mathbb{G}_2\mathbb{G}_4 - \mathbb{G}_6}{3} \text{ et } D(\mathbb{G}_6) = \frac{\mathbb{G}_2\mathbb{G}_6 - \mathbb{G}_4^2}{2}.$$

* Grâce à la relation donnée dans la proposition 2, on obtient en dérivant la relation que $D(\mathbb{G}_2) - \frac{1}{12}\mathbb{G}_2^2$ appartient à M_4 qui est de dimension 1 et engendré par $\mathbb{G}_4$. En examinant les premiers termes des q-développements, on trouve alors que :

  $$D(\mathbb{G}_2) - \frac{1}{12}\mathbb{G}_2^2 = -\frac{1}{12}\mathbb{G}_4.$$

  D'où :

  $$D(\mathbb{G}_2) = \frac{\mathbb{G}_2^2 - \mathbb{G}_4}{12}.$$

■

Cette propriété a été découverte pour la première fois par Ramanujan et possède beaucoup d'applications dont la suivante :

Proposition 10 :
Toute forme modulaire ou quasimodulaire sur $\mathrm{SL}_2(\mathbb{Z})$ vérifie une équation différentielle non linéaire de degré 3 à coefficients constants.

Preuve :
Puisque l'anneau $\widetilde{M_*}$ a pour degré de transcendance 3 (en effet, on a $\widetilde{M_*} \cong \mathbb{C}[X,Y,Z]$ et l'anneau $\mathbb{C}[X,Y,Z]$ a pour corps des fractions $\mathbb{C}(X,Y,Z)$ qui a pour degré de transcendance 3 sur $\mathbb{C}$) et est stable par dérivation, on en déduit que pour tout $f \in \widetilde{M_*}$, les fonctions f, $D(f)$, $D^2(f)$ et $D^3(f)$ sont algébriquement dépendantes sur $\mathbb{C}$ et la non-linéarité provient du poids de chacune des fonctions.

■

Par exemple, en appliquant plusieurs fois les résultats de la relation (5.10), on trouve que E_2 vérifie l'équation différentielle non linéaire $y''' - yy'' + \frac{3}{2}(y')^2 = 0$. Cette équation est appelée **équation de Chazy** et joue un rôle important dans la théorie des équations de Painlevé.

III.2 Crochet de Rankin-Cohen

Revenons désormais à la relation (5.9) décrivant la "presque modularité" de la dérivée $D(f)$ d'une forme modulaire $f \in M_k(\Gamma)$.

Si $g \in M_\ell(\Gamma)$ est une autre forme modulaire de poids ℓ pour le même sous-groupe, alors la relation (5.9) montre que la "non modularité" de $D(f)g$ est due au terme correctif $\frac{1}{2i\pi}kc(cz+d)^{k+\ell+1}f(z)g(z)$. Or ce terme correctif, multiplié par ℓ, est symétrique en f et g. Donc la différence $[f,g] = kfD(g) - \ell D(f)g$ est une forme modulaire de poids $k+\ell+2$ pour le sous-groupe Γ.

On peut alors vérifier que le crochet $[\cdot,\cdot]$ défini ci-dessus est anti-symétrique et vérifie l'identité de Jacobi, faisant de $M_*(\Gamma)$ une algèbre de Lie graduée par "le poids + 2". De plus, à f fixée, le crochet $g \longmapsto [f,g]$ est une dérivation par rapport à la multiplication usuelle et $M_*(\Gamma)$ acquiert ainsi une structure d'algèbre de Poisson.

