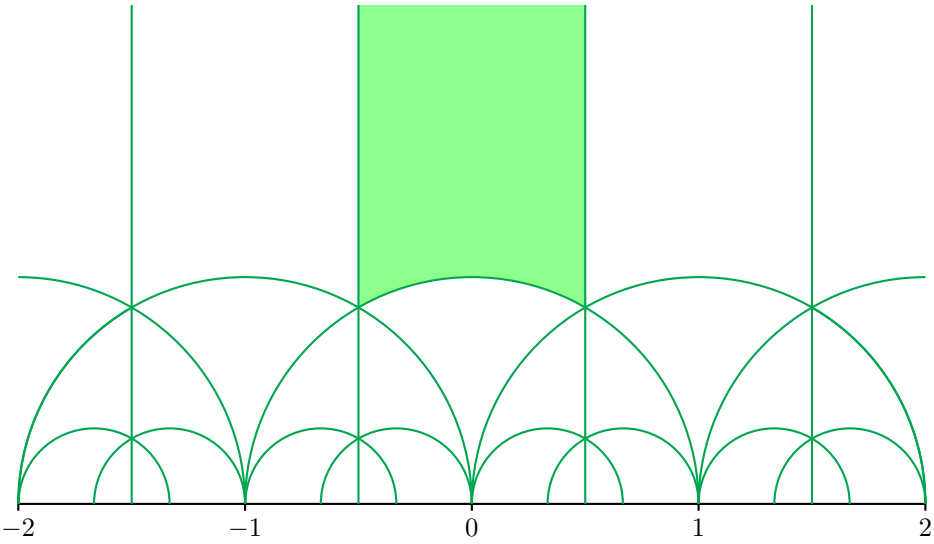
UNIVERSITÉ DE MONTPELLIER



Formes modulaires

Travail d'Étude et de Recherche
de Master 1 Mathématiques Fondamentales

AUTEURS

Paul CANTIÉ
Julia PHAM BA NIEN

ENCADRANT

João Pedro DOS SANTOS

FIGURES

Ivan LEJEUNE

Printemps 2026

Table des matières

1 Introduction

1.1 L'espace des modules des courbes elliptiques

Introduisons quelques notations et, sans rentrer trop tôt dans les détails, essayons de motiver quelque peu notre présentation. On appellera **groupe modulaire** et on notera $\mathbf{G} = \mathrm{SL}_2(\mathbf{Z})$ le groupe des matrices carrées de taille 2 à coefficients entiers de déterminant 1. On notera $\mathbf{H} = \{z \in \mathbf{C}, \mathrm{Im}(z) > 0\}$ le **demi-plan de Poincaré**. Le groupe $\mathbf{G}$ agit sur $\mathbf{H}$ par homographie : pour $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$ et $z \in \mathbf{H}$,

$$\gamma z = \frac{az+b}{cz+d}.$$

On verra dans notre premier chapitre que cette formule définit bien une action. On peut d'ores et déjà constater que l'identité agit trivialement, et un calcul simple montre que $\gamma z \in \mathbf{H}$:

$$\mathrm{Im}(\gamma z) = \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\mathrm{Im}((az+b)(c\bar{z}+d))}{|cz+d|^2} = \frac{\mathrm{Im}(ac|z|^2 + bd + adz + bc\bar{z})}{|cz+d|^2} = \frac{(ad-bc)\,\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0.$$

Le quotient $\mathbf{H}/\mathbf{G}$ sera d'une grande importance dans le reste de notre travail, en particulier quand on ramènera son usage à celui d'une certaine partie connexe de $\mathbf{C}$ contenant un représentant par orbite, son **domaine fondamental**. Essayons d'identifier ce quotient à un autre objet, de nature géométrique.

On appellera ici **courbe elliptique** (ou tore complexe) tout quotient de $\mathbf{C}$ par un **réseau** de $\mathbf{C}$, c'est-à-dire un sous-groupe $\Lambda = \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ tel $\mathbf{C}/\Lambda$ soit compact. On désigne par $\mathscr{R}$ l'ensemble des réseaux de $\mathbf{C}$. Pour pouvoir manipuler les réseaux par leurs bases, on pose $\mathscr{M} = \{(w_1, w_2) \in \mathbf{C}^2, w_1, w_2 \neq 0, \mathrm{Im}\left(\frac{w_1}{w_2}\right) > 0\}$, où on a choisi cette convention de telle sorte que le réseau "normalisé" (c'est-à-dire de deuxième générateur égal à 1)

$$\frac{1}{w_2}(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2) = \mathbf{Z}\frac{w_1}{w_2} \oplus \mathbf{Z}1$$

ait pour premier générateur un nombre complexe du demi-plan supérieur. Avec ces notations, on dispose donc d'une surjection

$$\begin{array}{ccc} \mathscr{M} & \to & \mathscr{R} \\ (w_1, w_2) & \mapsto & \mathbf{Z}w_1 \oplus \mathbf{Z}w_2 \end{array}$$

Le groupe $\mathbf{G}$ agit sur $\mathscr{M}$ par $\gamma(w_1, w_2) = (aw_1 + bw_2, cw_1 + dw_2)$. On verra dans un prochain chapitre que deux bases déterminent le même réseau si, et seulement si elles sont congrues modulo $\mathbf{G}$. Aussi a-t-on la bijection

$$\mathscr{M}/\mathbf{G} \simeq \mathscr{R}.$$

Faisons maintenant agir $\mathbf{C}^*$ sur $\mathscr{R}$ par multiplication scalaire et sur $\mathscr{M}$ par $\lambda(w_1, w_2) = (\lambda w_1, \lambda w_2)$, avec $\lambda \in \mathbf{C}^*$. On peut aisément donner une bijection pour identifier le quotient $\mathscr{M}/\mathbf{C}^*$ avec $\mathbf{H}$:

$$\begin{array}{ccc} \overline{(w_1, w_2)} & \mapsto & \dfrac{w_1}{w_2} \\ \overline{(z, 1)} & \hookleftarrow & z \end{array}$$

La linéarité du produit matriciel dans l'algèbre $\mathrm{M}_2(\mathbf{C})$ fait commuter l'action de $\mathbf{C}^*$ sur $\mathscr{M}$ avec celle de $\mathbf{G}$, si bien que $\mathscr{M}/\mathbf{C}^*/\mathbf{G} \simeq \mathscr{M}/\mathbf{G}/\mathbf{C}^*$, d'où l'on obtient, avec $\mathscr{M}/\mathbf{C}^* \simeq \mathbf{H}$, que

$$\mathbf{H}/\mathbf{G} \simeq \mathscr{R}/\mathbf{C}^*.$$

Or, deux courbes elliptiques sont isomorphes si, et seulement si leurs réseaux sont proportionnels : ainsi, le quotient $\mathbf{H}/\mathbf{G}$ s'identifie avec l'ensemble des courbes elliptiques à isomorphisme près, qui est aussi appelé **espace des modules des courbes elliptiques**. De plus, on verra qu'une certaine fonction, l'**invariant modulaire** j, réalisera une bijection $\mathbf{H}/\mathbf{G} \simeq \mathbf{C}$, si bien que ces deux ensembles "varient comme $\mathbf{C}$".

On adjoindra le qualificatif de **(faiblement) modulaire** à des fonctions méromorphes du demi-plan supérieur $f : \mathbf{H} \to \mathbf{C}$ qui vérifient une équation fonctionnelle par rapport à l'action de $\mathbf{G}$, à savoir, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$,

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

où l'entier k est le **poids** de f. On réservera le qualificatif de **fonction modulaire** et de **forme modulaire** à de telles fonctions suffisamment régulières qui possèdent de plus un certain comportement à l'infini, qui se lira sur leur q**-expansion**. La pertinence du point de vue des réseaux précédemment exposé sera mis en exergue quand on établira une correspondance entre les fonctions modulaires de poids k et certaines fonctions de réseaux $F : \mathscr{R} \to \mathbf{C}$ "de poids k", dans un sens que l'on précisera.

1.2 Des fragments d'histoire

Les débuts de la théorie

L'embryon de la théorie apparaît pour la première fois dans les travaux de Gauss du début du XIX$^{\text{ème}}$ siècle, où il manipule entre autres le sous-groupe de congruence de niveau deux du groupe modulaire et en explicite un "domaine fondamental", pour étendre la théorie des fonctions elliptiques. Riemann reprend les travaux de Gauss cinquante ans plus tard, dans ses leçons sur la fonction hypergéométrique. C'est lui qui introduit le terme même de modularité. Se succèdent alors les travaux de Fuchs, Dedekind et Klein sur le restant du siècle, pour ne citer qu'eux, qui développent la théorie des formes modulaires pour elle-même. Ces deux derniers introduisirent notamment des conventions de normalisation de l'invariant modulaire j. En particulier Klein utilise dès lors le domaine fondamental usuel de l'action du groupe modulaire sur le demi-plan de Poincaré sous sa forme actuelle, et étudie les sous-groupes de congruence de niveaux supérieurs du groupe modulaire.

Groupes fuchsiens, formes automorphes et fonctions L

Vers la fin du siècle, Poincaré étend le cadre d'étude en généralisant ces groupes de congruence aux groupes fuchsiens, qu'il introduit et nomme en l'honneur de Fuchs. Maass, Siegel et Poincaré vont, au début du XX$^{\text{ème}}$ siècle, jusqu'à considérer la situation suivante : l'action sur un groupe topologique quelconque par l'un de ses sous-groupes d'indice fini, et les fonctions de ce groupe vers un espace vectoriel complexe, qui satisfont à des propriétés de symétrie quant au sous-groupe donné, ainsi qu'une équation fonctionnelle. Ces fonctions, dites formes automorphes, généralisent entièrement la théorie des formes modulaires. En parallèle, sur la première moitié du siècle, Hecke et Petersson étudient les relations entre les formes modulaires, les séries de Dirichlet et leurs fonctions L associées. Hecke introduit les opérateurs linéaires sur les espaces de formes modulaires qui portent son nom, avec lesquels il caractérise l'existence d'équations fonctionnelles vérifiées par des fonctions L et démontre une partie de la conjecture de Ramanujan en 1937.

Les conjectures de Weil et Fermat et le programme de Langlands

Sur la deuxième moitié du siècle, la théorie des formes modulaires connaît un essor phénoménal pour ses applications arithmétiques. Elles sont en filigrane dans la preuve de Deligne des conjectures de Weil, qui lui valurent la médaille Fields en 1978. Comme corollaire, il démontre une conjecture de Ramanujan sur les coefficients de la q-expansion de la forme parabolique Δ. Elles sont au cœur de la conjecture de modularité, dont la preuve par Wiles en 1994 a achevé la démonstration du grand théorème de Fermat, grâce aux contributions de Serre, Ribet et Taylor. Elles jouent également un rôle important dans le programme de Langlands, suite entre autres aux travaux de Jacquet, Rankin, Selberg et Langlands lui-même sur cette période.

Les applications modernes des formes modulaires

Les formes modulaires apparaissent dans de nombreux domaines de recherche actuels, comme le programme de Langlands susmentionné, en théorie des nombres plus généralement, en géométrie algébrique, en topologie, en géométrie hyperbolique, en théorie des représentations ou encore en physique mathématique, où elles sont utilisés en théorie quantique des champs et en théorie des cordes.

1.3 L'esprit du travail et remerciements

L'esprit du travail

Dans notre discussion initiale, notre encadrant M. dos Santos nous a conseillé de rester fidèle à l'exposé de Serre dans son *Cours d'arithmétique*. "Quand on lit Shakespeare, on ne lit pas ses contemporains, ceux qu'il a influencé, ceux qu'ils l'ont analysés ou imités : on lit Shakespeare". C'est dans cet esprit que nous avons orienté notre travail. Le présent rapport essaie de restituer notre appropriation du livre de Serre, ce que nous en avons compris et ce que nous avons dû détailler pour nous convaincre. Nous avons consulté d'autres références, que nous mentionnons dans la bibliographie, mais nous suivons à peu de choses près son exposé dans son plan et ses thèmes abordés.

Les thèmes abordés

Chapitre 2. – Nous commençons par introduire le domaine fondamental du groupe modulaire, ce qui nous renseigne sur sa structure et sur son action sur le demi-plan de Poincaré. On explique brièvement ce que sont les sous-groupes de congruences, ce qui diffère de l'approche de Serre, qui ne développe la théorie que sur le groupe modulaire plein.

Chapitre 3. – Sont ensuite définies les fonctions et les formes modulaires, en détaillant pourquoi on peut en faire la q-expansion. On établit une correspondance entre ces fonctions et les fonctions de réseaux, en justifiant certains faits employés dans l'introduction. On donne ensuite des premiers exemples de formes modulaires, en la matière des séries d'Eisenstein de poids pairs et de la forme parabolique Δ de poids 12.

Chapitre 4. – On démontre ensuite la formule de valence, ouvrant la porte aux considérations dimensionnelles sur les espaces de formes modulaires. On montre plusieurs propriétés de l'invariant modulaire j.

Chapitre 5. – On développe les bases de la théorie de Hecke sur les réseaux et les fonctions de réseaux puis sur les formes modulaires, en nous fixant pour but de démontrer le premier volet de la conjecture de Ramanujan.

Les grands absents

Que ce soit en suivant l'exposé de Serre ou par manque de temps, nous avons laissé de côté plusieurs sujets majeurs immédiatement en lien avec la théorie des formes modulaires. On regrette particulièrement de ne pas avoir étudié plus en détail le lien avec la géométrie algébrique : plus précisément, avec la théorie des courbes elliptiques, et des diviseurs et formes différentielles sur les surfaces de Riemann. Elles permettent de munir les compactifiés du groupe modulaire et de ses sous-groupes de congruences de structures de variétés complexes. On sait également qu'elles donnent lieu à des simplifications spectaculaires : notre preuve la plus "coûteuse", celle de la formule de valence, tient en quelques lignes si l'on emploie le théorème de Riemann-Roch. Notons également la géométrie hyperbolique, le demi-plan de Poincaré étant un modèle du plan hyperbolique. Quant à la théorie des formes modulaires en elle-même, on ne fait que mentionner l'existence des théories parallèles basées sur les sous-groupes de congruences, on ne s'intéresse pas aux aspects liés au calcul formel par ordinateur, pourtant très développés, et on laisse de côté certaines considérations asymptotiques. Tous ces sujets deviennent pour nous d'excellentes pistes d'approfondissement, maintenant que nous avons des bases sur la théorie analytique classique.

Remerciements

Nous tenons à remercier M. dos Santos pour nous avoir proposé ce sujet, pour les discussions que nous avons eu ainsi que pour les conseils qu'il nous a transmis. Nous remercions également notre ami Ivan Lejeune, étudiant en M1 Algorithmique à l'Université de Montpellier, qui a gracieusement réalisé les figures que nous souhaitions, ainsi que la page de garde.

2 Le groupe modulaire

2.1 L'action sur le demi-plan de Poincaré

On rappelle les notations de l'introduction.

Définition 2.1. – *On note* $\mathbf{G} = \mathrm{SL}_2(\mathbf{Z})$ *le* **groupe modulaire** *et* $\mathbf{H} = \{z \in \mathbf{C}, \mathrm{Im}(z) > 0\}$ *le* **demi-plan de Poincaré**.

Remarque (très importante). – Comme $-I_2$ agit trivialement, on peut être tenté de remplacer $\mathbf{G}$ par $\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z})/\{\pm I_2\}$. Dans le reste de l'exposé, il sera question de l'ordre des sous-groupes de $\mathbf{G}$ et de faits qui dépendent de ces considérations : on précise donc que **dans la suite, on prendra** $\mathrm{PSL}_2(\mathbf{Z})$ **comme groupe modulaire**. Mais d'autres résultats sont également valables sur $\mathrm{SL}_2(\mathbf{Z})$: on essaiera de préciser quand c'est le cas.

Proposition 2.1. – *Le groupe modulaire* $\mathbf{G}$ *agit sur* $\mathbf{H}$ *: pour* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$ *et* $z \in \mathbf{H}$*, la formule*

$$\gamma z = \frac{az + b}{cz + d}$$

définit bien une action.

