
INTRODUCTION AUX FORMES MODULAIRES

par

Alberto Mínguez

December 15, 2016

Ce poly donne une introduction aux formes modulaires. Dans la première partie les références sont les notes de Chenevier [1] et le Cours d'arithmétique de Serre [6]. Pour cette partie le lecteur est supposé justifier la maîtrise des bases de l'analyse complexe. Dans la deuxième partie on suivra les notes de Dat [2] et le livre de Diamond-Shurman [3]. Dans cette deuxième partie le lecteur devrait être familiarisé avec les surfaces de Riemann.

Si vous trouvez des coquilles faites-le moi savoir !

1. Formes modulaires pour $SL_2(\mathbf{Z})$

1.1. Action de $SL_2(\mathbf{Z})$ sur le demi-plan de Poincaré.— Soit K un corps. Le groupe $GL_2(K)$ agit naturellement sur K^2 puis sur l'ensemble $\mathbf{P}^1(K)$ des droites vectorielles de ce dernier. Cette action est triviale sur le centre K^\times et se factorise en une action fidèle de $PGL_2(K)$. On pose

$$\widehat{K} = K \sqcup \{\infty\}.$$

Cet ensemble s'identifie à $\mathbf{P}^1(K)$ en envoyant tout élément $z \in K$ sur la droite engendrée par $\begin{pmatrix} z \\ 1 \end{pmatrix}$ et le symbole ∞ sur celle engendrée par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Par transport de structure on en déduit une action de $GL_2(K)$ sur \widehat{K} , que l'on notera $(\gamma, z) \mapsto \gamma z$. Explicitement, si γ désigne l'élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $GL_2(K)$ et si $z \in K$ est tel que $cz + d \neq 0$ on constate les égalités :

$$(1.1) \quad \gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az + b \\ cz + d \end{pmatrix} = (cz + d) \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix}$$

et l'on retrouve la formule bien connue $\gamma z = \frac{az+b}{cz+d}$. De plus si on a $c \neq 0$ (resp. $c = 0$) alors $\gamma \infty = \frac{a}{c}$ et $\gamma(\frac{-d}{c}) = \infty$ (resp. $d \neq 0$ et $\gamma \infty = \infty$). Ces bijections de \widehat{K} sont appelées

homographies : par exemple $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ correspond à l'homographie "affine" $z \mapsto az + b$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ à "l'inversion" $z \mapsto \frac{-1}{z}$.

Etant donné l'élément $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(\mathbf{K})$ il est coutume de noter $j(\gamma, z)$ l'application

$$\begin{aligned} \mathbf{K} &\rightarrow \mathbf{K} \\ z &\mapsto cz + d. \end{aligned}$$

La formule (1.1) nous dit que $j(\gamma, z)$ satisfait la relation dite de cocycle :

$$(1.2) \quad j(\gamma\gamma', z) = j(\gamma, \gamma'z)j(\gamma', z)$$

valable pour tous $\gamma, \gamma' \in \mathrm{GL}_2(\mathbf{K})$ et tout $z \in \mathbf{K}$.

1.1.1. Ces rappels s'appliquent à $\mathbf{K} = \mathbf{C}$ auquel cas $\widehat{\mathbf{C}}$ n'est autre que la sphère de Riemann. Le sous-groupe $\mathrm{GL}_2(\mathbf{R})$ de $\mathrm{GL}_2(\mathbf{C})$ agit par restriction sur cette sphère, en préservant $\widehat{\mathbf{R}}$, ainsi donc son complémentaire $\mathbf{C} - \mathbf{R}$. Cet ouvert a deux composantes connexes, l'une d'elles étant l'ouvert :

$$\mathbb{H} = \{\tau \in \mathbf{C} : \mathrm{Im} \tau > 0\}$$

appelé le demi-plan de Poincaré. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R})$ et $z \in \mathbf{C} - \mathbf{R}$ alors $cz + d \neq 0$ et

$$(1.3) \quad \mathrm{Im} \gamma z = \det \gamma \frac{\mathrm{Im} z}{|cz + d|^2}.$$

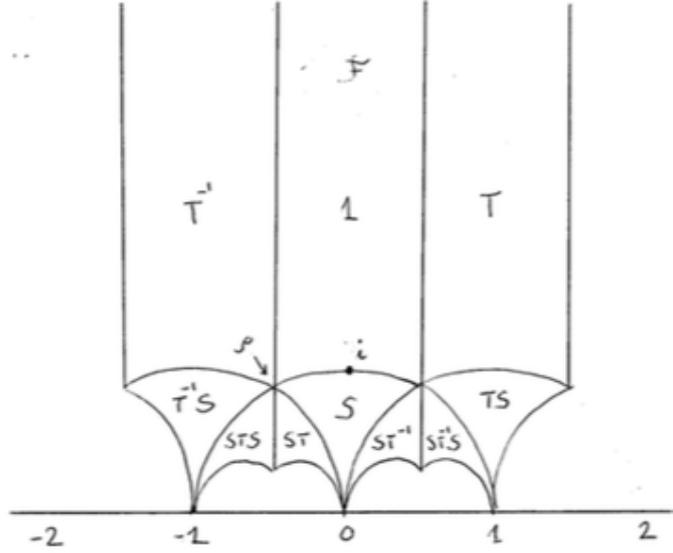
En particulier $\mathrm{SL}_2(\mathbf{R})$ préserve le demi-plan de Poincaré. L'action des homographies de la forme $a\tau + b$ avec $a \in \mathbf{R}_{>0}$, $b \in \mathbf{R}$ montre bien que l'action de $\mathrm{SL}_2(\mathbf{R})$ sur \mathbb{H} est transitive. Un petit calcul montre que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixe i si, et seulement si, $a = d$ et $b = -c$. La condition du déterminant donne en plus $a^2 + b^2 = 1$ donc le fixateur de i dans $\mathrm{SL}_2(\mathbf{R})$ est $\mathrm{SO}_2(\mathbf{R})$. Cela implique que l'application $\gamma \mapsto \gamma i$ induit une bijection

$$\mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R}) \simeq \mathbb{H}.$$

1.1.2. Analysons l'action du sous-groupe $\mathrm{SL}_2(\mathbf{Z})$ sur \mathbb{H} . Pour des raisons que l'on comprendra plus tard on note $\Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$. Deux éléments importants de ce groupe sont $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, c'est-à-dire $S\tau = -\frac{1}{\tau}$ et $T\tau = \tau + 1$. On a $S^2 = -I_2$, $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et donc $(ST)^3 = -I_2$, $S(i) = i$, $ST(\rho) = (\rho)$, où $\rho = e^{2i\pi/3}$.

On pose $\mathcal{F} = \{\tau \in \mathbb{H} : |\mathrm{Re} \tau| \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}$.

Théorème 1.1. — (1) Pour tout $\tau \in \mathbb{H}$, il existe $\gamma \in \Gamma(1)$ tel que $\gamma\tau \in \mathcal{F}$.

FIGURE 1. Le pavage de \mathbb{H} par la $\Gamma(1)$ -orbite de \mathcal{F}

- (2) Si τ, τ' sont deux points distincts de \mathcal{F} tels que $\Gamma(1)\tau = \Gamma(1)\tau'$ alors :
- (a) Soit $\operatorname{Re} \tau = \pm 1/2$ et $\tau' = \tau \pm 1$.
 - (b) Soit $|\tau| = 1$ et $\tau' = -\frac{1}{\tau}$.
- (3) Si $\tau \in \mathcal{F}$ alors le stabilisateur de τ dans $\Gamma(1)$ est $\{\pm 1\}$ sauf si $\tau = i$ (resp. $\rho, -\rho^2$), auquel cas c'est le sous-groupe engendré par S (resp. ST).

Démonstration. — Soit $\tau \in \mathbb{H}$ fixé. La forme quadratique

$$\begin{aligned} \mathbf{R}^2 &\rightarrow \mathbf{R}^2 \\ (c, d) &\mapsto |c\tau + d|^2 \end{aligned}$$

est définie positive. Elle admet donc un minimum sur $\mathbf{Z}^2 - 0$. D'après la formule (1.3) il y a donc un sens à considérer l'ensemble $E \subset \Gamma(1)\tau$ des éléments τ' tels que $\operatorname{Im} \tau'$ soit maximal. Il est invariant par $\tau' \mapsto \tau' + 1$ de sorte qu'il existe $\tau' \in E$ tel que $|\operatorname{Re} \tau'| \leq \frac{1}{2}$. Mais $-\frac{1}{\tau'} \in \Gamma(1)\tau$ et $\operatorname{Im} \frac{-1}{\tau'} = \frac{\operatorname{Im} \tau'}{|\tau'|^2}$ donc $|\tau'| \geq 1$. Ainsi $\tau' \in \Gamma(1)\tau \cap \mathcal{F}$.

Observons que cette démonstration montre en fait que $G\tau \cap \mathcal{F} \neq \emptyset$ où G désigne le sous-groupe de $\Gamma(1)$ engendré par S et T .

Pour montrer (2) et (3) considérons $\tau, \tau' \in \mathcal{F}$ (non nécessairement distincts) tels que $\operatorname{Im} \tau' \geq \operatorname{Im} \tau$ et tels que $\tau' = \gamma\tau$, où $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbf{Z})$. Par (1.3) on a $|c\tau + d| \leq 1$ et en particulier $|c\operatorname{Im} \tau| \leq 1$ donc $|c| \leq 1$. Si $c = 0$ alors $d = a = \pm 1$ donc $\pm\gamma$ est une puissance de T et on est dans le premier cas du (2). Sinon on peut supposer $c = 1$, quitte à remplacer γ par $-\gamma$. On voit sur le dessin que $|\tau + d| \leq 1$ entraîne $|\tau| = 1$ et que l'on est dans l'un de cas suivants.

(1) $\tau \neq \rho, -\rho^2$ et $d = 0$. On a encore $b = -1$ et $\tau' = a - \frac{1}{\tau}$, puis $a = 0$ car $|\operatorname{Re} \frac{-1}{\tau}| < 1/2$. Ainsi $\gamma = S$ et $\tau' = \tau = i$.

(2) $\tau = \rho$ et $d = 0, -1$. Si $d = 0$ on a encore $b = -1$, $\tau' = a - \frac{1}{\rho} = a - \rho^2$. Cela montre que soit $\tau' = \rho^2$, $a = 0$, $\gamma = \pm S$, soit $\tau' = \tau$, $a = -1$ et $\gamma = (ST)^2$.

(3) Le cas $\tau = -\rho^2$ et $d = 0, 1$ se traite de manière similaire au cas (2).

□

Définition 1.2. — Soit $\Gamma \subset \operatorname{SL}_2(\mathbf{R})$. Un *domaine fondamental* pour l'action de Γ dans \mathbb{H} est un ouvert connexe D tel que :

(1) Pour tout $\gamma \in \Gamma$, $\gamma D \cap D \neq \emptyset$ implique $\gamma = \pm 1$.

(2) On a $\mathbb{H} = \cup_{\gamma \in \Gamma} \gamma \overline{D}$ où \overline{D} désigné l'adhérence de D .

Corollaire 1.3. — $\operatorname{Int}(\mathcal{F})$ est un domaine fondamental de l'action de $\Gamma(1)$ sur \mathbb{H} .

On peut aussi profiter pour prouver le corollaire suivant (qui peut aussi être montré de manière directe sans difficulté).

Corollaire 1.4. — $\Gamma(1)$ est engendré par S et T .

Démonstration. — Soit G le sous-groupe de $\Gamma(1)$ engendré par S et T . Soit $\tau \in \operatorname{Int}(\mathcal{F})$ et soit $\gamma \in \Gamma(1)$. D'après la remarque après la preuve du (1) ci-dessus, il existe $g \in G$ tel que $g^{-1}\gamma\tau \in \mathcal{F}$. Ainsi $g^{-1}\gamma \in \operatorname{SL}_2(\mathbf{Z})$ fixe τ . On déduit de (3) que $g^{-1}\gamma = \pm I_2$. Au final on a $\gamma \in G$ car $-I_2 = S^2 \in G$. □

1.2. Formes modulaires pour $\Gamma(1)$. — L'application $(f, \gamma) \mapsto (\tau \mapsto f(\gamma\tau))$ définit une action à droite du groupe $\operatorname{SL}_2(\mathbf{R})$ sur le \mathbf{C} -espace vectoriel des fonctions $\mathbb{H} \rightarrow \mathbf{C}$, c'est même une représentation linéaire. Plus généralement, on définit une fonction $f[\gamma]_k : \mathbb{H} \rightarrow \mathbf{C}$ en posant

$$f[\gamma]_k(\tau) = j(\gamma, \tau)^{-k} f(\gamma\tau).$$

Cela a un sens car $j(\gamma, \tau) \neq 0$ pour tout $\gamma \in \operatorname{SL}_2(\mathbf{R})$ et tout $\tau \in \mathbb{H}$. On vérifie que (1.2) équivaut à dire que $(f, \gamma) \mapsto f[\gamma]_k$ est une action à droite de $\operatorname{SL}_2(\mathbf{R})$ sur l'espace des fonctions $\mathbb{H} \rightarrow \mathbf{C}$ appelée action de poids k .

Proposition-Définition 1.2.1. — Une fonction $f : \mathbb{H} \rightarrow \mathbf{C}$ est dite faiblement modulaire de poids k (de niveau $\Gamma(1)$) si $f = f[\gamma]_k$ pour tout $\gamma \in \operatorname{SL}_2(\mathbf{Z})$. Autrement dit si

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \quad \forall \tau \in \mathbb{H}, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbf{Z}).$$

où ce qui revient au même si $f(\tau + 1)f(\tau)$ et $f(-1/\tau) = \tau^k f(\tau)$ pour tout $\tau \in \mathbb{H}$. On dit aussi que que f satisfait la propriété d'automorphie ou encore que f est automorphe.

Démonstration. — Comme $\Gamma(1)$ est engendré par S et T , le fait d'être fixé par $\Gamma(1)$ équivaut à être fixé par S et T . □

Notons $\mathcal{O}(\mathbb{H})$ l'espace vectoriel des fonctions holomorphes $\mathbb{H} \rightarrow \mathbf{C}$. Les homographies de \mathbb{H} étant des transformations bi-holomorphes, l'action de poids k de $\mathrm{SL}_2(\mathbf{Z})$ préserve le sous-espace $\mathcal{O}(\mathbb{H})$.

Définition 1.5. — Une forme modulaire de poids k (de niveau $\Gamma(1)$) est une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbf{C}$ telle que :

- (1) f est faiblement modulaire de poids k (de niveau $\Gamma(1)$).
- (2) $f(\tau)$ admet une limite finie quand $\mathrm{Im} \tau \rightarrow \infty$; on la note $f(\infty)$.

On note $M_k(\Gamma(1))$ le sous-espace vectoriel de $\mathcal{O}(\mathbb{H})$ des formes modulaires de poids k (et niveau $\Gamma(1)$).

Remarque 1.6. — (1) Les relations $S^2 = -I_2$ et $f[-I_2]_k = (-1)^k f$ montrent que si $f \in M_k(\Gamma(1))$, alors $f = (-1)^k f$ de sorte que $M_k(\Gamma(1)) = 0$ si k est impair.

(2) De même si $f \in M_k(\Gamma(1))$ alors $f(i) = f[S]_k(i) = i^k f(i)$ et $f(\rho) = f[ST]_k(\rho) = \rho^k f(\rho)$ donc $f(i) = 0$ si $k \not\equiv 0 \pmod{4}$, et $f(\rho) = 0$ si $k \not\equiv 0 \pmod{3}$.

(3) Les fonctions constantes sont des poids 0 (on verra que ce sont les seules). La fonction 0 est une forme modulaire de poids quelconque.

(4) Si f et f' sont des formes modulaires de poids k et k' (et niveau $\Gamma(1)$) alors le produit ff' est une forme modulaire de poids $k + k'$ (et niveau $\Gamma(1)$) et donc l'espace

$$M(\Gamma(1)) = \bigoplus_{k \in \mathbf{Z}} M_k(\Gamma(1))$$

a une structure de \mathbf{C} -algèbre graduée.

(5) La condition (2) de la définition 1.5 rend l'espace $M_k(\Gamma(1))$ de dimension finie. L'une des choses que l'on fera c'est calculer les dimension de ces espaces.

Notons que si $z \in \mathbf{C}$, alors $|e^{2i\pi z}| = e^{-2\pi \mathrm{Im} z}$. Soit $D = \{z \in \mathbf{C} : |z| < 1\}$ le disque unité ouvert. On considère l'application

$$\begin{aligned} q : \mathbb{H} &\rightarrow D - \{0\} \\ \tau &\mapsto e^{2i\pi\tau}. \end{aligned}$$

Cette application induit une bijection $\langle T \rangle \backslash \mathbb{H} \simeq D - \{0\}$. Autrement dit, si $f : \mathbb{H} \rightarrow \mathbf{C}$ est telle que $f(\tau + 1) = f(\tau)$ il existe une unique fonction $\tilde{f} : D - \{0\} \rightarrow \mathbf{C}$ telle que $f(\tau) = \tilde{f}(q)$.

Soit $f : \mathbb{H} \rightarrow \mathbf{C}$ telle que $f(\tau + 1) = f(\tau)$. Observons que f est une fonction holomorphe si, et seulement si, \tilde{f} est une fonction holomorphe sur $D - \{0\}$. En effet, pour tout $\tau_0 \in \mathbb{H}$, l'application q induit une bijection bi-holomorphe entre le voisinage ouvert $\{\tau \in \mathbb{H} : |\mathrm{Re}(\tau - \tau_0)| < 1/2\}$ de τ_0 dans \mathbb{H} et le voisinage ouvert $D - \mathbf{R}_{\leq 0} e^{2i\pi \mathrm{Re} \tau_0}$ de $q(\tau_0)$ (un inverse s'obtient en considérant une branche du logarithme complexe). Si f est holomorphe il y a donc équivalence entre :

- (1) $f(\tau)$ admet une limite finie quand $\mathrm{Im} \tau \rightarrow \infty$;
- (2) $|f(\tau)|$ est bornée sur $\{\tau \in \mathbb{H} : \mathrm{Im} \tau > 1\}$;
- (3) $|\tilde{f}(q)|$ est bornée au voisinage de $q = 0$;
- (4) $\tilde{f}(q)$ se prolonge en une fonction holomorphe sur tout D ;

(5) $\tilde{f}(q)$ admet un développement en série entière en 0 de rayon de convergence ≥ 1 .

Dans ce cas on dira que f est *holomorphe à l'infini*.

Proposition-Définition 1.2.2. — Soit $f \in M_k(\Gamma(1))$. La forme f admet un unique développement

$$f(\tau) = \sum_{n \geq 0} a_n(f) q^n$$

avec $a_n(f) \in \mathbf{C}$ pour tout entier $n \geq 0$ normalement convergent sur toute partie de \mathbb{H} de la forme $\text{Im } \tau > A$, $A \in \mathbf{R}_{>0}$. Ce développement est appelé *développement de Fourier*, ou *q-développement*, de la forme f et les $a_n(f)$ sont ses coefficients de Fourier. On a $a_0(f) = f(\infty)$.

Remarque 1.7. — Comme nous le verrons, et de manière un peu surprenante, la suite des coefficients de Fourier de chaque forme modulaire est en général d'un intérêt arithmétique considérable.

Si on lâche un peu la contrainte de holomorphicité sur les formes modulaires on a la définition suivante.

Définition 1.8. — Une *fonction modulaire* de poids k (de niveau $\Gamma(1)$) est une fonction méromorphe $f : \mathbb{H} \rightarrow \mathbf{C}$ telle que :

- (1) f est faiblement modulaire de poids k (de niveau $\Gamma(1)$).
- (2) $f(\tau)$ est méromorphe à l'infini, c'est-à-dire, elle admet un q -développement de la forme $f(\tau) = \sum_{n \in \mathbf{Z}} a_n(f) q^n$, avec $a_n = 0$ si $n \ll 0$.

1.2.1. Formes modulaires comme fonctions de réseaux. — On rappelle qu'un réseau dans un \mathbf{R} -espace vectoriel V de dimension finie est un sous-groupe Λ de V satisfaisant aux conditions équivalentes suivantes :

- (1) Λ est discret et V/Λ est compact;
- (2) Λ est discret et engendre le \mathbf{R} -espace vectoriel V ;
- (3) Il existe une \mathbf{R} -base (e_1, \dots, e_n) de V qui est une \mathbf{Z} -base de Λ (c'est-à-dire $\Lambda = \mathbf{Z}e_1 \oplus \dots \oplus \mathbf{Z}e_n$).

Soit \mathcal{R} l'ensemble des réseaux de \mathbf{C} en tant que \mathbf{R} -espace vectoriel.

Maintenant, un réseau $\Lambda \in \mathcal{R}$ admet une base (ω_1, ω_2) comme \mathbf{Z} -module. Toutes les bases se déduisent l'une de l'autre par action de $\text{GL}_2(\mathbf{Z})$ sur le vecteur colonne $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbf{C}^2$. On peut ordonner la base de sorte que $\text{Im}(\omega_1/\omega_2) > 0$. Les bases ainsi ordonnées se déduisent l'une de l'autre par action de $\text{SL}_2(\mathbf{Z})$. On obtient ainsi une bijection entre l'ensemble \mathcal{R} des réseaux et l'ensemble $\text{SL}_2(\mathbf{Z}) \backslash \mathcal{V}$ des vecteurs $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbf{C}^2$ avec $\omega_1/\omega_2 \in \mathbb{H}$ modulo l'action de $\text{SL}_2(\mathbf{Z})$. Via cette bijection, l'action par homothétie de \mathbf{C}^\times sur \mathcal{R}

correspond à l'action par homothétie sur \mathcal{V} . L'application $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \omega_1/\omega_2$ induit une bijection de $\mathcal{V}/\mathbf{C}^\times$ sur \mathbb{H} . On déduit :

Proposition 1.9. — L'application $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \omega_1/\omega_2$ induit par passage au quotient une bijection entre

$$\mathcal{R}/\mathbf{C}^\times \simeq \mathbb{H}/\mathrm{SL}_2(\mathbf{Z}) := Y(1).$$

Remarque 1.10. — Vous avez vu que, à chaque réseau $\Lambda \in \mathbf{C}$ on peut lui associer une courbe elliptique $E_\Lambda = \mathbf{C}/\Lambda$. Vous avez aussi vu que deux réseaux Λ et Λ' définissent des courbes elliptiques isomorphes si et seulement si ils sont homothétiques. Cela donne une troisième interprétation de $Y(1)$: c'est l'ensemble des classes d'isomorphisme de courbes elliptiques (le mot "modulaire" renvoie à la notion d'"espace de module", *i.e.* d'espace qui classe certains objets.)

Revenons maintenant aux formes modulaires de niveau $\Gamma(1)$. Il est intéressant d'exprimer la propriété de modularité en termes de fonctions sur les réseaux.

Une fonction sur \mathcal{R} est dite homogène de poids k si

$$\forall \Lambda \in \mathcal{R}, \forall \alpha \in \mathbf{C}^\times, \varphi(\alpha\Lambda) = \alpha^{-k}\varphi(\Lambda)$$

Notons $\Lambda_\tau := \tau\mathbf{Z} \oplus \mathbf{Z}$. L'égalité $\Lambda_{\gamma\tau} = j(\gamma, \tau)^{-1}\Lambda_\tau$ montre que l'application $\varphi \mapsto f$ définie par $f(\tau) = \varphi(\Lambda_\tau)$ est une bijection

$$\{\text{Fonctions homogènes de poids } k \text{ sur } \mathcal{R}\} \leftrightarrow \{\text{Formes faiblement modulaires de poids } k \text{ de niveau } \Gamma(1)\}$$

dont la bijection réciproque est donnée par $\varphi(\Lambda) = \omega_2^{-k}f(\omega_1/\omega_2)$ où $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ est n'importe quelle base de Λ telle que $\omega_1/\omega_2 \in \mathbb{H}$.

On peut donc identifier les formes modulaires de poids k (et niveau $\Gamma(1)$) avec certaines fonctions de homogènes de poids k sur \mathcal{R} .

1.2.2. Exemples: séries d'Eisenstein. — La manière la plus naïve de fabriquer une fonction de poids k sur \mathcal{R} est de poser

$$G_k(\Lambda) := \sum_{\omega \in \Lambda^*} \frac{1}{\omega^k}$$

où $\Lambda^* = \Lambda \setminus \{0\}$. La fonction correspondante sur \mathbb{H} s'écrit

$$\sum_{(m,n) \in (\mathbf{Z}^2)^*} \frac{1}{(m\tau + n)^k}.$$

Proposition 1.11. — Soit $k \geq 4$ un entier pair. La série $\sum_{(m,n) \in (\mathbf{Z}^2)^*} \frac{1}{(m\tau + n)^k}$ est absolument convergente sur \mathbb{H} . On note $G_k(\tau)$ sa somme. Alors $G_k \in M_k(\Gamma(1))$ et $G_k(\infty) = 2\zeta(k)$. En particulier $G_k \neq 0$.

Démonstration. — Fixons $A, B \in \mathbf{R}_{>0}$ et notons $\mathcal{D}_{A,B}$ l'ensemble des $\tau \in \mathbb{H}$ tels que $\text{Im } \tau > A$ et $|\text{Re } \tau| < B$. Vérifions qu'il existe un réel $C > 0$ tel que pour tout $(\nu, \mu) \in \mathbf{R}^2 - \{0\}$ et tout $\tau \in \mathcal{D}_{A,B}$ alors $|\nu\tau + \mu| > C \sup(|\nu|, |\mu|)$.

Soit $\tau \in \mathcal{D}_{A,B}$. D'une part pour tout $\lambda \in \mathbf{R}$ on a $|\tau + \lambda| > A$. D'autre part le cône $\{\lambda x : x \in \mathcal{D}_{A,B}, \lambda \in \mathbf{R}\}$ a pour frontière les droites vectorielles engendrées respectivement par $B + iA$ et $-B + iA$. En particulier il existe $\delta > 0$ tel que $|\lambda\tau + 1| > \delta$ pour tout $\lambda \in \mathbf{R}$. Ainsi $C = \min(A, \delta)$ convient.

Si $s \geq 1$ il y'a exactement $8s$ couples $(m, n) \in \mathbf{Z}^2$ tels que $\sup(|\nu|, |\mu|) = s$. On déduit la majoration

$$\sum_{(m,n) \in (\mathbf{Z}^2)^*} \frac{1}{|m\tau + n|^k} < \frac{1}{C^k} \sum_{s \geq 1} \frac{8s}{s^k}$$

pour tout $\tau \in \mathcal{D}_{A,B}$. Ainsi, la série de l'énoncé est normalement convergente sur $\mathcal{D}_{A,B}$. En particulier $G_k(\tau)$ est une fonction holomorphe dans \mathbb{H} . Par convergence absolue de $G_k(\tau)$ les bijections $(m, n) \mapsto (m, n + m)$ et $(m, n) \mapsto (n, -m)$ entraînent les identités $G_k(\tau + 1) = G_k(\tau)$ et $G_k(-1/\tau) = \tau^k G_k(\tau)$ pour tout $\tau \in \mathbb{H}$.