On peut alors continuer cette construction en trouvant d'autres combinaisons de dérivées plus élevées de f et g qui sont des formes modulaires. On a ainsi :

$$[f,g]_0 = fg,\ [f,g]_1 = kfD(g) - \ell D(f)g$$

$$\text{et } [f,g]_2 = \frac{k(k+1)}{2}fD^2(g) - (k+1)(\ell+1)D(f)D(g) + \frac{\ell(\ell+1)}{2}D^2(f)g.$$

On a alors plus généralement la définition suivante :

Définition 5 : n-ième crochet de Rankin-Cohen :
On considère $n \in \mathbb{N}$, Γ un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ et deux formes modulaires $f \in M_k(\Gamma)$ et $g \in M_\ell(\Gamma)$.
On appelle **n-ième crochet de Rankin-Cohen de f et g** l'application :

$$[f,g]_n = \sum_{\substack{r,s\geq 0\\ r+s=n}} (-1)^r \binom{k+n-1}{s}\binom{\ell+n-1}{r} D^r(f)D^s(g)$$

On a alors le résultat suivant dont la démonstration est admise (le lecteur pourra se référer à [9] pour une preuve) :

Proposition 11 :
Soient $n \in \mathbb{N}$, Γ un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ et deux formes modulaires $f \in M_k(\Gamma)$ et $g \in M_\ell(\Gamma)$.
La fonction $[f,g]_n$ appartient à $M_{k+\ell+2n}(\Gamma)$.

III.3 Retour sur les identités arithmétiques

Nous donnons ici une application des crochets de Rankin-Cohen :

Dans la sous-partie V.3 du chapitre 2, nous avons donné des identités impliquant la somme de puissances de diviseurs d'entiers naturels en tant que première application des formes modulaires. Or, en incluant désormais la forme quasimodulaire E_2, nous pouvons obtenir de nouvelles relations notamment grâce à la relation (5.10).

Proposition 12 :
Pour tout $n \in \mathbb{N}^*$, on a la relation :

$$5\sigma_3(n) - (6n-1)\sigma_1(n) = 12\sum_{m=1}^{n-1}\sigma_1(m)\sigma_1(n-m).$$

En particulier, pour tout nombre premier p, on a :

$$5p^3 - 6p^2 - 5p + 6 \equiv 0\ [12].$$

Preuve :
Par la relation (5.10), on a $\mathbb{G}_2^2 = \mathbb{G}_4 + 12D(\mathbb{G}_2)$.
Or on sait que pour tout $z \in \mathcal{H}$:

$$\mathbb{G}_2(z) = 1 - \frac{8\pi^2}{2\zeta(2)}\sum_{n=1}^{+\infty}\sigma_1(n)q^n = 1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n,\ \mathbb{G}_4(z) = 1 + 240\sum_{n=1}^{+\infty}\sigma_3(n)q^n$$

$$\text{et } D(\mathbb{G}_2)(z) = -\frac{8\pi^2}{2\zeta(2)}\sum_{n=1}^{+\infty}n\sigma_1(n)q^n.$$

D'où :

$$\begin{aligned}\mathbb{G}_2(z)^2 &= \left(1 - \frac{8\pi^2}{2\zeta(2)}\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right)\left(1 - \frac{8\pi^2}{2\zeta(2)}\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right)\\ &= 1 + 48\sum_{n=1}^{+\infty}\sigma_1(n)q^n + 576\left(\sum_{n=1}^{+\infty}\sigma_1(n)q^n\right)^2\\ &= 1 + 48\sum_{n=1}^{+\infty}\sigma_1(n)q^n + 576\sum_{n=1}^{+\infty}\left(\sum_{m=1}^{n-1}\sigma_1(n)\sigma_1(n-m)\right)q^n\\ &= 1 + \sum_{n=1}^{+\infty}\left(48\sigma_1(n) + 576\sum_{m=1}^{n-1}\sigma_1(n)\sigma_1(n-m)\right)q^n\end{aligned}$$

et :

$$\mathbb{G}_4(z) + 12D(\mathbb{G}_2)(z) = 1 + 240\sum_{n=1}^{+\infty}\sigma_3(n)q^n - 288\sum_{n=1}^{+\infty}n\sigma_1(n)q^n = 1 + \sum_{n=1}^{+\infty}\left(240\sigma_3(n) - 288n\sigma_1(n)\right)q^n.$$