Preuve. L'identité agit trivialement et le calcul de l'introduction montre que $\gamma z \in \mathbf{H}$: il reste à montrer que $\gamma(\gamma' z)$ vaut bien ce que l'on pense, et en effet, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$,

$$\gamma(\gamma' z) = \frac{a\left(\dfrac{a'z + b'}{c'z + d'}\right) + b}{c\left(\dfrac{a'z + b'}{c'z + d'}\right) + d} = \frac{a(a'z + b') + b(c'z + d')}{c(a'z + b') + d(c'z + d')} = \frac{(aa' + bc')z + (ab' + bd')}{(ca' + dc')z + (cb' + dd')},$$

donc $\gamma(\gamma' z) = (\gamma\gamma')z$. □

2.2 Le domaine fondamental

On va étudier cette action ainsi que le groupe modulaire lui-même en introduisant son **domaine fondamental**. Il y a pléthore de définitions de ce terme dans la littérature. L'idée est la suivante. Compte tenu d'une action d'un groupe G sur un espace topologique X, on cherche une partie D de X qui soit "raisonnable" (on demande en général a minima la connexité, parfois la lissité par morceaux du bord quand X a plus de structure) et qui croise chaque orbite de l'action suffisamment de fois pour pouvoir écrire X comme l'union des gD ou des $g\overline{D}$ pour $g \in G$. Cela permet de ramener l'étude de n'importe quel point de X à celui du représentant de sa classe dans D. Pour notre part, nous fixons la définition suivante.

Définition 2.2. – *Avec les mêmes notations, un* **domaine fondamental** *pour l'action de* G *sur* X *est une partie connexe de* X *dont l'adhérence contient au moins un représentant par orbite et dont l'intérieur contient au plus un représentant par orbite.*

Remarque. – Si D est un domaine fondamental pour l'action de G sur X, alors la restriction à $\overline{D}$ de la surjection canonique $X \twoheadrightarrow X/G$ est surjective, et sa restriction à $\overset{\circ}{D}$ est injective. Réciproquement, si D' est connexe et vérifie cette propriété, c'est un domaine fondamental pour l'action de G sur X.

Exemple. – Les courbes elliptiques vues dans l'introduction sont les quotients de $\mathbf{C}$ par un réseau, c'est-à-dire un sous-groupe discret Λ tel que $\mathbf{C}/\Lambda$ soit compact : pour $\mathbf{C}$, ils sont de la forme $\mathbf{Z}w_1 \oplus \mathbf{Z}w_2$. Un domaine fondamental pour l'action d'un tel réseau $\mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ sur $\mathbf{C}$ est le **parallélogramme fondamental**, c'est-à-dire l'enveloppe convexe de $\{0, w_1, w_2, w_1 + w_2\}$.

On pose alors $\mathbf{D} = \{z \in \mathbf{H}, -\frac{1}{2} \leqslant \mathrm{Re}(z) \leqslant \frac{1}{2}, |z| \geqslant 1\}$. C'est un fermé connexe de $\mathbf{H}$, et on va montrer que c'est un domaine fondamental pour l'action de $\mathbf{G}$ sur $\mathbf{H}$. La définition de $\mathbf{D}$ nous demande de deviner la structure de $\mathbf{G}$, précisée dans la proposition ci-dessous. Mais l'intérêt d'introduire $\mathbf{D}$ est justement de simplifier ce genre de considérations : aussi, nous ne la démontrerons qu'après avoir prouvé le théorème qui la succède.

Proposition 2.2. – *Le groupe modulaire* $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$ *a pour présentation* $\langle S, T; S^2 = (ST)^3 = I_2 \rangle$, *où*

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

Pour tout $z \in \mathbf{H}$, $Sz = -\frac{1}{z}$ *et* $Tz = z + 1$.

Théorème 2.1. – *L'ensemble* $\mathbf{D}$ *est un domaine fondamental pour l'action de* $\mathbf{G}$ *sur* $\mathbf{H}$, *ce qui découle des faits suivants :*

1) *Si* $z \in \mathbf{H}$, *il existe* $\gamma \in \mathbf{G}$ *tel que* $\gamma z \in \mathbf{D}$.
2) *Si deux points distincts* $z, z' \in \mathbf{D}$ *sont congrus modulo* $\mathbf{G}$, *alors ils sont sur le bord de* $\mathbf{D}$. *Plus explicitement, soit* $\mathrm{Re}(z) = \pm\frac{1}{2}$, *et dans ce cas* $z' = z \pm 1$, *soit* $|z| = 1$ *et* $z' = -\frac{1}{z}$.
3) *Les stabilisateurs dans* $\mathbf{G}$ *des éléments de* $\mathbf{D}$ *sont triviaux, à l'exception de* i, ρ *et* $-\overline{\rho}$, *où* $\rho = e^{\frac{2i\pi}{3}}$. *Pour ces points,*
   — $\mathrm{Stab}(i) = \langle S \rangle$ *est un sous-groupe d'ordre 2 ;*
   — $\mathrm{Stab}(\rho) = \langle ST \rangle$ *est un sous-groupe d'ordre 3 ;*
   — $\mathrm{Stab}(-\overline{\rho}) = \langle TS \rangle$ *est un sous-groupe d'ordre 3.*

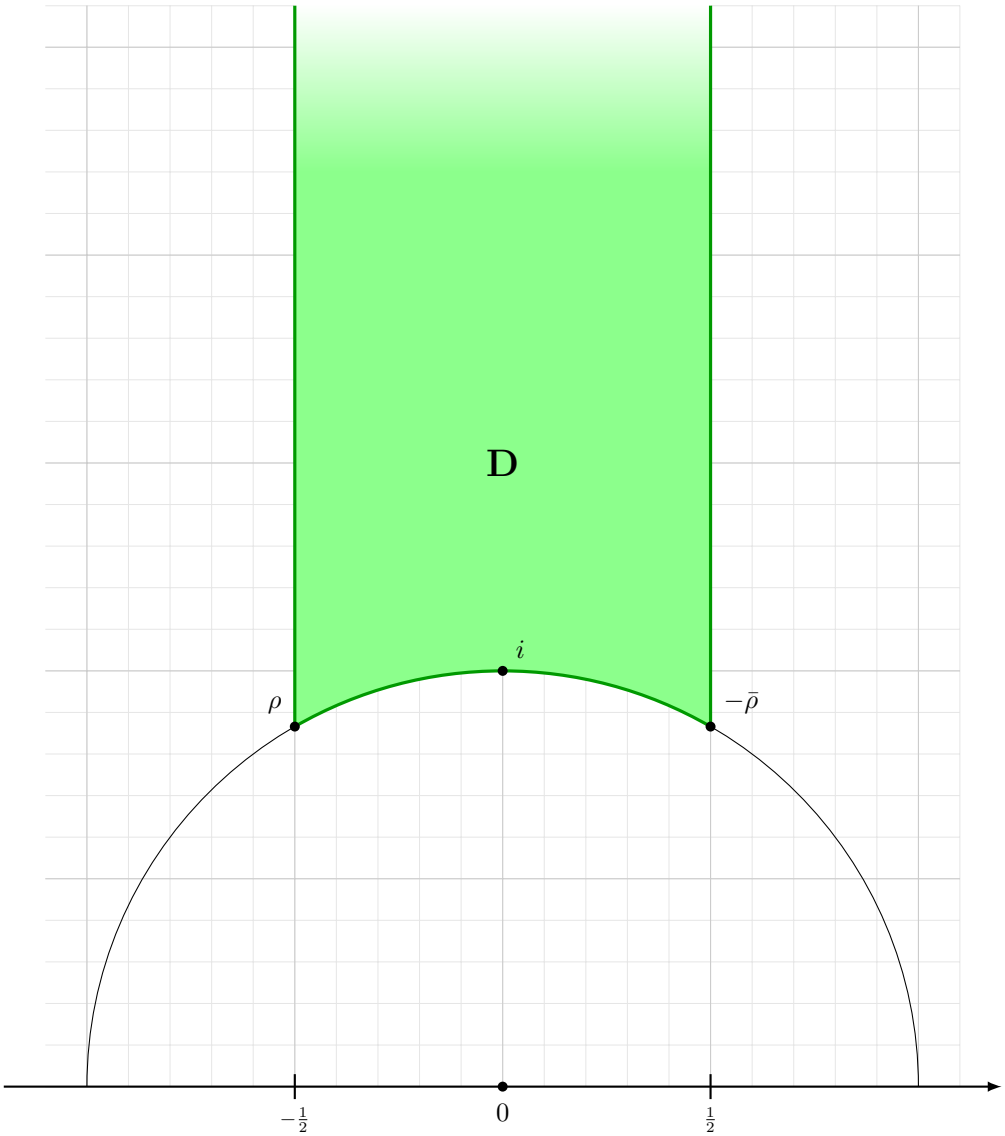


FIGURE 2.1 – Le domaine fondamental $\mathbf{D}$

Preuve. Posons $\mathbf{G}' = \langle S, T\rangle$.

1) Pour $z \in \mathbf{H}$ fixé et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a montré dans l'introduction que

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

et puisque $c, d \in \mathbf{Z}$, il n'y a qu'un nombre fini de $\gamma \in \mathbf{G}$ tels que $|cz+d|$ soit plus petit qu'une quantité donnée, ou autrement dit, tel que $\mathrm{Im}(\gamma z)$ soit plus grand qu'une quantité donnée. Soit donc γ, que l'on prend dans $\mathbf{G}'$, maximisant $\mathrm{Im}(\gamma z)$. Il existe un entier $n \in \mathbf{Z}$ tel que $T^n\gamma z$ soit dans la bande $\{w \in \mathbf{H}, -\frac{1}{2} \leqslant \mathrm{Re}(w) \leqslant \frac{1}{2}\}$. Comme T ne change pas la partie imaginaire, on a $\mathrm{Im}(T^n\gamma z) = \mathrm{Im}(\gamma z)$. Puisqu'on a choisi $\mathrm{Im}(\gamma z)$ comme étant maximal, on a $|T^n\gamma z| \geqslant 1$ et $T^n\gamma z \in \mathbf{D}$: en effet, on ne peut pas avoir $|T^n\gamma z| < 1$, sinon $ST^n\gamma z$ aurait une partie imaginaire strictement supérieure à celle de $T^n\gamma z$, ce qui contredirait la maximalité. Cela montre 1), où d'ailleurs la transformation ramenant z dans $\mathbf{D}$ est "seulement" un élément de $\mathbf{G}'$.

2) Soit maintenant $z \in \mathbf{D}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$ tel que $\gamma z \in \mathbf{D}$. Quitte à remplacer γ par γ^{-1}, on peut choisir $\mathrm{Im}(\gamma z) \geqslant \mathrm{Im}(z)$, ce qui revient à supposer avec le calcul précédent que $|cz+d| \leqslant 1$. Cela impose $|c| \leqslant 1$, ce qui laisse trois choix pour la valeur de c puisqu'il est entier.
   - Si $c = 0$, alors $d = \pm 1$. Comme $\det(\gamma) = 1$, alors $a = d$ et γ est une translation. Comme on a $|\mathrm{Re}(z)|, |\mathrm{Re}(\gamma z)| \leqslant \frac{1}{2}$, soit γ est l'identité, soit γ vaut T ou T^{-1} et $\mathrm{Re}(z) = -\mathrm{Re}(\gamma z) = \pm\frac{1}{2}$.
   - Si $c = 1$, supposons que $z \neq \rho, -\overline{\rho}$. Puisque $|z+d| \leqslant 1$, on a $d = 0$, donc $|z| \leqslant 1$, et puisque $z \in \mathbf{D}$, $|z| = 1$. Comme $\det(\gamma) = 1$, alors $b = -c = -1$ et $\gamma z = a - \frac{1}{z}$, ce qui force $a = 0$ par le point précédent, car $|\mathrm{Re}(z)| < \frac{1}{2}$ puisqu'on a supposé $z \neq \rho, -\overline{\rho}$. On a donc $\gamma = S$ et $|z| = |\gamma z| = 1$.
   - Le cas $c = -1$ est identique au cas précédent en remplaçant γ par $-\gamma$, qui sont égaux dans $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$.

   Ces remarques montrent 2), si l'on précise que $|\rho| = |-\overline{\rho}| = 1$ et $-\overline{\rho} = S\rho$, et que $\mathrm{Re}(\rho) = -\mathrm{Re}(-\overline{\rho}) = -\frac{1}{2}$ et $-\overline{\rho} = T\rho$. Les deux premiers points montrent que $\mathbf{D}$ est un domaine fondamental pour l'action de $\mathbf{G}$ sur $\mathbf{H}$: en effet, $\mathbf{D}$ est connexe, $\mathbf{D} \to \mathbf{H}/\mathbf{G}$ est surjective par 1) et $\overset{\circ}{\mathbf{D}} \to \mathbf{H}/\mathbf{G}$ est injective par 2).

3) On voit également que si $z \neq \rho, -\overline{\rho}$, alors $z = \gamma z$ si, et seulement si $c = \pm 1$ et $z = i$. Cela montre que tous les stabilisateurs des éléments différents de i, ρ et $-\overline{\rho}$ sont triviaux et que $\mathrm{Stab}(i) = \langle S\rangle$. Il reste à traiter le cas de ρ et $-\overline{\rho}$: cela demande de détailler ce qu'il se passe quand $c = 1$.
   - Pour ρ, on pouvait également avoir $d = 1$. Si c'est le cas, comme $\det(\gamma) = a - b = 1$, on a $\gamma = \left(\begin{smallmatrix} a & a-1 \\ 1 & 1 \end{smallmatrix}\right)$, donc $\gamma\rho = a - \frac{1}{1+\rho} = a + \rho$. On a soit $a = 0$, $\gamma\rho = \rho$ et $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) = ST$, soit $a = 1$ et $\gamma\rho = -\overline{\rho}$.
   - De même pour $-\overline{\rho}$, on pouvait avoir $d = -1$. Si c'est le cas, comme $\det(\gamma) = -a - b = 1$, on a $\gamma = \left(\begin{smallmatrix} a & -a-1 \\ 1 & -1 \end{smallmatrix}\right)$, donc $\gamma(-\overline{\rho}) = a - \frac{1}{-\overline{\rho}-1} = a - \overline{\rho}$. On a soit $a = 0$, $\gamma(-\overline{\rho}) = -\overline{\rho}$ et $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right) = TS$, soit $a = -1$ et $\gamma(-\overline{\rho}) = \rho$.

   Cela achève de montrer 3). □

Preuve de la proposition. Soit $z \in \overset{\circ}{\mathbf{D}}$ et $\gamma \in \mathbf{G}$. D'après la preuve précédente du point 1), il existe $\gamma' \in \mathbf{G}'$ tel que $\gamma'\gamma z \in \mathbf{D}$. Or d'après 2), puisque $z, \gamma'\gamma z \in \mathbf{D}$ sont congrus modulo $\mathbf{G}$ et que z est intérieur à $\mathbf{D}$, alors $z = \gamma'\gamma z$. D'après 3), puisque z est intérieur à $\mathbf{D}$, $\gamma'\gamma = I_2$, ce qui montre que $\mathbf{G} \subseteq \mathbf{G}'$, l'autre inclusion allant de soi. Un calcul simple permet de vérifier les relations $S^2 = I_2 = (ST)^3$. □

Remarque. – On utilise la notation ρ à la place de j pour la racine 3-ième de l'unité $e^{\frac{2i\pi}{3}}$, puisque c'est la lettre historiquement associée à l'invariant modulaire j que l'on étudiera dans notre quatrième chapitre.

2.3 Les sous-groupes de congruences

L'approche de Serre traite de la théorie classique des formes modulaires, de groupe de base $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$. Mais l'importance des autres théories de formes modulaires basées sur certains sous-groupes particuliers de $\mathbf{G}$, appelés sous-groupes de congruences, nous ferait regretter de ne pas les mentionner.