Enfin faisons tendre $\text{Im } \tau$ vers l'infini. Par invariance sous T , on peut garder $\tau \in \mathcal{D}_{1,1}$. La fonction $\tau \mapsto \frac{1}{(m\tau + n)^k}$ tend vers $\frac{1}{n^k}$ ou 0 selon que $m = 0$ ou non. Par convergence uniforme de G_k sur $\mathcal{D}_{1,1}$ on peut intervertir limite et sommation et l'on obtient que $G_k(\tau) \rightarrow 2\zeta(k)$. □

Remarque 1.12. — Si $k \geq 4$ on pose $E_k = \frac{1}{2\zeta(k)} G_k \in M_k(\Gamma(1))$ la série de Eisenstein normalisée de sorte que l'on ait $E_k(\infty) = 1$. L'application :

$$\begin{aligned} M_k(\Gamma(1)) &\rightarrow \mathbf{C} \\ f &\mapsto f(\infty) \end{aligned}$$

est une application linéaire. Son noyau, noté $S_k(\Gamma(1))$, est le sous-espace des formes modulaires paraboliques ("cuspidal" en anglais). Si $k \geq 4$ il est donc engendré par tous les éléments de la forme $f - f(\infty)E_k$.

Corollaire 1.13. — Pour tout entier pair $k \geq 4$ on a $M_k = S_k \oplus \mathbf{C}G_k$.

Remarque 1.14 (Lien avec les courbes elliptiques). — Soit $\Lambda \in \mathcal{R}$ et considérons la série de la variable $x \in \mathbf{C}$

$$\wp'_\Lambda(x) = -2 \sum_{\omega \in \Lambda} \frac{1}{(x - \omega)^3}.$$

Elle converge normalement sur tout domaine fondamental pour Λ , une fois qu'on enlève le nombre fini de termes qui y ont un pôle. Cette fonction est donc Λ -périodique, holomorphe en dehors de Λ et possède des pôles d'ordre 3 en chaque $\omega \in \Lambda$. Cette fonction admet une primitive, la fonction \wp_Λ de Weierstrass en $x \in \mathbf{C}$

$$\wp_\Lambda(x) = \frac{1}{x^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(x - \omega)^2} - \frac{1}{\omega^2} \right)$$

elle aussi Λ -périodique et méromorphe, mais avec des pôles d'ordre 2 en $\omega \in \Lambda$.

Ainsi \wp_Λ et \wp'_Λ descendent en des fonctions méromorphes sur \mathbf{C}/Λ . Les $G_k(\Lambda)$ apparaissent dans le développement de Laurent de \wp_Λ :

$$\wp_\Lambda(x) = \frac{1}{x^2} + \sum_{k=2}^{\infty} (2k-1)G_{2k}(\Lambda)x^{2k-2}.$$

En raisonnant sur les pôles possibles d'une fonction méromorphe générale sur \mathbf{C}/Λ , on montre que les corps de fonctions méromorphes Λ -périodiques $\mathcal{M}_{\mathbf{C}/\Lambda}$ est égal à $\mathbf{C}(\wp_\Lambda, \wp'_\Lambda)$. Avec le même genre d'idées, on montre que la fonction

$$\wp_\Gamma^2 - 4\wp_\Lambda^3 + g_2(\Lambda)\wp_\Lambda + g_3(\Lambda)$$

(où $g_2(\Lambda) = 60G_4(\Lambda)$ et $g_3(\Lambda) = 140G_6(\Lambda)$) est holomorphe, donc constante, puis nulle. Ceci donne une présentation du corps $\mathcal{M}_{\mathbf{C}/\Lambda}$ et montre que l'application

$$\mathbf{C}/\Lambda \longrightarrow \mathbf{P}^2(\mathbf{C}), \quad x \neq 0 \mapsto [\wp(x) : \wp'(x) : 1], \quad 0 \mapsto [0 : 1 : 0]$$

est un isomorphisme de \mathbf{C}/Λ sur la surface de Riemann associée à la courbe elliptique d'équation

$$(1.4) \quad y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Cette courbe est non-singulière : si $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbf{C}^2$ est une base de Γ et que l'on note $e_1 = \wp_\Lambda(\omega_1/2)$, $e_2 = \wp_\Lambda(\omega_2/2)$ et $e_3 = \wp_\Lambda(\frac{\omega_1+\omega_2}{2})$ on montre que (1.4) s'écrit sous la forme

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3).$$

Définition 1.15 (Fonction Δ de Jacobi). — La fonction $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ est une forme modulaire parabolique de poids 12 et niveau $\Gamma(1)$.

On verra plus tard qu'elle est non nulle (d'après la remarque 1.6(2.16) il suffit de voir que $E_4(i) \neq 0$). On peut aussi montrer que, à une constante non nulle près elle coïncide avec les discriminant de la courbe (1.4).

1.3. Calcul des dimensions. — Le théorème principal de cette section est le suivant :

Théorème 1.16. — Soit $k \in \mathbf{Z}$.

(1) L'espace $M_k(\Gamma(1))$ admet pour base les $E_4^r E_6^s$ avec $(r, s) \in \mathbf{N}^2$ vérifiant $4r + 6s = k$ (c'est-à-dire l'algèbre $M(\Gamma(1))$ est l'algèbre des polynômes en E_4 et E_6).

(2)

$$\dim_{\mathbf{C}}(M_k(\Gamma(1))) = \begin{cases} 0 & \text{si } k \text{ impair} \\ \lfloor \frac{k}{12} \rfloor & \text{si } k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{si } k \equiv 0, 4, 6, 8, 10 \pmod{12} \end{cases}$$

(3) La multiplication par Δ définit un isomorphisme :

$$\begin{aligned} M_{k-12}(\Gamma(1)) &\simeq S_k(\Gamma(1)) \\ f &\mapsto \Delta f. \end{aligned}$$

Démonstration. — Le plan de la preuve est le suivant :

- (1) On calcule à la main les dimensions de $M_k(\Gamma(1))$, $k \leq 10$.
- (2) On prouve (3).
- (3) Par récurrence et le corollaire 1.13 on déduit (2).
- (4) On prouve (1).

Soient $f \in M_k(\Gamma(1))$ et $P \in \mathbb{H}$. L'entier n tel que $f(\tau)/(\tau - P)^n$ est holomorphe et non-zéro en P s'appelle l'ordre de f en P et on le note $v_P(f)$. On note aussi e_P le cardinal du stabilisateur de P dans $\mathrm{PSL}_2(\mathbf{Z})$. Les entiers $v_P(f)$ et e_P ne dépendent que de la $\Gamma(1)$ -orbite de P (pour e_P c'est clair; pour $v_P(f)$ cela découle du fait que pour tout $\gamma \in \Gamma(1)$, on a $f(\gamma P) = j(\gamma, P)^k f(P)$).

De plus d'après le théorème 1.1, on a $e_i = 2$, $e_\rho = 3$ et $e_P = 1$ si P n'est pas dans l'orbite de i ou ρ . On note enfin $v_\infty(f)$ l'ordre d'annulation de \tilde{f} en 0. La clé dans la preuve du théorème 1.16 est le lemme suivant :

Lemme 1.17 (Lemme $k/12$). — Soient $k \in \mathbf{Z}$, $f \in M_k(\Gamma(1))$ non nulle. On a la relation :

$$v_\infty(f) + \sum_{P \in \Gamma \backslash \mathbb{H}} \frac{v_P(f)}{e_P} = \frac{k}{12}.$$

Remarque 1.18. — On peut aussi écrire cette formule sous la forme

$$(1.5) \quad v_\infty(f) + \frac{v_i(f)}{2} + \frac{v_\rho(f)}{3} + \sum_P v_P(f) = \frac{k}{12}$$

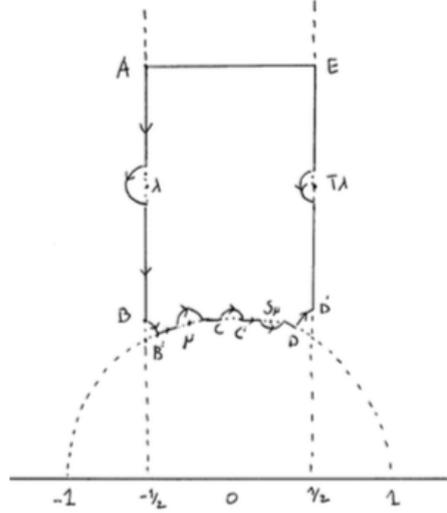
la somme portant sur les points de $\Gamma \backslash \mathbb{H}$ différents des classes de i et de ρ .

Remarque 1.19. — Toutes les quantités de cet énoncé sont positives et il fait partie de l'énoncé que la somme de gauche est une somme finie.

Démonstration. — Soit $f \in M_k(\Gamma(1))$ non nulle. Rappelons que la $\Gamma(1)$ -orbite de tout zéro de f rencontre le domaine \mathcal{F} . Si $r > 0$ est un réel, posons $\Omega_r = \{\tau \in \mathbb{H}, \mathrm{Im} \tau > r\}$. La fonction \tilde{f} étant holomorphe en 0, il existe $r > 0$ tel que f n'admette pas de zéro dans Ω_r . La partie $\mathcal{F} - \Omega_r$ étant compacte, la fonction holomorphe f n'y admet qu'un nombre fini de zéros (qui sont isolés). Cela montre que le nombre de $\Gamma(1)$ -orbites de points constitués de zéros de f est fini (et donc que la somme apparaissant dans la formule (1.5) a tous ses termes nuls sauf au plus un nombre fini d'entre eux).

Considérons le contour \mathcal{C} indiqué par la figure 2. Sur cette figure, les zéros éventuels de f qui sont dans $\partial \mathcal{F} - \{i, \rho, -\rho^2\}$ et de partie réelle $1/2$ (resp. de module 1) sont notés λ (resp. μ). En particulier ce contour ne contient aucun zéro de f . On suppose que chaque portion de cercle dessinée est de rayon suffisamment petit de sorte que le disque bordé ne contienne que le point indiqué pour éventuel zéro (c'est-à-dire $i, \rho, -\rho^2$, l'un des $\lambda, \lambda + 1$ ou l'un des $\mu, -1/\mu$).

Nous noterons γ_{XY} le chemin portion de \mathcal{C} allant de X à Y (dans ce sens). Le chemin $\gamma_{D'E}$ est par définition le chemin $T\gamma_{BA}$. De même on a choisi $\gamma_{C'D} = S\gamma_{CB'}$. Enfin on suppose que γ_{EA} est de partie imaginaire r suffisamment grande de sorte qu'aucun zéro de

FIGURE 2. Le contour \mathcal{C} dans la preuve du lemma $k/12$

f ne soit de partie imaginaire $> r$. L'existence d'un tel contour est justifié par le fait que les zéros sont isolés. Remarquons qu'on a construit notre parcours de sorte que chaque $\Gamma(1)$ -orbite d'un zéro contient exactement un représentant dans l'intérieur de \mathcal{C} sauf pour i et ρ qu'on laisse à l'extérieur.

La formule des résidus s'écrit alors :

$$\frac{1}{2i\pi} \int_{\mathcal{C}} \frac{f'(\tau)}{f(\tau)} d\tau = \sum_P v_P(f)$$

la somme portant sur les points de $\Gamma \backslash \mathbb{H}$ différents des classes de i et de ρ .

Examinons maintenant les contributions des diverses portions du contour.

(1) Les fonctions f et f' étant T -invariantes on observe d'abord que :

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

(2) Le chemin $\omega(t) := e^{2\pi i \gamma_{EA}(t)}$ est un cercle de centre 0 dans D faisant un tour dans le sens indirect. On en déduit :

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

(3) De plus par modularité on a

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

de sorte que :

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

avec $\gamma_{C'D} = S\gamma_{CB'}$.

Lorsque le point B' tend vers ρ , C tend vers i , et lorsque les portions de cercles autour des points notés μ sont de rayon tendant vers 0 alors l'intégrale $\frac{1}{i} \int_{\gamma_{B'C}} \frac{1}{\tau}$ tend vers l'angle orienté défini par ρ , 0 et i c'est-à-dire $-\frac{\pi}{6}$.

(4) De même lorsque B et B' tendent vers ρ alors l'intégrale de chemin

$$\frac{1}{i} \int_{\gamma_{BB'}} \frac{f'(\tau)}{f(\tau)} d\tau$$

tend vers l'angle orienté défini par B , i et B' (c'est-à-dire $-\frac{\pi}{3}$) multiplié par $v_\rho(f)$.

(5) Enfin lorsque C et C' tendent vers i alors l'intégrale de chemin

$$\frac{1}{i} \int_{\gamma_{CC'}} \frac{f'(\tau)}{f(\tau)} d\tau$$

tend vers $\pi v_i(f)$.

On conclut mettant les identités bout à bout. \square

Montrons finalement le théorème 1.16

On sait que $M_k(\Gamma(1))$ est nul si k est impair. Si on fait $k = 2$ ou $k < 0$, puisque chacun des $\text{ord}_\tau(f)$ dans (1.5) est ≥ 0 , on constate qu'il n'y a pas de f satisfaisant cette égalité. Donc

$$M_k(\Gamma(1)) = 0$$

si $k = 2$ ou $k < 0$.

On a pour les mêmes raisons que $S_k = 0$ si $k < 12$ car $v_\infty(f) \geq 1$ et $M_0 = \mathbf{C}$. On déduit du corollaire 1.13 que $S_k = \mathbf{C}E_k$ si $k = 4, 6, 8$ ou 10 .

Si on applique la formule (1.5) à $k = 4$ et $f = E_4$ on déduit que $E_4(i) \neq 0$ (car $E_4(\rho) = 0$ par la remarque 1.6(2.16)) et donc $\Delta \neq 0$ car $\Delta(i) = \frac{1}{1728} E_4(i)^3$.

Si on applique la formule (1.5) à Δ , on en déduit que

$$S_{12}(\Gamma(1)) = \mathbf{C} \cdot \Delta.$$

Maintenant, puisque Δ est inversible en tant que fonction sur \mathbb{H} , l'application $f \mapsto \Delta \cdot f$ induit un isomorphisme

$$M_k(\Gamma(1)) \simeq S_{k+12}(\Gamma(1))$$

pour tout $k \in \mathbf{N}$. Grâce aux calculs des M_k pour $k < 12$ et au corollaire 1.13 on en déduit

$$\dim_{\mathbf{C}}(M_k(\Gamma(1))) = \begin{cases} 0 & \text{si } k \text{ impair} \\ \lfloor \frac{k}{12} \rfloor & \text{si } k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{si } k \equiv 0, 4, 6, 8, 10 \pmod{12} \end{cases}$$

Prouvons enfin que l'algèbre $M(\Gamma(1))$ est l'algèbre des polynômes en E_4 et E_6 .

Il s'agit de montrer que pour $k \in 2\mathbf{N}$, la famille des $E_4^n E_6^m$ où $n, m \in \mathbf{N}$ et $4n + 6m = k$ est une base de $M_k(\Gamma(1))$. On l'a déjà vérifié pour $k \leq 10$.

Montrons par récurrence que cette famille est génératrice pour $k \geq 12$. Choisissons pour cela n, m tels que $4n + 6m = k$, et soit $f \in M_k$. Puisque $E_4^n E_6^m(\infty) = 1$ alors $f - E_4^n E_6^m f(\infty)$ est parabolique. Mais alors $f - \lambda E_4^n E_6^m f(\infty) = \Delta g$ pour $g \in M_{k-12}$, et par récurrence, on conclut que $f \in \mathbf{C}[E_4, E_6]$.

Montrons maintenant que cette famille est libre. Soit (n_0, m_0) tel que $4n_0 + 6m_0 = k$ avec m_0 maximal. En divisant par $E_4^{n_0} E_6^{m_0}$, une relation de dépendance linéaire fournit un polynôme dans $\mathbf{C}[T]$ qui annule la fonction méromorphe $E_4^3 E_6^{-2}$, laquelle devrait donc être constante, ce qui n'est pas le cas. □

Remarque 1.20. — Le lemme $k/12$ est aussi vrai pour des *fonctions* modulaires. Dans ce cas les $v_P(f)$ sont des entiers non nécessairement positifs.

1.4. Exemples. — La théorie de formes modulaires a fait l'objet de plusieurs conjectures célèbres comme la conjecture de Ramanujan ou la conjecture de Shimura-Taniyama-Weil. L'une des beautés de cette théorie ce sont les applications arithmétiques intéressantes qu'elle a. On va voir dans ce paragraphe quelques exemples.

1.4.1. Posons $q = \exp(2i\pi z)$. Les formes ou fonctions modulaires ci-dessus ont des q -développements remarquables obtenus à une époque où les "fonctions spéciales" étaient peut-être mieux maîtrisées que maintenant. Un exercice de TD expliquera le développement

$$(1.6) \quad E_k(z) := \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

où les B_k sont les nombres de Bernoulli et $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. On montrera que les B_k sont rationnels et faciles à calculer. En particulier E_4 et E_6 sont à coefficients entiers comme le montre le tableau suivant : Ainsi $M_k(\Gamma(1))$ possède une \mathbf{C} -base constitué de

k	2	4	6	8	10	12	14	16
$-\frac{2k}{B_k}$	-24	240	-504	480	-264	65520/691	-24	16320/3617

formes modulaires à coefficients entiers, un phénomène inattendu. Par dimensions on a $E_4^2 = E_8$ et donc on trouve

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma_3(i) \sigma_3(n-i)$$

On a aussi $E_4E_6 = E_{10}$ d'où on peut déduire la relation

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{i=1}^{n-1} \sigma_3(i)\sigma_5(n-i).$$

Ces identités sont tout à fait non triviales!

On peut maintenant expliquer la normalisation $\frac{1}{1728}$ de Δ . Puisque $1728 = 2 \times 504 + 3 \times 240$, en développant la définition 1.15 et la formule (1.6) pour $k = 4, 6$ on trouve que :

$$\Delta = q - 24q^2 + 252q^3 + \dots$$

On verra toute à l'heure plus de propriétés de coefficients de Δ .

1.4.2. L'invariant j . — On définit $j = \frac{E_4^3}{\Delta}$

Proposition 1.21. — (1) j est une fonction modulaire de poids 0.

(2) j a un zéro en $\tau = \rho$ et un pôle simple à l'infini.

(3) Par passage au quotient j définit une bijection :

$$j : \Gamma(1) \backslash \mathbb{H} \rightarrow \mathbf{C}.$$

Démonstration. — 1) est une conséquence du fait que $E_4^3, \Delta \in M_{12}(\Gamma(1))$. 2) découle de l'étude de zéros de E_4 et Δ dans la preuve du théorème 1.16. Prouvons 3). Soit $\lambda \in \mathbf{C}$. Il suffit alors de montrer que la forme modulaire $f_\lambda = E_4^3 - \lambda\Delta$ a un unique zéro modulo $\Gamma(1)$. Si on applique le lemme $k/12$ à f_λ on voit que les seules solutions possibles sont :

(1) Il existe $P \neq i, \rho$ tel que f_λ a un zéro simple en P et pas d'autre zéros ailleurs.

(2) i est un zéro double de f_λ qui n'a pas d'autre zéro ailleurs.

(3) ρ est un zéro triple de f_λ qui n'a pas d'autre zéro ailleurs.

Dans tous les cas on conclut que f_λ a un et un seul zéro. □

Remarque 1.22. — Si on note $\{Ell\}$ l'ensemble de courbes elliptiques à isomorphisme près on a vu une série des bijections :

$$\{Ell\} \longleftrightarrow \mathcal{R}/\mathbf{C} \longleftrightarrow \Gamma(1) \backslash \mathbb{H} \longleftrightarrow \mathbf{C}$$

$$E_\Lambda \longleftarrow \Lambda \longrightarrow \tau_\Lambda \longrightarrow j(\tau_\Lambda)$$

Via ces bijection on associe à chaque courbe elliptique E_Λ un invariant $j(\tau_\Lambda)$, appelé invariant j , qui a des très bonnes propriétés.

Proposition 1.23. — Soit $f : \mathbb{H} \rightarrow \mathbf{C}$ une fonction méromorphe. Les propriétés suivantes sont équivalentes :

(i) f est une fonction modulaire de poids 0.

(ii) f est le quotient de deux formes modulaires de même poids.

(iii) f est une fonction rationnelle en j .

Démonstration. — Il est clair que (iii) implique (ii) et que (ii) implique (i). Montrons que (i) implique (iii). Soit f une fonction modulaire. Puisque j n'a qu'un seul zéro (en ρ), quitte à multiplier f par un polynôme en j on peut supposer que f est holomorphe sur \mathbb{H} . De même il existe n tel que $g := \Delta^n f$ est holomorphe à l'infini. Alors $g \in M_{12n}(\Gamma(1))$. Elle donc une combinaison linéaire des $E_4^r E_6^s$ avec $4s + 6r = 12n$. Par linéarité il suffit donc de montrer la proposition pour $g = E_4^r E_6^s$ avec $4s + 6r = 12n$, c'est-à-dire, $f = \frac{E_4^r E_6^s}{\Delta^n}$. Mais $4s + 6r = 12n$ implique que s est de la forme $3k$ et r est de la forme $2k'$ avec $k + k' = n$. Alors $f = \frac{E_4^{3k} E_6^{2k'}}{\Delta^{k+k'}}$. Il suffit enfin de montrer que $\frac{E_4^3}{\Delta}$ et $\frac{E_6^2}{\Delta}$ sont des fractions rationnelles en j ce qui est évident. \square

1.4.3. La série de Eisenstein E_2 . — On définit la série d'Eisenstein de poids 2 et niveau $\Gamma(1)$ par (le symbole \sum' veut dire que $n \neq 0$ si $m = 0$).

$$\begin{aligned} E_2(\tau) &= \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau + n)^2} \\ &= 1 + \frac{3}{\pi^2} \sum_{m \neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau + n)^2} \\ &= 1 + \frac{6}{\pi^2} \sum_{m \geq 1} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau + n)^2} \end{aligned}$$

La même preuve qu'en TD montre que

$$\sum_{n=-\infty}^{\infty} \frac{1}{(m\tau + n)^2} = \frac{-4}{B_2} \zeta(2) \sum_{d=1}^{\infty} dq^{dm}$$

d'où :

$$E_2 = 1 - 24 \sum_{m \geq 1} \sum_{d=1}^{\infty} dq^{dm}$$

Comme $|q| < 1$ il est facile de voir que la somme sur m et d est absolument convergente et comme dans le TD on trouve que

$$E_2 = 1 - 24 \sum_{m \geq 1} \sigma_1(m) q^m$$

Comme pour les E_k , E_2 est donc une fonction holomorphe sur \mathbb{H} , périodique de période 1 et holomorphe à l'infini. Pour que ce soit une forme modulaire on aurait besoin, en plus,

que $E_2(\tau)$ soit égal à :

$$\begin{aligned}\tau^{-2}E_2\left(\frac{-1}{\tau}\right) &= \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \sum_{n=\infty}^{\infty} \frac{1}{(-m+n\tau)^2} \\ &= 1 + \frac{3}{\pi^2} \sum_{n=\infty}^{\infty} \sum_{m \neq 0} \frac{1}{(m\tau+n)^2}\end{aligned}$$

Proposition 1.24. — On a $\tau^{-2}E_2\left(\frac{-1}{\tau}\right) = E_2(\tau) + \frac{12}{2\pi i\tau}$.

Démonstration. — L'idée de la preuve est la suivante. On va chercher une double suite $a_{m,n}(\tau)$ telle que

$$\sum_{m \neq 0} \sum_{n=\infty}^{\infty} \frac{1}{(m\tau+n)^2} - a_{m,n}(\tau)$$

soit absolument convergente. On pourra alors intervertir l'ordre des sommes et la différence entre $\sum_{n=\infty}^{\infty} \sum_{m \neq 0} \frac{1}{(m\tau+n)^2}$ et $\sum_{m \neq 0} \sum_{n=\infty}^{\infty} \frac{1}{(m\tau+n)^2}$ sera alors la différence entre $\sum_{m \neq 0} \sum_{n=\infty}^{\infty} a_{m,n}(\tau)$ et $\sum_{n=\infty}^{\infty} \sum_{m \neq 0} a_{m,n}(\tau)$. On va donc choisir une double suite $a_{m,n}(\tau)$ "proche" de $\frac{1}{(m\tau+n)^2}$ mais dont la somme soit plus facile à calculer.

On pose :

$$a_{m,n}(\tau) = \frac{1}{(m\tau+n-1)(m\tau+n)} = \frac{1}{(m\tau+n-1)} - \frac{1}{(m\tau+n)}$$

D'un côté, on a

$$\frac{1}{(m\tau+n)^2} - a_{m,n}(\tau) = \frac{1}{(m\tau+n-1)(m\tau+n)^2}$$

de sorte que la série modifiée :

$$\tilde{E}_2(\tau) = 1 + \frac{3}{\pi^2} \sum_{m \neq 0} \sum_{n=\infty}^{\infty} \frac{1}{(m\tau+n)^2} - a_{m,n}(\tau)$$

est absolument convergente.

En plus, étant une somme télescopique il est clair que $\sum_{m \neq 0} \sum_{n=\infty}^{\infty} a_{m,n}(\tau) = 0$ (donc en fait $\tilde{E}_2(\tau) = E_2(\tau)$). Un petit calcul (exercice!) nous donne que $\sum_{n=\infty}^{\infty} \sum_{m \neq 0} a_{m,n}(\tau) = \frac{-2i\pi}{\tau}$. Le résultat s'ensuit. \square

1.4.4. La fonction η de Dedekind. — On pose

$$(1.7) \quad \eta(\tau) = e^{2\pi i\tau/24} \prod_{n=1}^{\infty} (1 - q^n), \quad (q = e^{2\pi i\tau})$$

Proposition 1.25. — (1) On a $\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau)$.
 (2) On a

$$(1.8) \quad \eta\left(\frac{-1}{\tau}\right) = \sqrt{\frac{\tau}{i}} \eta(\tau)$$

(dans cette formule la notation désigne la racine carrée de $\frac{\tau}{i}$ dont la partie réelle est > 0 .)

Démonstration. — Le produit (1.7) converge vers une valeur non zéro pour tout $\tau \in \mathbb{H}$ et définit une fonction holomorphe sur \mathbb{H} . La première égalité est évidente, étant donné l'invariance de q sous $\tau \mapsto \tau + 1$. On va montrer que les dérivés logarithmiques de deux termes de (1.8) sont égales. Il s'en suit que ces deux termes sont égaux à une constante multiplicative près. Mais $\eta\left(\frac{-1}{i}\right) = \eta(i) = \sqrt{\frac{i}{i}}\eta(i)$. Donc cette constante vaut 1. On a

$$\begin{aligned} \frac{\eta'(\tau)}{\eta(\tau)} &= \frac{2\pi i}{24} \left(1 - 24 \sum_{n=1}^{\infty} \frac{nq^n}{1 - q^n} \right) \\ &= \frac{2\pi i}{24} \left(1 - 24 \sum_{n=1}^{\infty} \sum_{t=1}^{\infty} nq^n q^{nt} \right) \\ &= \frac{2\pi i}{24} \left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n)q^n \right) \\ &= \frac{2\pi i}{24} E_2(\tau). \end{aligned}$$

Montrer que

$$\frac{\eta'\left(\frac{-1}{\tau}\right)}{\eta\left(\frac{-1}{\tau}\right)} \tau^{-2} = \frac{1}{2\tau} + \frac{\eta'(\tau)}{\eta(\tau)}$$

revient donc à montrer $\tau^{-2}E_2\left(\frac{-1}{\tau}\right) = E_2(\tau) + \frac{12}{2\pi i\tau}$ et ceci est la proposition 1.24

□

Remarque 1.26. — (1) La fonction η va nous permettre de construire de formes modulaires de niveau $\neq \Gamma(1)$.