Par unicité des coefficients du q-développement, on obtient que :

$$\forall n \in \mathbb{N}^*,\ 48\sigma_1(n) + 576\sum_{m=1}^{n-1}\sigma_1(n)\sigma_1(n-m) = 240\sigma_3(n) - 288n\sigma_1(n).$$

D'où :

$$\forall n \in \mathbb{N}^*,\ \sum_{m=1}^{n-1}\sigma_1(n)\sigma_1(n-m) = \frac{240}{576}\sigma_3(n) - \frac{288n-48}{576}\sigma_1(n) = \frac{1}{12}\left(5\sigma_3(n) - (6n-1)\sigma_1(n)\right).$$

Finalement, on a :

$$\forall n \in \mathbb{N}^*,\ 5\sigma_3(n) - (6n-1)\sigma_1(n) = 12\sum_{m=1}^{n-1} \sigma_1(m)\sigma_1(n-m).$$

En particulier, pour tout nombre premier p, on a $\sigma_3(p) = 1 + p^3$ et $\sigma_1(p) = 1 + p$, d'où :

$$5\left(1+p^3\right) - (6p-1)(1+p) \equiv 0\ [12]$$

soit :

$$5 + 5p^3 - (6p + 6p^2 - 1 - p) \equiv 0\ [12]$$

ou encore :

$$5p^3 - 6p^2 - 5p + 6 \equiv 0\ [12].$$

■

Remarque :
Il est possible d'obtenir des formules similaires avec les deux autres relations de (5.10).

Cependant, en utilisant les crochets de Rankin-Cohen, on peut obtenir plus !

Proposition 13 :
Pour tout $n \in \mathbb{N}^*$, on a :

$$\tau(n) = \frac{n}{12}\left(\sigma_5(n) + 5\sigma_3(n)\right) - 70\sum_{m=1}^{n-1}(5m-2n)\sigma_3(m)\sigma_5(n-m)$$

En particulier, pour tout nombre premier p, on a :

$$12\tau(p) \equiv p\left(p^5 + 5p^3 + 6\right)\ [70]$$

Preuve :
Par la proposition 11, on obtient que $[\mathbb{G}_4, \mathbb{G}_6]_1$ est une forme modulaire de poids 12 et de niveau 1 et dont le coefficient constant est nul. Ainsi, on sait que $[\mathbb{G}_4, \mathbb{G}_6]_1$ est proportionnel à la forme modulaire Δ (par le corollaire 3 du chapitre 2).

En identifiant alors les coefficients du q-développement de $[\mathbb{G}_4, \mathbb{G}_6]_1$ avec ceux du q-développement de Δ, on obtient :

$$\forall n \in \mathbb{N}^*,\ \tau(n) = \frac{n}{12}\left(\sigma_5(n) + 5\sigma_3(n)\right) - 70\sum_{m=1}^{n-1}(5m-2n)\sigma_3(m)\sigma_5(n-m).$$

En particulier, pour tout nombre premier p, on a $\sigma_3(p) = 1 + p^3$ et $\sigma_5(p) = 1 + p^5$, d'où :

$$12\tau(p) \equiv p(p^5 + 5p^3 + 6)\ [70]$$

■

IV Dernier théorème de Fermat

Cette dernière partie a uniquement un but historique et donc ne contiendra pas de preuves.

Dans les années 1970, Yves Hellegouarch a été amené à considérer la courbe elliptique dont l'équation est donnée par $y^2 = (x-a^n)(x-b^n)(x-c^n)$ et où a, b et c satisfont l'équation de Fermat $a^n + b^n = c^n$. Une décennie plus tard, Gerhard Frey a étudié la même courbe elliptique et a découvert que la représentation galoisienne associée avait des propriétés qui contredisaient les propriétés que les représentations galoisiennes de courbes elliptiques devaient satisfaire.