Définition 2.3. – *Soit $N \in \mathbf{N}$. On note $\mathrm{SL}_2(\mathbf{Z}) \xrightarrow{\pi_N} \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ le morphisme de réduction termes à termes modulo N.*

- *On appelle* **sous-groupe de congruences principal de niveau** *N le noyau de π_N, que l'on note $\Gamma(N)$.*
- *On appelle* **sous-groupe de congruences** *un sous-groupe Γ de $\mathrm{SL}_2(\mathbf{Z})$ qui contient $\Gamma(N)$, pour un $N \in \mathbf{N}$. Le plus petit tel N est appelé le* **niveau** *de Γ.*

Remarques. – Avec ces notations, $\Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$ est le groupe modulaire plein.

– Les sous-groupes de congruences vont posséder des domaines fondamentaux différents, et des fonctions invariantes sous leur action différentes, donnant ainsi lieu à des théories parallèles de formes modulaires.

– L'image réciproque par π_N d'un sous-groupe de $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ est un sous-groupe de congruences.

Exemples. – La remarque précédente nous permet de donner deux exemples de sous-groupes de congruences omniprésents dans la littérature :

— Le sous-groupe $\Gamma_0(N)$, image réciproque de $\{\left(\begin{smallmatrix}\star & \star\\ 0 & \star\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})\}$.

— Le sous-groupe $\Gamma_1(N)$, image réciproque de $\{\left(\begin{smallmatrix}1 & \star\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})\}$.

On a $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \Gamma(1)$. Pour $N = 1$, toutes ces inclusions sont des égalités. Cependant, si $N > 1$, alors $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_1(N)$ n'est pas une matrice de $\Gamma(N)$ et si $N > 2$, alors $-I_2 \in \Gamma_0(N)$ n'est pas une matrice de $\Gamma_1(N)$. On a toutefois $\Gamma_0(2) = \Gamma_1(2)$. En effet, si $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_0(2)$, alors c est pair, ce qui impose à ad d'être impair, donc a et d sont tous deux impairs, congrus à 1 modulo 2 : on a ainsi $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_1(2)$.

Comme $\Gamma(N)$ est le noyau d'un morphisme de groupes, il est distingué, ce qui donne un isomorphisme $\Gamma(1)/\Gamma(N) \simeq \pi_N(\Gamma(1))$, et comme $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ est fini, $\Gamma(N)$ est d'indice fini dans $\Gamma(1)$. On a même mieux.

Proposition 2.3. – *Soit $N \in \mathbf{N}^*$. Alors la suite courte suivante est exacte :*

$$1 \longrightarrow \Gamma(N) \longrightarrow \Gamma(1) \xrightarrow{\pi_N} \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \longrightarrow 1.$$

Preuve. On a bien $\mathrm{Ker}(\pi_N) = \Gamma(N)$, par définition. Il reste à vérifier la surjectivité de π_N. Soit $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{Z})$ telle que $ad - bc \equiv 1\ [N]$. Par le théorème de Bézout, $c \wedge d \wedge N = 1$. Soit n un entier tel que $c \wedge (d + nN) = 1$: le produit des nombres premiers qui interviennent dans la décomposition de c mais pas dans celle de d convient. En effet, si p est un nombre premier qui divise c, on a deux cas.

— Si $p \mid d$, alors $p \nmid n$ mais comme $c \wedge d \wedge N = 1$ et $p \mid c, d$, alors $p \wedge N = 1$ et $p \nmid (d + nN)$.

— Si $p \nmid d$, alors $p \mid n$ et $d + nN \equiv d\ [p]$, mais comme $p \nmid d$ alors $p \nmid (d + nN)$.

Il existe donc $u, v \in \mathbf{Z}$ tels que $cu + (d + nN)v = 1$. Comme $a(d + nN) - bc \equiv ad - bc \equiv 1\ [N]$, il existe m tel que $a(d + nN) - bc - mN = 1$. Puisque $mNcu + mN(d + nN) = mN$, en remplaçant dans l'égalité précédente, on a

$$(d + nN)(a - vmN) - c(b - umN) = 1.$$

Ainsi, la matrice $\begin{pmatrix} a - vmN & b + umN \\ c & d + nN \end{pmatrix}$, d'image $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par π_N, est de déterminant 1. □

On en déduit que $\Gamma(1)/\Gamma(N) \simeq \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ et $[\Gamma(1) : \Gamma(N)] = |\,\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})|$. Si l'on admet que pour un nombre premier p donné et $n \in \mathbf{N}^*$ on a $|\,\mathrm{SL}_2(\mathbf{Z}/p^n\mathbf{Z})| = p^{3n}(1 - p^{-2})$, on peut facilement calculer cet indice.

Proposition 2.4. – $[\Gamma(1) : \Gamma(N)] = N^3 \prod_{p \mid N} (1 - p^{-2})$.

Preuve. Le lemme chinois nous donne un isomorphisme $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \simeq \prod_{p \mid N} \mathrm{SL}_2(\mathbf{Z}/p^{v_p(N)}\mathbf{Z})$. Avec le résultat que l'on vient d'admettre, on a bien $|\,\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})| = \prod_{p \mid N} p^{3v_p(N)}(1 - p^{-2}) = N^3 \prod_{p \mid N} (1 - p^{-2})$. □

3 Les formes modulaires

3.1 La q-expansion et les formes modulaires

Pour le reste de cette section, considérons une fonction $f : \mathbf{H} \to \mathbf{C}$ et un entier k.

Définition 3.1. – *On dit que f est une* **fonction faiblement modulaire de poids** k *si elle est méromorphe sur* $\mathbf{H}$ *et que pour tout $z \in \mathbf{H}$, pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$,*

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

On note $\mathbf{M}_k^w$ l'ensemble des fonctions faiblement modulaires de poids k.

Remarque. – De l'étude du domaine fondamental $\mathbf{D}$ et de la structure de $\mathbf{G} = \langle S, T \rangle$, on en déduit que si f est méromorphe, elle est faiblement modulaire de poids k si, et seulement si, pour tout $z \in \mathbf{H}$,

$$f(z) = f(z+1) \quad \text{et} \quad f(z) = z^{-k} f\left(-\frac{1}{z}\right).$$

Proposition 3.1. – *Pour tout entier k, $\mathbf{M}_k^w$ est un $\mathbf{C}$-espace vectoriel.*

Preuve. Si $\lambda \in \mathbf{C}$, $f, g \in \mathbf{M}_k^w$, alors $\lambda f + g$ est méromorphe sur $\mathbf{H}$ et si $z \in \mathbf{H}, \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$, on a :

$$(\lambda f + g)(z) = \lambda(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) + (cz+d)^{-k} g\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k}(\lambda f + g)\left(\frac{az+b}{cz+d}\right),$$

ce qui prouve le résultat. □

Définition 3.2. – *Pour $z \in \mathbf{H}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$, le facteur $J(\gamma, z) = (cz+d)^k$ est appelé* **facteur de modularité**.

Remarque. – Si k est impair, alors $\mathbf{M}_k^w = \{0\}$. En effet, $-I_2$ agit trivialement mais les facteurs de modularités de I_2 et $-I_2$ ne sont pas égaux. Si f est faiblement modulaire de poids k impair, pour tout $z \in \mathbf{H}$,

$$f(z) = (-1)^{-k} f(-I_2 z) = (-1) f(I_2 z) = -f(z),$$

donc f est identiquement nulle.

Pour cette raison, dans la suite, on s'intéressera quasi-exclusivement aux fonctions et formes modulaires de poids pair. Notons qu'on a la proposition suivante.

Proposition 3.2. – *Si $f : \mathbf{H} \to \mathbf{C}$ alors f est faiblement modulaire de poids k pour $\mathrm{PSL}_2(\mathbf{Z})$ si, et seulement si, elle est faiblement modulaire de poids k pour $\mathrm{SL}_2(\mathbf{Z})$.*

Proposition 3.3. – *Soit $z \in \mathbf{H}$ et $\gamma, \gamma' \in \mathbf{G}$. Le facteur de modularité vérifie la relation suivante, dites de 1-cocyle :*

$$J(\gamma\gamma', z) = J(\gamma, \gamma' z) J(\gamma' z).$$

Preuve. En effet, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$, on a

$$J(\gamma\gamma', z) = ((ca'+dc')z + (cb'+dd'))^k = ((ca'z+cb') + (dc'z+dd'))^k = \left(\left(c\left(\frac{a'z+b'}{c'z+d'}\right) + d\right)(c'z+d')\right)^k$$

avec $\left(c\left(\frac{a'z+b'}{c'z+d'}\right) + d\right)^k = J(\gamma, \gamma' z)$ et $(c'z+d')^k = J(\gamma' z)$, ce qui montre la propriété. □

Remarque. – Le fait que cette relation soit valable peut paraître anodin. Cependant, si $f \in \mathbf{M}_k^w$, $z \in \mathbf{H}$ et $\gamma, \gamma' \in \mathbf{G}$, on peut constater que

$$f(\gamma\gamma' z) = J(\gamma\gamma', z) f(z)$$

d'une part et que d'autre part,

$$f(\gamma\gamma' z) = J(\gamma, \gamma' z) f(\gamma' z) = J(\gamma, \gamma' z) J(\gamma', z) f(z).$$

De ce fait, si la relation de 1-cocycle n'est pas vérifiée en $z \in \mathbf{H}$ pour un certain couple (γ, γ'), alors $f(z) = 0$.

On va définir ce qu'est une fonction modulaire et une forme modulaire. Pour ce faire, nous devons décrire le comportement à l'infini des fonctions faiblement modulaires. Elles sont 1-périodiques : ainsi, elles vont posséder une q-expansion, c'est-à-dire une transformée de Fourier, et leur régularité à l'infini équivaudra par définition à la régularité en zéro de leur q-expansion. La justification de l'existence de la q-expansion est généralement considérée comme évidente dans la littérature, mais nous en donnons quand même une preuve aussi complète que possible.

Théorème 3.1. – *Supposons que $f : \mathbf{H} \to \mathbf{C}$ est méromorphe (respectivement holomorphe) et 1-périodique. Pour $z \in \mathbf{H}$, on pose $q(z) = e^{2i\pi z}$. Notons $\mathscr{D} = D(0,1)$ le disque unité de $\mathbf{C}$, et $\mathscr{D}^*$ le disque épointé en 0. Alors $q(\mathbf{H}) = \mathscr{D}^*$ et il existe une unique fonction $F : \mathscr{D}^* \to \mathbf{C}$, méromorphe (respectivement holomorphe), telle que $F \circ q = f$.*

Preuve. Soit $z = x + iy \in \mathbf{H}$, $y > 0$.

1) On a
$$q(z) = e^{2i\pi z} = e^{2i\pi(x+iy)} = e^{-2\pi y} e^{2i\pi x}$$
où $0 < e^{-2\pi y} < 1$ car $y > 0$ et l'exponentielle ne s'annule pas : donc $q(\mathbf{H}) \subseteq \mathscr{D}^*$. Mais on voit qu'on a égalité car $t \mapsto e^{-2i\pi t}$ est une bijection de $\mathbf{R}_+^*$ dans $]0,1[$, de réciproque $s \mapsto -\frac{\ln(s)}{2i\pi}$: ainsi $e^{-2\pi y}$ parcourt $]0,1[$ quand y parcourt $\mathbf{R}_+^*$ et $e^{2i\pi x}$ parcourt le cercle unité quand x parcourt $\mathbf{R}$. La fonction $q : \mathbf{H} \to \mathscr{D}^*$ est donc holomorphe et surjective. De plus, sa dérivée ne s'annule en aucun point de $\mathbf{H}$, c'est donc un biholomorphisme local par le théorème d'inversion locale holomorphe.
2) Comme f est 1-périodique, alors il existe une fonction $F : \mathscr{D}^* \to \mathbf{C}$ telle que $F \circ q = f$, associant à $w \in \mathscr{D}^*$ l'unique valeur de f sur l'ensemble $\frac{\mathrm{Log}(w)}{2i\pi}$. Comme q est surjective, on a dû définir F de manière unique sur tout $\mathscr{D}^*$, donc F est unique (il n'y a aucun point de $\mathscr{D}^*$ sans antécédents par q, auquel on aurait donc pu donner une valeur différente).
3) Soit $w \in \mathscr{D}^*$, et $w_0 \in \mathbf{H}$ un antécédent de w par q. Puisque q est un biholomorphisme local, il existe :
   — un voisinage U de w_0 dans $\mathbf{H}$,
   — un voisinage V de w dans $\mathscr{D}^*$,

   tels que $U \xrightarrow{q} V$ est un biholomorphisme. Supposons f méromorphe (respectivement holomorphe). Comme la méromorphie et l'holomorphie sont des propriétés conservées par un biholomorphisme, alors $F = f(q^{-1})$ est méromorphe (resp. holomorphe) de V dans $\mathbf{C}$. Puisque ce sont des propriétés locales et que F l'est dans un voisinage autour de chacun de ses points, alors F est méromorphe (resp. holomorphe) sur $\mathscr{D}^*$. □

Remarques. – Si $f \in \mathbf{M}_k^w$, alors elle est méromorphe et 1-périodique, donc elle vérifie les hypothèses du théorème précédent. Dans ce cas, par abus de notation, on notera $f(q)$, où $0 < |q| < 1$, pour $F(q(z))$, où $z \in \mathbf{H}$.

– La fonction F est méromorphe sur $\mathscr{D}^*$ donc elle admet un développement en série de Laurent au voisinage épointé de 0 : pour $w \in \mathscr{D}^*$, $F(w) = \sum_{n=-\infty}^{+\infty} a_n w^n$.

Définition 3.3. – *En combinant les remarques précédentes, si f est faiblement modulaire, alors :*

— *On dit que $f(q) = \sum_{n=-\infty}^{+\infty} a_n q^n$ est la q-**expansion** de f.*

— *Si F se prolonge en une fonction méromorphe au voisinage épointé de 0, on dit que f est* **méromorphe à l'infini**. *En termes de la q-expansion de f, il existe $M \in \mathbf{N}$ tel que $f(q) = \sum_{n=-M}^{+\infty} a_n q^n$.*

— *Si F se prolonge en une fonction holomorphe au voisinage épointé de 0, on dit que f est* **holomorphe à l'infini**. *En termes de la q-expansion de f, on a $f(q) = \sum_{n=0}^{+\infty} a_n q^n$. On définit sa* **valeur à l'infini** *comme étant $f(\infty) = F(0) = a_0$.*

Définition 3.4. – *Soit $f \in \mathbf{M}_k^w$ une fonction faiblement modulaire de poids k.*

— *On dit que f est une* **fonction modulaire de poids** *k si elle est méromorphe à l'infini.*

— *On dit que f est une* **forme modulaire de poids** *k si elle est holomorphe partout, c'est-à-dire sur tout $\mathbf{H}$ et en l'infini. On note $\mathbf{M}_k$ l'ensemble des formes modulaires de poids k.*

— *On dit que f est une* **forme parabolique de poids** *k (on dit aussi forme cuspidale) si c'est une forme modulaire de poids k qui s'annule à l'infini. On note $\mathbf{S}_k$ l'ensemble des formes paraboliques de poids k (le S venant de Spitzenform, l'allemand pour forme cuspidale).*

Remarque. – Soit $f : \mathbf{H} \to \mathbf{C}$ quelconque, admettant une q-expansion de la forme $f(q) = \sum_{n=0}^{+\infty} a_n q^n$. Si cette série converge, comme q est 1-périodique, alors f est invariante sous l'action de T. Ainsi, pour que f soit une forme modulaire de poids k, il faut et il suffit que $f(q)$ converge pour $0 < |q| < 1$ et que pour tout $z \in \mathbf{H}$,

$$f(z) = z^{-k} f(-\tfrac{1}{z}).$$

Exemple. – Nous ne produirons des exemples de fonctions et de formes modulaires que dans la dernière partie de ce chapitre. Bornons-nous ici à mentionner que $\Delta(q) = (2\pi)^{12} q \prod_{n=1}^{+\infty} (1-q^n)^{24}$ est une forme parabolique de poids 12.