(2) Soient x, y deux entiers premiers entre eux avec $y > 0$. La somme de Dedekind $s(x, y)$ est définie par

$$s(x, y) = \sum_{j=1}^{y-1} \frac{j}{y} \left(\frac{jx}{y} - \left[\frac{jx}{y} \right] - \frac{1}{2} \right).$$

On peut montrer plus généralement que si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, avec $c > 0$ la fonction η de Dedekind satisfait l'équation

$$\eta(\gamma\tau) = e^{2\pi i\Phi(\gamma)/24} \sqrt{\frac{j(\gamma, \tau)}{i}} \eta(\tau)$$

Dans cette formule la notation désigne encore la racine carrée de $\frac{\tau}{i}$ dont la partie réelle est > 0 et $\Phi(\gamma)$ est donné par la formule

$$\Phi(\gamma) = \frac{1}{c} + \frac{d}{c} - 12s(d, c)$$

En fait les sommes de Dedekind $s(x, y)$ satisfont beaucoup de relations intéressantes. En particulier la loi de réciprocité de Dedekind : soient $x, y > 0$ premiers entre eux. Alors :

$$12s(x, y) + 12s(y, x) = \frac{x}{y} + \frac{y}{x} + \frac{1}{xy} - 3.$$

Voir le livre de Gosswald-Rademacher pour plus de détails.

1.4.5. La fonction τ de Ramanujan. —

Proposition 1.27. — On a

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n), \quad (q = e^{2\pi i\tau})^{24}.$$

En particulier les coefficients de Δ sont entiers.

Démonstration. — Notons $f(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$. Alors f est holomorphe sur \mathbb{H} et 0 à l'infini. On a $f(\tau + 1) = f(\tau)$. En plus on a $f(\tau) = (\eta(\tau))^{24}$. On déduit de (1.8) que $f(-1/\tau) = \tau^{12} f(\tau)$, c'est-à-dire, f est une forme parabolique de poids 12. Par le théorème 1.16, on déduit que f est proportionnel à Δ . En comparant le premier coefficient de chaque série on déduit le résultat. \square

Remarque 1.28. — (1) On a $\frac{\Delta'(\tau)}{\Delta(\tau)} = 2\pi i E_2(\tau)$.

(2) On a

$$\begin{aligned} j(\tau) &:= \frac{E_4^3(\tau)}{\Delta(\tau)} = \frac{(1 + 204q + 2160q^2 + \dots)^3}{q - 24q^2 + 252q^3 + \dots} \\ &= \frac{1}{q} \frac{(1 + 204q + 2160q^2 + \dots)^3}{1 - 24q + 252q^2 + \dots} \\ &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots \end{aligned}$$

Tous les coefficients de j sont donc aussi des entiers. Si on écrit

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

les $c(n)$ satisfont des congruences remarquables :

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

Voir le livre d'Apostol pour une preuve. Les coefficients $c(n)$ ont aussi un rapport avec les représentations du groupe Monstre, voir les articles de Conway.

On écrit maintenant

$$\Delta(\tau) = \sum_{n=1}^{\infty} \tau(n)q^n.$$

Cela définit les $\tau(n)$. La fonction $n \mapsto \tau(n)$ est appelée la fonction de Ramanujan. Il a calculé les premiers 30 valeurs de $\tau(n)$ en 1915.

n	1	2	3	4	5	6	7	8	9	10
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744	84480	-113643	-115920

et a observé plusieurs propriétés :

(1) $\tau(nm) = \tau(n)\tau(m)$ si n et m sont premiers entre eux. Et $\tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1})$ si p est premier.

(2) $|\tau(p)| \leq 2\sqrt{p^{11}}$, pour p premier.

La première conjecture a été montré par Mordell un an plus tard (on verra une preuve un peu plus tard dans le cours). Par contre la conjecture 2) s'est révélée beaucoup plus profonde et n'a été prouvé qu'en 1974 par Deligne comme conséquence de sa preuve des conjectures de Weil (et son résultat, aussi profond, que ces conjectures impliquent celle de Ramanujan).

En TD on se contentera de la proposition suivante :

Proposition 1.29 (Hecke 1930). — Soit $f \in S_k(\Gamma(1))$, $f = \sum_{n \geq 1} a_n q^n$. Alors $a_n = O(n^{k/2})$, c'est-à-dire il existe une constante C telle que $|a_n| \leq Cn^{k/2}$ pour tout $n \geq 1$.

Démonstration. — Comme f est parabolique, $a_0 = 0$ de sorte que

$$(1.9) \quad |f(\tau)| = O(q) = O(e^{-2\pi y}), \quad (y = \text{Im } \tau),$$

quand q tend vers 0. Posons $\phi(\tau) = |f(\tau)|y^{k/2}$. Aussi ϕ est $\Gamma(1)$ -invariante et continue sur \mathcal{F} . Alors (1.9) montre que $\phi(\tau)$ tend vers 0 quand y tend vers l'infini. Cela implique que ϕ est bornée, c'est-à-dire il existe M telle que $|f(\tau)| \leq My^{-k/2}$.

Fixons y et faisons varier x entre 0 et 1. Le point $q = e^{2\pi i(x+iy)}$ parcourt le cercle C_y de centre 0 et rayon y . Alors par la formule de résidus :

$$a_n = \frac{1}{2\pi i} \int_{C_y} f(\tau) q^{-n-1} dq = \int_0^1 f(x+iy) q^{-n} dx.$$

On déduit que

$$\begin{aligned} |a_n| &\leq \int_0^1 |f(x+iy)| |q^{-n}| dx \\ &\leq \int_0^1 M y^{-k/2} e^{2\pi n y} dx \\ &= M y^{-k/2} e^{2\pi n y}. \end{aligned}$$

Cela est vrai pour tout $y > 0$. On pose $y = 1/n$ et on trouve que $|a_n| \leq C n^{k/2}$ avec $C = M e^{2\pi}$. □

2. Formes modulaires de niveau $\Gamma \subset \Gamma(1)$

Après avoir vu les applications de formes modulaires de niveau $\Gamma(1)$ on pourrait se demander si la définition 1.5 pourrait être généralisée et si cette éventuelle nouvelle définition donnerait lieu à une théorie aussi riche que la précédente. On pourrait commencer cette section donnant la définition de formes modulaires de niveau quelconque et ensuite voir des exemples et applications. Mais on va procéder dans le sens inverse. On va commencer avec un problème classique de théorie de nombres et on va essayer de construire une théorie qui puisse fournir une réponse à notre problème.

La problème est le suivant : Soient n et k deux entiers positifs. Combien y-a t'il de représentations de n comme somme de k carrés ? C'est-à-dire, quel est le nombre de $(n_1, \dots, n_k) \in \mathbf{Z}^k$ tels que $\sum_i n_i^2 = n$?

Ce problème est lié aux fonctions thêta. Rappelons le cadre :

2.1. Les fonctions thêta de Jacobi. —

2.1.1. La fonction θ . — Considérons la fonction d'une variable réelle $t > 0$ définie par la somme :

$$\theta(t) = \sum_{n \in \mathbf{Z}} e^{-t\pi n^2}.$$

Cette série (à termes positifs) est bien évidemment convergente, et fonction décroissante de $t > 0$. Elle satisfait l'équation fonctionnel suivante, due à Poisson, qui est un ingrédient clé dans la preuve de l'équation fonctionnelle de la fonction ζ de Riemann.

Proposition 2.1. — Pour tout réel $t > 0$ on a :

$$\theta(1/t) = \sqrt{t} \theta(t).$$

Démonstration. — Notons $\mathcal{S}(\mathbf{R})$ l'espace de fonctions de Schwartz, c'est-à-dire, l'espace des fonctions \mathcal{C}^∞ telles que pour tous entiers $n, m > 0$ on ait $x^n f^{(m)}(x) \rightarrow 0$ quand $|x| \rightarrow \infty$. Si $f \in \mathcal{S}(\mathbf{R})$, f est en particulier sommable de sorte que sa transformée de Fourier :

$$\begin{aligned} \widehat{f} : \mathbf{R} &\rightarrow \mathbf{C} \\ y &\mapsto \int_{\mathbf{R}} f(x) e^{-2\pi i x y} dx \end{aligned}$$

est bien définie.

Lemme 2.2 (Formule de Poisson). — *Pour tout $f \in \mathcal{S}(\mathbf{R})$ on a :*

$$\sum_{n \in \mathbf{Z}} f(n) = \sum_{n \in \mathbf{Z}} \widehat{f}(n).$$

Démonstration. — Soit $\phi(x) = \sum_{m \in \mathbf{Z}} f(x + m)$. Cette série de fonctions converge normalement sur tout segment, ainsi que toutes ses dérivées, par hypothèse sur f . Elle définit donc une fonction \mathcal{C}^∞ et 1-périodique de la variable réelle x . Ses coefficients de Fourier sont données par la formule :

$$\begin{aligned} c_n &= \int_0^1 \phi(x) e^{-2\pi i x n} dx = \sum_{m \in \mathbf{Z}} \int_m^{m+1} f(x) e^{-2\pi i x n} dx \\ &= \int_{\mathbf{R}} f(x) e^{-2\pi i x n} dx = \widehat{f}(n). \end{aligned}$$

(L'intervention somme/intégrale est loisible car f est sommable sur \mathbf{R}). La fonction ϕ étant \mathcal{C}^∞ , sa série de Fourier $\sum_{n \in \mathbf{Z}} \widehat{f}(n) e^{2\pi i n x}$ est absolument convergente vers $\phi(x)$ pour tout $x \in \mathbf{R}$. On conclut en prenant $x = 0$, et montrons au passage que les deux sommes de l'énoncé sont absolument convergentes. □

Lemme 2.3. — *Si $t \in \mathbf{R}_{>0}$, la fonction :*

$$f_t : x \mapsto e^{-\pi t x^2}$$

est dans $\mathcal{S}(\mathbf{R})$ et vérifie :

$$\widehat{f}_t(y) = \frac{1}{\sqrt{t}} f_{1/t}(y).$$

Démonstration. — Il est clair que $f_t \in \mathcal{S}(\mathbf{R})$. On a :

$$\begin{aligned} \widehat{f}_t(y) &= \int_{\mathbf{R}} e^{-\pi t x^2} e^{-2\pi i x y} dx \\ &= \frac{1}{\sqrt{t}} \int_{\mathbf{R}} e^{-\pi x^2} e^{-2\pi i x \frac{y}{\sqrt{t}}} dx \\ &= \frac{1}{\sqrt{t}} \widehat{f}_1\left(\frac{y}{\sqrt{t}}\right). \end{aligned}$$

Il suffit donc de montrer que $\widehat{f}_1 = f_1$, c'est-à-dire que la fonction $x \mapsto e^{-\pi x^2}$ est égale à sa transformée de Fourier. C'est un fait bien connu du à Gauss (et laissé en exercice). \square

Pour conclure la preuve de la proposition 2.1, il suffit d'appliquer la formule de Poisson à la fonction f_t . \square

2.1.2. La fonction Θ . — Jacobi a introduit une variante à deux variables de la fonction θ . Si $z \in \mathbf{C}$ et $\tau \in \mathbb{H}$ il pose

$$\Theta(z; \tau) = \sum_{n \in \mathbf{Z}} e^{\pi i \tau n^2 + 2\pi i n z}.$$

Cette série est manifestement normalement convergente sur toute partie de $\mathbf{C} \times \mathbb{H}$ de la forme $\{(z, \tau) : \operatorname{Im} z > A, \operatorname{Im} \tau > B\}$ où $A \in \mathbf{R}$ et $B \in \mathbf{R}_{>0}$. Cela justifie la définition, et montre que la fonction $(z, \tau) \mapsto \Theta(z; \tau)$ est holomorphe en chacune de variables, l'autre étant fixée. On observe que si $t > 0$, alors $\Theta(0; it) = \theta(t)$: on retrouve la fonction précédente sur l'axe imaginaire, quand $z = 0$.

Il est clair que :

$$\Theta(z + 1; \tau) = \Theta(z; \tau) \quad \text{et} \quad \Theta(z + \tau; \tau) = e^{-i\pi\tau - 2i\pi z} \Theta(z; \tau).$$

Ainsi à τ fixé ces formules expriment le comportement de la fonction $z \mapsto \Theta(z; \tau)$ par rapport au réseau $\mathbf{Z} + \tau\mathbf{Z}$ de \mathbf{C} ; leur application originale est d'ailleurs à la construction de fonctions méromorphes sur \mathbf{C} invariantes par un tel réseau. Leur dépendance en la variable τ , que l'on peut voir comme paramétrant le réseau $\mathbf{Z} + \tau\mathbf{Z}$ est encore plus remarquable.

Proposition 2.4. — *Pour tout $z \in \mathbf{C}$ et tout $\tau \in \mathbb{H}$ on a les relations :*

$$\Theta(z; \tau + 2) = \Theta(z; \tau) \quad \text{et} \quad \Theta(z; -1/\tau) = \sqrt{-i\tau} e^{\pi i \tau z^2} \Theta(\tau z; \tau)$$

(dans cette formule la notation désigne la racine carrée de $\sqrt{-i\tau}$ dont la partie réelle est > 0 .)

Démonstration. — L'identité $\Theta(z; \tau + 2) = \Theta(z; \tau)$ est immédiate. Pour la seconde on a besoin d'un lemme :

Lemme 2.5. — *Si $z \in \mathbf{C}$ et $\tau \in \mathbb{H}$, la fonction :*

$$\begin{aligned} \psi : \mathbf{R} &\rightarrow \mathbf{C} \\ x &\mapsto e^{i\pi\tau x^2 + 2\pi i z x} \end{aligned}$$

est dans $\mathcal{S}(\mathbf{R})$ et de transformée de Fourier

$$\widehat{\psi} : y \mapsto \frac{1}{\sqrt{-i\tau}} e^{-\frac{i\pi}{\tau}(y-z)^2}.$$

Démonstration. — Posons $g_\tau(x) = e^{i\pi\tau x^2}$. La transformée de Fourier de $x \mapsto g_\tau(x)e^{2i\pi zx}$ et $\tilde{g}_\tau(y - z)$. Du coup on peut supposer $z = 0$. Fixons $y \in \mathbf{R}$. On veut démontrer l'égalité :

$$\tilde{g}_\tau(y) = \frac{1}{\sqrt{-i\tau}} g_{-1/\tau}(y).$$

Lorsque $\tau = it$ avec t réel positif c'est exactement le lemme 2.3. D'après le principe de zéros isolés, il suffit donc de vérifier que les deux termes de cette égalité sont des fonction holomorphes de la variable τ dans \mathbb{H} . C'est clair pour $\tau \mapsto g_{-1/\tau}(y)$ et $\tau \mapsto \sqrt{-i\tau}$ (cette dernière est une racine continue de la fonction $\tau \mapsto -i\tau$ qui n s'annule pas sur \mathbb{H}). En ce qui concerne $\tilde{g}_\tau(y)$ cela se déduit de l'holomorphie de $\tau \mapsto g_\tau(x)$ pour tout $x \in \mathbf{R}$ et de l'inégalité $|e^{\pi i\tau x^2}| \leq e^{-\pi \operatorname{Im} \tau x^2}$. □

Revenons à la preuve de la proposition 2.4. On applique l'identité de Poisson à ψ et on déduit le résultat voulu. □

2.1.3. La fonction ϑ . — Notons J le sous-groupe de $\Gamma(1)$ engendré par T^2 et S . Certains auteurs appellent J le ϑ -groupe. Notons $\vartheta : \mathbb{H} \rightarrow \mathbf{C}$ la fonction

$$\vartheta(\tau) = \Theta(0; \tau) = \sum_{n \in \mathbf{Z}} e^{i\pi\tau n^2}.$$

Elle est non identiquement nulle car $\vartheta(it) = \theta(t) > 0$ si t est un réel positif.

Corollaire 2.6. — *Il existe un unique morphisme de groupes $\chi : J \rightarrow \{\pm i, \pm 1\}$ tel que $\chi(S) = -i$, $\chi(T) = 1$. De plus, pour tout $\gamma \in J$ on a la relation :*

$$\vartheta^2[\gamma]_1 = \chi(\gamma)\vartheta^2.$$

Démonstration. — La proposition 2.4 entraîne que $\vartheta^2[S]_1 = -i\vartheta^2$ et aussi $\vartheta^2[T^2]_1 = \vartheta^2$. Autrement dit la fonction ϑ^2 est vecteur propre pour l'action de poids 1 de S et T^2 de valeurs propres respectives $-i$ et 1. Ces éléments engendrent J , et on en déduit d'une part l'existence et l'unicité de χ comme dans l'énoncé et d'autre part la seconde assertion. □

Observons que l'on a manifestement $\vartheta(2\tau) = \sum_{n \in \mathbf{Z}} q^{n^2}$ de sorte que pour tout entier $k \geq 1$ on a la relation :

$$\vartheta^k(2t) = \left(\sum_{n \in \mathbf{Z}} q^{n^2} \right)^k = \sum_{(n_1, \dots, n_k) \in \mathbf{Z}^k} q^{n_1^2 + \dots + n_k^2} = \sum_{n \in \mathbf{Z}} r_k(n) q^n$$

où $r_k(n)$ désigne le nombre de k -uples $(n_1, \dots, n_k) \in \mathbf{Z}^k$ telles que $n = \sum_{i=1}^k n_i^2$. Autrement dit comme série en t , la fonction $\vartheta^k(2t)$ n'est autre que la série génératrice du nombre de façons d'écrire un entier $n \geq 0$ comme somme de k carrés d'entiers. C'était notre point de départ et le point de départ du lien entre les formes quadratiques et les formes modulaires.

2.1.4. Les fonctions $\tilde{\vartheta}$ et $\tilde{\tilde{\vartheta}}$. — Jacobi a également introduit les fonctions $\mathbb{H} \rightarrow \mathbf{C}$

$$\begin{aligned}\tilde{\vartheta} &:= \Theta(1/2; \tau) = \sum_{n \in \mathbf{Z}} (-1)^n e^{i\pi\tau n^2} \\ \tilde{\tilde{\vartheta}} &:= e^{\frac{i\pi\tau}{4}} \Theta(\tau/2; \tau) = \sum_{n \in \mathbf{Z}} e^{i\pi\tau(n+1/2)^2} = e^{\frac{i\pi\tau}{4}} \sum_{n \in \mathbf{Z}} q^{\frac{n(n+1)}{2}}.\end{aligned}$$

On a $\theta(\tau+1) = \tilde{\vartheta}$ et $\tilde{\tilde{\vartheta}} = \frac{1}{\sqrt{-i\tau}} \theta(1-1/\tau)$. (On trouve cette dernière identité en appliquant la Proposition 2.4 à $z = 1/2$)

2.1.5. Fonctions faiblement modulaires de niveau quelconque. — La définition suivante devient maintenant naturelle :

Définition 2.7. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère. Une fonction $f : \mathbb{H} \rightarrow \mathbf{C}$ est faiblement modulaire de poids k , niveau Γ et caractère χ si

$$f[\gamma]_k(\tau) = \chi(\gamma)f(\tau), \quad \forall \gamma \in \Gamma.$$

Si χ est le caractère trivial on dit simplement que f est faiblement modulaire de poids k et niveau Γ .

Remarque 2.8. — Il est clair que si $\Gamma' \subset \Gamma$ sont deux sous-groupes de $\Gamma(1)$ et f est faiblement modulaire de poids k , niveau Γ et caractère χ alors f est aussi faiblement modulaire de poids k , niveau Γ' et caractère $\chi|_{\Gamma'}$.

Pour définir les formes modulaires, il nous reste à généraliser à niveau quelconque la condition d'holomorphicité à l'infini. Rappelons que cette condition nous avait assuré, grace au lemme $k/12$, la finitude des dimensions des espaces $M_k(\Gamma(1))$ et $S_k(\Gamma(1))$.

2.2. La géométrie des pointes. —

2.2.1. Un exemple. — Travaillons un peu autour du groupe J .

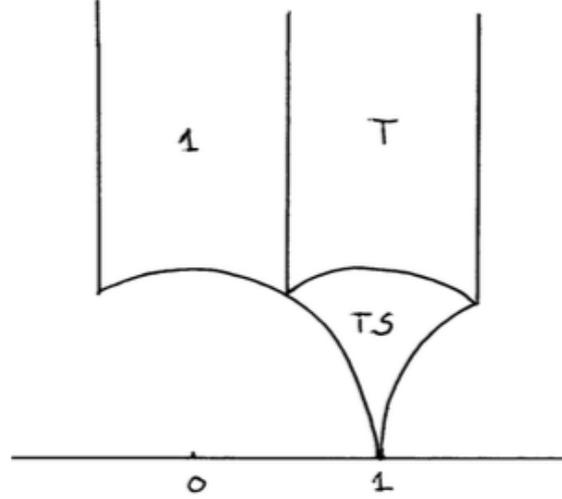
Proposition 2.9. — (1) *Les éléments $1, T$ et TS forment un système de représentants de $J \backslash \mathrm{SL}_2(\mathbf{Z})$. En particulier, J est d'indice 3 dans $\mathrm{SL}_2(\mathbf{Z})$.*

(2) *Pour tout $\tau \in \mathbb{H}$, il existe $g \in J$ tel que*

$$g\tau \in \mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}.$$

Démonstration. — Vérifions d'abord (2). Observons que $\mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}$ est l'ensemble des $\tau \in \mathbb{H}$ tels que $-1/2 \leq \mathrm{Re} \tau \leq 3/2$, $|\tau| \geq 1$ et $|\tau - 2| \geq 1$ (voir Figure 3). Comme les éléments S et ST^{-2} d'homographies associées $\tau \mapsto -1/\tau$ et $\tau \mapsto -1/(\tau - 2)$ sont dans J l'argument de maximalisé donné dans la démonstration du théorème 1.1(1) démontre le (2). Montrons maintenant (1). Choisissons un point τ dans l'intérieur de \mathcal{F} . Alors $\mathrm{Stab}_{\mathrm{SL}_2(\mathbf{Z})}(\tau) = \pm I_2$. Soit $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. D'après le (2) appliqué à $\gamma\tau$ il existe $g \in J$ tel que $g\gamma\tau$ soit dans $\mathcal{F} \cup T\mathcal{F} \cup TS\mathcal{F}$. Ainsi le théorème 1.1(3) entraîne que $\pm g\gamma$ doit être égal à I_2, T ou TS . Comme $-I_2 = S^2 \in J$ on a montré que

$$\mathrm{SL}_2(\mathbf{Z}) = J \cup JT \cup JTS$$

FIGURE 3. Le pavage de \mathbb{H} par la $\Gamma(1)$ -orbite de \mathcal{F}

Cette réunion est clairement disjointe ce qui prouve la proposition. □

Si on veut essayer d'établir un lemme similaire au lemme $k/12$, donnant lieu à la finitude de dimensions, on devrait imposer que la fonction f , pour être une forme modulaire soit, en plus de holomorphe sur \mathbb{H} et l'infini, holomorphe en la "pointe" 1. Il nous reste alors à comprendre ce qu'une "pointe" et ce que "holomorphe" voudrait dire.

Comme premier essaie vérifions d'abord si $\lim_{\tau \rightarrow 1} \vartheta^2(\tau)$ et $\lim_{\text{Im } \tau \rightarrow \infty} \vartheta^2(\tau)$ sont finies. La deuxième limite est clairement 1. Voyons la première

$$\begin{aligned}
 \lim_{\tau \rightarrow 1} \vartheta^2(\tau) &= \lim_{ST^{-1}\tau \rightarrow \infty} \vartheta^2(\tau) \\
 &= \lim_{\text{Im } \tau \rightarrow \infty} \vartheta^2(TS\tau) \\
 &= \lim_{\text{Im } \tau \rightarrow \infty} \vartheta^2(1 - 1/\tau) \\
 &= \lim_{\text{Im } \tau \rightarrow \infty} -i\tau \overset{\sim 2}{\vartheta}(\tau) \\
 &= 0.
 \end{aligned}$$

Mais définir l'holomorphie de f en la "pointe" 1 équivalent à la finitude de la limite $\lim_{\tau \rightarrow 1} f(\tau)$ pose un problème : les formes modulaires (non paraboliques) de niveau $\Gamma(1)$ ne satisferaient pas à cette condition ! En effet $\lim_{\tau \rightarrow 1} f(\tau) = \lim_{\text{Im } \tau \rightarrow \infty} f(TS\tau) = \lim_{\text{Im } \tau \rightarrow \infty} j(TS, \tau)^k f(\tau) = \infty!!$

Il vaudrait lors mieux définir l'holomorphie de f en la pointe 1 équivalent à la finitude de la limite $\lim_{\text{Im } \tau \rightarrow \infty} f[\gamma]_k(\tau)$ pour $\gamma = TS \in \text{SL}_2(\mathbf{Z})$. Ça marche pour les formes

modulaires de niveau $\Gamma(1)$ et pour ϑ :

$$\lim_{\operatorname{Im} \tau \rightarrow \infty} \vartheta^2[TS]_1(\tau) = \lim_{\operatorname{Im} \tau \rightarrow \infty} -i \tilde{\vartheta}^2(\tau) = 0.$$

Et même si $TS \notin J$ on a que $\vartheta^2[TS]_1(\tau)$ peut être développé autour de 0 en une série en $q_4 := e^{2i\pi\tau/4}$. On verra plus tard que ce sera toujours le cas.

Avant de donner la définition de forme modulaire de niveau quelconque, comprenons un peu mieux la géométrie de "pointes" et des sous-groupes de $\mathrm{SL}_2(\mathbf{Z})$ qu'on va considérer ici.

2.2.2. Sous-groupes discrets de $\mathrm{SL}_2(\mathbf{R})$. — Un élément $\gamma \in \mathrm{SL}_2(\mathbf{R})$ possède 2 valeurs propres (en comptant la multiplicité) dans \mathbf{C} . On dit que γ est

- *elliptique* si ses valeurs propres ne sont pas réelles,
- *hyperbolique* si ses valeurs propres sont réelles et distinctes,
- *parabolique* si ses valeurs propres sont égales (et donc réelles) et $\gamma \neq \pm 1$.

En raisonnant sur le polynôme caractéristique on voit que (γ elliptique) $\Leftrightarrow |\operatorname{tr}(\gamma)| < 2$, que (γ hyperbolique) $\Leftrightarrow |\operatorname{tr}(\gamma)| > 2$, et que (γ parabolique) $\Leftrightarrow (|\operatorname{tr}(\gamma)| = 2 \text{ et } \gamma \neq \pm 1)$. Ainsi un élément $\gamma \neq \pm 1$ tombe dans l'une (et une seule) des trois classes. On peut aussi caractériser cette terminologie par les points fixes de γ dans $\mathbf{P}^1(\mathbf{C})$ (voir le paragraphe 1.1).