Des conjectures précises sur la modularité de certaines représentations galoisiennes ont été faites par Jean-Pierre Serre et ces mêmes conjectures échoueraient pour les représentations associées à la courbe d'Hellegouarch-Frey, de sorte que l'exactitude de ces conjectures impliquent l'insolubilité de l'équation de Fermat (très grossièrement, ces conjectures impliquent que, si la représentation galoisienne associée à la courbe ci-dessus est modulaire, alors la forme parabolique correspondante devrait être congruente modulo n à une forme parabolique de poids 2 et niveau 1 ou 2, et il n'y en a pas d'autres).

En 1990, Kenneth Alan Ribet a démontré un cas particulier des conjectures de Serre (le cas général est désormais connu grâce aux travaux récents de Chandrashekhar Khare, Jean-Pierre Wintenberger, Luis Dieulefait et Mark Kisin), ce qui était suffisant pour donner la même implication. La preuve par Andrew Wiles et Richard Taylor de la conjecture Taniyama-Weil (toujours avec quelques restrictions mineures sur la courbe elliptique qui ont ensuite été levées, mais avec une généralité suffisante pour rendre applicable le résultat de Ribet) suffisait donc à apporter la preuve du théorème suivant, d'abord affirmé par Fermat en 1637 :

Théorème 2 : Dernier théorème de Fermat :
Soient $x, y, z \in \mathbb{N}^*$ premiers entre-eux.
Pour tout entier naturel $n \geq 3$, il n'existe pas de solution entière non triviale à l'équation $x^n + y^n = z^n$.

Bibliographie

[1] Théophile Cailliau. Théorème des quatre carrés et formes modulaires (2022). https://lesesvre.perso.math.cnrs.fr/rapport-cailleau.pdf.

[2] Xavier Gourdon. Les maths en tête, Analyse (2020). Ellipses.

[3] Peter Bruin & Sander Dahmen. Modular Forms (2018). https://www.math.ens.psl.eu/ odegaay/Modular-Forms2018.pdf.

[4] Henri Cohen, Fredrik Stromberg. Modular Forms, A Classical Approach (2017). American Mathematical society.

[5] Gäetan Chenevier. Introduction aux formes modulaires (2015). http://gaetan.chenevier.perso.math.cnrs.fr/coursENS/notes_chenevier.pdf.

[6] Maarten Derickx & Mark Van Hoeij & Jinxiang Zeng. Computing Galois representations and equations for modular curves $X_H(\ell)$ (2013). https://arxiv.org/pdf/1312.6819.

[7] Nobushige Kurokawa & Masato Kurihara & Takeshi Saito. Number Theory 3, Iwasawa Theory and Modular Forms (2012). Translations of mathematical monographs, volume 242, American Mathematical Society.

[8] Yves Hellegouarch. Invitation aux Mathématiques de Fermat-Wiles, 2^e édition (2009). Dunod.

[9] Jan Hendrik Bruinier & Gerard van der Geer & Günter Harder & Don Zagier. The 1-2-3 of Modular Forms (2008). Springer-Verlag.

[10] Joseph Hillel Silverman. The Arithmetic of Elliptic Curves, 2nd Edition (2008). Springer.

[11] William Stein. Modular Forms, A Computational Approach (2007). American Mathematical society.

[12] François Martin & Emmanuel Royer. Formes modulaires et périodes (2005). Société Mathématique de France.

[13] Fred Diamond & Jerry Shurman. A first course in modular forms (2005). Graduate Texts in Mathematics, vol. 228, Springer-Verlag.

[14] Keith Ball, Tanguy Rivoal. Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs (2001). Inventiones mathematicae.

[15] Kevin Buzzard. On the eigenvalues of the Hecke operator T_2 (1996). J. Number Theory 57, no. 1, 130-132.

[16] Gorō Shimura. Introduction to the arithmetic theory of automorphic functions (1994). Princeton University Press.

[17] Toshitsune Miyake. Modular forms (1989). Springer-Verlag.

[18] Jean-Pierre Serre. Cours d'arithmétique (1970). Presses universitaires de France.