Définition 3.5. – *Soient A une $\mathbf{C}$-algèbre et $(A_k)_{k\in\mathbf{Z}}$ des $\mathbf{C}$-espaces vectoriels tels $A = \bigoplus_{k=-\infty}^{+\infty} A_k$. On dit que A est une* **algèbre graduée** *si pour tout $i, j \in \mathbf{Z}$, $A_i A_j \subseteq A_{i+j}$.*

Proposition 3.4. – *Posons $\mathbf{M} = \bigoplus_{k=-\infty}^{+\infty} \mathbf{M}_k$ et $\mathbf{S} = \bigoplus_{k=-\infty}^{+\infty} \mathbf{S}_k$.*

1) L'ensemble $\mathbf{M}$ de toutes les formes modulaires est une algèbre graduée, où la graduation est donnée par le poids.

2) L'ensemble $\mathbf{S}$ de toutes les formes paraboliques est une algèbre graduée, où la graduation est donnée par le poids.

Preuve. On doit prouver que les $\mathbf{M}_k$ et les $\mathbf{S}_k$ sont des $\mathbf{C}$-espaces vectoriels vérifiant la graduation.

1) Soit $f \in \mathbf{M}_k$ et $g \in \mathbf{M}_l$, de q-expansions $f(q) = \sum_{n=0}^{+\infty} f_n q^n$ et $g(q) = \sum_{n=0}^{+\infty} g_n q^n$. Pour $z \in \mathbf{H}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a :

$$(fg)(z) = f(z)g(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-l} g\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-(k+l)} (fg)\left(\frac{az+b}{cz+d}\right),$$

donc $fg \in \mathbf{M}_{k+l}^w$. En regardant le produit des q-expansions de f et g, comme f et g sont holomorphes sur $\mathbf{H}$ et à l'infini, alors la q-expansion de fg n'aura pas de termes d'ordre négatif non nuls, donc $fg \in \mathbf{M}_{k+l}$. Les $\mathbf{M}_k^w$ sont des espaces vectoriels, donc si $h \in \mathbf{M}_k$ et $\lambda \in \mathbf{C}$, alors $\lambda f + h \in \mathbf{M}_k^w$ et en regardant la q-expansion de la somme $\lambda f + h$, comme λf et h sont holomorphes sur $\mathbf{H}$ et à l'infini, alors la q-expansion de $\lambda f + h$ n'aura pas de termes d'ordre négatif non nuls, donc $\lambda f + h \in \mathbf{M}_k$. Les $\mathbf{M}_k$ sont donc bien des $\mathbf{C}$-espaces vectoriels et $\mathbf{M}$ a une structure d'algèbre graduée.

2) Le même calcul avec $f \in \mathbf{S}_k$ et $g \in \mathbf{S}_l$ montre que $fg \in \mathbf{M}_{k+l}$. En regardant le terme constant du produit des q-expansions de f et g, on voit que $(fg)(\infty) = f_0 g_0 = 0$, donc que $fg \in \mathbf{S}_{k+l}$. Si $h \in \mathbf{S}_k$ et $\lambda \in \mathbf{C}$, encore en regardant le terme constant de la q-expansion de la somme $\lambda f + h$, on voit que $(\lambda f + h)(\infty) = \lambda f_0 + h_0 = 0$, donc que $\mathbf{S}_k$ est un $\mathbf{C}$-espace vectoriel. Ainsi, $\mathbf{S}$ est également une algèbre graduée. □

Proposition 3.5. – *Soit k un entier. Si $\mathbf{M}_k \neq \mathbf{S}_k$, soit $f \in \mathbf{M}_k$, non parabolique. Alors $\mathbf{M}_k = \mathbf{S}_k \oplus \mathbf{C}f$.*

Preuve. S'il existe une forme modulaire f de poids k non parabolique (autrement dit, telle que $f(\infty) = f_0 \neq 0$), alors si $g \in \mathbf{M}_k$, puisque rajouter une forme parabolique à f ne change pas le terme constant de sa q-expansion, il existe une unique manière d'écrire g comme la somme d'une forme parabolique de poids k et d'un multiple scalaire de f, à savoir $g = \left(g - \frac{g_0}{f_0} f\right) + \frac{g_0}{f_0} f$. □

3.2 Réseaux et fonctions de réseaux

Pendant l'introduction, on a motivé notre travail en faisant agir le groupe modulaire sur des objets liés aux courbes elliptiques. Revenons sur les résultats montrés ou annoncés, et établissons une correspondance entre les formes modulaires et les fonctions de réseaux. Ici, $\mathbf{G} = \mathrm{SL}_2(\mathbf{Z})$.

Définition 3.6. – *Commençons par rappeler quelques notations.*

— *L'ensemble des réseaux de* $\mathbf{C}$ *est noté* $\mathscr{R} = \{\Lambda = \mathbf{Z}w_1 \oplus \mathbf{Z}w_2, \mathbf{C}/\Lambda \text{ compact}\}$.

— *L'ensemble des bases de réseaux est noté* $\mathscr{M} = \{(w_1, w_2) \in \mathbf{C}^2, w_1, w_2 \neq 0, \mathrm{Im}\left(\frac{w_1}{w_2}\right) > 0\}$.

— *Une action de* $\mathbf{G}$ *sur* $\mathscr{M}$ *est donnée par* $\gamma(w_1, w_2) = (aw_1 + bw_2, cw_1 + dw_2)$.

Proposition 3.6. – *On a une bijection* $\mathscr{M}/\mathbf{G} \simeq \mathscr{R}$. *Cela découle des deux faits suivants :*

1) *L'application* $\varphi : \mathscr{M} \to \mathscr{R}, (w_1, w_2) \mapsto \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ *est surjective.*
2) *Pour deux bases* $(w_1, w_2), (w_1', w_2') \in \mathscr{M}$, *on a* $\varphi(w_1, w_2) = \varphi(w_1', w_2')$ *si, et seulement si* (w_1, w_2) *et* (w_1', w_2') *sont congrues modulo* $\mathbf{G}$.

Preuve. Le point 2) montrera que $\overline{(w_1, w_2)} \mapsto \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ est bien définie et injective.

1) Si $\mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ est un réseau, alors forcément $\mathrm{Im}\left(\frac{w_1}{w_2}\right) > 0$ ou $\mathrm{Im}\left(\frac{w_1}{w_2}\right) < 0$, mais dans le second cas le réseau $\mathbf{Z}w_2 \oplus \mathbf{Z}w_1$ est bien égal au premier et a un antécédent par φ.
2) Soit $(w_1, w_2) \in \mathscr{M}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$. Posons $(w_1', w_2') = \gamma(w_1, w_2)$. Alors $\gamma^{-1}(w_1', w_2') = (w_1, w_2)$, donc on peut écrire une base à partir de l'autre et elles définissent le même réseau. Comme $\frac{w_1'}{w_2'} = \gamma\frac{w_1}{w_2}$ et que $(w_1, w_2) \in \mathscr{M}$, alors $\mathrm{Im}\left(\frac{w_1'}{w_2'}\right) > 0$ et $(w_1', w_2') \in \mathscr{M}$.

   Réciproquement, si deux bases $(w_1, w_2), (w_1', w_2') \in \mathscr{M}$ définissent le même réseau, il existe $\gamma \in \mathrm{GL}_2(\mathbf{Z})$ tel que $\gamma(w_1, w_2) = (w_1', w_2')$. On a alors

$$\mathrm{Im}\left(\frac{w_1'}{w_2'}\right) = \mathrm{Im}\left(\frac{\frac{w_1'}{w_2}}{\frac{w_2'}{w_2}}\right) = \mathrm{Im}\left(\frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d}\right) = \frac{\det(\gamma)\,\mathrm{Im}\left(\frac{w_1}{w_2}\right)}{\left|c\frac{w_1}{w_2} + d\right|^2}.$$

   Mais comme $\mathrm{Im}\left(\frac{w_1}{w_2}\right), \mathrm{Im}\left(\frac{w_1'}{w_2'}\right) > 0$, on a forcément $\det(\gamma) = 1$ et $\gamma \in \mathbf{G}$. □

Rappelons ce que l'on a déduit de ce résultat dans l'introduction : on fait agir $\mathbf{C}^*$ sur $\mathscr{R}$ par multiplication scalaire ; on fait agir $\mathbf{C}^*$ sur $\mathscr{M}$ par $\lambda(w_1, w_2) = (\lambda w_1, \lambda w_2)$; les applications $\overline{(w_1, w_2)} \mapsto \frac{w_1}{w_2}$ et $z \mapsto \overline{(z, 1)}$ sont des bijections réciproques l'une de l'autre, donc $\mathscr{M}/\mathbf{C}^* \simeq \mathbf{H}$; l'action de $\mathbf{G}$ sur $\mathscr{M}$ commute à celle de $\mathbf{C}^*$, donc $\mathscr{M}/\mathbf{C}^*/\mathbf{G} \simeq \mathscr{M}/\mathbf{G}/\mathbf{C}^*$; des deux points précédents, on obtient que $\mathbf{H}/\mathbf{G} \simeq \mathscr{R}/\mathbf{C}^*$.

Définition 3.7. *Soit* $F : \mathscr{R} \to \mathbf{C}$ *une fonction de réseaux et* k *un entier. On dit que* F *est* **homogène de poids** k *si pour tout* $\alpha \in \mathbf{C}^*$, $\Lambda \in \mathscr{R}$, *on a*

$$F(\alpha\Lambda) = \alpha^{-k}F(\Lambda).$$

Remarques. – Si F est une fonction de réseaux homogène de poids k, alors on peut définir une fonction de bases $F' : \mathscr{M} \to \mathbf{C}$ qui à (w_1, w_2) associe $F(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2)$. Puisque deux bases définissent le même réseau si, et seulement si elles sont congrues modulo $\mathbf{G}$, cette fonction est invariante sous l'action de $\mathbf{G}$ et vérifie la relation d'homogénéité de poids k

$$F'(\alpha w_1, \alpha w_2) = \alpha^{-k}F'(w_1, w_2).$$

Réciproquement, une fonction de bases $F' : \mathscr{M} \to \mathbf{C}$ homogène de poids k et invariante sous l'action de $\mathbf{G}$ passe au quotient $\mathscr{M}/\mathbf{G} \simeq \mathscr{R}$ et définit donc une fonction de réseaux $F : \mathscr{R} \to \mathbf{C}$, homogène de poids k, qui à $\Lambda = \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ associe $F'(w_1, w_2)$.

– Soit $F' : \mathscr{M} \to \mathbf{C}$ une fonction de bases homogène de poids k et invariante sous l'action de $\mathbf{G}$. En écrivant la relation d'homogénéité de F' en $(w_1, w_2) \in \mathscr{M}$ et $\alpha = \frac{1}{w_2}$, on voit que

$$F'\left(\frac{w_1}{w_2}, 1\right) = F'\left(\frac{1}{w_2}(w_1, w_2)\right) = w_2^k F'(w_1, w_2).$$

Ainsi, la valeur de $F'(w_1, w_2) = w_2^{-k} F'(\frac{w_1}{w_2}, 1)$ ne dépend que de $\frac{w_1}{w_2} \in \mathbf{H}$. Notons $f : \mathbf{H} \to \mathbf{C}$ la fonction qui à $z \in \mathbf{H}$ associe $F'(z, 1)$. L'invariance de F' sous l'action de $\mathbf{G}$ montre que pour $z \in \mathbf{H}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$,

$$f(\gamma z) = F'\left(\frac{az+b}{cz+d}, 1\right) = (cz+d)^k F'(az+b, cz+d) = (cz+d)^k F'(\gamma(z,1)) = (cz+d)^k F'(z,1) = (cz+d)^k f(z).$$

Donc f vérifie l'équation de modularité de poids k. Réciproquement, si $f : \mathbf{H} \to \mathbf{C}$ vérifie l'équation de modularité de poids k, notons $F' : \mathscr{M} \to \mathbf{C}$ la fonction de bases qui à (w_1, w_2) associe $w_2^{-k} f(\frac{w_1}{w_2})$. Par définition de F', pour $(w_1, w_2) \in \mathscr{M}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{G}$, on a :

$$F'(\gamma(w_1, w_2)) = F'(aw_1 + bw_2, cw_1 + dw_2) = (cw_1 + dw_2)^{-k} f\left(\frac{aw_1 + bw_2}{cw_1 + dw_2}\right) = (cw_1 + dw_2)^{-k} f\left(\gamma \frac{w_1}{w_2}\right).$$

Puisque f vérifie l'équation de modularité de poids k, on obtient

$$F'(\gamma(w_1, w_2)) = (cw_1 + dw_2)^{-k} \left(c\frac{w_1}{w_2} + d\right)^k f\left(\frac{w_1}{w_2}\right) = w_2^{-k} f\left(\frac{w_1}{w_2}\right) = F'(w_1, w_2),$$

ce qui montre que F' est invariante sous l'action de $\mathbf{G}$, et si $\alpha \in \mathbf{C}^*$, alors

$$F'(\alpha(w_1, w_2)) = F'(\alpha w_1, \alpha w_2) = (\alpha w_2)^{-k} f\left(\frac{\alpha w_1}{\alpha w_2}\right) = \alpha^{-k} F'(w_1, w_2),$$

d'où l'on voit que F' est également homogène de poids k.

Avec les deux remarques précédentes, on vient de construire, pour k un entier :

1) une correspondance bijective entre les fonctions de réseaux homogènes de poids k et les fonctions de bases homogènes de poids k invariantes sous l'action de $\mathbf{G}$, donnée par :

$$\begin{array}{ccc} F & \mapsto & F'(w_1, w_2) = F(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2) \\ F(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2) = F'(w_1, w_2) & \leftarrow\!\shortmid & F' \end{array}$$

2) une correspondance bijective entre les fonctions de bases homogènes de poids k invariantes sous l'action de $\mathbf{G}$ et les fonctions de $\mathbf{H}$ vérifiant l'équation de modularité de poids k, donnée par :

$$\begin{array}{ccc} F' & \mapsto & f(z) = F'(z, 1) \\ F'(w_1, w_2) = w_2^{-k} f\left(\frac{w_1}{w_2}\right) & \leftarrow\!\shortmid & f \end{array}$$

La composition de ces bijections intermédiaires nous permet d'établir le résultat suivant.

Théorème 3.2. – *Soient $f : \mathbf{H} \to \mathbf{C}$ et $F : \mathscr{R} \to \mathbf{C}$ qui soient issues l'une de l'autre, c'est-à-dire que*

$$F(\mathbf{Z}w_1 \oplus \mathbf{Z}w_2) = w_2^{-k} f\left(\frac{w_1}{w_2}\right) \quad \textit{ou} \quad f(z) = F(\mathbf{Z}z + \mathbf{Z}).$$

Alors F est homogène de poids k si, et seulement si f vérifie l'équation de modularité de poids k.

Remarque. – Si une fonction $f : \mathbf{H} \to \mathbf{C}$ est issue d'une fonction de réseaux homogène de poids k, alors si elle est méromorphe, c'est une fonction faiblement modulaire de poids k sur $\mathrm{SL}_2(\mathbf{Z})$, donc sur $\mathrm{PSL}_2(\mathbf{Z})$.

3.3 Premiers exemples de formes modulaires

On va produire nos premiers exemples de formes modulaires (non identiquement nulles) de poids pair, les séries d'Eisenstein. On montrera que ces fonctions sont en fait les "particules élémentaires" de la théorie sur le groupe modulaire plein $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$ dans notre prochain chapitre.

Définition 3.8. – *Soit $k > 2$ un entier et $z \in \mathbf{H}$. On note $G_k(z) = \sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}$ la k-ème* **série d'Eisenstein**.

Pour montrer que G_k est une forme modulaire de poids k si $k \geqslant 3$, on va employer les différentes méthodes que l'on a développé jusqu'à présent. Après en avoir établi la convergence et la régularité, on observera qu'elle est issue d'une fonction de réseaux homogène de poids k, et on en déduira qu'étant méromorphe, elle est faiblement modulaire de poids k. Il ne restera plus qu'à montrer qu'elle est holomorphe à l'infini.

Dans la suite, on considère $k \geqslant 4$ un entier **pair**.

Lemme 3.1. – *La série G_k converge normalement sur tout compact de $\mathbf{H}$, et sa somme est holomorphe sur $\mathbf{H}$.*

Preuve. Commençons par montrer la convergence simple, ce qui sera utile pour la remarque suivante.