Lemme 2.10. — *Soit $\gamma \in \mathrm{SL}_2(\mathbf{R})$.*

(1) γ est elliptique si et seulement si γ a un point fixe dans \mathbb{H} . Ce point est alors unique, et γ est conjugué dans $\mathrm{SL}_2(\mathbf{R})$ à une rotation $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in \mathrm{SO}_2(\mathbf{R})$.

(2) γ est hyperbolique si et seulement si γ a deux points fixes dans $\mathbf{P}^1(\mathbf{R})$.

(3) γ est parabolique si et seulement si γ a un unique point fixe dans $\mathbf{P}^1(\mathbf{R})$. De plus, γ est conjugué dans $\mathrm{GL}_2(\mathbf{R})$ à une matrice de la forme $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Démonstration. — (1) γ est elliptique si et seulement si, vu comme élément de $\mathrm{GL}_2(\mathbf{R})$, il est diagonalisable sur \mathbf{C} mais pas sur \mathbf{R} . Il a alors exactement 2 droites propres dans \mathbf{C}^2 et aucune dans \mathbf{R}^2 . Il ne fixe donc aucun point de $\mathbf{P}^1(\mathbf{R})$ et fixe 2 points conjugués dans $\mathbf{P}^1(\mathbf{C}) \setminus \mathbf{P}^1(\mathbf{R})$. Un et un seul de ces 2 points est donc dans \mathbb{H} . Ce point est équivalent à i sous $\mathrm{SL}_2(\mathbf{R})$, donc γ est conjugué à un élément du fixateur de i qui est $\mathrm{SO}_2(\mathbf{R})$.

(2) est clair. (3) par définition, γ est parabolique si et seulement si il est conjugué dans $\mathrm{GL}_2(\mathbf{R})$ à une matrice de la forme $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ différente de ± 1 . Comme $\det \gamma = 1$, on a $a = \pm 1$. En conjuguant par $\begin{pmatrix} 1 & 0 \\ 0 & \pm b \end{pmatrix}$ on obtient la matrice $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Celle-ci a un unique point fixe dans $\mathbf{P}^1(\mathbf{C})$, à savoir ∞ . \square

Pour tout sous-groupe Γ de $\mathrm{SL}_2(\mathbf{R})$ on note $\bar{\Gamma}$ le groupe $\Gamma/\{\pm I_2\}$ si $-I_2 \in \Gamma$, et $\bar{\Gamma} = \Gamma$ sinon.

Définition 2.11. — Un sous-groupe Γ de $\mathrm{SL}_2(\mathbf{R})$ est dit *discret* s'il est discret pour la topologie induite.

Le premier exemple est $\mathrm{SL}_2(\mathbf{Z})$, qu'on appelle *groupe modulaire* et qu'on notera aussi $\Gamma(1)$. Plus généralement, on notera pour $N \in \mathbf{N}$

$$\Gamma(N) := \ker(\mathrm{SL}_2(\mathbf{Z}) \longrightarrow \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Ce sont des sous-groupes d'indice fini de $\mathrm{SL}_2(\mathbf{Z})$ appelés *sous-groupes de congruences principale* de niveau N (voir TD pour le calcul d'indices). On a $\overline{\Gamma(2)} = \Gamma(2)/\{\pm I_2\}$ et $\overline{\Gamma(N)} = \Gamma(N)$, si $N > 2$. Aussi, si $N|N'$ on a $\Gamma(N') \subset \Gamma(N)$.

Définition 2.12. — Un sous-groupe Γ de $\mathrm{SL}_2(\mathbf{R})$ est dit *sous-groupe de congruence* s'il contient $\Gamma(N)$ pour un certain $N \geq 1$

Par exemple le ϑ -groupe J est de congruence car il contient $\Gamma(2)$ d'après le TD.

Dans ce cours, les groupes de congruence qui nous intéresseront particulièrement sont

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

On a $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$.

Il y a beaucoup d'autres exemples de sous-groupes discrets de $\mathrm{SL}_2(\mathbf{R})$ qui ne sont pas "commensurables" à $\mathrm{SL}_2(\mathbf{Z})$, au sens où $\Gamma \cap \mathrm{SL}_2(\mathbf{Z})$ n'est pas d'indice fini dans $\mathrm{SL}_2(\mathbf{Z})$ ni dans Γ . Certains, obtenus à partir d'algèbres de quaternions, jouent aussi un rôle important en théorie des nombres.

Les sous-groupes discrets de $\mathrm{SL}_2(\mathbf{R})$ commensurables à $\mathrm{SL}_2(\mathbf{Z})$ sont souvent appelés *groupes arithmétiques*. Les sous-groupes de congruence sont des sous-groupes arithmétiques mais ils sont rares parmi les groupes arithmétiques : si on note $N(m)$ le nombre de sous-groupes de congruence de $\mathrm{SL}_2(\mathbf{Z})$ d'indice $< m$ et $N'(m)$ le nombre de sous-groupes de $\mathrm{SL}_2(\mathbf{Z})$ d'indice $< m$ alors $N(m)/N'(m) \rightarrow 0$ quand $m \rightarrow \infty$. C'est une caractéristique très particulière de SL_2 . Margulis a prouvé (ce que lui a valu la médaille fields) que sous certaines faibles hypothèses (que SL_2 ne satisfait pas) tout sous-groupe discret Γ de $G(\mathbf{R})$ tel que $G(\mathbf{R})/\Gamma$ a mesure fini est un sous-groupe arithmétique et pour beaucoup de groupes on sait que tout ses sous-groupes arithmétiques sont de congruence.

Tout sous-groupe discret de $\mathrm{SL}_2(\mathbf{R})$ admet un domaine fondamental. Cela découle de l'existence d'une distance $d(\tau, \tau')$ sur \mathbb{H} qui est invariante par $\mathrm{SL}_2(\mathbf{R})$. En effet, ayant choisi un τ_0 , on peut alors prendre

$$D = \{\tau \in \mathbb{H}, \forall \gamma \in \Gamma \setminus \{\pm 1\}, d(\tau, \tau_0) < d(\tau, \gamma\tau_0)\}.$$

La distance $d(\tau, \tau')$ est la distance géodésique pour la *métrique de Poincaré* $\frac{d\tau \cdot d\bar{\tau}}{|\mathrm{Im}(\tau)|^2}$ dont on voit facilement qu'elle est invariante par $\mathrm{SL}_2(\mathbf{R})$. Pour cette métrique, les courbes géodésiques sont les demi-cercles perpendiculaires à l'axe réel et les droites verticales.

Supposons Γ un sous-groupe d'indice fini de $\Gamma(1)$. Soit $d := |\bar{\Gamma} \backslash \bar{\Gamma}(1)|$. Si on choisit $\gamma_1, \dots, \gamma_d$ tels que $\bar{\Gamma}(1) = \bigsqcup_i \bar{\Gamma} \bar{\gamma}_i$, alors la réunion $\mathcal{F}' = \gamma_1 \mathcal{F} \sqcup \dots \sqcup \gamma_d \mathcal{F}$ a toutes les vertus d'un domaine fondamental sauf celle d'être connexe. Le jeu, dans les cas concrets, consiste alors à choisir les γ_i de sorte que l'adhérence $\bar{\mathcal{F}}'$ soit connexe. Dans ce cas, l'intérieur de $\bar{\mathcal{F}}'$ est un domaine fondamental pour Γ (voir TD pour des exemples).

2.2.3. Pointes. — Un point x de $\mathbf{P}^1(\mathbf{R})$ est appelé *pointe* de Γ (en anglais, un *cusp*) s'il existe un élément parabolique de Γ qui fixe x . Dans ce cas, si on note Γ_x le fixateur de x dans Γ et si on choisit $\gamma \in \mathrm{SL}_2(\mathbf{R})$ tel que $\gamma\infty = x$, alors $\gamma^{-1}\Gamma_x\gamma$ est un sous-groupe discret du fixateur de ∞ , ce dont on déduit qu'il existe $h > 0$ tel que

$$(2.1) \quad \gamma^{-1}\Gamma_x\gamma \cdot \{\pm 1\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m, m \in \mathbf{Z} \right\}.$$

On note $P_\Gamma \subset \mathbf{P}^1(\mathbf{R})$ l'ensemble des pointes de Γ .

Exemple 2.13. — (1) $P_{\Gamma(1)} = \mathbf{P}^1(\mathbf{Q})$. En effet ∞ est le point fixé par l'élément parabolique T . Si $m/n \in \mathbf{Q}$, avec m et n premiers entre eux, alors il existe $r, s \in \mathbf{Z}$ tels que $\gamma = \begin{pmatrix} m & s \\ n & r \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, $\gamma(\infty) = m/n$ et m/n est fixé par l'élément parabolique $\gamma T \gamma^{-1}$. Réciproquement, tout élément parabolique α de $\Gamma(1)$ est conjugué à $\pm T$, disons $\alpha = \pm \gamma T \gamma^{-1}$, $\gamma \in \mathrm{GL}_2(\mathbf{Q})$. Le point fixé par α est $\gamma\infty \in \mathbf{P}^1(\mathbf{Q})$.

(2) Supposons maintenant $\Gamma \subset \Gamma(1)$ d'indice fini. Il est clair que $P_\Gamma \subset P_{\Gamma(1)} = \mathbf{P}^1(\mathbf{Q})$. Mais comme $\Gamma(1)_x$ est infini pour toute pointe $x \in \mathbf{P}^1(\mathbf{Q})$ et Γ d'indice fini, on a aussi Γ_x infini et x est donc une pointe. Donc $P_\Gamma = \mathbf{P}^1(\mathbf{Q})$. Par contre, en général il y a plusieurs Γ -orbites dans $\mathbf{P}^1(\mathbf{Q})$. Comme le stabilisateur de ∞ dans $\Gamma(1)$ est le sous-groupe engendré par T et $\pm I_2$, l'ensemble de Γ -orbites dans $\mathbf{P}^1(\mathbf{Q})$ s'identifie à $\Gamma \backslash \Gamma(1) / \langle T, \pm I_2 \rangle$.

En particulier, d'après la proposition 2.9, J n'a que deux pointes, les classes de ∞ et 1.

2.3. Formes modulaires de niveau quelconque : définition et propriétés. — Dans ce cours on va se contenter de travailler le cas où $\Gamma \subset \Gamma(1)$ est d'indice fini. Le plus souvent on supposera aussi que Γ est un sous-groupe de congruence.

En tâtonnant on trouve donc la définition suivante.

Définition 2.14. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe d'indice fini et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère. Soit $f : \mathbb{H} \rightarrow \mathbf{C}$ une fonction faiblement modulaire de poids k , niveau Γ et caractère χ . Soit $\alpha = \gamma_0\infty$ une pointe de Γ , $\gamma_0 \in \mathrm{SL}_2(\mathbf{Z})$. On dit que f est holomorphe en α si $f[\gamma_0]_k(\tau)$ admet une limite finie quand $\mathrm{Im} \tau \rightarrow \infty$. On note (avec précaution !) cette limite $f(\alpha)$.

On définit enfin :

Définition 2.15. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe d'indice fini et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère. Une forme modulaire de poids k , niveau Γ et caractère χ est une fonction holomorphe $f : \mathbb{H} \rightarrow \mathbf{C}$ telle que :

- (1) f est faiblement modulaire de poids k , niveau Γ et caractère χ .

(2) f est holomorphe aux pointes de Γ ou de façon équivalente si $f[\gamma_0]_k(\tau)$ admet une limite finie quand $\text{Im } \tau \rightarrow \infty$ pour tout $\gamma_0 \in \text{SL}_2(\mathbf{Z})$.

On note $M_k(\Gamma, \chi)$ le sous-espace vectoriel de $\mathcal{O}(\mathbb{H})$ des formes modulaires de poids k , niveau Γ et caractère χ . Si χ est le caractère trivial on dit simplement que f est une forme modulaire de poids k et niveau Γ et on note $M_k(\Gamma)$ le sous-espace vectoriel de $\mathcal{O}(\mathbb{H})$ formé des formes modulaires de poids k et niveau Γ .

Remarque 2.16. — (1) Si $\Gamma' \subset \Gamma$ sont deux sous-groupes d'indice fini de $\Gamma(1)$ et f est une forme modulaire de poids k , niveau Γ et caractère χ alors f est aussi une forme modulaire de poids k , niveau Γ' et caractère χ .

(2) Soit $f \in M_k(\Gamma, \chi)$. La relation $f[-I_2]_k = (-1)^k \chi(-I_2) f$ montre que si $-I_2 \in J$, alors $M_k(\Gamma, \chi) = 0$ si $(-1)^k \neq \chi(-I_2)$.

(3) Si $f \in M_k(\Gamma, \chi)$ et $f' \in M_k(\Gamma, \chi')$ alors le produit $ff' \in M_{k+k'}(\Gamma, \chi\chi')$ et donc l'espace

$$M(\Gamma) = \bigoplus_{k \in \mathbf{Z}} M_k(\Gamma)$$

a une structure de \mathbf{C} -algèbre graduée.

(4) Il suffit de vérifier la condition d'holomorphie de pointes dans chaque Γ -classe. En effet, $f[\gamma_0]_k(\tau)$ ne dépend que de la classe de γ_0 dans $\Gamma \backslash \text{SL}_2(\mathbf{Z})$ et donc en particulier si $\gamma \in \Gamma$ et $\gamma_0 \in \text{SL}_2(\mathbf{Z})$, $f[\gamma_0]_k(\tau)$ admet une limite finie quand $\text{Im } \tau \rightarrow \infty$ si et seulement si $f[\gamma\gamma_0]_k(\tau)$ admet une limite finie quand $\text{Im } \tau \rightarrow \infty$.

Définition 2.17. — Soit $f \in M_k(\Gamma, \chi)$. On dit que f est une forme parabolique si la limite de $f[\gamma_0]_k(\tau)$ quand $\text{Im } \tau \rightarrow \infty$ vaut 0 pour tout $\gamma_0 \in \text{SL}_2(\mathbf{Z})$. On note $S_k(\Gamma, \chi)$ l'espace de telles fonctions.

Comme dans le cas de formes modulaires de niveau $\Gamma(1)$ on voudrait développer nos formes modulaires en série de Fourier pour vérifier l'holomorphie aux pointes. Plus précisément on voudrait développer en série de Fourier $f[\gamma_0]_k(\tau)$ pour tout $\gamma_0 \in \text{SL}_2(\mathbf{Z})$.

Proposition 2.18. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe d'indice fini et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère d'image finie. Soit f une fonction faiblement modulaire de poids k , niveau Γ et caractère χ . Soit $\gamma_0 \in \Gamma(1)$. Alors il existe $h \in \mathbf{N}$ (dépendant de γ_0) tel que $f[\gamma_0]_k(\tau + h) = f[\gamma]_k(\tau)$ pour tout $\tau \in \mathbb{H}$.

Démonstration. — Si on note χ^{γ_0} le caractère de $\gamma_0^{-1}\Gamma\gamma_0$, $\gamma_0^{-1}\gamma\gamma_0 \mapsto \chi(\gamma)$ on a que $f[\gamma_0]_k$ est une fonction faiblement modulaire de poids k , niveau $\gamma_0^{-1}\Gamma\gamma_0$ et caractère χ^{γ_0} . Il suffit donc de montrer la proposition pour $\gamma_0 = I_2$. Puisque $\Gamma \subset \Gamma(1)$ est un sous-groupe d'indice fini, on a que $\langle T \rangle \cap \Gamma \neq I_2$. Aussi, puisque $\chi : \Gamma \rightarrow \mathbf{C}^\times$ est un caractère d'image finie, il existe k tel que $T^k \in \Gamma$ et $\chi(T^k) = 1$. La proposition en découle. \square

Corollaire 2.19. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe d'indice fini et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère d'image finie. Soit $f \in M_k(\Gamma)$. Pour tout $\gamma_0 \in \text{SL}_2(\mathbf{Z})$, la forme $f[\gamma_0]_k$

admet un unique développement

$$f[\gamma_0]_k(\tau) = \sum_{n \geq 0} a_n(f) q_h^n$$

avec, $q_h = e^{2\pi i \tau / h}$ et $a_n(f) \in \mathbf{C}$ pour tout entier $n \geq 0$ normalement convergent sur toute partie de \mathbb{H} de la forme $\text{Im } \tau > A$, $A \in \mathbf{R}_{>0}$. Ce développement est appelé développement de Fourier, ou q_h -développement, de la forme f et les $a_n(f)$ sont ses coefficients de Fourier. On a $a_0(f)$ est la limite de $f[\gamma_0]_k(\tau)$ quand $\text{Im } \tau \rightarrow \infty$.

Si on lâche un peu la contrainte de holomorphicité sur les formes modulaires on à nouveau a la définition suivante.

Définition 2.20. — Soient $k \in \mathbf{Z}$, $\Gamma \subset \Gamma(1)$ un sous-groupe d'indice fini et $\chi : \Gamma \rightarrow \mathbf{C}^\times$ un caractère d'image finie. Une fonction modulaire de poids k , de niveau Γ et caractère χ est une fonction méromorphe $f : \mathbb{H} \rightarrow \mathbf{C}$ telle que :

- (1) f est faiblement modulaire de poids k , de niveau Γ et caractère χ .
- (2) Pour tout $\gamma_0 \in \text{SL}_2(\mathbf{Z})$, la fonction $f[\gamma_0]_k$ est méromorphe à l'infini, c'est-à-dire, elle admet un q_h -développement de la forme $f[\gamma_0]_k(\tau) = \sum_{n \in \mathbf{Z}} a_n(f) q_h^n$, avec $h \geq 1$ et $a_n = 0$ si $n \ll 0$.

Remarque 2.21. — On verra plus tard que la définition de méromorphité ci-dessus devient naturelle du point de vue géométrique.

Proposition 2.22. — Soit Γ d'indice fini m dans $\text{SL}_2(\mathbf{Z})$ et χ un caractère d'image finie. On a :

$$\dim M_k(\Gamma, \chi) \leq \frac{km}{12} + 1$$

pour tout entier $k \geq 0$. En particulier $M_0\Gamma = \mathbf{C}$. De plus on a $M_k(\Gamma, \chi) = 0$ si $k < 0$.

Démonstration. — Commençons par quelques remarques. Si χ est d'image finie on note e son ordre, c'est-à-dire, le plus petit entier $e \geq 1$ tel que $\chi^e = 1$. Tout-sous-groupe fini de \mathbf{C}^\times étant cyclique on a bien $e = |\chi(\Gamma)|$. De la remarque 2.16(3), on déduit que si $M_k(\Gamma, \chi)$ alors $f^e \in M_{ke}(\Gamma)$. Comme $f[\gamma]_k$ ne dépend que de la classe de $\bar{\gamma}$ de γ dans $\Gamma \backslash \text{SL}_2(\mathbf{Z})$, nous la noterons $f[\bar{\gamma}]_k$. En particulier, si $f \in M_k(\Gamma)$ il y a un sens à poser

$$\text{Norme } f = \prod_{\bar{\gamma} \in \Gamma \backslash \text{SL}_2(\mathbf{Z})} f[\bar{\gamma}]_k.$$

Lemme 2.23. — Supposons Γ d'indice fini m dans $\text{SL}_2(\mathbf{Z})$, $k \in \mathbf{Z}$, $f \in M_k(\Gamma)$. Alors $\text{Norme } f \in M_{km}(\Gamma(1))$. De plus $\text{Norme } f = 0$ si et seulement si $f = 0$.

Démonstration. — $\text{Norme } f$ est une fonction holomorphe sur \mathbb{H} , qui admet une limite finie quand $\text{Im } \tau \rightarrow \infty$ par hypothèse sur f . Si $\gamma \in \text{SL}_2(\mathbf{Z})$, la multiplication à droite par γ sur l'ensemble fini $\Gamma \backslash \text{SL}_2(\mathbf{Z})$ est bien entendu une bijection de sorte que $(\text{Norme } f)[\gamma]_{mk} = \text{Norme } f$. On a montré $\text{Norme } f \in M_{km}(\Gamma(1))$. Par intégrité de l'anneau des fonctions

holomorphes sur le connexe \mathbb{H} (ie par le principe des zéros isolés), Norme $f = 0$ entraîne qu'il existe $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ telle que $f[\gamma]_k = 0$ ce qui implique que $f = (f[\gamma]_k)[\gamma]_k^{-1} = 0$. \square

Terminons la preuve de la proposition 2.22. Soit N un entier positif tel que $N > \frac{mk}{12}$. Soit $\mathcal{P} \subset \mathrm{int}\mathcal{F}$ un sous-ensemble fini de cardinal N . Considérons l'application linéaire

$$\begin{aligned} M_k(\Gamma, \chi) &\rightarrow \mathbf{C}^N \\ f &\mapsto (f(p))_{p \in \mathcal{P}}. \end{aligned}$$

Il suffit de démontrer qu'elle est injective pour déduire la proposition. Soient f dans son noyau et e l'ordre de χ . Alors la fonction $g = \mathrm{Norme} f^e$ est dans $M_{ekm}(\Gamma(1))$. De plus, g est le produit de f^e par une fonction holomorphe, et s'annule donc en chacun des N points de \mathcal{P} avec un ordre d'annulation $\geq e$. La formule $k/12$, appliquée à la forme g de poids ekm , montre donc que $g = \mathrm{Norme} f^e = 0$ puis $f^e = f = 0$. \square

Remarque 2.24. — On verra plus tard, à l'aide du théorème de Riemann-Roch, le calcul exact de dimension des espaces $M_k(\Gamma)$.

Remarque 2.25. — Une autre conséquence est que trois formes modulaires quelconques f, g, h sont toujours algébriquement dépendantes. Sinon pour $k \gg 0$ la dimension de $M_k(\Gamma)$ serait au moins le nombre de monômes en f, g, h de poids total k , ce qui est plus grand qu'un multiple positif de k^2 , et qui contredit la proposition. De façon équivalente deux fonctions modulaires quelconques de niveau Γ sont algébriquement dépendantes puisque chaque fonction modulaire est un quotient de formes modulaires. C'est un cas particulier du fait que dans une variété algébrique de dimension n on ne peut pas avoir plus que n fonctions algébriques algébriquement indépendantes.

Mais une conséquence très pratique est la suivante : imaginez qu'on dispose deux suites $\{a_n\}$ et $\{b_n\}$ et que l'on veut montrer qu'elles sont égales. Si l'on arrive à montrer que les séries $\sum a_n q^n$ et $\sum b_n q^n$ sont des formes modulaires de même niveau et même poids, il suffit alors de montrer que $a_n = b_n$ pour un nombre fini de n pour avoir l'égalité $a_n = b_n$ pour tout $n \in \mathbf{N}$!

2.4. Exemples. —

2.4.1. Les fonctions $\vartheta, \tilde{\vartheta}$ et $\tilde{\tilde{\vartheta}}$. — Reprenant les calculs qu'on avait faits au paragraphe 2.1, on déduit la proposition suivante :

Proposition 2.26. — On a $\vartheta^2 \in M_1(J, \chi)$. De plus $\vartheta^2(\infty) = 1$ et $\vartheta^2(1) = 0$. Plus précisément $\vartheta^2[TS]_1(\tau) = -i\tilde{\tilde{\vartheta}}^2(\tau)$.

Corollaire 2.27. —

- (1) On a $\vartheta^{2k} \in M_k(J, \chi^k)$.
- (2) (Jacobi) On a l'identité :

$$(\vartheta\tilde{\tilde{\vartheta}})^8 = 2^8 \Delta.$$

Démonstration. — (1) est clair. Montrons (2). On a $\vartheta[T]_1 = \tilde{\vartheta}$ et $\vartheta^2[TS]_1(\tau) = -i\tilde{\vartheta}^2(\tau)$. On déduit que $(\vartheta\tilde{\vartheta})^8 = \text{Norme } \vartheta^8 \in M_{12}(\Gamma(1))$. De plus $(\vartheta\tilde{\vartheta})^8(\infty) = 0$ donc $(\vartheta\tilde{\vartheta})^8 = \text{Norme } \vartheta^8 \in S_{12}(\Gamma(1))$ et elle est de la forme $c\Delta$. On calcule c à la main et on trouve $c = 2^8$. \square

Remarque 2.28. — $\vartheta^2, \vartheta^4, \vartheta^6$ appartiennent donc à des espace vectoriel de dimension 1, et ϑ^8 à un espace vectoriel de dimension au plus 2. Nous devons construire d'autres formes modulaires !

On en a déjà certaines. Les formes modulaires de niveau $\Gamma(1)$ sont aussi de niveau Γ pour tout $\Gamma \subset \Gamma(1)$.

2.4.2. Séries de Poincaré. — Nous présentons ici une méthode générale pour fabriquer des formes modulaires de niveau Γ . La façon standard pour construire de fonctions Γ -invariantes à partir d'une fonction quelconque f est de construire la somme

$$\sum_{\gamma \in \Gamma} f(\gamma x).$$

Le problème est que le plus souvent cette somme ne converge pas !

Pour construire une forme modulaire de niveau γ une idée naïve serait alors de partir d'une fonction quelconque f et de fabriquer la série $\varphi(\tau) = \sum_{\gamma \in \Gamma} f(\gamma\tau)/j(\gamma, \tau)^k$. La formule $j(\gamma\gamma', \tau) = j(\gamma, \gamma'\tau)j(\gamma', \tau)$ montre qu'une telle fonction serait bien faiblement modulaire de poids k pour Γ . Le problème est qu'une telle série ne peut pas converger car, par exemple, $j(\gamma, \tau) = 1$ pour une infinité de γ . Justement, pour contourner le problème, notons

$$\Gamma_{\infty}^+ := \{\gamma \in \Gamma, j(\gamma, \tau) = 1\} = \Gamma \cap \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbf{Z} \right\} = \Gamma \cap \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right)^{\mathbf{Z}},$$

un sous-groupe d'indice 1 ou 2 dans Γ_{∞} (le fixateur de ∞ dans Γ), et partons d'une fonction f qui est déjà invariante par Γ_{∞}^+ . Alors la fonction $\varphi(\tau) = \sum_{\gamma \in \Gamma_{\infty}^+ \setminus \Gamma} f(\gamma\tau)/j(\gamma, \tau)^k$ a plus de chance de converger (absolument), et dans ce cas elle serait encore faiblement modulaire de poids k . Dans cette somme, γ décrit un ensemble de représentants des classes à gauche selon Γ_{∞}^+ dans Γ .

Soit h tel que $\Gamma_{\infty}^+ = \left(\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right)^{\mathbf{Z}}$. Des exemples typiques de fonctions holomorphes f invariantes sous Γ_{∞}^+ sont les $f(\tau) = \exp(2i\pi n\tau/h)$, $n \in \mathbf{Z}$.

Proposition 2.29. — *La série de Poincaré de poids $k \geq 3$ et "caractère" $n \in \mathbf{N}$*

$$\varphi_n(\tau) := \sum_{\gamma \in \Gamma_{\infty}^+ \setminus \Gamma} j(\gamma, \tau)^{-k} \exp(2i\pi n\gamma\tau/h)$$

définit une forme modulaire $\varphi_n \in M_k(\Gamma)$. De plus :

- (1) Si $n > 0$, $\varphi_n \in S_k(\Gamma)$.