1) Soit $z \in \mathbf{H}$ et $n \in \mathbf{N}^*$. Le nombre de points de $\mathbf{Z}z \oplus \mathbf{Z}$ dans l'anneau $\overline{A(0,n,n+1)}$ est équivalent en l'infini à $\pi(n+1)^2 - \pi n^2$, qui est un $O(n)$, donc $G_k(z)$ est majorée au produit par une constante près par la série convergente $\sum_{n\in\mathbf{N}^*} \frac{1}{n^k}$, qui converge effectivement car $k > 2$. Cela montre la convergence simple.
2) Soit $z \in \mathbf{D}$ et $m, n \in \mathbf{Z}$, $(m,n) \neq (0,0)$. Comme ρ atteint le minimum en module et en partie réelle de $\mathbf{D}$, on a
$$|mz+n|^2 = m^2 z\overline{z} + 2mn\,\mathrm{Re}(z) + n^2 \geqslant m^2|\rho| + 2mn\,\mathrm{Re}(\rho) + n^2 = m^2 - mn + n^2 = ||m|\rho - |n||^2$$
et comme la série $\sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m\rho+n)^k}$ est convergente par 1), alors $G_k(z)$ converge normalement sur $\mathbf{D}$, d'où l'on déduit que $G_k(z)$ converge normalement sur tout compact de $\mathbf{H}$ par les deux faits suivants, eux-mêmes conséquences des résultats établis au chapitre précédent :
   — comme $\mathbf{D}$ est un domaine fondamental de l'action de $\mathbf{G}$ sur $\mathbf{H}$, on a $\mathbf{H} = \bigcup_{\gamma\in\mathbf{G}} \gamma\mathbf{D}$;
   — comme les stabilisateurs de tous les points de $\mathbf{D}$ sont finis, on peut trouver autour de chaque point $z \in \mathbf{H}$ un voisinage n'intersectant qu'un nombre fini de $\gamma\mathbf{D}$.
3) Les fonctions $z \mapsto \frac{1}{mz+n}$ avec $m, n \in \mathbf{Z}$, $(m,n) \neq (0,0)$, n'ont pas de pôles dans $\mathbf{H}$ donc sont holomorphes sur $\mathbf{H}$, ainsi G_k est holomorphe sur $\mathbf{H}$ comme sa convergence y est normale sur tout compact. □

Remarque. – La preuve précédente de la convergence simple montre que la fonction de réseaux $F_k : \Lambda \mapsto \sum_{z\in\Lambda^*} \frac{1}{z^k}$, clairement homogène de poids k, est bien définie. Comme k est pair et que la fonction de $\mathbf{H}$ induite par F_k est
$$F_k(z,1) = \sum_{w\in(\mathbf{Z}z\oplus\mathbf{Z})^*} \frac{1}{w^k} = \sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^k} = G_k(z)$$
et que G_k est méromorphe, alors G_k est faiblement modulaire de poids k. Par abus de notation, on notera $F_k = G_k$.

Proposition 3.7. – *La k-ème série d'Eisenstein est une forme modulaire de poids k et de valeur à l'infini*
$$G_k(\infty) = 2\zeta(k),$$
où ζ est la fonction zêta de Riemann.

Preuve. On vient de voir que G_k est holomorphe sur $\mathbf{H}$ et faiblement modulaire de poids k. La limite en 0 dans $\mathscr{D}^*$ de sa q-expansion est égale à la limite dans $\mathbf{H}$ de $G_k(z)$ quand $\mathrm{Im}(z)$ tend vers $+\infty$. Cette dernière est la même si $z \in \mathbf{D}$, où la convergence est normale donc uniforme et où on peut donc intervertir limites et sommes.

Ainsi, pour $z \in \mathbf{D}$, on a :

$$\lim_{\mathrm{Im}(z)\to+\infty} G_k(z) = \sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}} \lim_{\mathrm{Im}(z)\to+\infty} \frac{1}{(mz+n)^k} = \sum_{k\in\mathbf{Z}^*} \frac{1}{n^k} + \sum_{\substack{m,n\in\mathbf{Z}\\m\neq 0}} \lim_{\mathrm{Im}(z)\to+\infty} \frac{1}{(mz+n)^k}.$$

Or, la somme de droite vaut 0 et puisque k est pair, $\sum_{n\in\mathbf{Z}^*} \frac{1}{n^k} = 2\sum_{n=1}^{+\infty} \frac{1}{n^k} = 2\zeta(k)$, ce qui montre le résultat. □

On ne fait que mentionner, sans démonstration, la formule donnant la q-expansion des séries d'Eisenstein. Elle peut être prouvée en utilisant une équation fonctionnelle satisfaite par la fonction cotangente.

Proposition 3.8. – *La q-expansion de la série d'Eisenstein de poids k est*

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{+\infty} \sigma_{k-1}(n)q^n,$$

où $\sigma_k(n) = \sum_{d|n} d^k$ est la somme des puissances k-ème des diviseurs de n.

Remarque. – On rappelle que

$$\zeta(4) = \frac{\pi^4}{90} \quad \text{et} \quad \zeta(6) = \frac{\pi^6}{945}.$$

Cela indique une normalisation possible des séries d'Eisenstein de plus petit poids, G_4 et G_6, issue de la théorie des courbes elliptiques.

Définition 3.9. – *On définit les deux* **séries d'Eisenstein "normalisées"** *par $g_4 = 60G_4$ et $g_6 = 140G_6$, de valeurs à l'infini $g_4(\infty) = 120\zeta(4) = \frac{4}{3}\pi^4$ et $g_6(\infty) = 280\zeta(6) = \frac{8}{27}\pi^6$.*

Remarque. – On observe alors que

$$(g_4^3 - 27g_6^2)(\infty) = \frac{64}{27}\pi^{12} - 27 \times \frac{64}{27^2}\pi^{12} = 0.$$

Comme $\mathbf{M}$ est une algèbre graduée, on peut faire la définition suivante.

Définition 3.10. – *On définit le* **discriminant** *comme étant $\Delta = g_4^3 - 27g_6^2$. C'est une forme parabolique de poids 12.*

Remarque. – On peut également construire une fonction modulaire de poids 0 non triviale, comme quotient de deux formes modulaires non nulles de mêmes poids. C'est ce que l'on fait dans la dernière définition de ce chapitre. La normalisation peut paraître étrange : elle est faite de telle manière à ce que la fonction ait un résidu 1 en l'infini, et en fait même que tous les coefficients de sa q-expansion soient entiers.

Définition 3.11. – *On définit* **l'invariant modulaire** *comme étant $j = 1728\frac{g_4^3}{\Delta}$. C'est une fonction modulaire de poids 0.*

Remarque. – Mentionnons brièvement le lien entre ces fonctions et la théorie des fonctions elliptiques. Fixons $\Lambda = \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$ un réseau de $\mathbf{C}$. Une **fonction elliptique** (par rapport à Λ) est une fonction méromorphe sur $\mathbf{C}$ qui est w_1-périodique et w_2-périodique. L'exemple typique d'une telle fonction est la **fonction $\wp$ de Weierstrass** :

$$\wp(z) = \frac{1}{z^2} + \sum_{w\in\Lambda^*}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{+\infty}(2k-1)G_k(\Lambda)z^{2k-2},$$

qui vérifie l'équation différentielle

$$(\wp')^2 = 4\wp^3 - g_4\wp - g_6.$$

La forme parabolique que l'on vient de définir, $\Delta = g_4^3 - 27g_6^2$, est le discriminant du polynôme de droite :

$$\Delta = \mathrm{Disc}(4X^3 - g_4X - g_6).$$

4 Les espaces de formes modulaires

4.1 La formule de valence

Le but de cette section est de prouver la formule de valence, qui établit une condition vérifiée par les zéros et les pôles de toute fonction modulaire non identiquement nulle, et dont la preuve utilise de manière cruciale le domaine fondamental $\mathbf{D}$. Elle va nous permettre de calculer les dimensions des espaces vectoriels de formes modulaires pour $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$. Pour le reste de cette section, on considère une fonction modulaire $f : \mathbf{H} \to \mathbf{C}$ de poids k non identiquement nulle : on a donc forcément k pair.

Définition 4.1. – *Soit $p \in \mathbf{H}$. On appelle* **ordre de f en** *p, que l'on note $v_p(f)$, l'unique entier $n \in \mathbf{Z}$ tel que $z \mapsto \dfrac{f(z)}{(z-p)^n}$ soit holomorphe en p et ne s'annule pas en p. On définit l'***ordre de f en l'infini** *par $v_\infty(f) = v_0(F)$, où F est la fonction de $q \in \mathscr{D}^*$ qui apparaît dans la q-expansion de f.*

Remarque. – Puisque f vérifie l'équation de modularité de poids k, l'ordre en un point $p \in \mathbf{H}$ de f est égal à celui en tous ses translatés γp : en effet, le facteur de modularité $(cz+d)^k$ n'a ni zéros ni pôles dans $\mathbf{H}$. L'ordre de f en un point de $\mathbf{H}$ ne dépend donc que de la classe de ce point dans $\mathbf{H}/\mathbf{G}$.

Théorème 4.1. – *Si f est une fonction modulaire de poids k non identiquement nulle, on a*

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

Preuve. On commence par vérifier la bonne définition du terme de gauche, puis on définit un domaine sur le bord duquel on va appliquer le théorème des résidus logarithmiques, pour enfin calculer la même intégrale bout à bout.

1) **Bonne définition.** Commençons par remarquer que f n'a qu'un nombre fini de zéros et de pôles dans $\mathbf{D}$, ce qui justifie que la somme sur $\mathbf{H}/\mathbf{G}$ est bien définie. Par méromorphie de F en 0, il existe $0 < r < 1$ tel que F n'ait aucun zéros ou pôles pour $0 < |q| < r$, donc que f n'ait aucun zéros ou pôles pour $\mathrm{Im}(z) > R = \frac{1}{2}\ln(\frac{1}{r})$. Ainsi, sur la partie compacte $\mathbf{D}_R = \{z \in \mathbf{D}, \mathrm{Im}(z) \leqslant R\}$, f n'a qu'un nombre fini de pôles par méromorphie, et qu'un nombre fini de zéros par le principe des zéros isolés (par holomorphie de f sur l'ouvert connexe de l'union de petits disques de rayon fixé autour des points de $\mathbf{D}_R$, privée des pôles de f).

2) **Le domaine et son contour.** Soit $\varepsilon > 0$ tel que $\varepsilon < \dfrac{1}{R}$, ce qui implique que :
   - dans $\{z \in \mathbf{H}, \mathrm{Im}(z) > \frac{1}{\varepsilon}\} \subseteq \{z \in \mathbf{H}, \mathrm{Im}(z) > R\}$, f n'a ni zéros ni pôles ;
   - dans $D(0, e^{-\frac{2\pi}{\varepsilon}}) \subseteq D(0,r)$, F n'a ni zéros ni pôles sauf peut être 0 ;
   - la partie $\mathbf{D}_{\varepsilon^{-1}}$ contient au moins un représentant de la classe de chaque zéro et pôle de f : il y en a exactement un si le zéro ou le pôle est intérieur à $\mathbf{D}$, deux s'il est sur le bord de $\mathbf{D}$, à l'exception de i qui n'en a qu'un.

   Notons Z l'ensemble des zéros et des pôles de f, $\partial\mathbf{D}$ le bord de $\mathbf{D}$, $\partial Z = Z \cap \partial\mathbf{D}$ les zéros et pôles de f sur le bord de $\mathbf{D}$ et $\overset{\circ}{Z} = Z \cap \overset{\circ}{\mathbf{D}}$ ceux dans l'intérieur de $\mathbf{D}$. On va en fait choisir ε plus petit encore, de telle sorte à ce que :
   - pour tout $p, p' \in \partial Z \cup \overset{\circ}{Z}$ distincts, $D(p,\varepsilon)$ ne rencontre pas le disque $D(p',\varepsilon)$;
   - pour tout $p \in \partial Z \cup \overset{\circ}{Z}$, $D(p,\varepsilon)$ ne rencontre pas les disques $D(i,\varepsilon)$, $D(\rho,\varepsilon)$ et $D(-\overline{\rho},\varepsilon)$.

   Cela est possible par finitude des zéros et des pôles de f dans $\mathbf{D}$. Définissons alors

$$K_\varepsilon = \mathbf{D}_{\varepsilon^{-1}} \cap \left(\bigcup_{p \in \partial Z \cup \{i,\rho,-\overline{\rho}\}} D(p,\varepsilon) \right)^c$$

Soit ψ un lacet simple paramétrant ∂K_ε dans le sens trigonométrique, qui évite donc tous les pôles et les zéros de f sur $\partial\mathbf{D}$ et contient tous ceux dans $\overset{\circ}{\mathbf{D}}$, qui sont les mêmes que ceux dans K_ε. Le théorème des résidus logarithmiques donne alors

$$\frac{1}{2i\pi}\int_\psi \frac{f'}{f} = \sum_{p\in K_\varepsilon} v_p(f) = \sum_{\substack{p\in\mathbf{H}/\mathbf{G}\\ \text{intérieur}}} v_p(f).$$

3) On va calculer l'intégrale ci-dessus d'une autre manière, en découpant le contour d'intégration en morceaux selon la figure ci-dessous et en interprétant pour chacun d'entre-eux leur contribution à l'intégrale.

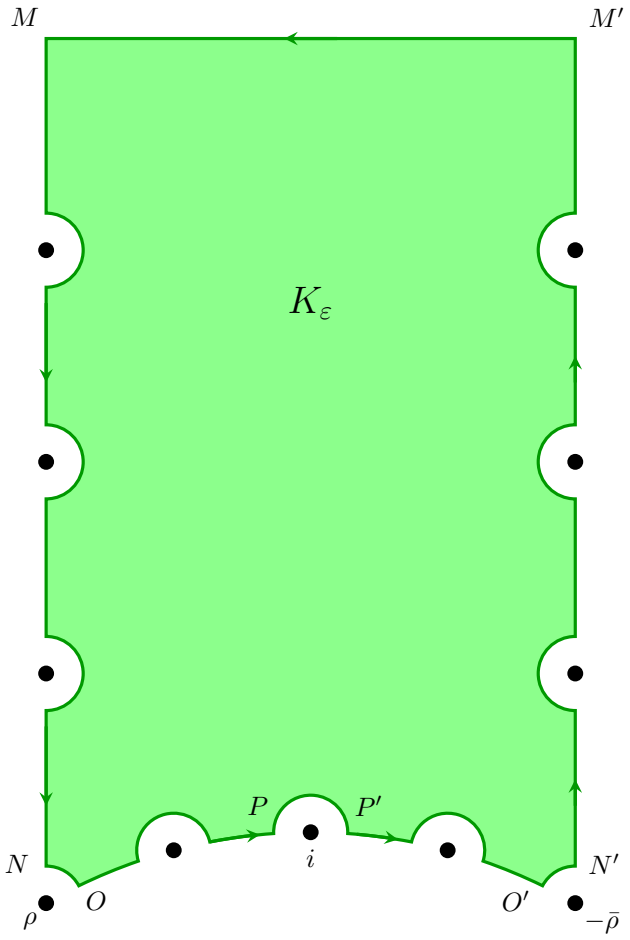


FIGURE 4.1 – Le contour de K_ε

(a) **Les deux segments verticaux privés des demi-cercles.** Par 1-périodicité de f et comme T envoie MN sur $M'N'$, l'intégrale le long de MN privé des demi-cercles vaut l'opposé de l'intégrale le long de $M'N'$ privé des demi-cercles puisqu'elles sont prises dans des sens contraires. Leur somme vaut donc 0.

(b) **Les demi-cercles des deux segments verticaux.** Si $p \in \partial Z$ est de partie réelle $\pm\frac{1}{2}$, alors $p \pm 1$ est un zéro ou un pôle de f de partie réelle opposée. Il est donc entouré d'un demi-cercle symétrique à celui de p, que l'on peut envoyer par T ou T^{-1} pour former un cercle complet autour de p, pris dans le sens anti-trigonométrique. Comme f est 1-périodique, on a, par le théorème des résidus logarithmiques :

$$\frac{1}{2i\pi}\int_{\partial D_{\text{demi}}(p,\varepsilon)} \frac{f'}{f} + \frac{1}{2i\pi}\int_{\partial D_{\text{demi}}(p+1,\varepsilon)} \frac{f'}{f} = \frac{1}{2i\pi}\int_{\partial D(p,\varepsilon)} \frac{f'}{f} = -\operatorname{Res}\left(\frac{f'}{f}, p\right) = -v_p(f).$$

La contribution de la classe de p dans $\mathbf{H}/\mathbf{G}$ vaut donc $-v_p(f)$.