(2) Pour $n = 0$, φ_0 s'annule à toutes les pointes $x \neq \infty$ et on a

$$\varphi_0(\infty) = \begin{cases} [\Gamma_\infty^+ \setminus \Gamma_\infty] & \text{si } k \text{ est pair ou } \Gamma_\infty^+ = \Gamma_\infty \\ 0 & \text{sinon} \end{cases}$$

Remarque 2.30. — On verra plus tard que, avec certaines hypothèses, les séries de Poincaré engendrent $M_k(\Gamma)$.

Démonstration. — Pour trouver un ensemble agréable de représentants de $\Gamma_\infty^+ \setminus \Gamma$, partons de l'égalité $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + mc & b + md \\ c & d \end{pmatrix}$. Elle nous dit que $\gamma' \in \Gamma_\infty^+ \gamma \Rightarrow (a', b') \equiv (a, b) \pmod{h}$. Réciproquement, si γ' vérifie $(a', b') \equiv (a, b) \pmod{h}$ et $(c', d') = (c, d)$, alors la condition de déterminant $\det \gamma = \det \gamma' = 1$ implique $a - a' = cm$ et $b - b' = dm$ avec $h|m$, donc implique $\gamma' \in \Gamma_\infty^+ \gamma$. Finalement, on voit que pour tout $(c, d) \in \mathbf{Z}^2$ il existe au plus h^2 classes d'éléments $\gamma_{c,d} \in \Gamma_\infty^+ \setminus \Gamma$ dont la deuxième ligne est (c, d) .

Il s'ensuit que $\sum_{\Gamma_\infty^+ \setminus \Gamma} |j(\gamma, \tau)^{-k} \exp(2i\pi n \gamma \tau / h)| \leq \sum_{(c,d) \neq (0,0)} h^{-2} \frac{1}{|c\tau + d|^k}$ dont on a vu qu'elle converge uniformément sur un domaine fondamental dès que $k \geq 3$. On en déduit la convergence normale sur les domaines fondamentaux (et donc sur les compacts) de la série de Poincaré et donc son holomorphicité sur \mathbb{H} .

Pour $\alpha \in \mathrm{SL}_2(\mathbf{Z})$, et $\mu_h = e^{2\pi i/h}$ la formule

$$\begin{aligned} \varphi_n(\alpha\tau) &= \sum_{\gamma \in \Gamma_\infty^+ \setminus \Gamma} j(\gamma, \alpha\tau)^{-k} \mu_h^{n\gamma\alpha\tau} = j(\alpha, \tau)^k \sum_{\gamma \in \Gamma_\infty^+ \setminus \Gamma} j(\gamma\alpha, \tau)^{-k} \mu_h^{n\gamma\alpha\tau} \\ &= j(\alpha, \tau)^k \sum_{\gamma \in \Gamma_\infty^+ \setminus \Gamma\alpha} j(\gamma, \tau)^{-k} \mu_h^{n\gamma\tau}. \end{aligned}$$

montre, d'un côté, lorsqu'on prend $\alpha \in \Gamma$ que φ_n est bien faiblement modulaire de poids k et niveau Γ .

D'un autre côté, puisque $j(\gamma, \tau)^{-k} \rightarrow 0$ lorsque $\mathrm{Im}(\tau) \rightarrow \infty$ et $\gamma \notin \Gamma(1)_\infty$, la convergence normale sur un domaine fondamental nous donne aussi pour $\alpha \in \Gamma(1)$

$$\lim_{\mathrm{Im}(\tau) \rightarrow \infty} \varphi_n[\alpha]_k(\tau) = \sum_{\gamma \in \Gamma_\infty^+ \setminus (\Gamma\alpha \cap \Gamma(1)_\infty)} \lim_{\mathrm{Im}(\tau) \rightarrow \infty} (j(\gamma, \tau)^{-k} \cdot \exp(2i\pi n \gamma \tau / h)).$$

La somme qui apparait ici est finie et on en déduit que $\varphi_n|_k \alpha$ est holomorphe en ∞ ce qui équivaut à dire que φ_n est holomorphe en la pointe $x = \alpha\infty$. Distinguons deux cas.

Si la pointe x n'est pas Γ -équivalente à ∞ , c'est-à-dire si $\infty \notin \Gamma x$, alors $\Gamma\alpha \cap \Gamma(1)_\infty = \emptyset$ donc la somme ci-dessus est trivialement nulle pour tout $n \geq 0$.

En la pointe ∞ , on peut prendre $\alpha = 1$ et on s'aperçoit que la limite ci-dessus est nulle si $n > 0$ tandis qu'on obtient la formule de l'énoncé pour $\varphi_0(\infty)$, puisqu'ici $j(\gamma, \tau) = -1$ si $\gamma \in \Gamma_\infty \setminus \Gamma_\infty^+$ et $j(\gamma, \tau) = 1$ pour $\gamma \in \Gamma_\infty^+$. \square

2.4.3. Lien avec les séries d'Eisenstein. — Supposons $\Gamma = \Gamma(1)$ (et donc k pair) et $n = 0$. Comme dans la preuve précédente, on peut prendre des représentants de $\Gamma(1)_\infty^+ \backslash \Gamma(1)$ de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où (c, d) décrit l'ensemble des lignes possibles pour une matrice dans $\Gamma(1)$, c'est-à-dire tous les (c, d) dont le pgcd vaut 1. On a donc

$$\varphi_0(\tau) = \sum_{\gamma \in \Gamma(1)_\infty^+ \backslash \Gamma(1)} j(\gamma, \tau)^{-k} = \sum_{\text{pgcd}(c,d)=1} \frac{1}{(c\tau + d)^k}.$$

La ressemblance avec G_k n'est pas parfaite, mais on peut réarranger G_k comme on l'a vu en TD :

$$G_k(\tau) = \sum_{(c,d) \neq (0,0)} \frac{1}{(c\tau + d)^k} = \sum_{n=1}^{\infty} \sum_{\text{pgcd}(c,d)=1} \frac{1}{(cn\tau + dn)^k} = \sum_{n=1}^{\infty} \frac{1}{n^k} \sum_{\text{pgcd}(c,d)=1} \frac{1}{(c\tau + d)^k}$$

pour obtenir que $G_k(\tau) = \zeta(k)\varphi_0(\tau)$ et finalement $\varphi_0(\tau) = 2E_k(\tau)$.

2.4.4. Séries d'Eisenstein pour $\Gamma(N)$. — Supposons Γ distingué dans $\Gamma(1)$. On suppose aussi $\Gamma_\infty^+ = \Gamma_\infty$ si k est impair de sorte que $\phi_0(\infty) \neq 0$. On pense par exemple à $\Gamma = \Gamma(N)$ (avec k pair si $N \leq 2$).

Pour tout $\alpha \in \Gamma(1)$, la fonction $\varphi_0[\alpha]_k$ est dans $M_k(\alpha^{-1}\Gamma\alpha) = M_k(\Gamma)$ et s'annule, par hypothèse, à toutes les pointes sauf $x := \alpha^{-1}\infty$. Si α' est un autre élément de $\Gamma(1)$ tel que $x = \alpha'^{-1}\infty$, alors il existe $\sigma \in \Gamma(1)_\infty$ tel que $\alpha' = \sigma\alpha$ et on calcule, grâce à $j(\sigma\gamma, \tau) = j(\sigma, \gamma\tau)j(\gamma, \tau) = j_\sigma \cdot j(\gamma, \tau)$ où $j_\sigma = \pm 1$ (selon que $\sigma \in \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\mathbf{Z}}$),

$$\varphi_0[\alpha']_k(\tau) = \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma\alpha'} j(\gamma, \tau)^{-k} = \sum_{\gamma \in \Gamma_\infty^+ \backslash \sigma\Gamma\alpha} j(\gamma, \tau)^{-k} = j_\sigma^{-k} \varphi_0[\alpha]_k(\tau)$$

ce qui montre que $\varphi_0[\alpha]_k$ ne dépend que de la classe de α dans $\Gamma \backslash \Gamma(1) / \Gamma(1)_\infty^+$ lorsque k est impair, et que de la classe de α dans $\Gamma \backslash \Gamma(1) / \Gamma(1)_\infty$, c'est-à-dire de la pointe x , lorsque k est pair. Si on impose en plus à $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la condition $d > 0$, alors $\varphi_0[\alpha]_k$ ne dépend que de la pointe x pour tout k , et on peut lui associer la "série d'Eisenstein"

$$E_k^x := [\Gamma_\infty : \Gamma_\infty^+]^{-1} \cdot \varphi_0[\alpha]_k$$

Puisque E_k^x ne s'annule pas en x et s'annule aux autres pointes, la famille $(E_k^x)_{x \in \Gamma \backslash \mathbf{P}^1(\mathbf{Q})}$ est libre dans $M_k(\Gamma)$.

Lorsque $\Gamma = \Gamma(N)$, deux pointes $x = r/t$ et $x' = r'/t'$ (où $\text{pgcd}(r,t) = 1$ et $t, t' > 0$) sont équivalentes si et seulement si $(r, t) \equiv (r', t')[N]$ (exercice). On calcule alors que

$$E_k^x(\tau) = \sum_{\substack{\text{pgcd}(c,d)=1 \\ (c,d) \equiv (t,-r)[N]}} \frac{1}{(c\tau + d)^k},$$

de sorte que la somme $\sum_x E_k^x$ est la série d'Eisenstein E_k pour $\Gamma(1)$. Cela suggère d'indexer les séries d'Eisenstein par un vecteur ligne $\bar{v} \in \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ d'ordre N . On peut alors

poser

$$E_k^{\bar{v}}(\tau) = \epsilon_N \sum_{\substack{\text{pgcd}(c,d)=1 \\ (c,d) \equiv \bar{v}[N]}} \frac{1}{(c\tau + d)^k}, \quad \text{et} \quad G_k^{\bar{v}}(\tau) := \sum_{(c,d) \equiv \bar{v}[N]} \frac{1}{(c\tau + d)^k},$$

avec $\epsilon_N = 1/2$ si $N = 1, 2$ (et donc k pair) et 1 si $N > 2$. Un calcul similaire au cas $\Gamma(1)$ (voir TD) montre la formule

$$G_k^{\bar{v}}(\tau) = \epsilon_N \sum_{n \in \mathbf{Z}/N\mathbf{Z}^\times} \zeta_{n,N}(k) E_k^{n\bar{v}}(\tau) \quad \text{avec} \quad \zeta_{n,N}(k) = \sum_{\substack{m=1 \\ m \equiv n[N]}}^{\infty} \frac{1}{m^k}.$$

la fonction ζ de Riemann modifiée (essentiellement la fonction ζ de Hurwitz).

Théorème 2.31. — Soient $N \geq 1$ et $k \geq 3$ deux entiers. On suppose k pair si $N \leq 2$.

(1) Pour tout vecteur $\bar{v} = (c_v, d_v) \in \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ d'ordre N , on a $E_k^{\bar{v}}(\tau), G_k^{\bar{v}}(\tau) \in M_k(\Gamma(N))$.

(2) Les familles $\{E_k^{\bar{v}}(\tau)\}$ et les $\{G_k^{\bar{v}}(\tau)\}$ (quand \bar{v} parcourt l'ensemble de vecteurs ligne $\bar{v} \in \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ d'ordre N modulo la relation $\bar{v} \sim \bar{w} \Leftrightarrow \bar{v} \equiv \pm \bar{w}[N]$) sont libres.

(3) Soit $\bar{v} = (c_v, d_v) \in \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ d'ordre N . Le développement de Fourier de $G_k^{\bar{v}}(\tau)$ est :

$$G_k^{\bar{v}}(\tau) = \delta_{\bar{c}_v, \bar{0}} \zeta_{d_v, N}(k) + \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sigma_{k-1}^{\bar{v}}(n) q_N^n, \quad q_N = e^{2\pi i \tau / N},$$

où

$$\delta_{\bar{c}_v, \bar{0}} = \begin{cases} 1 & \text{si } c_v \equiv 0[N] \\ 0 & \text{si } c_v \not\equiv 0[N], \end{cases} \quad \zeta_{d_v, N}(k) = \sum_{\substack{m=1 \\ m \equiv d_v[N]}}^{\infty} \frac{1}{m^k},$$

et

$$C_k = \frac{(-2\pi i)^k}{(k-1)!}, \quad \sigma_{k-1}^{\bar{v}}(n) = \sum_{\substack{n/m \equiv c_v[N] \\ m|n}} \text{sgn}(m) m^{k-1} \mu_N^{d_v m}, \quad \mu_N = e^{2\pi i / N}.$$

Les sommes pour $\zeta_{d_v, N}(k)$ et $\sigma_{k-1}^{\bar{v}}(n)$ portent sur des entiers non nuls (positifs ou négatifs).

Démonstration. — On a déjà montré (1). On a aussi vu que la famille $\{E_k^{\bar{v}}(\tau)\}$ est libre. On a vu en TD que la famille $\{G_k^{\bar{v}}(\tau)\}$ est aussi libre, ce qui achève la preuve de (2).

Montrons (3). On sépare la somme définissant $G_k^{\bar{v}}(\tau)$ en trois parties :

$$G_k^{\bar{v}}(\tau) := \sum_{(c,d) \equiv \bar{v}[N]} \frac{1}{(c\tau + d)^k} = A + B^+ + B^-$$

avec

$$A = \sum_{\substack{(c,d) \equiv \bar{v}[N] \\ c=0}} \frac{1}{(c\tau + d)^k}, \quad B^\pm = \sum_{\substack{(c,d) \equiv \bar{v}[N] \\ \pm c > 0}} \frac{1}{(c\tau + d)^k}.$$

On a clairement $A = \delta_{\bar{c}_v, \bar{0}} \zeta_{d_v, N}(k)$. On va utiliser la résultat suivant du TD:

$$(2.2) \quad \sum_{d \in \mathbf{Z}} \frac{1}{(\tau + d)^k} = C_k \sum_{m=1}^{\infty} m^{k-1} q^m, \quad \text{si } \tau \in \mathbb{H} \text{ et } k \geq 2.$$

Alors

$$B^{\pm} = \frac{1}{N^k} \sum_{\substack{c \equiv c_v [N] \\ \pm c > 0}} \sum_{d \in \mathbf{Z}} \frac{1}{\left(\frac{c\tau + d_v}{N} + d\right)^k}.$$

Si $c > 0$ alors $\frac{c\tau + d_v}{N} \in \mathbb{H}$ et (2.2) nous donne

$$B^+ = \frac{C_k}{N^k} \sum_{\substack{c \equiv c_v [N] \\ c > 0}} \sum_{m=1}^{\infty} m^{k-1} \mu_N^{d_v m} q_N^{cm} = \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sum_{\substack{m|n \\ n/m \equiv c_v [N] \\ m > 0}} m^{k-1} \mu_N^{d_v m} q_N^n.$$

Si $c < 0$ alors $-\frac{c\tau + d_v}{N} \in \mathbb{H}$ et (2.2) nous donne

$$B^- = (-1)^k \frac{C_k}{N^k} \sum_{\substack{c \equiv c_v [N] \\ c < 0}} \sum_{m=1}^{\infty} m^{k-1} \mu_N^{-d_v m} q_N^{-cm} = \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sum_{\substack{m|n \\ n/m \equiv c_v [N] \\ m < 0}} -m^{k-1} \mu_N^{d_v m} q_N^n.$$

On conclut mettant toutes ces identités bout à bout. \square

2.4.5. Somme de huit carrés. — On rappelle qu'on a $\vartheta^8(2\tau) = \sum r_8(n)q^n$ où $r_8(n)$ denote le nombre de $(n_1, \dots, n_8) \in \mathbf{Z}^8$ tels que $\sum_{i=1}^8 n_i^2 = n$. On a aussi vu que $\vartheta^8(2\tau) \in M_4(J)$ et la dimension ce dernier espace est au plus égal à 2. On sait que $\Gamma(2)$ est contenu dans J (on a $J = \Gamma(2) \sqcup S\Gamma(2)$), $E_4 \in M_4(J)$ et $G_4^{(0,1)}, G_4^{(1,0)}, G_4^{(1,1)} \in M_4(\Gamma(2))$.

Etant donné un sous-groupe de congruence $\Gamma(N) \subset \Gamma$, en choisissant des représentants $\Gamma = \sqcup_{1 \leq i \leq r} \gamma_i \Gamma(N)$ on a

$$E_{k, \Gamma}^{\bar{v}} = \sum_{1 \leq i \leq r} E_k^{\bar{v}}[\gamma_i]_k = \sum_{1 \leq i \leq r} E_k^{\bar{v}\gamma_i} \in M_k(\Gamma).$$

Ce faisant ou bien avec un simple calcul, on voit que en fait $G_4^{(1,1)} \in M_4(J)$. Puisque $G_4^{(1,1)}(\infty) = 0$ on déduit que $\dim(M_4(J)) = 2$ et il est engendré par E_4 et $G_4^{(1,1)}$. Les développement de Fourier :

$$\begin{aligned} E_4 &= 1 + 240q + \dots \\ G_4^* &:= \frac{2^5}{C_4} G_4^{(1,1)} = -2q^{\frac{1}{2}} + \dots \\ \vartheta^8 &= 1 + 16q^{\frac{1}{2}} + \dots \end{aligned}$$

nous montrent alors que

$$(2.3) \quad \vartheta^8 = E_4 - 8G_4^*.$$

Corollaire 2.32. — On a :

$$r_8(n) = 16 \sum_{\substack{d>0 \\ d|n}} (-1)^{n-d} d^3.$$

Démonstration. — L'identité (2.3) se traduit par

$$r_8(n) = 240\sigma_3\left(\frac{n}{2}\right) - 8\sigma_3^{(1,1)}(n),$$

où $\sigma_3\left(\frac{n}{2}\right) = 0$ si n est impair et

$$\sigma_3^{(1,1)}(n) = \sum_{\substack{n/d \equiv 1[2] \\ d \in \mathbf{Z}, d|n}} \operatorname{sgn}(d) d^3 (-1)^d.$$

Si n est impair on a donc

$$r_8(n) = -8\sigma_3^{(1,1)}(n) = 16\sigma_3(n) = 16 \sum_{\substack{d>0 \\ d|n}} (-1)^{n-d} d^3.$$

Si n est pair on utilise la relation évidente $16\sigma_3\left(\frac{n}{2}\right) = 2 \sum_{2|d|n} d^3$ pour montrer :

$$\begin{aligned} r_8(n) &= 16\left(15\sigma_3\left(\frac{n}{2}\right) - \sum_{\substack{n/d \equiv 1[2] \\ d>0, d|n}} d^3 (-1)^d\right) \\ &= 16\left(2 \sum_{2|d|n} d^3 - \sigma_3\left(\frac{n}{2}\right) - \sum_{\substack{n/d \equiv 1[2] \\ d>0, d|n}} d^3 (-1)^d\right) \\ &= 16\left(2 \sum_{2|d|n} d^3 - \sigma_3(n)\right) \\ &= 16 \sum_{\substack{d>0 \\ d|n}} (-1)^{n-d} d^3. \end{aligned}$$

□

2.5. Produit scalaire de Petersson. — On rappelle que \mathbb{H} possède une mesure invariante sous $\mathrm{SL}_2(\mathbf{R})$, dite “mesure de Poincaré”, et donnée par $d\mu(\tau) = \frac{1}{y^2} dx dy = \frac{i}{2\operatorname{Im}(\tau)^2} d\tau d\bar{\tau}$.

Si $f : \mathbb{H} \rightarrow \mathbf{C}$ est une fonction continue et bornée, alors pour tout $\alpha \in \mathrm{SL}_2(\mathbf{Z})$, l'intégrale $\int_{\mathcal{F}} f(\alpha\tau) d\mu(\tau)$ de f sur le domaine fondamental $\mathcal{F} = \{\tau, |\operatorname{Re}(\tau)| \leq 1/2, |\tau| \geq 1\}$ converge absolument.

Soit maintenant Γ un sous-groupe de congruences de $\mathrm{SL}_2(\mathbf{Z})$, notons $X(\Gamma) = \Gamma \backslash \mathbb{H}$ et supposons f invariante par Γ (et toujours bornée). Si on écrit $\Gamma(1) = \bigsqcup_{i=1}^r \Gamma \alpha_i$, alors la somme

$$\int_{X(\Gamma)} f.d\mu := \sum_{i=1}^r \int_{\mathcal{F}} f(\alpha_i \tau) d\mu(\tau)$$

est indépendante du choix des représentants α_i . En d'autres termes, si \mathcal{F}_Γ est un domaine fondamental de Γ dans \mathbb{H} , alors $\int_{\mathcal{F}_\Gamma} f(\tau) d\mu(\tau)$ existe et

$$\int_{X(\Gamma)} f.d\mu = \int_{\mathcal{F}_\Gamma} f(\tau) d\mu(\tau).$$

Cela s'applique à la fonction constante 1 et on note $V_\Gamma := \int_{X(\Gamma)} d\mu$ le *volume* de $X(\Gamma)$. Si $\Gamma' \subset \Gamma$ est d'indice fini, on a $V_{\Gamma'} = [\Gamma \{ \pm 1 \} : \Gamma' \{ \pm 1 \}] V_\Gamma$ (exercice). On a donc en général $V_\Gamma = [\Gamma(1) : \Gamma' \{ \pm 1 \}] V_{\Gamma(1)}$ et on peut calculer⁽¹⁾ $V_{\Gamma(1)} = \pi/3$.

Soit maintenant $f, g \in M_k(\Gamma)$. La relation $\mathrm{Im}(\gamma\tau) = \mathrm{Im}(\tau) |j(\gamma, \tau)|^{-2}$ montre que la fonction $h(\tau) := \mathrm{Im}(\tau)^k f(\tau) \overline{g(\tau)}$ est invariante par Γ .

Lemme 2.33. — *Si de plus, l'une des deux formes f ou g est parabolique, alors cette fonction h est bornée sur \mathbb{H} .*

Démonstration. — La preuve est la même que celle de la proposition 1.29. En effet, il suffit de voir que pour $\alpha \in \Gamma \backslash \Gamma(1)$, la fonction $h(\alpha\tau)$ est bornée au voisinage de ∞ . Si h est la "largeur" (i.e. l'ordre) de la pointe $\alpha\infty$, on a un développement $h(\tau) = \mathrm{Im}(\tau)^k \sum_{n=0}^{\infty} a_n q_h^n$ où $q_h = \exp(2i\pi\tau/h)$. Or, si l'une des deux formes est parabolique, alors $a_0 = 0$, et $h(x+iy) = O(y^k \exp(-cy))$. Comme $h(\alpha\tau)$ est aussi horizontalement périodique, elle est donc bornée au voisinage de ∞ . \square

Définition 2.34. — Pour $f \in S_k(\Gamma)$, $g \in M_k(\Gamma)$, on appelle

$$\langle f, g \rangle_\Gamma := \frac{1}{V_\Gamma} \int_{X(\Gamma)} \mathrm{Im}(\tau)^k f(\tau) \overline{g(\tau)} d\mu(\tau)$$

le produit scalaire de Petersson de f et g .

La restriction à $S_k(\Gamma) \times S_k(\Gamma)$ est un produit hermitien défini positif. La normalisation par le volume permet d'avoir $\langle f, g \rangle_{\Gamma'} = \langle f, g \rangle_\Gamma$ pour $\Gamma' \subset \Gamma$.

Théorème 2.35. — *Soit $f \in S_k(\Gamma)$ de développement $f(\tau) = \sum_{n=1}^{\infty} a_n q_h^n$ avec $q_h = \exp(2i\pi\tau/h)$. Alors pour toute série de Poincaré $\varphi_n(\tau) := \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} j(\gamma, \tau)^{-k} \exp(2i\pi n\gamma\tau/h)$ on a*

$$\langle f, \varphi_n \rangle_\Gamma = \begin{cases} 0 & \text{si } n = 0 \\ \frac{h^k (k-2)!}{V_\Gamma (4\pi n)^{k-1}} a_n & \text{pour } n \geq 1 \end{cases}$$

⁽¹⁾Plus généralement, on peut montrer que l'aire d'un triangle géodésique dans $\mathbb{H} \cup \mathbf{P}^1(\mathbf{R})$ vaut π moins la somme des angles

La conséquence la plus intéressante de ce théorème est que toutes les formes paraboliques sont combinaisons linéaires de séries de Poincaré. En effet, toute forme parabolique orthogonale aux φ_n , $n > 0$ est nulle.

Corollaire 2.36. — $S_k(\Gamma)$ est engendré par les φ_n , $n > 0$.

Démonstration (du théorème). — Vu l'absolue convergence de la série définissant φ_n on peut écrire (en notant \mathcal{F}_Γ un domaine fondamental pour Γ)

$$\begin{aligned}
\langle f, \varphi_n \rangle_\Gamma &= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \frac{1}{V_\Gamma} \int_{\mathcal{F}_\Gamma} \operatorname{Im}(\tau)^k f(\tau) \overline{j(\gamma, \tau)}^{-k} \exp(-2i\pi n \overline{\gamma\tau}/h) d\mu(\tau) \\
&= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \frac{1}{V_\Gamma} \int_{\mathcal{F}_\Gamma} \operatorname{Im}(\gamma\tau)^k j(\gamma, \tau)^k f(\tau) \exp(-2i\pi n \overline{\gamma\tau}/h) d\mu(\tau) \\
&= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \frac{1}{V_\Gamma} \int_{\mathcal{F}_\Gamma} \operatorname{Im}(\gamma\tau)^k j(\gamma^{-1}, \gamma\tau)^{-k} f(\gamma^{-1}\gamma\tau) \exp(-2i\pi n \overline{\gamma\tau}/h) d\mu(\tau) \\
&= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \frac{1}{V_\Gamma} \int_{\mathcal{F}_\Gamma} \operatorname{Im}(\gamma\tau)^k f(\gamma\tau) \exp(-2i\pi n \overline{\gamma\tau}/h) d\mu(\tau) \\
&= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \frac{1}{V_\Gamma} \int_{\gamma\mathcal{F}_\Gamma} \operatorname{Im}(\tau)^k f(\tau) \exp(-2i\pi n \overline{\tau}/h) d\mu(\tau)
\end{aligned}$$

Pour la deuxième ligne on utilise $\operatorname{Im}(\tau) = \operatorname{Im}(\gamma\tau)|j(\gamma, \tau)|^2$, pour la troisième ligne on utilise $1 = j(\gamma^{-1}\gamma, \tau) = j(\gamma^{-1}, \gamma\tau)j(\gamma, \tau)$ et pour la quatrième on utilise l'automorphie de f . Maintenant, on remarque que $\bigsqcup_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \gamma\mathcal{F}_\Gamma$ est un domaine fondamental pour Γ_∞^+ , qui dépend du choix de représentants des Γ_∞^+ -classes à gauche. On peut choisir ces représentants de sorte que cette réunion soit (un ouvert dense du) le domaine fondamental agréable $\mathcal{F}_h = \{\tau, 0 \leq \operatorname{Re}(\tau) \leq h\}$. On peut donc écrire

$$\langle f, \varphi_n \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{y=0}^{\infty} \int_{x=0}^h y^{k-2} f(x+iy) \exp(-2i\pi nx/h) \exp(-2\pi ny/h) dx dy$$

Insérons le développement $f(x+iy) = \sum_{m>0} a_m \exp(2i\pi mx/h) \exp(-2\pi my/h)$ et intervertissons intégrales et sommes. On obtient

$$\langle f, \varphi_n \rangle_\Gamma = \frac{h}{V_\Gamma} a_n \int_0^\infty y^{k-2} \exp(-4\pi ny/h) dy$$

et des intégrations par parties montrent la formule annoncée. \square

2.6. Formes modulaires de niveau $\Gamma_0(N)$ et $\Gamma_1(N)$. — Pour les applications arithmétiques (comme la somme de k carrés, avec k non un multiple de 8), il serait intéressant de construire de formes modulaires à caractère non trivial et pour des niveaux différents de $\Gamma(N)$. Dans ce paragraphe on esquisse la construction pour les niveaux

$\Gamma_0(N)$ et $\Gamma_1(N)$. Il serait aussi intéressant de étudier le cas $k \leq 2$ qui pose de problèmes de convergence mais cela ne sera pas traité ici.