(c) **Le segment horizontal.** Le changement de variable donné par $q(z) = e^{2i\pi z}$ transforme MM' en le cercle $\partial D(0, e^{-\frac{2\pi}{\varepsilon}})$ parcouru dans le sens anti-trigonométrique. Comme on a choisi ε de telle sorte à ce que la fonction méromorphe F n'ait ni zéro ni pôle dans $D(0, e^{-\frac{2\pi}{\varepsilon}})$ sauf peut être en 0, on a, par le théorème des résidus logarithmiques appliqué à F :

$$\frac{1}{2i\pi}\int_{MM'}\frac{f'}{f} = \frac{1}{2i\pi}\int_{MM'}\frac{F'(q(z))q'(z)}{F(q(z))}\,dz = -\frac{1}{2i\pi}\int_{\partial D(0,e^{-2\pi\varepsilon^{-1}})}\frac{F'}{F} = -v_0(F) = -v_\infty(f).$$

(d) **Les deux segments hyperboliques privés des arcs de cercle.** Comme f est vérifie l'équation modulaire en S, la dérivée logarithmique de $z \mapsto f(Sz)$ vaut $z \mapsto \frac{f'}{f} + \frac{k}{z}$. Le segment hyperbolique OP privé des arcs de cercle est envoyé par S sur $O'P'$ privé des arcs de cercle, parcouru dans le sens contraire. On a :

$$\frac{1}{2i\pi}\int_{OP}\frac{f'}{f} + \frac{1}{2i\pi}\int_{O'P'}\frac{f'}{f} = \frac{1}{2i\pi}\int_{OP}\left(\frac{f'(z)}{f(z)} - \left(\frac{k}{z} + \frac{f'(z)}{f(z)}\right)\right)\,dz = -\frac{k}{2i\pi}\int_{OP}\frac{1}{z}\,dz.$$

L'intégrale de droite tend vers $-\frac{i\pi}{6}$ quand ε tend vers 0 : plus ε est petit, plus elle se rapproche de la valeur de l'intégrale de $\frac{1}{z}$ sur le segment hyperbolique de ρ à i :

$$\int_{\frac{2\pi}{6}}^{\frac{\pi}{2}}\frac{ie^{it}}{e^{it}}\,dt = i\left(\frac{2\pi}{6} - \frac{\pi}{2}\right) = -\frac{i\pi}{6}.$$

Ainsi, l'intégrale le long des deux segments hyperboliques privés des arcs de cercle tend vers $\frac{k}{12}$ quand ε tend vers 0.

(e) **Les arcs de cercles de i, ρ et $-\overline{\rho}$, et des deux segments hyperboliques.** On calcule la contribution de l'arc de cercle autour de i et la preuve s'adaptera facilement aux cas de ρ, $-\overline{\rho}$ et $p \in \partial Z$ de module 1. Soit $n = v_i(f)$. Alors il existe une fonction méromorphe g qui est holomorphe en i telle que

$$f(z) = (z-i)^n g(z), \quad \text{d'où l'on a} \quad \frac{f'(z)}{f(z)} = \frac{n}{z-i} + \frac{g'(z)}{g(z)}.$$

Comme g est holomorphe donc a fortiori bornée dans un voisinage de i,

$$\frac{1}{2i\pi}\int_{PP'}\frac{g'(z)}{g(z)} \xrightarrow[\varepsilon\to 0]{} 0.$$

Pour le terme de gauche de la somme, on applique le même raisonnement que pour (c), sauf qu'ici l'arc de cercle ne tend qu'à décrire un angle de π. On a donc

$$\frac{1}{2i\pi}\int_{PP'}\frac{n}{z-i}\,dz \xrightarrow[\varepsilon\to 0]{} \frac{n}{2i\pi}\int_{\pi}^{0}\frac{i\varepsilon e^{it}}{i+\varepsilon e^{it}-i}\,dt = -i\pi\frac{n}{2i\pi} = -\frac{1}{2}v_i(f).$$

Donc la contribution de la classe de i dans $\mathbf{H}/\mathbf{G}$ vaut $-\frac{1}{2}v_i(f)$ quand ε tend vers 0.

Le cas de $p \in \partial Z$ de module 1 est identique et sa contribution tend vers $-\frac{1}{2}v_p(f)$ quand ε tend vers 0. Mais Sp est un zéro ou un pôle de f de module 1 sur l'autre segment hyperbolique qui apporte la même contribution donc la contribution globale de la classe de p dans $\mathbf{H}/\mathbf{G}$ vaut $-v_p(f)$ quand ε tend vers 0.

Pour ρ et $-\overline{\rho}$, la seule différence dans le calcul est l'angle de l'arc de cercle, qui vaut $\frac{\pi}{3}$, si bien que leurs contributions respectives valent

$$-\frac{1}{6}v_\rho(f) \quad \text{et} \quad -\frac{1}{6}v_{-\overline{\rho}}(f)$$

et que la contribution de la classe de ρ dans $\mathbf{H}/\mathbf{G}$ vaut $-\frac{1}{3}v_\rho(f)$, quand ε tend vers 0.

4) **Conclusion.** Regroupons les termes avec la bonne orientation : on a

$$\sum_{\substack{p\in\mathbf{H}/\mathbf{G}\\ \text{intérieur}}} v_p(f) = \frac{1}{2i\pi}\int_\psi \frac{f'}{f} = \frac{k}{12} - v_\infty(f) - \frac{1}{2}v_i(f) - \frac{1}{3}v_\rho(f) - \sum_{\substack{p\in\mathbf{H}/\mathbf{G},\ p\neq i,\rho\\ \text{sur le bord}}} v_p(f).$$

En passant les termes de l'autre côté, on obtient bien la formule de valence. □

4.2 Les dimensions et les bases des espaces

La formule de valence va nous permettre de calculer les dimensions des espaces de formes modulaires et de voir qu'en tant qu'algèbre, $\mathbf{M}$ est engendrée par G_4 et G_6, si bien que ce sont effectivement les particules élémentaires de la théorie sur $\mathbf{G} = \mathrm{PSL}_2(\mathbf{Z})$. On regroupe ces considérations dans les deux théorèmes suivants.

Théorème 4.2. – *On détermine la dimension de $\mathbf{M}_k$ pour tout $k \in \mathbf{Z}$.*

1) Si $k < 0$ ou $k = 1, 2$ ou k est impair, alors $\mathbf{M}_k = \{0\}$.

2) Pour tout $k \in \mathbf{Z}$, l'application de multiplication par Δ donne lieu à un isomorphisme

$$\begin{array}{ccc} \mathbf{M}_k & \simeq & \mathbf{S}_{k+12} \\ f & \mapsto & \Delta f \end{array}$$

3) Pour $k = 0, 4, 6, 8, 10$, $\mathbf{S}_k = \{0\}$.

4) On a $\dim \mathbf{M}_0 = 1$ et $\mathbf{M}_0 = \langle 1\rangle$ et pour $k = 4, 6, 8, 10$, on a $\dim \mathbf{M}_k = 1$ et $\mathbf{M}_k = \langle G_k\rangle$.

5) Pour tout $k \geqslant 0$ pair,

$$\begin{cases} \dim \mathbf{M}_k = \left\lfloor \dfrac{k}{12} \right\rfloor & \text{si } k \equiv 2\ [12] \\ \dim \mathbf{M}_k = \left\lfloor \dfrac{k}{12} \right\rfloor + 1 & \text{si } k \not\equiv 2\ [12]. \end{cases}$$

Preuve. Si f est une forme modulaire de poids k non identiquement nulle, la formule de valence donne

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

où tous les termes de gauche sont positifs par holomorphie de f sur $\mathbf{H}$ et en l'infini.

1) On a vu que si k est impair alors $\mathbf{M}_k = \{0\}$. Si $k < 0$, il ne peut pas y avoir de forme modulaire non identiquement nulle de poids k à cause de la positivité dans la remarque ci-dessus. Il ne peut pas y en avoir non plus pour $k = 1, 2$ car $\frac{1}{12}, \frac{2}{12}$ ne peuvent pas s'écrire sous la forme $n + \frac{n'}{2} + \frac{n''}{3}$ avec $n, n', n'' \in \mathbf{N}$.

2) La multiplication par Δ est bien linéaire et bijective, donc un isomorphisme linéaire, à condition qu'elle envoie effectivement $\mathbf{M}_k$ dans $\mathbf{S}_{k+12}$ et que la division par Δ envoie $\mathbf{S}_{k+12}$ dans $\mathbf{M}_k$.
Soit $f \in \mathbf{M}_k$, comme Δ est parabolique de poids 12, il est clair que Δf est modulaire de poids 12 et s'annule à l'infini, avec les remarques faites dans le chapitre précédent.
Réciproquement, soit $g \in \mathbf{S}_{k+12}$.
   — Appliquons la remarque à la forme modulaire non nulle G_4 : puisqu'on ne peut écrire $\frac{4}{12}$ que sous la forme $n = 0, n' = 0, n'' = 1$, alors G_4 a un zéro d'ordre 1 en ρ et $-\overline{\rho}$ et ne s'annule nulle par ailleurs.
   — La remarque appliquée à G_6 donne, puisqu'on ne peut écrire $\frac{6}{12}$ qu'avec $n = 0, n' = 1, n'' = 0$, que G_6 a un zéro d'ordre 1 en i et ne s'annule nulle part ailleurs.
   — Entre autres, on déduit des deux points précédents que $v_i(\Delta) = 0$ donc Δ n'est pas identiquement nulle. La remarque ci-dessus appliquée à Δ qui est de poids 12 montre, puisque $v_\infty(\Delta) \geqslant 1$, que l'on a forcément $n = 1, n' = 0, n'' = 0$. Ainsi, $v_\infty(\Delta) = 1$ et Δ ne s'annule nulle part ailleurs.

   On pose alors $f = \frac{g}{\Delta}$. C'est une fonction faiblement modulaire de poids $k - 12$. Si $p \in \mathbf{H}$, comme g est holomorphe sur $\mathbf{H}$ alors

$$v_p(f) = v_p(g) - v_p(\Delta) = v_p(g) \geqslant 0$$

donc f est holomorphe sur $\mathbf{H}$ et

$$v_\infty(f) = v_\infty(g) - v_\infty(\Delta) = v_\infty(g) - 1 \geqslant 0$$

car g s'annule en l'infini donc f est holomorphe en l'infini et $f \in \mathbf{M}_k$.

3) Le point précédent montre que $\mathbf{S}_k$ et $\mathbf{M}_{k-12}$ sont isomorphes donc si $k = 0, 4, 6, 8, 10$, alors $k - 12 < 0$ et $\mathbf{M}_{k-12}$ est réduit à 0 par le premier point donc $\mathbf{S}_k = \{0\}$.
4) Si $k = 0, 4, 6, 8, 10$, puisqu'il existe des formes modulaires non paraboliques de chacun de ces poids, en la matière de $1, G_4, G_6, G_8$ et G_{10}, alors par une proposition du chapitre précédent on a

$$\mathbf{M}_0 = \mathbf{S}_0 \oplus \mathbf{C}1 \quad \text{et} \quad \mathbf{M}_k = \mathbf{S}_k \oplus \mathbf{C}G_k \text{ pour } k = 4, 6, 8, 10.$$

Avec le point précédent, $\mathbf{S}_k = \{0\}$, ce qui montre le résultat.
5) D'après 4), la formule est vraie pour $0 \leqslant k < 12$ et quand on rajoute 12 à k, alors la partie entière de $\frac{k}{12}$ est incrémentée de 1, donc la formule est vraie pour tout $k \geqslant 0$. □

Remarque. – On déduit du point 5) quelques identités sur les séries d'Eisenstein, du type

$$G_4^2(z) = G_8(z), \quad G_4(z)G_6(z) = G_{10}(z), \quad G_6(z)G_8(z) = G_4(z)G_{10}(z) = G_{14}(z),$$

valables à une constante multiplicative près : ce serait des égalités si on avait normalisé les séries d'Eisenstein pour valoir 1 en l'infini, en posant $E_k = (2\zeta(k))^{-1}G_k$.

Proposition 4.1. – *Si $k \in \mathbf{Z}$, alors la famille des $G_4^a G_6^b$, avec $a, b \in \mathbf{N}$ vérifiant $4a + 6b = k$ (potentiellement la famille vide si $\dim \mathbf{M}_k = 0$), est une base de $\mathbf{M}_k$.*

Preuve. On montre que la famille est libre et génératrice.

1) Si la famille n'est pas libre, alors $G_4^6 G_6^{-4}$ est solution d'une équation polynômiale (linéaire) non triviale dans $\mathbf{C}$, donc est égal à une constante puisqu'un polynôme non constant ne peut pas avoir une infinité de racines. Cela n'est pas possible car $v_\rho(G_4) = 1$ et $v_\rho(G_6) = 0$.
2) D'après les résultats précédents, la famille est génératrice pour $k \leqslant 6$. On vient d'initier une récurrence forte. Si la propriété est vraie pour $k \geqslant 7$, alors soient $c, d \in \mathbf{N}$ tels que $4c + 6d = k$ (c'est possible car $k \geqslant 4$). Soit $f \in \mathbf{M}_k$. Comme $g = G_4^c G_6^d$ une forme modulaire non parabolique de poids k, il existe $\lambda \in \mathbf{C}$ tel que $f - \lambda g \in \mathbf{S}_k$, donc égale à Δh où $h \in \mathbf{M}_{k-12}$ vérifie à l'hypothèse de récurrence. Comme Δ, h et g sont générées par des monômes de la forme souhaitée, f l'est également. □

En conséquence immédiate de la proposition précédente, on a le théorème escompté sur la génération de $\mathbf{M}$.

Théorème 4.3. – *On a un isomorphisme d'algèbre $\mathbf{M} \simeq \mathbf{C}[G_4, G_6]$.*

4.3 L'invariant modulaire j

On a défini l'invariant modulaire par $j = 1728\dfrac{g_4^3}{\Delta}$, qui est une fonction modulaire de poids 0 comme quotient de deux formes modulaires de mêmes poids. On montre dans un premier temps quelques propriétés de j, puis, que d'une manière analogue à ce que les séries d'Eisenstein sont pour les formes modulaires, elle est l'atome des fonctions modulaires de poids 0.

Proposition 4.2. – *L'invariant modulaire j est holomorphe sur $\mathbf{H}$, a un pôle simple en l'infini, et définit une bijection de $\mathbf{H}/\mathbf{G}$ dans $\mathbf{C}$ par passage au quotient.*

Preuve. On a montré dans la section précédente que Δ ne s'annule pas sur $\mathbf{H}$. Comme Δ et g_4 sont holomorphes sur $\mathbf{H}$, j l'est aussi. Comme Δ a un zéro simple en l'infini et que g_4 ne s'annule pas en l'infini, alors j a un pôle simple en l'infini.