Rappelons les sous-groupes de congruence

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

Soit χ un caractère de Dirichlet modulo N , c'est-à-dire, un morphisme de groupes $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \rightarrow \mathbf{C}^\times$. On le prolonge en une fonction, aussi notée χ , de $\mathbf{Z}/N\mathbf{Z}$ vers \mathbf{C} en posant $\chi(d) = 0$ si d n'est pas premier à N .

A tout caractère de Dirichlet χ on peut lui associer un caractère de $\Gamma_0(N)$ trivial sur $\Gamma_1(N)$ par $\chi(\gamma) = \chi(d)$ si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Tout caractère de $\Gamma_0(N)$ trivial sur $\Gamma_1(N)$ est de cette forme là puisque $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times$.

Lemme 2.37. — *Pour tout entier positif N on a*

$$\begin{aligned} M_k(\Gamma_1(N)) &= \bigoplus_x M_k(\Gamma_0(N), \chi) \\ S_k(\Gamma_1(N)) &= \bigoplus_x S_k(\Gamma_0(N), \chi) \end{aligned}$$

où χ parcourt l'ensemble de caractères de Dirichlet.

Démonstration. — Puisque $\Gamma_1(N)$ est distingué dans $\Gamma_0(N)$, ce dernier agit sur $M_k(\Gamma_1(N))$ par $f \mapsto f[\gamma]_k$, pour $g \in \Gamma_0(N)$. Cette action induit une action de $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbf{Z}/N\mathbf{Z})^\times$ sur $M_k(\Gamma_1(N))$. Les représentations irréductibles de $(\mathbf{Z}/N\mathbf{Z})^\times$, étant commutatif, sont les caractères de Dirichlet. On déduit donc le lemme en décomposant la représentation en somme de représentations irréductibles. La même preuve marche pour $S_k(\Gamma_1(N))$. \square

Il suffit donc de comprendre les espaces $M_k(\Gamma_0(N), \chi)$.

Pour construire des séries d'Eisenstein de niveau Γ_0 , on peut faire de même que pour J . Notant que pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ on a $\overline{(0, v)\gamma} = \overline{(0, dv)}$ on voit que la série

$$\sum_{d \in (\mathbf{Z}/N\mathbf{Z})^\times} G_k^{(0, d)}$$

appartient à $M_k(\Gamma_0(N))$. De même si χ est un caractère de Dirichlet on a que

$$\sum_{d \in (\mathbf{Z}/N\mathbf{Z})^\times} \overline{\chi(d)} G_k^{(0, d)}$$

appartient à $M_k(\Gamma_0(N), \chi)$.

Avec le même type d'idées on peut construire toutes les séries d'Eisenstein de $M_k(\Gamma_0(N), \chi)$. Soient $u, v \in \mathbf{N}$ avec $uv = N$, ϕ un caractère de Dirichlet modulo u et ψ un caractère de Dirichlet modulo v , avec $\phi\psi(-1) = (-1)^k$ et ϕ primitif. Alors la série

$$G_k^{\phi, \psi}(\tau) = \sum_{c=0}^{u-1} \sum_{d=0}^{v-1} \sum_{e=0}^{u-1} \phi(c) \overline{\psi}(d) G_k^{\overline{(cv, d+ev)}}(\tau)$$

appartient à $M_k(\Gamma_0(N), \phi\psi)$. On peut construire ainsi toutes les série d'Eisenstein. Pour plus de détails voir la section 4.5 de [3].

3. Interprétation géométrique des formes modulaires

3.1. La courbe modulaire $Y(\Gamma)$ comme surface de Riemann. — Soit Γ un sous-groupe discret de $\mathrm{SL}_2(\mathbf{R})$. On rappelle qu'on note $\bar{\Gamma}$ le groupe $\Gamma/\{\pm I_2\}$ si $-I_2 \in \Gamma$, et $\bar{\Gamma} = \Gamma$ sinon.

Γ agit sur \mathbb{H} , notons $\pi : \mathbb{H} \rightarrow \Gamma \backslash \mathbb{H}$ la projection canonique. La proposition suivante montre que l'espace quotient $Y(\Gamma) := \Gamma \backslash \mathbb{H}$, muni de la topologie quotient, est séparé.

Proposition 3.1. — *Soit Γ un sous-groupe discret de $\mathrm{SL}_2(\mathbf{R})$.*

- (1) *Pour tout $\tau \in \mathbb{H}$, le fixateur Γ_τ de τ dans Γ est cyclique (et en particulier, fini).*
- (2) *Tout $\tau \in \mathbb{H}$ admet un voisinage ouvert U tel que $\forall \gamma \in \Gamma, \gamma U \cap U \neq \emptyset \Rightarrow \gamma\tau = \tau$.*
- (3) *Deux orbites distinctes $\Gamma\tau$ et $\Gamma\tau'$ admettent des voisinages ouverts disjoints.*

Démonstration. — (1) Le fixateur de τ est conjugué à un sous-groupe discret de $\mathrm{SO}_2(\mathbf{R}) \simeq \mathbf{C}^1$, donc fini et cyclique.

Pour (2) et (3) on utilise le fait suivant : si A, B sont deux compacts dans \mathbb{H} , alors $\mathrm{SL}_2(\mathbf{R})_{A,B} := \{\gamma \in \mathrm{SL}_2(\mathbf{R}), \gamma A \cap B \neq \emptyset\}$ est compact dans $\mathrm{SL}_2(\mathbf{R})$. En effet si π désigne l'application $\gamma \mapsto \gamma i$ et ι sa section $x + iy \mapsto \begin{pmatrix} y^{1/2} & -xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}$, alors $\mathrm{SL}_2(\mathbf{R})_{A,B} = \{\gamma \in \mathrm{SL}_2(\mathbf{R}), \gamma\pi^{-1}(A) \cap \pi^{-1}(B) \neq \emptyset\}$ est compact puisque $\pi^{-1}(A) = \iota(A)\mathrm{SO}_2(\mathbf{R})$ et $\pi(B)$ le sont.

(2) On applique ceci à V un voisinage compact de τ . Alors $\Gamma_V := \{\gamma \in \Gamma, \gamma V \cap V \neq \emptyset\}$ est un compact dans Γ , donc est fini. Pour chaque $\gamma \in \Gamma_V$ qui ne fixe pas τ on peut trouver un voisinage ouvert U_γ de τ tel que $\gamma U_\gamma \cap U_\gamma = \emptyset$. Prenant l'intersection (finie) sur de tels γ on obtient un U comme dans l'énoncé.

(3) Comme ci-dessus, si V' est un voisinage compact de τ' , l'ensemble $\Gamma_{V,V'} := \{\gamma \in \Gamma, \gamma V \cap V' \neq \emptyset\}$ est fini et on en déduit U voisinage ouvert de τ et U' de τ' tels que $\gamma U \cap U' = \emptyset$ pour tout γ . Alors $\bigcup_\gamma \gamma U$ et $\bigcup_\gamma \gamma U'$ sont deux voisinages disjoints de $\Gamma\tau$ et $\Gamma\tau'$ respectivement. \square

On voudrait définir sur $Y(\Gamma)$ une structure de surface de Riemann, c'est-à-dire, une structure de variété complexe de dimension 1.

Ceci est facile et classique lorsque Γ (ou plutôt $\bar{\Gamma}$) agit *librement* sur \mathbb{H} (i.e. $\forall \gamma \in \Gamma, \forall \tau \in \mathbb{H}, \gamma\tau = \tau \Rightarrow \gamma = 1$). Cependant $\mathrm{PSL}_2(\mathbf{Z})$ n'agit pas librement !

Les points problématiques sont dits points elliptiques, plus précisément :

Définition 3.2. — Soit Γ un sous-groupe discret de $\mathrm{SL}_2(\mathbf{R})$. Pour $\tau \in \mathbb{H}$, on note h_τ le cardinal de $\bar{\Gamma}_\tau$. Un point $\tau \in \mathbb{H}$ est un *point elliptique* de Γ si $h_\tau > 1$. On dit aussi que $\pi(\tau) \in \Gamma \backslash \mathbb{H}$ est un point elliptique.

Ainsi, $\bar{\Gamma}$ agit librement si et seulement si il ne possède pas de point elliptique.

Exemple 3.3. — On a vu que pour $\Gamma = \Gamma(1)$ les points elliptiques sont ceux qui appartiennent aux $\Gamma(1)$ -classes de i et ρ . On a $h_i = 2$ et $h_\rho = 3$. Dans le cas où Γ est un sous-groupe discret de $\mathrm{SL}_2(\mathbf{R})$ la proposition 3.1 montre que pour tout $\tau \in \mathbb{H}$, le fixateur Γ_τ est cyclique fini.

On rappelle que pour définir une structure complexe de dimension 1 sur un espace topologique X , on peut se donner un atlas holomorphe (ou sa classe d'équivalence), ou encore se donner un faisceau de fonctions \mathcal{O}_X tel que tout point $x \in X$ possède un voisinage ouvert U tel que $(U, (\mathcal{O}_X)|_U)$ soit isomorphe, en tant qu'espace annelé, à un ouvert de \mathbf{C} muni de son faisceau de fonctions holomorphes.

Exemple 3.4. — Dans le cas de surfaces définies comme quotient d'une surface de Riemann par l'action d'un groupe, il y a deux exemples type :

(1) Le groupe \mathbf{Z} opère par translation sur le plan complexe \mathbf{C} . Cette action n'a pas de points elliptiques et la fonction \mathbf{Z} -périodique $z \mapsto e^{2\pi iz}$ induit un isomorphisme :

$$\mathbf{C}/\mathbf{Z} \rightarrow \mathbf{C}^\times.$$

(2) Considérons le disque unité \mathbb{D} . Le groupe $\mathbb{U}_n \simeq \mathbf{Z}/N\mathbf{Z}$ des racines de l'unité opère par multiplication sur \mathbb{D} . L'action n'est pas libre, néanmoins l'application \mathbb{U}_n -invariante $z \mapsto z^n$ induit un isomorphisme

$$\mathbb{D}/\mathbb{U}_n \simeq \mathbb{D}.$$

Le quotient est donc bien lisse bien que l'action ne soit pas libre. Notons π la projection canonique $\mathbb{D} \rightarrow \mathbb{D}/\mathbb{U}_n$. L'application $f \mapsto f \circ \pi$ est une bijection entre les fonctions holomorphes sur $U \subset \mathbb{D}/\mathbb{U}_n$ vers les fonctions holomorphes en z^n sur $\pi^{-1}(U)$. Mais ces fonctions sont précisément les fonctions holomorphes sur $\pi^{-1}(U)$ invariantes sous l'action de \mathbb{U}_n .

Proposition 3.5. — Notons $\pi : \mathbb{H} \rightarrow \Gamma \backslash \mathbb{H}$ la projection canonique et posons, pour tout ouvert U de $\Gamma \backslash \mathbb{H}$,

$$\mathcal{O}_{\Gamma \backslash \mathbb{H}}(U) := \mathcal{O}_{\mathbb{H}}(\pi^{-1}(U))^\Gamma \text{ (fonctions holomorphes sur } \pi^{-1}(U) \text{ invariantes sous } \Gamma).$$

Alors $\mathcal{O}_{\Gamma \backslash \mathbb{H}}$ est un faisceau et définit une structure complexe sur $\Gamma \backslash \mathbb{H}$ pour laquelle π est holomorphe. On notera $Y(\Gamma)$ cette surface de Riemann.

Démonstration. — Il est clair que $\mathcal{O}_{\Gamma \backslash \mathbb{H}}$ est un faisceau. Si τ est un point non-elliptique, on peut trouver V voisinage ouvert de τ tel que $\pi|_V$ est un homéomorphisme $V \xrightarrow{\sim} \pi(V)$. Dans ce cas π induit un isomorphisme $(V, \mathcal{O}_V) \xrightarrow{\sim} (\pi(V), \mathcal{O}_{\pi(V)})$ comme souhaité. Si τ est un point elliptique, choisissons $\gamma_0 \in \mathrm{SL}_2(\mathbf{C})$ tel que $\gamma_0(\mathbb{H}) = \mathbb{D}$ et $\gamma_0\tau = 0$ (on prend

γ_0 l'élément $\begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix}$ divisé par son déterminant). Les éléments de $\gamma_0\Gamma_\tau\gamma_0^{-1}$ sont des automorphismes du disque unité \mathbb{D} fixant 0 et donc le lemme de Schwarz assure qu'ils sont de la forme $z \mapsto az$ avec $|a| = 1$. Mais $\gamma_0\Gamma_\tau\gamma_0^{-1}$ étant fini cyclique on a qu'il agit par rotations sur \mathbb{D} . Plus précisément il existe un isomorphisme de groupe $\iota : \Gamma_\tau \xrightarrow{\sim} \mathbb{U}_{h_\tau}$ (racines de l'unité d'ordre h_τ) tel que $\gamma_0(\gamma\tau') = \iota(\gamma)\gamma_0(\tau')$ pour tout $\tau' \in \mathbb{H}$ et tout $\gamma \in \Gamma_\tau$. Pour tout rayon $r < 1$, l'ouvert $V := \gamma_0^{-1}(D(0, r))$ est stable par Γ_τ , et pour r suffisamment petit on a $\gamma V \cap V \neq \emptyset \Rightarrow \gamma \in \Gamma_\tau$ d'après le (2) de la proposition 3.1. On a alors un diagramme commutatif

$$\begin{array}{ccc} V & \xrightarrow[\gamma_0]{\sim} & D(0, r) \\ \pi \downarrow & & \downarrow x \mapsto x^{h_\tau} \\ \pi(V) = \Gamma_\tau \backslash V & \xrightarrow[\bar{\gamma}_0]{\sim} & \mathbb{U}_{h_\tau} \backslash D(0, r^{h_\tau}) \end{array}$$

où $\bar{\gamma}_0$ est un homéomorphisme. Comme pour tout $U \subset \pi(V)$ on a $\mathcal{O}(U) = \mathcal{O}(\pi^{-1}(U) \cap V)^{\Gamma_\tau}$, on voit que $\bar{\gamma}_0$ transporte le faisceau de fonction $\mathcal{O}_{\pi(V)}$ vers le faisceau des fonctions holomorphes en $x \in D(0, r)$ invariantes sous \mathbb{U}_{h_τ} , qui est aussi le faisceau des fonctions holomorphes en x^{h_τ} , donc le faisceau des fonctions holomorphes usuel sur $D(0, r^{h_\tau})$.

Le faisceau de l'énoncé définit donc bien une structure complexe sur $\Gamma \backslash \mathbb{H}$ et π est visiblement holomorphe. On retiendra que $\tau' \mapsto \gamma_0(\tau')^{h_\tau}$ descend en une coordonnée locale au voisinage de $\pi(\tau)$ dans $\Gamma \backslash \mathbb{H}$. \square

3.2. La courbe modulaire $X(\Gamma)$ comme surface de Riemann. — On note $\mathbb{H}^* = \mathbb{H}_\Gamma^* := \mathbb{H} \sqcup P_\Gamma$. On munit \mathbb{H}^* de la topologie engendrée par les ouverts de \mathbb{H} et les ensembles de la forme $V_{\rho, r} := \rho(U_r \sqcup \{\infty\})$, où

- $r > 0$ et $U_r = \{\tau \in \mathbb{H}, \text{Im}(\tau) > r\}$
- $\rho \in \text{SL}_2(\mathbf{R})$ et $\rho.\infty \in P_\Gamma$.

Si on écrit $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $\rho(U_r)$ est le disque ouvert de diamètre $r^{-1}c^{-2}$ contenu dans \mathbb{H} et dont l'adhérence dans $\mathbf{P}^1(\mathbf{C})$ contient $\rho\infty = a/b$. Par construction, l'action de Γ sur \mathbb{H}^* préserve cette topologie (*i.e.* est continue), et on peut donc munir le quotient $Y(\Gamma) := \Gamma \backslash \mathbb{H}^*$ de la topologie quotient.

Lemme 3.6. — *Si $x_1, x_2 \in P_\Gamma$, il existe un voisinage $V_{\rho_1, r}$ de x_1 et un voisinage $V_{\rho_2, r}$ de x_2 tels que*

$$\forall \gamma \in \Gamma, \gamma V_{\rho_1, r} \cap V_{\rho_2, r} \neq \emptyset \Rightarrow \gamma x_1 = x_2.$$

En particulier, l'espace $\Gamma \backslash \mathbb{H}^$ est séparé et le sous-ensemble $\Gamma \backslash P_\Gamma$ y est discret.*

Démonstration. — Quitte à conjuguer la situation on peut supposer $x_2 = \infty$ et donc $V_{\rho_2, r} = U_r$. On a alors un $h_\infty > 0$ tel que $\Gamma_\infty \cdot \{\pm 1\} = \{\pm \gamma_\infty^m, m \in \mathbf{Z}\}$ avec $\gamma_\infty = \begin{pmatrix} 1 & h_\infty \\ 0 & 1 \end{pmatrix}$. Notons $x = x_1$ et fixons $\rho = \rho_1$ tel que $\rho\infty = x$, ce qui nous donne

$h = h_x > 0$ comme ci-dessus. Nous allons alors vérifier que tout r tel que $r^2 > h.h_\infty$ convient.

Pour cela, soit $\gamma \in \Gamma$ et supposons que $\gamma\rho U_r \cap U_r \neq \emptyset$. On doit montrer que $\gamma x = \gamma\rho\infty = \infty$. En notant $c(\sigma)$ la coordonnée $(2, 1)$ d'une matrice $\sigma \in \mathrm{SL}_2(\mathbf{R})$, on veut donc montrer que $c(\gamma\rho) = 0$. Vu la description de $\gamma\rho U_r$, l'hypothèse $\gamma\rho U_r \cap U_r \neq \emptyset$ implique que $r < r^{-1}c(\gamma\rho)^{-2}$, ou encore $c(\gamma\rho)^2 < r^{-2}$.

Posons $\delta_1 := \rho^{-1}\gamma^{-1}\gamma_\infty\gamma\rho$, qui est un élément du groupe discret $\rho^{-1}\Gamma\rho$. Un calcul montre que $c(\delta_1) = -c(\gamma\rho)^2 h_\infty$, et donc $|c(\delta_1)h| < 1$ d'après notre choix de r . On doit montrer que $c(\delta_1) = 0$.

Pour cela, posons $\delta_{n+1} := \delta_n \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \delta_n^{-1}$, qui est un élément de $\rho^{-1}\Gamma\rho$. Le même calcul montre que $c(\delta_{n+1}) = -c(\delta_n)^2 h$, mais aussi $b(\delta_{n+1}) = a(\delta_n)^2 h$ et $a(\delta_{n+1}) = 1 - a(\delta_n)c(\delta_n)h$.

Il s'en suit que $c(\delta_n) = -c(\delta_1)(c(\delta_1)h)^{2^n - 1}$ tend vers 0 quand $n \rightarrow \infty$ et donc que δ_n tend vers la matrice $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. Or, le groupe $\rho^{-1}\Gamma\rho$ étant discret, cela implique $\delta_n = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ pour n assez grand, donc $c(\delta_n) = 0$ et finalement $c(\delta_1) = 0$.

On laisse au lecteur les conséquences annoncées. \square

Considérons maintenant l'application $\tau \mapsto \exp(2i\pi\tau/h)$. Elle réalise un homéomorphisme envoyant ∞ sur 0

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^{\mathbf{Z}} \backslash (U_r \sqcup \{\infty\}) \xrightarrow{\sim} D(0, r')$$

où $r' = \exp(-2\pi r/h)$, ce qui munit $U_r \sqcup \{\infty\}$ d'une structure complexe. Si $x = \gamma_0\infty$ est une pointe de Γ et h est comme au début, le lemme précédent nous dit que pour r assez grand on a un diagramme

$$\begin{array}{ccc} V_{\gamma_0, r} & \xrightarrow[\gamma_0^{-1}]{\sim} & U_r \sqcup \{\infty\} \\ \pi \downarrow & & \downarrow \tau \mapsto \exp(2i\pi\tau/h) \\ \pi(V_{\gamma_0, r}) = \Gamma_x \backslash V_{\gamma_0, r} & \xrightarrow[\tilde{\gamma}_0^{-1}]{\sim} & D(0, r') \end{array}$$

ce qui munit $\pi(V_{\gamma_0, r})$ d'une structure complexe. Concrètement, la fonction $\exp(2i\pi\gamma_0(\tau)/h)$ fournit une coordonnée locale au voisinage de $\pi(x)$. On laisse au lecteur le soin de vérifier que ces structures se recollent avec celle sur $\Gamma \backslash \mathbb{H}$ pour munir $\Gamma \backslash \mathbb{H}^*$ d'une structure de surface de Riemann. On notera généralement $X(\Gamma)$ cette surface de Riemann.

Corollaire 3.7. — *La surface de Riemann $Y(1) = \Gamma(1) \backslash \mathbb{H}$ est isomorphe au plan complexe, tandis que $X(1) = \Gamma(1) \backslash \mathbb{H}^*$ est isomorphe à la sphère de Riemann.*

Démonstration. — Une fois on aura vu l'interprétation géométrique des formes modulaires le corollaire sera une conséquence de la proposition 1.21. L'invariant j réalise les

biholomorphismes souhaités:

$$\begin{aligned} j &: \Gamma(1)\backslash\mathbb{H} \rightarrow \mathbf{C} \\ \bar{j} &: \Gamma(1)\backslash\mathbb{H}^* \rightarrow \mathbf{P}^1(\mathbf{C}). \end{aligned}$$

Nous donnons ici une explication topologique utilisant la classification des surfaces de Riemann compactes.

Il suffit de montrer que $X(1)$ est compacte et de genre 0. Pour la compacité, vu la description des pointes, on remarque que $X(1)$ est l'image par $\pi : \mathbb{H}^* \rightarrow \Gamma(1)\backslash\mathbb{H}^*$ de $\tilde{\mathcal{F}}^* := \tilde{\mathcal{F}} \sqcup \{\infty\}$. Or il est clair que $\tilde{\mathcal{F}}^*$ est compact : si on a un recouvrement ouvert, l'un de ces ouverts est de la forme $(U_r \sqcup \{\infty\}) \cap \tilde{\mathcal{F}}^*$ et son complémentaire est compact dans $\tilde{\mathcal{F}}$.

Pour le genre 0, plusieurs arguments géométriques sont possibles, que l'on ne formalisera pas. En voici un. Topologiquement, on peut obtenir $Y(1)$ en deux étapes à partir de $\tilde{\mathcal{F}}$:

- identification des demi-droites $\operatorname{Re}(\tau) = 1/2$ et $\operatorname{Re}(\tau) = -1/2$
- identification du “segment” $[i, \rho]$ avec le segment $[i, S\rho]$.

La première étape fournit un cylindre de base un “cercle” obtenu en identifiant les extrémités ρ et $S\rho$ du segment géodésique $[\rho, S\rho]$. La deuxième étape ferme ce cylindre en “applatissant” le cercle sur un segment $[i, \rho]$. On “voit” alors que la rétraction géodésique “verticale” de $\tilde{\mathcal{F}}$ sur le segment $[\rho, S\rho]$ passe au quotient pour donner une rétraction de $Y(1)$ sur l'image de $[\rho, S\rho]$. Mais celle-ci est un segment. Donc l'espace obtenu est simplement connexe. Il s'ensuit que $Y(1)$ est isomorphe à \mathbf{C} ou \mathbb{D} , mais puisqu'on peut la compactifier par un point, c'est de \mathbf{C} qu'il s'agit. Par suite $X(1)$ est isomorphe à $\mathbf{P}^1(\mathbf{C})$. \square

Soit Γ un sous-groupe d'indice fini de $\operatorname{SL}_2(\mathbf{Z})$. Notons d l'indice de $\Gamma\{\pm I_2\}$ dans $\operatorname{SL}_2(\mathbf{Z})$. On note n_∞ le nombre de Γ -orbites dans P_Γ . Si τ est un point elliptique de Γ , il est conjugué à i ou ρ sous $\Gamma(1)$. On note n_2 le nombre de Γ -orbites de points elliptiques conjugués à i (ils sont d'ordre $h = 2$) et n_3 le nombre de Γ -orbites de points elliptiques conjugués à ρ (ils sont d'ordre $h = 3$). Le théorème suivant calcule le genre de $X(\Gamma)$ en fonction de d , n_2 , n_3 et n_∞ .

Théorème 3.8. — *Soit Γ un sous-groupe d'indice fini de $\operatorname{SL}_2(\mathbf{Z})$. Notons d l'indice de $\Gamma\{\pm I_2\}$ dans $\operatorname{SL}_2(\mathbf{Z})$, n_2 , n_3 et n_∞ comme ci-dessus. La surface de Riemann $X(\Gamma)$ est compacte. La projection $X(\Gamma) \rightarrow X(1)$ est holomorphe de degré (ou valence) d et le genre de $X(\Gamma)$ est*

$$g = 1 + d/12 - n_2/4 - n_3/3 - n_\infty/2.$$

Démonstration. — La compacité se prouve comme pour $\Gamma(1)$ en remarquant que, si $\operatorname{SL}_2(\mathbf{Z}) = \sqcup \gamma_i \Gamma\{\pm I_2\}$ alors $X(\Gamma)$ est l'image de la réunion $\gamma_1 \tilde{\mathcal{F}}^* \cup \dots \cup \gamma_d \tilde{\mathcal{F}}^*$ qui est compact. Le fait que l'application $Y(N) \rightarrow Y(1)$ est holomorphe découle de la définition des structures complexes, et de même pour l'holomorphie de $X(N) \rightarrow X(1)$ au voisinage des pointes. Comme elle est non-constante, elle a un degré (aussi appelé valence) qu'on peut calculer en comptant la préimage d'un point “ordinaire” (ni elliptique ni pointe).

On obtient d , vu la forme d'un domaine fondamental. Pour calculer le genre, on utilise la formule d'Hurwitz

$$\chi(X(\Gamma)) = d \cdot \chi(X(1)) + \sum_P (e_P - 1)$$

où $\chi(X) = 2g(X) - 2$ est la caractéristique d'Euler d'une surface de Riemann compacte X , et e_P désigne l'indice de ramification de $f : X(\Gamma) \rightarrow X(1)$ en $P \in X(\Gamma)$ (i.e., localement autour de P , f est de la forme $\tau \mapsto \tau^{e_P}$). Dans notre cas, cela donne

$$g(X(\Gamma)) = 1 - d + \frac{1}{2} \sum_P (e_P - 1).$$

Notons $\pi : \mathbb{H}^* \rightarrow X(1)$ la projection canonique. On a vu que le degré de ramification de π en un point de \mathbb{H} est fini, égal à 1 pour un point ordinaire, 2 pour un point elliptique équivalent à i ou 3 pour un point elliptique équivalent à ρ . Par multiplicativité des indices de ramification, l'indice e_P de f en un point qui n'est pas une pointe est aussi 1, 2 ou 3.