Puisque j est une fonction modulaire de poids 0, elle est simplement invariante sous l'action de $\mathbf{G}$, donc elle passe au quotient $\mathbf{H}/\mathbf{G}$. Soit $\lambda \in \mathbf{C}$, dont on va montrer qu'il a un unique inverse par j modulo $\mathbf{G}$, ce qui revient à montrer que la fonction $f_\lambda = 1728g_4^3 - \lambda\Delta$ a un unique zéro modulo $\mathbf{G}$, puisque

$$f_\lambda(z) = 1728g_4^3(z) - \lambda\Delta(z) = 0 \quad \text{si, et seulement si} \quad j(z) = 1728\frac{g_4^3(z)}{\Delta(z)} = \lambda.$$

Or, la formule de valence appliquée à la forme modulaire non nulle f_λ de poids 12 montre, étant donné les écritures possibles de 1 comme $n + \frac{n'}{2} + \frac{n''}{3}$ avec $n, n', n'' \in \mathbf{N}$, que f_λ a dans tous les cas un unique zéro, soit en l'infini d'ordre 1, soit en i d'ordre 2, soit en ρ d'ordre 3. □

Théorème 4.4. – *Soit f une fonction méromorphe sur $\mathbf{H}$. Les trois propriétés suivantes sont équivalentes.*

1) *f est une fonction rationnelle en j.*
2) *f est le quotient de deux formes modulaires de même poids.*
3) *f est une fonction modulaire de poids 0.*

Preuve. Il est clair que 1) ⇒ 2) et que 2) ⇒ 3). Montrons que 3) ⇒ 1). Soit f une fonction modulaire de poids 0. Elle n'a qu'un nombre fini de pôles $p_1, \dots p_n$ dans $\mathbf{H}/\mathbf{G}$. Le polynôme

$$Q(X) = \sum_{k=1}^{n} (X - j(p_k))^{-v_{p_k}(f)}$$

est non identiquement nul et $g = Q(j)f$ est holomorphe sur $\mathbf{H}$: par $\mathbf{G}$-invariance de j, si $0 \leqslant k \leqslant n$,

$$v_{p_k}(g) = v_{p_k}(Q(j)) + v_{p_k}(f) = -v_{p_k}(f) + v_{p_k}(f) = 0.$$

Notons $m = v_\infty(g)$. Comme $v_\infty(\Delta) = 1$, alors $h = \Delta^m g$ est holomorphe à l'infini : c'est donc une forme modulaire de poids $12m$. Par la section précédente, il existe des coefficients $c(a, b)$ tels que

$$h = \sum_{\substack{a,b \in \mathbf{N} \\ 4a+6b=12m}} c(a,b) G_4^a G_6^b, \quad \text{donc tels que} \quad g = \sum_{\substack{a,b \in \mathbf{N} \\ 4a+6b=12m}} c(a,b) \frac{G_4^a G_6^b}{\Delta^m}.$$

Si $4a + 6b = 12m$, ou autrement dit si $2a + 3b = 6m$, alors $3|a$ et $2|b$ donc en posant $p = \dfrac{a}{3}$ et $q = \dfrac{b}{2}$, on peut écrire

$$g = \sum_{p+q=m} c(3p, 2q) \frac{G_4^{3p} G_6^{2q}}{\Delta^{p+q}}.$$

Or, on peut écrire $\dfrac{G_4^3}{\Delta}$ et $\dfrac{G_6^2}{\Delta}$ comme fonctions rationnelles de j :

$$\frac{G_4^3}{\Delta} = \frac{j}{1728 \times 60^3} = \frac{j}{373248000}, \quad \frac{G_6^2}{\Delta} = \frac{g_4^3 - \Delta}{27 \times 140^2 \Delta} = \frac{j-1}{529200}.$$

Ainsi, en posant

$$P(X) = g = \sum_{p+q=m} c(3p, 2q) \frac{X^p (X-1)^q}{373248000^p \times 529200^q},$$

on peut écrire f comme la fonction rationnelle $f = \dfrac{P(j)}{Q(j)}$. □

5 Opérateurs de Hecke

5.1 La fonction τ de Ramanujan

On propose, pour motiver notre dernier chapitre sur les opérateurs de Hecke, de présenter la fonction τ de Ramanujan, qui a été historiquement une des raisons pour lesquelles ils ont été introduits.

Définition 5.1. – *La* **fonction τ de Ramanujan** *est définie sur $\mathbf{N}^*$ comme étant la suite des coefficients de la q-expansion de la forme parabolique Δ de poids 12 normalisée (dont on admet l'expression, conséquence de la Proposition 3.8.) :*

$$(2\pi)^{-12}\Delta = q\prod_{n=1}^{+\infty}(1-q^n)^{24} = \sum_{n=1}^{+\infty}\tau(n)q^n.$$

Les premières valeurs de τ sont :

$$\tau(1)=1,\quad \tau(2)=-24,\quad \tau(3)=252,\quad \tau(4)=-1472,\quad \tau(5)=4830,\quad \tau(6)=-6048,\quad \tau(7)=-16744\ldots$$

Théorème 5.1. – *La fonction τ vérifie les propriétés suivantes.*

1) *Si $m\wedge n=1$, alors $\tau(mn)=\tau(m)\tau(n)$.*
2) *Si p est un nombre premier et $n\in\mathbf{N}^*$, $\tau(p^{n+1})=\tau(p)\tau(p^n)-p^{11}\tau(p^{n-1})$.*
3) *Si p est un nombre premier, $|\tau(p)|\leqslant 2p^{\frac{11}{2}}$.*

Remarque. – En 1915, Ramanujan calcule les trente premières valeurs de τ et conjecture les résultats du théorème précédent. À l'heure actuelle, ils ont tous été démontrés. En 1917, Mordell prouve 1) et 2), en utilisant avant l'heure des bribes de la théorie de Hecke. Ce dernier introduit les opérateurs qui portent son nom et redémontre 1) et 2) en 1937, en montrant que la forme Δ normalisée comme précédemment est une fonction propre normalisée de tous les opérateurs $T(n)$.

– Les deux identités multiplicatives ont des implications analytiques. Soit f une forme parabolique normalisée de poids k et de coefficients de q-expansion $(a_n)_{n\geqslant 1}$. On définit la fonction L associée à f comme étant la série

$$L(f,s)=\sum_{n=1}^{+\infty}\frac{a_n}{n^s}.$$

Les conditions 1) et 2) impliquent que $L(f,s)$ converge absolument pour $\mathrm{Re}(s)>k$ et qu'elle vérifie une équation fonctionnelle, appelée produit eulérien :

$$L(f,s)=\prod_{p\text{ premier}}^{+\infty}\frac{1}{1-a_pp^{-s}+p^{k-1-2s}},$$

où $1-a_pX+p^{k-1}X^2$ est le p-ème polynôme de Hecke de f. Hecke montre même que la série $L(f,s)$ se prolonge analytiquement en une fonction holomorphe sur tout le plan complexe.

– La borne 3) ne fut démontrée que plus tard par Deligne en 1974, comme corollaire de sa preuve des conjectures de Weil. Cette borne est liée au polynôme de Hecke, comme le prouve la proposition suivante.

Proposition 5.1. – *Soit p un nombre premier. Écrivons le p-ème polynôme de Hecke de Δ normalisée sous forme factorisée $1-\tau(p)X+p^{11}X^2=(1-aX)(1-a'X)$. Les propriétés suivantes sont équivalentes :*

1) *$|\tau(p)|\leqslant 2p^{\frac{11}{2}}$;*
2) *$|a|=|a'|=p^{\frac{11}{2}}$;*
3) *a et a' sont des nombres complexes conjugués.*

Preuve. Si on a 2), alors puisqu'on a $\tau(p) = a + a'$ par relation coefficients-racines, on a 1) par inégalité triangulaire. Si on a 3), comme $aa' = p^{11}$ par définition et que $aa' = a\overline{a} = |a|^2$, on a 2). Si on a 1), comme le discriminant du p-ème polynôme de Hecke vaut $\tau(p)^2 - 4p^{11}$, la borne implique ce discriminant est strictement négatif, donc que le polynôme a deux racines complexes conjuguées. Ces racines sont les inverses de a et a', et comme elles sont conjuguées, a et a' le sont également, ce qui montre 3). □

On se fixe pour but de développer dans le restant du chapitre la théorie de Hecke suffisante pour pouvoir montrer les identités multiplicatives vérifiées par la fonction τ de Ramanujan.

5.2 Les opérateurs de Hecke sur les réseaux

On commence par étudier les opérateurs de Hecke sur les réseaux, puis sur les fonctions de réseaux.

Définition 5.2. – *Soit $\Lambda \in \mathscr{R}$. Les deux* **opérateurs de Hecke** *sont les endomorphismes $\mathbf{Z}$-linéaires du groupe libre $\mathbf{Z}[\mathscr{R}]$ engendré par $\mathscr{R}$ suivants.*

1) *Pour $n \in \mathbf{N}^*$, on pose $T(n)\Lambda = \sum_{[\Lambda:\Lambda']=n} \Lambda'$.*
2) *Pour $\alpha \in \mathbf{C}^*$, on pose $R_\alpha \Lambda = \alpha\Lambda$.*

Afin de prouver les identités vérifiées par ces opérateurs, on établit un lemme matriciel et un résultat sur la décomposition des sous-réseaux.

Lemme 5.1. – *Soit $\Lambda \in \mathscr{R}$ et $n \in \mathbf{N}^*$. Notons*

$$S_n = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right),\ ad = n,\ a \geqslant 1,\ 0 \leqslant b < d\} \quad et \quad \Lambda(n) = \{\Lambda' \in \mathscr{R}, [\Lambda : \Lambda'] = n\}.$$

Alors $s \mapsto s\Lambda$ est une bijection de S_n dans $\Lambda(n)$.

Preuve. Soit $n \in \mathbf{N}^*$ et $s \in S_n$. On a $\det(s) = n$ donc $s\Lambda \in \Lambda(n)$. Disons que $\Lambda = \mathbf{Z}w_1 \oplus \mathbf{Z}w_2$. Soit $\Lambda' = \mathbf{Z}w_1' \oplus \mathbf{Z}w_2' \in \Lambda(n)$: montrons qu'il existe un unique $s \in S_n$ tel que $s\Lambda = \Lambda'$.

Posons $Y_1 = \Lambda/(\Lambda' \oplus \mathbf{Z}w_2)$. Comme Λ' est un sous réseau de Λ, alors il existe des entiers a', b', c', d' tels que

$$w_1' = a'w_1 + b'w_2 \quad \text{et} \quad w_2' = c'w_1 + d'w_2.$$

On voit alors que

$$Y_1 = \Lambda/(\Lambda' + \mathbf{Z}w_2) \simeq \mathbf{Z}w_1 \oplus \mathbf{Z}w_2/(\mathbf{Z}(a'w_1 + b'w_2) \oplus \mathbf{Z}(c'w_1 + d'w_2) \oplus \mathbf{Z}w_2) \simeq \mathbf{Z}w_1/\mathbf{Z}(a' \wedge c')w_1,$$

donc Y_1 est cyclique d'ordre $a = a' \wedge c'$. Posons $Y_2 = \mathbf{Z}w_2/(\Lambda' \cap \mathbf{Z}w_2)$: c'est un groupe cyclique d'ordre d. En considérant l'injection $\overline{y} \in Y_2 \mapsto \overline{yw_2} \in \Lambda/\Lambda'$ et la surjection $\overline{xw_1 + yw_2} \in \Lambda/\Lambda' \mapsto \overline{x} \in Y_1$, on voit qu'on a la suite exacte suivante :

$$1 \longrightarrow Y_2 \longrightarrow \Lambda/\Lambda' \longrightarrow Y_1 \longrightarrow 1,$$

ce qui montre que $ad = n$. Posons $w_2'' = dw_2 \in \Lambda'$. Il existe $w_1'' \in \Lambda'$ tel que w_1'' soit congru à aw_1 modulo $\mathbf{Z}w_2$. La famille (w_1'', w_2'') pouvant être obtenue par multiplication par une matrice de $\mathrm{SL}_2(\mathbf{Z})$ de la base (w_1', w_2'), c'est une base de Λ'. On a donc $w_1'' = aw_1 + bw_2$ avec b uniquement déterminé modulo d ou, de manière équivalente, uniquement déterminé pour $0 \leqslant b < d$. Les entiers a, b, d sont uniquement déterminés, $s = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n$ et $s\Lambda = \Lambda'$, ce qui est bien ce qu'on voulait. □

Définition 5.3. – *Pour $n \in \mathbf{N}$, on définit $\sigma(n) = \sigma_1(n)$ comme étant la* **somme des diviseurs (positifs) de** n.

Proposition 5.2. – *Pour tout $n \in \mathbf{N}^*$, on a $|\Lambda(n)| = \sigma(n)$.*

Preuve. Avec la bijection précédente, on a

$$|\Lambda(n)| = |S_n| = \sum_{d|n} \left|\left\{\begin{pmatrix} \frac{n}{d} & b \\ 0 & d \end{pmatrix}, 0 \leqslant b < d\right\}\right| = \sum_{d|n} d = \sigma(n),$$

et ce pour tout $n \in \mathbf{N}^*$. □

Proposition 5.3. – *La fonction σ a les propriétés suivantes.*

1) *σ est multiplicative : si $n, m \in \mathbf{N}$ sont premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.*
2) *Si p est un nombre premier et $k \in \mathbf{N}$, alors $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$.*

Preuve. Si m et n sont premiers entre eux, alors les diviseurs d du produit mn sont en correspondance bijective avec les paires composées d'un diviseur de n et d'un diviseur de n, par $d \mapsto (d \wedge n, d \wedge m)$. Ainsi

$$\sigma(mn) = \sum_{d|mn} d = \sum_{a|n} \sum_{b|m} ab = \sum_{a|n} a \sum_{b|m} b = \sum_{a|n} \sigma(m) = \sigma(n)\sigma(m).$$

Si p est premier, les diviseurs de p^k sont les p^i, $0 \leqslant i \leqslant k$: on a donc

$$\sigma(p^k) = \sum_{d|p^k} d = \sum_{i=0}^{k} p^i = \frac{p^{k+1}-1}{p-1},$$

ce qui est bien l'identité attendue. □

Théorème 5.2. – *Soit $\Lambda \in \mathscr{R}$ et Λ'' un sous-réseau de Λ d'indice mn, avec $m, n \in \mathbf{N}^*$ et $m \wedge n = 1$. Alors il existe un unique sous-réseau Λ' de Λ contenant Λ'' tel que $[\Lambda : \Lambda'] = n$ et $[\Lambda' : \Lambda''] = m$.*

Preuve. On montre l'existence avec le théorème de structures des groupes abéliens finis et l'unicité avec σ.

1) **Existence.** Le groupe abélien Λ/Λ'' est fini d'ordre nm. D'après le théorème de classification des groupes abéliens finis, il existe d'uniques entiers $r \geqslant 1$ et $2 \geqslant d_1 | \dots | d_r$ tel que

$$\Lambda/\Lambda'' \simeq \prod_{i=1}^{r} \mathbf{Z}/d_i\mathbf{Z}.$$

Avec le lemme chinois, on peut décomposer tous les termes du produit selon les décompositions en produit de facteurs premiers des d_i, puis regrouper les facteurs en deux sous-groupes de Λ/Λ'' selon si l'ordre du facteur divise m ou n, puisqu'ils sont premiers entre eux. On obtient alors un sous-groupe d'ordre n et un sous-groupe d'ordre m, puisque $d_1 \dots d_r = mn$. Le sous-groupe d'ordre n de Λ/Λ'' correspond à un sous-groupe Λ' de Λ contenant Λ'', et il est clair sous cette forme que $[\Lambda : \Lambda'] = n$ et $[\Lambda' : \Lambda''] = m$.

2) **Unicité.** La fonction $\chi : S_m \times S_n \to \Lambda(mn)$ qui à (s_1, s_2) associe $s_1 s_2 \Lambda$ est une surjection et par multiplicativité de σ et le lemme matriciel,

$$|S_m \times S_n| = \sigma(m)\sigma(n) = \sigma(mn) = |S_{mn}| = |\Lambda(mn)|,$$

donc c'est une bijection. Donc il existe un unique couple (s_1, s_2) tel que $\chi(s_1, s_2) = \Lambda''$: ainsi, $\Lambda' = s_1\Lambda$ est l'unique sous-réseau vérifiant les propriétés escomptées. □

Théorème 5.3. – *Soient $m, n \in \mathbf{N}^*$, $\alpha, \beta \in \mathbf{C}^*$ et p un nombre premier. On a les relations suivantes.*

1) *$R_\alpha R_\beta = R_{\alpha\beta}$.*
2) *$R_\alpha T(n) = T(n) R_\alpha$.*
3) *Si $m \wedge n = 1$, alors $T(mn) = T(m)T(n)$.*
4) *Pour $r \in \mathbf{N}^*$, on a $T(p^{r+1}) = pT(p^{r-1})R_p - T(p^r)T(p)$.*

Preuve. Soit $\Lambda \in \mathscr{R}$ un réseau.