Plus précisément, considérons la fibre $f^{-1}(\pi(i))$. Pour P dans cette fibre, on a

- $e_P = 1$ si P est (l'image d') un point elliptique pour Γ .
- $e_P = 2$ si P est (l'image d') un point ordinaire pour Γ .

Par définition de n_2 , il y a donc n_2 points $P \in f^{-1}(\pi(i))$ tels que $e_P = 1$. Vu les propriétés du degré (on a $\sum_{P \rightarrow \pi(i)} e_P = d$), il y a donc $\frac{d-n_2}{2}$ points $P \in f^{-1}(\pi(i))$ tels que $e_P = 2$. D'où une contribution $\sum_{P \rightarrow \pi(i)} (e_P - 1) = (d - n_2)/2$ à la formule de Hurwitz.

Considérons maintenant la fibre $f^{-1}(\pi(\rho))$. Pour P dans cette fibre, on a

- $e_P = 1$ si P est (l'image d') un point elliptique pour Γ .
- $e_P = 3$ si P est (l'image d') un point ordinaire pour Γ .

Par définition de n_3 , il y a donc n_3 points $P \in f^{-1}(\pi(\rho))$ tels que $e_P = 1$. Vu les propriétés du degré, il y a donc $\frac{d-n_3}{3}$ points $P \in f^{-1}(\pi(\rho))$ tels que $e_P = 3$. D'où une contribution $\sum_{P \rightarrow \pi(\rho)} (e_P - 1) = 2(d - n_3)/3$ à la formule de Hurwitz.

Considérons enfin la fibre $f^{-1}(\pi(\infty))$, qui est l'ensemble des (images de) pointes de $X(\Gamma)$. Son cardinal est n_∞ et $\sum_{P \rightarrow \pi(\infty)} e_P = d$. D'où une contribution $\sum_{P \rightarrow \pi(\infty)} (e_P - 1) = d - n_\infty$ à la formule de Hurwitz.

Il ne reste plus qu'à rassembler les termes. □

Remarque 3.9. — Supposons que $x \in \mathbf{P}^1(\mathbf{R})$ est une pointe pour Γ , d'image P dans $X(\Gamma)$. Son stabilisateur $\Gamma_x\{\pm 1\}$ est un sous-groupe d'indice fini h de $\Gamma(1)_x$. Si l'on ramène x au point ∞ par un élément de γ_0 de $\Gamma(1)$, on a vu qu'une coordonnée locale autour de P est donnée par $\exp(2i\pi\gamma_0(\tau)/h)$ tandis qu'une coordonnée locale autour de $\pi(\tau)$ est $\exp(2i\pi\gamma_0(\tau))$. Dans ces coordonnées, la projection $X(\Gamma) \rightarrow X(1)$ prend donc la forme $x \mapsto x^h$, ce qui montre que h est l'indice de ramification de cette projection au point P .

3.3. Formes et fonctions modulaires. —

3.3.1. Fonctions modulaires de poids 0. — On rappelle qu'une fonction méromorphe $X \dashrightarrow \mathbf{C}$ sur une surface de Riemann X (donc définie en dehors de ses pôles) se prolonge de manière unique en une application holomorphe $X \rightarrow \mathbf{P}^1(\mathbf{C})$. On note M_X le corps des fonctions méromorphes sur X . Par exemple $M_{\mathbf{P}^1(\mathbf{C})} \simeq \mathbf{C}(z)$. Un résultat spectaculaire de la théorie (dont nous n'avons pas besoin) dit que $X \mapsto M_X$ est une équivalence entre la catégorie des surfaces de Riemann compactes munie des applications holomorphes non-constantes, et la catégorie des corps à engendrement fini et degré de transcendance 1 sur \mathbf{C} . C'est une motivation pour étudier le corps $M_{X(\Gamma)}$.

Soit φ une fonction méromorphe $X(\Gamma) \rightarrow \mathbf{P}^1(\mathbf{C})$. Notons f la composée $\mathbb{H} \rightarrow X(\Gamma) \xrightarrow{\varphi} \mathbf{P}^1(\mathbf{C})$. C'est une fonction méromorphe Γ -invariante sur \mathbb{H} . Réciproquement, si on se donne une telle fonction f , celle-ci descend bien à $Y(\Gamma)$ mais pour pouvoir la prolonger à $X(\Gamma)$, il faut une condition de *méromorphie aux pointes*.

On définit la condition de méromorphie aux pointes comme dans le chapitre précédent (voir définition 2.14). On le rappelle. Partons plus généralement d'une fonction méromorphe f sur \mathbb{H} qui est *horizontalement périodique* au sens où il existe un entier non nul h tel que $f(\tau) = f(\tau + h)$ (autrement dit, f est invariante par une matrice $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$). Elle s'écrit comme une fonction méromorphe en $q = \exp(2i\pi\tau/h) \in \mathbb{D} \setminus \{0\}$ et admet donc un développement

$$f(\tau) = \sum_{n \in \mathbf{Z}} a_n q^n$$

au voisinage de $q = 0$ (donc de $\tau = \infty$). On dit que f est *méromorphe à l'infini* si cette fonction de q est méromorphe en 0, c'est à dire si $a_n = 0$ pour $n \ll 0$. On note alors

$$\text{ord}_{\infty, h}(f) \text{ le plus petit } n \in \mathbf{Z} \text{ tel que } a_n \neq 0,$$

et on dit que f est *holomorphe à l'infini* si $\text{ord}_{\infty, h}(f) \geq 0$. On peut remarquer que ces notions ne dépendent pas du choix de h tel que f soit $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ -invariante (mais bien-sûr l'entier $\text{ord}_{\infty, h}$ dépend de h).

Revenons à une fonction méromorphe Γ -invariante. Pour une pointe $x \in \mathbf{P}^1(\mathbf{Q})$, on choisit $\gamma_0 \in \text{SL}_2(\mathbf{Z})$ tel que $\gamma_0 x = \infty$, et on dit que f est *méromorphe ou holomorphe à la pointe x* si $\gamma_0^* f : \tau \mapsto f(\gamma_0^{-1}\tau)$, qui est horizontalement périodique, est méromorphe ou holomorphe à l'infini. Cela ne dépend pas du choix de γ_0 , pas plus que l'entier

$$\text{ord}_{x, h}(f) := \text{ord}_{\infty, h}(\gamma_0^* f)$$

au sens précédent.

Les fonctions modulaires de niveau Γ et poids 0, $f : \mathbb{H} \rightarrow \mathbf{C}$, correspondent donc aux fonctions méromorphes sur $X(\Gamma)$.

De même, les formes modulaires de niveau Γ et poids 0, $f : \mathbb{H} \rightarrow \mathbf{C}$, correspondent aux fonctions holomorphes sur $X(\Gamma)$, et (comme on l'avait déjà vu) sont donc ... constantes !

Remarque 3.10. — On a vu que $M_{X(1)} \simeq \mathbf{C}(j)$.

3.3.2. Fonctions modulaires de poids 2. — Rappelons que pour un réseau $\Lambda \subset \mathbf{C}$, on avait construit les fonctions \wp et \wp' . La fonction \wp' était construite de façon très naturelle, en moyennant sur le réseau tandis que la construction de la fonction \wp était un peu plus compliquée. On pourrait alors se demander si ce ne serait pas plus facile de construire des *formes différentielles* méromorphes sur $X(\Gamma)$ au lieu de fonctions méromorphes.

Sur un ouvert U de \mathbf{C} une forme différentielle holomorphe, resp. méromorphe, s'écrit $\omega = f(z)dz$ avec f holomorphe, resp. méromorphe. Si $\varphi : V \xrightarrow{\sim} U$ est un biholomorphisme sur un autre ouvert de \mathbf{C} , on peut transporter ω en $\varphi^*\omega = f(\varphi(z))\varphi'(z)dz$. Sur une surface de Riemann X plus générale, une *forme différentielle* est la donnée, pour chaque carte $X \supseteq O \xrightarrow{\sim} U \subset \mathbf{C}$, d'une forme différentielle sur U , et ce de manière compatible avec la formule de changement de carte ci-dessus.

Soit $\pi : \mathbb{H} \rightarrow X(\Gamma)$ la restriction de la projection canonique à $\mathbb{H} \subset \mathbb{H}^*$. Une forme différentielle méromorphe ω sur $X(\Gamma)$ induit une forme différentielle méromorphe Γ -invariante $\pi^*\omega = f(\tau)d\tau$. La condition d'invariance s'écrit :

$$\forall \gamma \in \Gamma, f(\gamma\tau)d(\gamma\tau) = f(\tau)d\tau$$

et un calcul montre que pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a

$$d(\gamma\tau) = j(\gamma, \tau)^{-2}d\tau.$$

On a donc que la fonction f est faiblement modulaire de poids 2 et niveau Γ . La méromorphité aux pointes est définie comme dans le chapitre précédent (voir définition 2.14). On a vu que toute fonction f satisfaisant cette propriété de modularité est horizontalement périodique. De même, pour tout $\gamma_0 \in \mathrm{SL}_2(\mathbf{Z})$, la forme différentielle $\gamma_0^*(f.d\tau) = j(\gamma_0, \tau)^{-2}f(\gamma_0\tau)d\tau$ est invariante sous $\gamma_0^{-1}\Gamma\gamma_0$ donc la fonction $j(\gamma_0, \tau)^{-2}f(\gamma_0\tau)$ est horizontalement périodique. On dit alors que f est méromorphe ou holomorphe à la pointe $\gamma_0\infty$ si la fonction $\tau \mapsto j(\gamma_0, \tau)^{-2}f(\gamma_0\tau)$ est méromorphe ou holomorphe à l'infini. Cela ne dépend pas du choix de γ_0 , pas plus que l'entier

$$\mathrm{ord}_{x,h}(f) := \mathrm{ord}_{\infty,h}(j(\gamma_0, \tau)^{-2}f(\gamma_0\tau)).$$

Sous cette identification la "méromorphité" de la fonction f en une pointe x dans le sens de la définition 2.14 correspond à la méromorphité de la forme différentielle ω dans la pointe x .

Les fonctions modulaires de niveau Γ et poids 2 sur \mathbb{H} se correspondent donc aux formes différentielles méromorphes sur $X(\Gamma)$.

3.3.3. Fonctions modulaires de poids $k \in 2\mathbf{N}$. — Lorsque $k = 2k'$ est pair, on peut interpréter les formes modulaires de poids k comme certaines k' -formes différentielles sur $X(\Gamma)$. Une k' -*forme différentielle* sur un ouvert de \mathbf{C} est une expression de la forme $\omega = f(\tau)(d\tau)^{k'}$. Si φ est une application biholomorphe entre deux ouverts on transporte une telle forme par la formule $\varphi^*\omega = f(\varphi(\tau))\varphi'(\tau)^{k'}(d\tau)^{k'}$. Ceci permet de définir ce qu'est une k' -forme différentielle sur une variété comme la donnée d'une k' -forme sur

chaque carte de X , avec compatibilité au changement de carte. On se retrouve alors dans une situation semblable au poids 2, avec notamment une correspondance

$$\begin{aligned} & \{\text{Fonctions modulaires } f \text{ de poids } k \text{ niveau } \Gamma\} \\ \leftrightarrow & \{k'\text{-formes différentielles } \omega \text{ méromorphes sur } X(\Gamma)\} \end{aligned}$$

donnée par l'égalité $\pi^*\omega = f(\tau)(d\tau)^{k'}$.

3.3.4. Formes modulaires de poids $k \in 2\mathbf{N}$. — Attention : l'holomorphie de f n'est pas équivalente à celle de ω !! Les formes modulaires ne se correspondent *pas* aux formes différentielles holomorphes !

Pour expliquer cela, introduisons la notation $\text{ord}_P(f)$ pour l'ordre du zéro ou du pôle en un point P d'une fonction méromorphe f sur une surface de Riemann. Si on développe $f = g(\tau)$ dans une coordonnée locale τ au voisinage de P on a $\text{ord}_P(f) = \text{ord}_0(g)$. De même, si dans cette coordonnée on développe une forme différentielle méromorphe sous la forme $\omega = g(\tau)d\tau$, alors l'entier $\text{ord}_0(g)$ ne dépend pas du choix de la coordonnée et se note $\text{ord}_P(\omega)$. Bien sûr ω est holomorphe en P si et seulement si $\text{ord}_P(\omega) \geq 0$.

Lemme 3.11. — Soit ω une k' -forme différentielle méromorphe sur $X(\Gamma)$ et soit f la fonction méromorphe sur \mathbb{H} telle que $\pi^*\omega = f(\tau)(d\tau)^{k'}$. Alors on a les égalités suivantes :

- i) $\text{ord}_P(f) = \text{ord}_{\pi(P)}(\omega)$ si P est un point de \mathbb{H} ordinaire pour Γ .
- ii) $\text{ord}_P(f) = e \cdot \text{ord}_{\pi(P)}(\omega) + k'(e - 1)$ si P est un point elliptique d'ordre e (égal à 2 ou 3).
- iii) $\text{ord}_{x,h}(f) = \text{ord}_{\pi(x)}(\omega) + k'$ si x est une pointe d'ordre h .

Démonstration. — i) et ii). On a vu qu'au voisinage d'un point P de \mathbb{H} , il existe une coordonnée locale $\tau' = \gamma_0(\tau)$ telle que π est de la forme $\tau' \mapsto \tau'^e$, avec $e = 1$ si P est ordinaire. La fonction $u = \tau'^e$ descend donc en une coordonnée locale autour de $\pi(P)$. Il s'ensuit que si $\omega = g(u)(du)^{k'}$ au voisinage de $\pi(\tau_0)$, alors $\pi^*\omega = g(\tau'^e)d(\tau'^e)^{k'} = e^{k'}\tau'^{k'(e-1)}g(\tau'^e)d(\tau')^{k'}$ et donc $\text{ord}_P(f) = \text{ord}_P(\pi^*\omega) = \text{ord}_0(\tau'^{k'(e-1)}g(\tau'^e)) = e \cdot \text{ord}_0(g) + k'(e - 1) = e \cdot \text{ord}_{\pi(P)}(\omega) + k'(e - 1)$.

iii) Quitte à translater par un $\gamma_0 \in \text{SL}_2(\mathbf{Z})$ on peut supposer que $x = \infty$. Dans ce cas, on a vu que $q = \exp(2i\pi\tau/h)$ est une coordonnée locale autour de $\pi(x)$. Ainsi si ω est de la forme $g(q)(dq)^{k'}$, $\pi^*\omega$ est de la forme $(2i\pi/h)^{k'} \cdot g(\exp(2i\pi\tau/h)) \cdot \exp(2ik'\pi\tau/h)(d\tau)^{k'} = f(\tau)(d\tau)^{k'}$, de sorte que $f(\tau) = (2i\pi/h)^{k'} q^{k'} \cdot g(q)$, et finalement $\text{ord}_{\infty,h}(f) = \text{ord}_0(q^{k'} \cdot g(q)) = \text{ord}_0(g(q)) + k' = \text{ord}_{\pi(x)}\omega + k'$. \square

Corollaire 3.12. — La correspondance (3.3.3) induit une bijection entre les formes modulaires (paraboliques) f de poids $2k'$ niveau Γ et les k' -formes différentielles ω méromorphes sur $X(\Gamma)$ telles que :

- (1) ω est holomorphe aux points ordinaires;
- (2) $\text{ord}_{\pi(P)}(\omega) \geq -\frac{k'(e-1)}{e}$ si P est un point elliptique d'ordre e (égal à 2 ou 3);
- (3) $\text{ord}_{\pi(x)}(\omega) \geq -k'$ ($\text{ord}_{\pi(x)}(\omega) \geq -k' + 1$) si x est une pointe.

donnée par l'égalité $\pi^*\omega = f(\tau)(d\tau)^{k'}$.

Remarque 3.13. — En particulier $M_2(\Gamma)$ est en bijection avec les formes différentielles ω méromorphes sur $X(\Gamma)$, holomorphes sur $Y(\Gamma)$ telles que $\text{ord}_{\tau(x)}(\omega) \geq -1$ si x est une pointe. On a donc que $S_2(\Gamma)$ est en bijection avec les formes différentielles ω holomorphes sur $X(\Gamma)$,

3.4. Calcul de dimensions. — La théorie des diviseurs de Weil et en particulier le théorème de Riemann-Roch montre que ces espaces sont de dimension finie et permet de calculer leur dimension. Faisons quelques rappels à ce sujet.

– Un *diviseur sur X* est une somme $\sum_{P \in X} a_P [P]$ où $a_P \in \mathbf{Z}$ est nul sauf pour un nombre fini de points. L'ensemble des diviseurs $\text{Div}(X)$ est donc le groupe abélien libre de base X . Il est partiellement ordonné par la relation $\sum_P a_P [P] \leq \sum_P b_P [P]$ si $a_P \leq b_P$ pour tout P .

– Le *dégré d'un diviseur* est défini par $\text{deg}(\sum_P a_P [P]) = \sum_P a_P \in \mathbf{Z}$.

– A toute fonction méromorphe non-nulle f on associe son diviseur

$$\text{div}(f) := \sum_P \text{ord}_P(f) [P].$$

On a $\text{div}(fg) = \text{div}(f) + \text{div}(g)$ et $\text{div}(f + g) \geq \inf(\text{div}(f), \text{div}(g))$.⁽²⁾ On obtient ainsi un homomorphisme de groupe $M_X^\times \xrightarrow{\text{div}} \text{Div}(X)$ dont l'image est notée $\text{Div.pr}(X)$. Un tel diviseur est dit *principal*. Le quotient $\text{Div}(X)/\text{Div.pr}(X)$ s'appelle *groupe de Picard de X* et se note $\text{Pic}(X)$. (C'est l'analogue du groupe des classes d'un corps de nombres).

– L'application deg se factorise par $\text{Pic}(X)$. En effet, si l'on considère $f \in M_X^\times$ comme une application holomorphe $X \rightarrow \mathbf{P}^1(\mathbf{C})$ dont on note e_P l'indice de ramification en un point $P \in X$, alors

$$\text{div}(f) = \sum_{P \rightarrow 0} e_P [P] - \sum_{P \rightarrow \infty} e_P [P]$$

donc son degré est nul.

– De même à toute forme différentielle méromorphe on associe

$$\text{div}(\omega) = \sum_P \text{ord}_P(\omega) [P].$$

Comme $\text{div}(f\omega) = \text{div}(f) + \text{div}(\omega)$, $\forall f \in M_X^\times$, l'image de ω dans $\text{Pic}(X)$ ne dépend pas de ω , s'appelle le *diviseur canonique de X* , et se note K .

– Si $D \in \text{Div}(X)$, on note

$$L(D) := \{f \in M_X^\times, \text{div}(f) + D \geq 0\} \sqcup \{0\}.$$

C'est un \mathbf{C} -espace vectoriel dont la dimension $l(D) := \dim_{\mathbf{C}} L(D)$ ne dépend que de l'image de D dans $\text{Pic}(X)$, puisque pour $f_0 \in M_X^\times$, la multiplication par f_0 induit un isomorphisme linéaire $L(D) \xrightarrow{\sim} L(D + \text{div}(f_0))$.

⁽²⁾Ici la notation \inf est à prendre comme un "pgcd" pour la relation d'ordre partiel sur les diviseurs. C'est donc l'élément maximal parmi les éléments inférieurs à $\text{div}(f)$ et $\text{div}(g)$.

– Le *théorème de Riemann-Roch* affirme que

$$l(D) = \deg(D) + 1 - g + l(K - D)$$

où g est le genre de X . Sachant que $l(0) = 1$ (fonctions holomorphes sur X compacte, donc constantes), on voit en particulier, en prenant $D = 0$ puis $D = K$, que

$$l(K) = g \text{ et } \deg(K) = 2g - 2.$$

Il s'ensuit que si $\deg(D) > 2g - 2$, alors $\deg(K - D) < 0$ donc $L(K - D) = \{0\}$ (puisque un diviseur positif a un degré positif) et

$$l(D) = \deg(D) + 1 - g.$$

Le lien entre le diviseurs et le calcul de dimensions des espaces de formes modulaires est le suivant : On écrit $X = X(\Gamma)$ et notons $D_\pi := \sum_{P \in X(\Gamma)} (1 - 1/e_P)[P] \in \text{Div}(X(\Gamma)) \otimes_{\mathbf{Z}} \mathbf{Q}$ où e_P vaut 1 pour un point ordinaire, 2 ou 3 pour un point elliptique, et $+\infty$ pour une pointe. Soient ω une k' -forme différentielle et soit f telle que $\pi^*\omega = f(\tau)(d\tau)^{k'}$. Alors $\text{div}(f) = \text{div}(\omega) + k'D_\pi$. La correspondance du corollaire 3.12 s'écrit alors comme une bijection entre les formes modulaires (paraboliques) f de poids $2k'$ niveau Γ et les k' -formes différentielles ω méromorphes sur $X(\Gamma)$ telles que $\text{div}(\omega) + k'D_\pi \geq 0$ ($\text{div}(\omega) + k'D_\pi - \sum_{P \rightarrow \infty} [P] \geq 0$).

Notons finalement que $\deg(D_\pi) = \frac{1}{2}n_2 + \frac{2}{3}n_3 + n_\infty$.

3.4.1. Calcul de dimensions en poids 2. — On va faire d'abord le calcul en poids $k = 2$. Même si ce n'est pas nécessaire de traiter le cas $k = 2$ à part, ce calcul illustre de façon très simple l'idée de l'utilisation du théorème de Riemann-Roch.

Corollaire 3.14. — *On a les égalités*

- $\dim_{\mathbf{C}}(M_2(\Gamma)) = l(D_\pi + K) = g - 1 + n_\infty$,
- $\dim_{\mathbf{C}}(S_2(\Gamma)) = l(K) = g$.

Démonstration. — On vient de voir que l'application $\omega \mapsto f$ définie par $\pi^*\omega = f(\tau)d\tau$ induit un isomorphisme

$$\{\omega, \text{div}(\omega) + D_\pi \geq 0\} \sqcup \{0\} \xrightarrow{\sim} M_2(\Gamma).$$

Fixons une forme différentielle méromorphe ω_0 sur $X(\Gamma)^{(3)}$, et écrivons les autres sous la forme $\omega = g\omega_0$, alors puisque $\text{div}(\omega) = \text{div}(g) + \text{div}(\omega_0)$, l'application $g \mapsto g\omega_0 \mapsto f$ induit un isomorphisme

$$L(\text{div}(\omega_0) + D_\pi) \xrightarrow{\sim} M_2(\Gamma).$$

La même application induit l'isomorphisme

$$L(\text{div}(\omega_0) + D_\pi - \sum_{P \rightarrow \infty} [P]) \xrightarrow{\sim} S_2(\Gamma).$$

⁽³⁾Il en existe toujours. Par exemple, sur $X(1) = \mathbf{P}^1$ on peut prendre $d\tau$ (qui a $\text{div}(d\tau) = -2[\infty]$) puis tirer en arrière $d\tau$ via $X(\Gamma) \rightarrow X(1)$

Notons $\lfloor D_\pi \rfloor$ la partie entière de D_π , c'est-à-dire $\lfloor D_\pi \rfloor = \sum_{P \rightarrow \infty} \lfloor P \rfloor$. Alors bien-sûr, on a $L(\operatorname{div}(\omega_0) + D_\pi) = L(\operatorname{div}(\omega_0) + \lfloor D_\pi \rfloor)$. Il s'ensuit que

$$\dim_{\mathbf{C}}(M_2(\Gamma)) = l(\operatorname{div}(\omega_0) + \lfloor D_\pi \rfloor) = l(K + \lfloor D_\pi \rfloor) = l(K + \sum_{P \rightarrow \infty} \lfloor P \rfloor).$$

On a $\deg(K + \sum_{P \rightarrow \infty} \lfloor P \rfloor) = 2g - 2 + n_\infty > 2g - 2$ de sorte que la forme simplifiée du théorème de Riemann-Roch s'applique pour donner

$$l(K + \sum_{P \rightarrow \infty} \lfloor P \rfloor) = \deg(K + \sum_{P \rightarrow \infty} \lfloor P \rfloor) + 1 - g = g - 1 + n_\infty.$$

Par le même raisonnement, on obtient que

$$\dim_{\mathbf{C}}(S_2(\Gamma)) = l(\operatorname{div}(\omega_0) + \lfloor D_\pi \rfloor - \sum_{P \rightarrow \infty} \lfloor P \rfloor) = l(K) = g.$$

□

3.4.2. Calcul de dimensions en poids quelconque. — La calcul de dimension en poids quelconque suit les mêmes idées que dans le cas $k = 2$: le calcul est juste un peu plus élaboré.

Proposition 3.15. — *Soit f une fonction modulaire non nulle de poids k et niveau Γ . Alors*

$$\sum_{P \in \Gamma \backslash \mathbb{H}} \frac{\operatorname{ord}_P(f)}{e_P} + \sum_{x \in \Gamma \backslash P_\Gamma} \operatorname{ord}_{x, h_x}(f) = \frac{k}{2}(2g - 2 + \frac{1}{2}n_2 + \frac{2}{3}n_3 + n_\infty) = \frac{kd}{12}$$

où l'on rappelle que $d = [\Gamma(1) : \Gamma\{\pm 1\}]$.

Démonstration. — Lorsque $k = 2k'$ est pair, le lemme 3.11 montre que le terme de gauche s'identifie à $\deg(\operatorname{div}(\omega)) + k' \deg(D_\pi)$. Le degré $\deg(\operatorname{div}(\omega))$ ne dépend pas de ω (puisque les autres sont de la forme $g\omega$ avec $g \in M_{X(\Gamma)}^\times$). On peut le calculer en prenant ω' de la forme $\omega_1^{k'}$ où ω_1 est une 1-forme différentielle méromorphe sur $X(\Gamma)$ et $\omega_1^{k'}$ désigne la k' -forme différentielle donnée par $\omega_1^{k'} = f(\tau)^{k'}(d\tau)^{k'}$ sur une carte où $\omega_1 = f(\tau)d\tau$. On obtient $\deg(\operatorname{div}(\omega)) = k' \deg(\operatorname{div}(\omega_1)) = k'(2g - 2)$, dont on déduit la première égalité. La seconde vient de la formule donnant le genre.

Lorsque k est impair, il suffit d'appliquer le cas pair à f^2 . □

Remarque 3.16. — Pour $\Gamma = \Gamma(1)$, la formule devient

$$\operatorname{ord}_{\infty, 1}(f) + \frac{1}{2}\operatorname{ord}_i(f) + \frac{1}{3}\operatorname{ord}_j(f) + \sum_{P \neq i, j, \infty} \operatorname{ord}_P(f) = k/12.$$

On retrouve le lemme $k/12$.