1) On a $R_\alpha R_\beta \Lambda = R_\alpha \beta \Lambda = \alpha\beta\Lambda = R_{\alpha\beta}\Lambda$.
2) On a $R_\alpha T(n)\Lambda = R_\alpha \sum_{[\Lambda:\Lambda']=n} \Lambda' = \sum_{[\Lambda:\Lambda']=n} \alpha\Lambda' = T(n)R_\alpha\Lambda$.
3) Comme m et n sont premiers entre eux, alors par le théorème précédent, les sous-réseaux d'indice m des sous-réseaux d'indice n de Λ sont en correspondance bijective avec les sous-réseaux d'indice mn de Λ. On en déduit que les deux sommes de réseaux $T(mn)$ et $T(m)T(n)$ sont égales.

4) Les trois termes de l'égalité évaluée en Λ sont des sommes de sous-réseaux de Λ d'indice p^{r+1} (on précise que l'indice $R_p\Lambda$ dans Λ est p^2). Soit Λ'' un sous-réseau de Λ d'indice p^{r+1} et notons a, b, c ses coefficients respectifs dans les sommes $T(p^r)T(p)\Lambda$, $T(p^{r+1})\Lambda$ et $pT(p^{r-1})R_p\Lambda$. Il faut donc montrer que $a = b + pc$: or $b = 1$ par définition de $T(p^{n+1})$. On distingue deux cas.
   — Si $\Lambda'' \not\subseteq p\Lambda$, alors $c = 0$ et a est le nombre de sous-réseaux Λ' de Λ contenant Λ'' et d'indice p dans Λ. Ces réseaux contiennent $p\Lambda$ et leurs images d'indice p' dans $\Lambda/p\Lambda$ contiennent l'image de Λ'' d'ordre p dans $\Lambda/p\Lambda$, et donc également d'indice p comme $\Lambda/p\Lambda$ est d'ordre p^2. Donc $a = 1$ car un seul tel Λ' convient.
   — Si $\Lambda'' \subseteq p\Lambda$, alors $c = 1$ et comme tout sous-réseau de Λ d'indice p dans Λ contient $p\Lambda$ donc également Λ''. Ainsi, $a = \sigma(p) = p + 1$.

   Donc dans tous les cas, l'égalité est vraie. □

Remarque. – On en déduit que pour $r \in \mathbf{N}^*$, $T(p^r)$ est un polynôme en $T(p)$ et R_p, et par décomposition en produits de facteurs premiers, que $T(n)$ est un polynôme en les $T(p)$ et R_p pour tout $n \in \mathbf{N}^*$. Les relations ci-dessus montrent que le produit de ces opérateurs est commutatif, si bien que l'on peut énoncer la définition suivante.

Définition 5.4. – *La sous-$\mathbf{Z}$-algèbre de $End_{\mathbf{Z}}(\mathbf{Z}[\mathscr{R}])$ engendrée par les R_α avec $\alpha \in \mathbf{C}^*$ et les $T(p)$ pour p premier est commutative pour la composition et contient tous les $T(n)$, $n \in \mathbf{N}^*$. On l'appelle* **algèbre de Hecke**.

On fait agir les opérateurs de Hecke sur les fonctions de réseaux de la manière suivante. Si $F : \mathscr{R} \to \mathbf{C}$ est une fonction de réseaux, $\alpha \in \mathbf{C}^*$ et $n \in \mathbf{N}^*$, on pose, pour tout $\Lambda \in \mathscr{R}$:

$$R_\alpha F(\Lambda) = F(\alpha\Lambda) \quad \text{et} \quad T(n)F(\Lambda) = \sum_{[\Lambda:\Lambda']=n} F(\Lambda').$$

Théorème 5.4. – *Soient $m, n \in \mathbf{N}^*$, $\alpha \in \mathbf{C}^*$, p un nombre premier et $F : \mathscr{R} \to \mathbf{C}$ une fonction de réseaux homogène de poids k. On a les relations suivantes.*

1) $R_\alpha F = \alpha^{-k} F$.

2) Si $m \wedge n = 1$, alors $T(mn)F = T(m)T(n)F$.

3) Pour $r \in \mathbf{N}^*$, on a $T(p)T(p^r)F = T(p^{r+1})F + p^{1-k}T(p^{r-1})F$.

Preuve. Soit $\Lambda \in \mathscr{R}$ un réseau.

1) On a $R_\alpha F(\Lambda) = F(\alpha\Lambda) = \alpha^{-k}F(\Lambda)$ par homogénéité.
2) On a $T(m)T(n)F(\Lambda) = F(T(m)T(n)\Lambda) = F(T(mn)\Lambda) = T(mn)F(\Lambda)$.
3) On a $T(p)T(p^r)F(\Lambda) = F(T(p^r)T(p)\Lambda) = F(T(p^{r+1})\Lambda + pT(p^{r-1})R_p\Lambda) = T(p^{r+1})F(\Lambda) + pF(T(p^{r-1})R_p\Lambda)$, et on conclut avec le point 1) et la commutativité des opérateurs. □

5.3 Les opérateurs de Hecke sur les formes modulaires

On fait agir les opérateurs de Hecke sur les fonctions faiblement modulaires, d'où l'on observera deux choses :

— que les propriétés de régularités de ces fonctions sont conservées par les opérateurs de Hecke ;

— que les identités des opérateurs de Hecke se traduisent en des identités sur les coefficients des q-expansions des fonctions qui sont vecteurs propres de tous les $T(n)$.

Soit $f : \mathbf{H} \to \mathbf{C}$ une fonction faiblement modulaire de poids k et $F : \mathscr{R} \to \mathbf{C}$ sa fonction de réseaux homogène de poids k associée. Pour tout $n \in \mathbf{N}^*$ et $z \in \mathbf{H}$, on pose

$$T(n)f(z) = n^{k-1}T(n)F(\mathbf{Z}z \oplus \mathbf{Z}).$$

Le facteur n^{k-1} permet aux $T(n)$ d'envoyer des formes modulaires de coefficients de q-expansion entiers vers des formes modulaires de coefficients de q-expansion également entiers. Du fait du lemme matriciel de la section précédente et de la faible modularité de f, on peut écrire

$$T(n)f(z) = n^{k-1} \sum_{\substack{ad=n, a\geqslant 1 \\ 0\leqslant b<d}} d^{-k} f\left(\frac{az+b}{d}\right) = n^{k-1} \sum_{s\in S_n} f(sz).$$

Proposition 5.4. – *Si f est faiblement modulaire de poids k, alors $T(n)f$ est faiblement modulaire de poids k et si f est holomorphe, alors $T(n)f$ l'est également.*

Preuve. Avec la première écriture ci-dessus, comme $T(n)F$ est également homogène de poids k, alors $T(n)f$ vérifie l'équation de modularité de poids k. Avec la deuxième écriture ci-dessus, $T(n)f$ est une somme finie de fonctions méromorphes sur $\mathbf{H}$ donc elle est méromorphe sur $\mathbf{H}$ et faiblement modulaire de poids k. Pour les mêmes raisons, si f est holomorphe sur $\mathbf{H}$, alors $T(n)f$ l'est également. □

Proposition 5.5. – *Soit f une fonction faiblement modulaire de poids k, et p un nombre premier. On a les relations suivantes.*

1) *Si $m \wedge n = 1$, alors $T(mn)f = T(m)T(n)f$.*
2) *Pour $r \in \mathbf{N}^*$, on a $T(p)T(p^r)f = T(p^{r+1})f + p^{k-1}T(p^{r-1})f$.*

Preuve. Remarquons que si m et n sont premiers entre eux, alors $S_m S_n = S_{mn}$ (modulo $\mathrm{SL}_2(\mathbf{Z})$). Ainsi,

$$T(m)T(n)f(z) = T(m)n^{k-1}\sum_{s\in S_n} f(sz) = n^{k-1}m^{k-1}\sum_{s\in S_n}\sum_{s'\in S_m} f(s'sz) = (mn)^{k-1}\sum_{s''\in S_{mn}} f(s''z) = T(mn)f(z).$$

On a la deuxième égalité à un facteur près issu du n^{k-1} dans la définition, car $T(n)F(\Lambda) = n^{1-k}T(n)f(z)$. Plus précisément, on a

$$p^{r-kr+1-k}T(p)T(p^r)f(z) = p^{r-kr+1-k}T(p^{r+1})f(z) + p^{r-kr}T(p^{r-1})f(z),$$

donc en divisant par $p^{r-kr+1-k}$, on obtient bien l'égalité avec le facteur p^{k-1} devant le troisième terme. □

Théorème 5.5. – *Soit $f = \sum_{m\in\mathbf{Z}} c(m)q^m$ une fonction modulaire de poids k. Alors $T(n)f$ est une fonction modulaire de poids k dont on connaît les coefficients de la q-expansion :*

$$T(n)f(z) = \sum_{m\in\mathbf{Z}} t(m)q^m \quad \textit{avec} \quad t(m) = \sum_{a|n\wedge m, a\geqslant 1} a^{k-1}c\Big(\frac{mn}{a^2}\Big).$$

Preuve. Par définition de $T(n)f(z)$, en faisant la q-expansion de f, on a :

$$T(n)f(z) = n^{k-1}\sum_{\substack{ad=n,a\geqslant 1\\ 0\leqslant b<d}} d^{-k}\sum_{m\in\mathbf{Z}} c(m)e^{\frac{2i\pi m(ax+b)}{d}} = n^{k-1}\sum_{m\in\mathbf{Z}} c(m)\sum_{\substack{ad=n,a\geqslant 1\\ 0\leqslant b<d}} d^{-k}e^{\frac{2i\pi m(ax+b)}{d}}.$$

Or $\sum_{0\leqslant b<d} e^{\frac{2i\pi bm}{d}} = d$ si $d|m$ et 0 sinon, ainsi on a, en posant $m' = \dfrac{m}{d}$:

$$T(n)f(z) = n^{k-1}\sum_{ad=n,a\geqslant 1}\sum_{m'\in\mathbf{Z}} d^{1-k}c(dm')q^{am'} = \sum_{m''\in\mathbf{Z}} q^{m''}\sum_{a|m''\wedge n,a\geqslant 1}\Big(\frac{n}{d}\Big)^{k-1}c\left(\frac{m''d}{a}\right),$$

qui est la formule souhaitée car $ad = n$. Comme f est faiblement modulaire de poids k, alors $T(n)$ l'est également. Comme f est méromorphe à l'infini, alors tout les $c(m)$ sont nuls pour $m < N$, donc $c(\frac{md}{a}) = 0$ pour $m < nN$ et $T(n)f$ est méromorphe à l'infini. □

Remarque. – On déduit assez immédiatement du théorème précédent ces deux faits (les notations sont les mêmes) :

— $t(0) = \sigma_{k-1}(n)c(0)$ et $t(1) = c(n)$, où $\sigma_{k-1}(n)$ est la somme des puissances $(k-1)$-èmes des diviseurs de n ;

— en regardant la nullité des coefficients de la q-expansion, si f est une forme modulaire (respectivement une forme parabolique), alors $T(n)f$ l'est également.

Définition 5.5. – *Soit f une forme modulaire non identiquement nulle. On dit que c'est une* **fonction propre** *des $T(n)$ (eighenfunction en anglais) s'il existe une suite $(\lambda_n)_{n\in\mathbf{N}^*}$ de nombres complexes telles que pour tout $n \in \mathbf{N}^*$, $T(n)f = \lambda_n f$. On dit qu'elle est* **normalisée** *si $c(1) = 1$, où les $c(m)$ sont les coefficients de sa q-expansion.*

Proposition 5.6. – *Soit $f = \sum_{m=0}^{+\infty} c(m)q^m$ une fonction propre des $T(n)$ de poids k. On a les propriétés suivantes.*

1) *$c(1)$ est non nul, donc on peut toujours normaliser une fonction propre.*
2) *Si f est normalisée, alors $c(n) = \lambda_n$ pour tout $n \in \mathbf{N}^*$.*
3) *Si f est normalisée, alors pour tout $m, n \in \mathbf{N}^*$ et p premier, les coefficients de f vérifient les relations suivantes.*
   — *Si $m \wedge n = 1$, alors $c(mn) = c(m)c(n)$.*
   — *Pour $r \in \mathbf{N}^*$, on a $c(p)c(p^r) = c(p^{r+1}) + p^{k-1}c(p^{r-1})$.*

Preuve. Gardons les mêmes notations que le théorème précédent. Soit $n \in \mathbf{N}^*$. Notons $t(m)$ le m-ème coefficient de la q-expansion de $T(n)f$.

1) On a $t(1) = c(n)$ par la remarque précédente et comme f est fonction propre des $T(n)$, alors $t(1) = \lambda_n c(1)$. Si $c(1)$ était nul, alors les $c(n)$ également et f serait identiquement nulle alors qu'on a supposé le contraire.
2) Si $c(1) = 1$, comme $c(n) = \lambda_n c(1)$, on a bien $c(n) = \lambda_n$.
3) Les valeurs propres λ_m vérifient les relations demandées car f vérifie les identités des opérateurs de Hecke. Avec le point précédent, les $c(m)$ les vérifient également. □

Théorème 5.6. – *La forme Δ normalisée, c'est-à-dire $(2\pi)^{-12}\Delta$ est une fonction propre normalisée des $T(n)$.*

Preuve. On a vu que $\mathbf{S}_{12}$ est de dimension 1 et que Δ est une forme parabolique de poids 12 non identiquement nulle. Si $n \in \mathbf{N}^*$, comme $T(n)\Delta$ est également une forme parabolique de poids 12, alors c'est un multiple scalaire de Δ : c'est donc une fonction propre des $T(n)$. Si on normalise Δ, ce qui est possible car son coefficient $c(1)$ est non nul puisqu'elle est fonction propre, par le même raisonnement, $(2\pi)^{-12}\Delta$ est une fonction propre normalisée des $T(n)$ (on admet que $c(1) = (2\pi)^{12}$). □

Les coefficients de la q-expansion de la forme Δ normalisée étant donnés par la fonction τ, on en déduit donc que cette dernière vérifie les deux identités multiplicatives conjecturées par Ramanujan :

1) si $m \wedge n = 1$, alors $\tau(mn) = \tau(m)\tau(n)$;
2) si p est un nombre premier et $n \in \mathbf{N}^*$, $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$.

B Bibliographie

[BvdGHZ08] Bruinier, Jan Hendrik, Gerard van der Geer, Günter Harder et Don Zagier: *The 1-2-3 of Modular Forms*. Universitext. Springer, 2008.

[Col12] Colmez, Pierre: *Éléments d'analyse et d'algèbre*. Éditions de l'École Polytechnique, 2012.

[CS17] Cohen, Henri et Fredrik Strömberg: *Modular Forms : A Classical Approach*, tome 179 de *Graduate Studies in Mathematics*. American Mathematical Society, 2017.

[Die86] Dieudonné, Jean: *Abrégé d'histoire des mathématiques*. Hermann, 1986.

[DS05] Diamond, Fred et Jerry Shurman: *A First Course in Modular Forms*, tome 228 de *Graduate Texts in Mathematics*. Springer, 2005.

[God03] Godement, Roger: *Analyse mathématique IV*. Springer, 2003.

[Lan87] Lang, Serge: *Elliptic Functions*, tome 112 de *Graduate Texts in Mathematics*. Springer, 1987.

[LR11] Lozano-Robledo, Álvaro: *Elliptic Curves, Modular Forms, and Their L-functions*, tome 58 de *Student Mathematical Library*. American Mathematical Society, 2011.

[Mil17] Milne, James S.: *Modular Functions and Modular Forms (v1.31)*, 2017. Available at www.jmilne.org/math/.

[Ser97] Serre, Jean Pierre: *Cours d'arithmétique*. Presses Universitaires de France, 1997.

[Shi94] Shimura, Goro: *Introduction to the Arithmetic Theory of Automorphic Functions*, tome 11 de *Publications of the Mathematical Society of Japan*. Princeton University Press, 1994.