Théorème 3.17. — *Pour $k > 2$ on a les formules de dimension suivantes.*

- $\dim_{\mathbf{C}}(M_k(\Gamma)) = (k - 1)(g - 1) + \lfloor \frac{k}{4} \rfloor n_2 + \lfloor \frac{k}{3} \rfloor n_3 + \frac{k}{2} n_\infty$
- $\dim_{\mathbf{C}}(S_k(\Gamma)) = \dim_{\mathbf{C}}(M_k(\Gamma)) - n_\infty$

Remarque 3.18. — En utilisant la formule donnant le genre, on peut aussi écrire

$$\dim_{\mathbf{C}}(M_k(\Gamma)) = \frac{kd}{12} - g + 1 + \left(\frac{k}{4} - \left\lfloor \frac{k}{4} \right\rfloor \right) n_2 + \left(\frac{k}{3} - \left\lfloor \frac{k}{3} \right\rfloor \right) n_3$$

Ainsi, si k est divisible par 12, alors $\dim_{\mathbf{C}}(M_k(\Gamma)) = \frac{kd}{12} - g + 1$.

Démonstration. — On écrit $k = 2k'$, on procède comme on l'a fait en poids $k = 2$. On fixe une k' -forme différentielle méromorphe ω_0 sur $X(\Gamma)$ (par exemple de la forme $\omega_0 = \omega_1^{k'}$ avec ω_1 une 1-forme), on note f la fonction modulaire de poids k associée et. De la correspondance du corollaire 3.12 on déduit que l'application $g \mapsto g\omega_0 \mapsto f$ induit des isomorphismes

$$L(\operatorname{div}(\omega_0) + [k'D_\pi]) \xrightarrow{\sim} M_k(\Gamma)$$

et

$$L\left(\operatorname{div}(\omega_0) + [k'D_\pi] - \sum_{P \rightarrow \infty} [P]\right) \xrightarrow{\sim} S_k(\Gamma)$$

où $D_\pi = \sum_{P \in X(\Gamma)} (1 - 1/e_P)[P]$.

On utilise alors la formule de Riemann-Roch pour calculer $\dim M_k(\Gamma)$, aidés par le fait que $\deg(k'K + [k'D_\pi]) > 2g - 2$. Dans ce cas la formule s'écrit :

$$l(D) = \deg(D) + 1 - g.$$

On en déduit que $\dim_{\mathbf{C}}(M_k(\Gamma)) = l(k'K + [k'D_\pi])$ avec

$$[k'D_\pi] = \sum_{P \rightarrow i} \left\lfloor \frac{k}{4} \right\rfloor [P] + \sum_{P \rightarrow j} \left\lfloor \frac{k}{3} \right\rfloor [P] + \sum_{P \rightarrow \infty} \frac{k}{2} [P].$$

Pour calculer la dimension de $S_k(\Gamma)$ il suffit de remplacer $\operatorname{div}(\omega_0)$ par $\operatorname{div}(\omega_0) - \sum_{P \rightarrow \infty} [P]$. Dans ce cas on a bien $\deg > 2g - 2$ dès que $k > 2$. □

Remarque 3.19. — Pour calculer la dimension des espaces de formes modulaires dans le cas où k est impair, on a besoin de la notion de *pointe irrégulière*. Cette notion vient de l'observation suivante : si f est une fonction telle que $f\left(\begin{pmatrix} -1 & h \\ 0 & -1 \end{pmatrix} \tau\right) = -f(\tau)$, c'est-à-dire $f(\tau + h) = -f(\tau)$, alors elle est $2h$ -périodique et dans son développement $f(\tau) = \sum_{n \in \mathbf{Z}} a_n q_{2h}^n$ où $q_{2h} = \exp(2i\pi\tau/2h)$, tous les a_n avec n pair sont nuls. En particulier, si elle est holomorphe à l'infini, elle s'y annule nécessairement.

Fort de cette observation, on dira que x est une *pointe irrégulière* pour (Γ, k) si

(1) k est impair et $-1 \notin \Gamma$

(2) écrivant $x = \gamma_0\infty$, le groupe $\gamma_0^{-1}\Gamma_x\gamma_0$ contient $\begin{pmatrix} -1 & h_x \\ 0 & -1 \end{pmatrix}$.

Si $x = \gamma_0\infty$ est irrégulière et f est modulaire de poids k , alors $f[\gamma_0]_k(\tau + h_x) = -f[\gamma_0]_k(\tau)$.

On décompose $n_\infty = n_\infty^{\text{reg}} + n_\infty^{\text{irr}}$ (et on a $n_\infty^{\text{reg}} = n_\infty$ et $n_\infty^{\text{irr}} = 0$ si k est pair).

(Les sous-groupes de congruence principaux $\Gamma(N)$ n'ont pas de pointes irrégulières. $-I_2 \in \Gamma(2)$ et lorsque $-1 \notin \Gamma(N)$ (ie lorsque $N > 2$) toutes les pointes sont visiblement régulières, puisqu'une matrice $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$ n'appartient pas à $\Gamma(N)$.)

Dans le cas impair, $k > 2$ on trouve les formules de dimension suivantes, où l'on suppose $-1 \notin \Gamma$.

$$\begin{aligned} - \dim_{\mathbf{C}}(M_k(\Gamma)) &= (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor n_2 + \lfloor \frac{k}{3} \rfloor n_3 + \frac{k}{2} n_{\infty}^{\text{reg}} + \lfloor \frac{k}{2} \rfloor n_{\infty}^{\text{irr}} \\ - \dim_{\mathbf{C}}(S_k(\Gamma)) &= \dim_{\mathbf{C}}(M_k(\Gamma)) - n_{\infty}^{\text{reg}} \end{aligned}$$

(En particulier on a $n_2 = 0$. Exercice !)

Pour prouver ces formules on suit un raisonnement similaire. Il nous faut connaître l'existence d'une fonction modulaire de poids k . Si $k \geq 3$ on a vu l'existence d'une telle fonction dans le paragraphe 2.4.2 et on a montré la non nullité dans le cas où Γ est distingué. *Admettons* l'existence d'une telle fonction f (à condition que $-1 \notin \Gamma$)⁽⁴⁾.

Alors f^2 est de poids $2k$ et correspond à une k -forme différentielle méromorphe ω_0 sur $X(\Gamma)$. Vu les formules

$$\begin{cases} \text{ord}_P(\pi^*(g)^2 f^2) = 2e_P \cdot \text{ord}_{\pi(P)}(g) + e_P \cdot \text{ord}_{\pi(P)}(\omega_0) + k(e_P - 1) & \text{si } P \in \mathbb{H} \\ \text{ord}_{x, h_x}(\pi^*(g)^2 f^2) = 2\text{ord}_{\pi(x)}(g) + \text{ord}_{\pi(x)}(\omega_0) + k & \text{si } x \text{ est une pointe} \end{cases}$$

on constate que l'application $g \mapsto \pi^*(g)f$ induit des isomorphismes

$$L\left(\frac{1}{2}\text{div}(\omega_0) + \frac{k}{2}D_{\pi}\right) \xrightarrow{\sim} M_k(\Gamma)$$

et

$$L\left(\frac{1}{2}\text{div}(\omega_0) + \frac{k}{2}D_{\pi} - \frac{1}{2}\sum_{P \rightarrow \infty} [P]\right) \xrightarrow{\sim} S_k(\Gamma).$$

Pour M_k , il faut alors calculer la partie entière du diviseur

$$\frac{1}{2}\text{div}(\omega_0) + \frac{k}{2}D_{\pi} = \sum_{P \in X(\Gamma)} \left(\frac{1}{2}\text{ord}_P(\omega_0) + \frac{k}{2}(1 - 1/e_P)\right) [P].$$

Pour un point P de $Y(\Gamma)$ et un point $\tilde{P} \in \mathbb{H}$ tel que $P = \pi(\tilde{P})$, on remarque que l'égalité

$$2\text{ord}_{\tilde{P}}(f) = e \cdot \text{ord}_P(\omega_0) + k(e - 1)$$

implique que $\text{ord}_P(\omega_0)$ est pair si $e = 1$ ou 3 . Comme $n_2 = 0$, ce nombre est donc pair pour tout $P \in Y(\Gamma)$, et il s'ensuit que

$$\left\lfloor \frac{1}{2}\text{ord}_P(\omega_0) + \frac{k}{2}(1 - 1/e_P) \right\rfloor = \frac{1}{2}\text{ord}_P(\omega_0) + \left\lfloor \frac{k}{2}(1 - 1/e_P) \right\rfloor$$

Pour une pointe $P \in X(\Gamma)$ et $x \in \mathbf{P}^1(\mathbf{Q})$ tel que $\pi(x) = P$, l'égalité

$$\text{ord}_{x, 2h_x}(f) = \text{ord}_{x, h_x}(f^2) = \text{ord}_P(\omega_0) + k$$

⁽⁴⁾Pour l'existence d'une telle fonction voir le poly de Dat [2], il est particulièrement difficile la construction dans le cas où $k = 1$

montre que :

– si $x = \gamma_0\infty$ est régulière, alors $f[\gamma_0]_k$ est h_x -périodique donc $\text{ord}_{x,2h_x}(f) = 2\text{ord}_{x,h_x}(f)$ et par conséquent $\text{ord}_P(\omega_0)$ est impair, et

$$\left\lfloor \frac{1}{2}\text{ord}_P(\omega_0) + \frac{k}{2}(1 - 1/e_P) \right\rfloor = \frac{1}{2}\text{ord}_P(\omega_0) + \frac{k}{2}.$$

– si $x = \gamma_0\infty$ est irrégulière, alors $f[\gamma_0]_k$ est $2h_x$ -périodique et vérifie $f[\gamma_0]_k(\tau + h_x) = -f[\gamma_0]_k(\tau)$. Donc dans le développement $f[\gamma_0]_k(\tau) = \sum_{n \in \mathbf{Z}} a_n q^n$ avec $q = \exp(2i\pi\tau/2h_x)$, on a $a_n = 0$ si n est pair, de sorte que $\text{ord}_{x,2h_x}(f)$ est impair, et finalement

$$\left\lfloor \frac{1}{2}\text{ord}_P(\omega_0) + \frac{k}{2}(1 - 1/e_P) \right\rfloor = \frac{1}{2}\text{ord}_P(\omega_0) + \frac{k-1}{2}.$$

On obtient donc

$$\left\lfloor \frac{1}{2}\text{div}(\omega_0) + \frac{k}{2}D_\pi \right\rfloor = \frac{1}{2}\text{div}(\omega_0) + \sum_{P \rightarrow j} \left\lfloor \frac{k}{3} \right\rfloor [P] + \sum_{P \rightarrow \infty, \text{reg}} \frac{k}{2}[P] + \sum_{P \rightarrow \infty, \text{irr}} \frac{k-1}{2}[P].$$

Pour $k \geq 3$, son degré est supérieur à $1/2 \deg(\text{div}(\omega_0)) = k/2(2g-2) > 2g-2$, donc la formule de Riemann-Roch simplifiée s'applique et on obtient la dimension annoncée pour $M_k(\Gamma)$.

Pour calculer la dimension de $S_k(\Gamma)$, il faut calculer la partie entière du diviseur $\frac{1}{2}\text{div}(\omega_0) + \frac{k}{2}D_\pi - \frac{1}{2}\sum_{P \rightarrow \infty} [P]$. Seule la discussion aux pointes est affectée, et les détails sont laissés en exercice.

Corollaire 3.20. — Soit Γ un sous-groupe d'indice fini de $\text{SL}_2(\mathbf{Z})$. Soit $k \in \mathbf{Z}$. Supposons que toutes les pointes de Γ soient régulières. Alors les séries d'Eisenstein $\{E_k^x\}_{x \in P_\Gamma}$ forment une base de $\mathcal{E}_k(\Gamma) = M_k(\Gamma)/S_k(\Gamma)$.

Démonstration. — On avait vu au paragraphe 2.4.4 l'indépendance linéaire de la famille $\{E_k^x\}_{x \in P_\Gamma}$. D'après le théorème 3.17 la dimension de $\mathcal{E}_k(\Gamma)$ vaut n_∞ . Le corollaire en découle. \square

4. Opérateurs de Hecke

4.1. Opérateurs de Hecke pour les formes modulaires de niveau $\Gamma(1)$. — Avant de définir les opérateurs de Hecke en niveau quelconque on va étudier leur action en niveau $\Gamma(1)$, beaucoup plus simple et intuitive. Rappelons la conjecture de Ramanujan $\tau(nm) = \tau(n)\tau(m)$ si n et m sont premiers entre eux. Même si c'était Mordell qui l'a prouvée c'est Hecke qui a développé une théorie générale qui montre que les coefficients de Fourier des formes modulaires ont de propriétés multiplicatives (remarquons que aussi pour les séries d'Eisenstein on a un résultat similaire puisque si n et m sont premiers entre eux alors $\sigma_k(n)\sigma_k(m) = \sigma_k(nm)$.)

L'idée de Hecke est la suivante. Supposons qu'on définit opérateur :

$$U_p\left(\sum a_n q^n\right) = \sum a_{pn} q^n.$$

Suppose que $\sum a_n q^n$ est une forme modulaire qui appartient à un espace de dimension 1. Si on peut montrer que U_p préserve cet espace, alors $U_p(\sum a_n q^n) = \lambda_p(\sum a_n q^n)$, pour un certain $\lambda_p \in \mathbf{C}$. Cela implique que $a_{pn} = a_n \lambda_p$. Si on normalise de sorte que $a_1 = 1$ alors $a_p = \lambda_p$ et donc $a_{pn} = a_n a_p$.

Par contre la fonction τ de Ramanujan n'est pas totalement multiplicative, on a $\tau(p^2) \neq \tau(p)^2$. Il a conjecturé que pour $p|n$ on devrait avoir $\tau(pn) = \tau(p)\tau(n) - p^{11}\tau(n/p)$. Si on avait donc à deviner le bon opérateur (en poids 12 ce serait

$$T_p(\sum a_n q^n) = \sum_{p \nmid n} a_{pn} q^n + \sum_{p|n} (a_{pn} + p^{11} a_{n/p}) q^n.$$

On pourrait définir les opérateurs de Hecke sur les coefficients de Fourier mais ce sera plus intéressant (et naturel) de définir leur action sur les réseaux. Soit \mathcal{R} l'ensemble des réseaux de \mathbf{C} . Notons $\mathbf{Z}(\mathcal{R})$ le \mathbf{Z} -module libre de base $\{[\Lambda] : \Lambda \in \mathcal{R}\}$. On définit deux familles d'opérateurs $T(n), R(n) : \mathbf{Z}(\mathcal{R}) \rightarrow \mathbf{Z}(\mathcal{R})$, $n \in \mathbf{N}$ par les formules

$$(4.1) \quad \begin{aligned} T(n)([\Lambda]) &:= \sum_{[\Lambda:\Lambda']=n} [\Lambda'] \\ R(n)([\Lambda]) &:= [n\Lambda]. \end{aligned}$$

La somme dans (4.1) est finie car tout $\Lambda \in \mathcal{R}$ tel que $[\Lambda : \Lambda'] = n$ vérifie que $n\Lambda \subset \Lambda'$ et $\Lambda/n\Lambda \simeq (\mathbf{Z}/n\mathbf{Z})^2$ est fini.

Proposition 4.1. — *Les opérateurs $T(n)$ et $R(n)$ satisfont les propriétés suivantes :*

- (1) $R(n) \circ R(m) = R(nm)$;
- (2) $R(n) \circ T(m) = T(m) \circ R(n)$.
- (3) $T(nm) = T(n) \circ T(m)$ si $(n, m) = 1$.
- (4) $T(p^{r+1}) = T(p^r) \circ T(p) - pR(p) \circ T(p^{r-1})$ si p est premier.

Démonstration. — (1) et (2) sont triviales. (3) et (4) seront prouvés en TD. □

Corollaire 4.2. — *Les $T(p^n)$ sont des polynômes en $T(p)$ et $R(p)$, pour p premier.*

On fait agir ces opérateurs sur les fonctions sur \mathcal{R} (étendues par linéarité en des fonctions sur $\mathbf{Z}(\mathcal{R})$). Plus précisément si $F : \mathcal{R} \rightarrow \mathbf{C}$ on a

$$\begin{aligned} (T(n)F)(\Lambda) &= \sum_{[\Lambda:\Lambda']=n} F(\Lambda'); \\ (R(n)F)(\Lambda) &= F(n\Lambda'). \end{aligned}$$

Il est clair que les fonctions homogènes de poids k sont préservées par ces opérateurs. On déduit de la correspondance entre formes homogènes de poids k et les fonctions faiblement modulaires de poids k et niveau $\Gamma(1)$, donnée par $F(\Lambda(\omega_1, \omega_2)) = \omega_2^{-k} f(\omega_1/\omega_2)$, une action sur les fonctions faiblement modulaires de poids k sous $\Gamma(1)$.

Le lemme suivant permet d'expliciter cette action :

Lemme 4.3. — Tout réseau d'indice n dans $\Lambda_\tau = \tau\mathbf{Z} \oplus \mathbf{Z}$ est de la forme $(a\tau + b)\mathbf{Z} \oplus d\mathbf{Z}$ pour une unique matrice $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ telle que $ad = n$, $a > 0$, et $0 \leq b < d$.

Démonstration. — Voir TD. □

Remarque 4.4. — En particulier si $n = p$ est premier les réseaux d'indice p de $\tau\mathbf{Z} \oplus \mathbf{Z}$ sont $p\tau\mathbf{Z} \oplus \mathbf{Z}$ et $(\tau + b)\mathbf{Z} \oplus p\mathbf{Z}$ avec $0 \leq b < p$.

Si f une fonction faiblement modulaire de poids k et niveau $\Gamma(1)$. Alors cette action se décrit de façon explicite par la formule suivante :

$$T(n)f(\tau) = n^{k-1} \sum_{\substack{a \geq 1, ad=n \\ 0 \leq b < d}} d^{-k} f\left(\frac{a\tau + b}{d}\right).$$

Le facteur de normalisation n^{k-1} qui apparaît dans la formule a été ajouté pour avoir de formules entières. En effet, on a la proposition suivante :

Proposition 4.5. — Soit f une fonction faiblement modulaire de poids k et niveau $\Gamma(1)$. Si $f(\tau) = \sum_m a_m q^m$ est le q -développement de f , alors $T(n)f(\tau) = \sum_m b_m q^m$ où

$$b_m = \sum_{d|(m,n)} d^{k-1} a_{mn/d^2}.$$

Démonstration. — Ce sera prouvée en TD. □

Corollaire 4.6. — Avec les mêmes notations on a $b_1 = a_n$.

Corollaire 4.7. — Les opérateurs $T(n)$ préservent $M_k(\Gamma(1))$ et $S_k(\Gamma(1))$.

Théorème 4.8. — Soit $f = \sum_m a_m q^m$ une forme modulaire non nulle de poids k et niveau $\Gamma(1)$. Supposons que f est vecteur propre de tous les $T(n)$, pour la valeur propre $\lambda(n)$. Alors :

- (1) $a_1 \neq 0$.
- (2) $a_n = a_1 \cdot \lambda(n)$

Démonstration. — Si f est vecteur propre de tous les $T(n)$, pour la valeur propre $\lambda(n)$, alors les coefficient b_1 de $T(n)f$ est $\lambda(n)a_1$. Mais le corollaire 4.6 nous dit que $b_1 = a_n$. Du coup $a_n = a_1 \cdot \lambda(n)$ pour tout n et comme f est non nulle on a $a_1 \neq 0$. □

Corollaire 4.9. — Deux formes modulaires de poids k et niveau $\Gamma(1)$ qui sont vecteurs propre de tous les $T(n)$, pour les mêmes valeurs propres $\lambda(n)$, sont proportionnels.

Corollaire 4.10. — Soit $f = \sum_m a_m q^m$ une forme modulaire non nulle de poids k et niveau $\Gamma(1)$. Supposons que f est vecteur propre de tous les $T(n)$, pour la valeur propre $\lambda(n)$. Supposons aussi que f est normalisée de sorte que $a_1 = 1$. Alors

- (1) $\alpha_{nm} = a_n a_m$ si n et m sont premiers entre eux.
- (2) $a_{p^{r+1}} = a_{p^r} a_p - p^{11} a_{p^{r-1}}$ si p est premier.

Démonstration. — En effet les valeurs propres $\lambda(n)$ satisfont les propriétés (3) et (4) de la proposition 4.1. \square

On déduit la première conjecture de Ramanujan.

Corollaire 4.11. — Soit $\Delta = \sum_n \tau(n)q^n$ le q -développement de la fonction Δ de Jacobi. Alors :

- (1) $\tau(nm) = \tau(n)\tau(m)$ si n et m sont premiers entre eux.
- (2) $\tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1})$ si p est premier.

Démonstration. — En effet $\Delta \in S_{12}(\Gamma(1))$ qui est un espace vectoriel de dimension 1 préservé par tous les $T(n)$. Elle est donc vecteur propre pour eux. Le corollaire découle du corollaire précédent. \square

4.2. L'anneau de Hecke en niveau $\Gamma(1)$. — Nous venons de définir une famille d'opérateurs

$$\begin{aligned} T(n) &: M_k(\Gamma(1)) \rightarrow M_k(\Gamma(1)) \\ &S_k(\Gamma(1)) \rightarrow S_k(\Gamma(1)), \end{aligned}$$

pour $n \in \mathbf{N}$. Ces opérateurs satisfont certaines bonnes propriétés de multiplicativité et leurs vecteurs propres sont des formes modulaires dont leurs coefficients de Fourier satisfont le mêmes bonnes propriétés multiplicatives. Ne pourrait-on pas définir une structure d'anneau sur l'ensemble $\{T(n)\}_{n \in \mathbf{N}}$?

4.3. L'anneau de Hecke en niveau $\Gamma(1)$. — Soit $\Delta = \Delta(1) = M_2(\mathbf{Z}) \cap GL_2(\mathbf{Q})_+$. Il est clair que Δ est stable par produit et contient $\Gamma(1)$. Nous allons d'abord décrire l'ensemble $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$.

Le conoyau $\text{Coker}(\alpha) = \mathbf{Z}^2 / \alpha(\mathbf{Z}^2)$ de $\alpha \in \Delta$ est de la forme $\mathbf{Z} / l\mathbf{Z} \oplus \mathbf{Z} / m\mathbf{Z}$ avec $l, m \geq 1$ uniquement déterminés si on demande $l|m$ (théorème des diviseurs élémentaires).

Lemme 4.12. — Notons $\Delta_{l,m}$ l'ensemble des matrices $\alpha \in \Delta$ de diviseurs élémentaires (l, m) . Alors $\Delta_{l,m} = \Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)$

Démonstration. — Supposons $\alpha = \gamma_1 \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \gamma_2$ avec $\gamma_1, \gamma_2 \in \Gamma(1)$. Alors $\alpha(\mathbf{Z}^2) = \gamma_1(l\mathbf{Z} \oplus m\mathbf{Z})$. Donc l'automorphisme γ_1 de \mathbf{Z}^2 induit un isomorphisme $\mathbf{Z}^2 / (l\mathbf{Z} \oplus m\mathbf{Z}) \xrightarrow{\sim} \text{Coker}(\alpha)$ qui montre que $\text{Coker}(\alpha)$ a pour diviseurs élémentaires (l, m) .

Réciproquement, supposons que α a pour diviseurs élémentaires (l, m) . Il existe alors une base (ω_1, ω_2) de \mathbf{Z}^2 telle que $(l\omega_1, m\omega_2)$ soit une base de $\alpha(\mathbf{Z}^2)$. Soit γ_1 la matrice de passage de la base canonique (e_1, e_2) de \mathbf{Z}^2 à (ω_1, ω_2) , et soit γ_2 la matrice de passage de la base $(l\omega_1, m\omega_2)$ de $\alpha(\mathbf{Z}^2)$ à la base $(\alpha(e_1), \alpha(e_2))$ de $\alpha(\mathbf{Z}^2)$. Alors on a $\alpha = \gamma_2 \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \gamma_1$.

A priori on a seulement $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbf{Z})$, mais quitte à changer γ_1 par $\gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et γ_2 par $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \gamma_2$, on voit que $\alpha \in \Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)$. \square

Notons $T(l, m) := [\Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)]$. D'après le lemme, les $T(l, m)$, $1 \leq l|m$, forment une base de $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$.

On peut définir une structure d'anneau sur $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$. Soient $\alpha, \beta \in \Delta$. Alors il existe α_i, β_j tels que :

$$\begin{aligned} \Gamma(1)\alpha\Gamma(1) &= \sqcup_i \Gamma(1)\alpha_i \\ \Gamma(1)\beta\Gamma(1) &= \sqcup_j \Gamma(1)\beta_j. \end{aligned}$$

Alors

$$\Gamma(1)\alpha\Gamma(1)\beta\Gamma(1) = \sqcup_{i,j} \Gamma(1)\alpha_i\beta_j.$$

On définit

$$(4.2) \quad [\Gamma(1)\alpha\Gamma(1)] \cdot [\Gamma(1)\beta\Gamma(1)] = \sum_{\gamma} c_{\gamma} [\Gamma(1)\gamma\Gamma(1)]$$

où γ parcourt l'ensemble des éléments de Δ tels que $\Gamma(1)\gamma\Gamma(1) \subset \Gamma(1)\alpha\Gamma(1)\beta\Gamma(1)$ et c_{γ} est le nombre de couples (i, j) tels que $\Gamma(1)\alpha_i\beta_j = \Gamma(1)\gamma$.

Cette multiplication est bien définie. Elle induit une structure d'anneau sur $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$. On dit que $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$ est l'anneau de Hecke en niveau $\Gamma(1)$. Pour rendre cette multiplication explicite on a besoin du lemme suivant :

Lemme 4.13. — *L'ensemble $\mathcal{L}(\Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, ad = lm, 0 \leq b < d \text{ et } (a, b, d) = l \right\}$ est un ensemble de représentants des $\Gamma(1)$ -classes à gauche dans $\Delta_{l,m}$*

Démonstration. — On utilise la remarque suivante :

$$\text{si } \beta, \beta' \in \Delta, \text{ alors } \beta\Gamma(1) = \beta'\Gamma(1) \Leftrightarrow \beta(\mathbf{Z}^2) = \beta'(\mathbf{Z}^2).$$

En effet, le sens \Rightarrow est clair et l'autre sens se voit en remarquant que $\beta' = \beta\gamma$ si γ désigne la matrice de passage de $(\beta(e_1), \beta(e_2))$ à $(\beta'(e_1), \beta'(e_2))$. Malheureusement, nous voulons des classes à gauche, pas à droite. Nous allons donc raisonner sur les transposées.

Soit $\alpha \in \Delta_{l,m}$. D'après la remarque ci-dessus, on a $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma(1)\alpha$ si et seulement si le réseau $\Lambda := {}^t\alpha(\mathbf{Z}^2)$ est engendré par $(ae_1 + be_2, de_2)$. Si tel est le cas, d est visiblement le plus petit entier k tel que $ke_2 \in \Lambda$, puis a est déterminé par $ad = lm$, ce qui détermine aussi b modulo d . On en déduit l'unicité d'une éventuelle matrice $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma(1)\alpha$ vérifiant $0 \leq b < d$. Pour prouver l'existence, considérons la suite exacte

$$0 \rightarrow (\Lambda + \mathbf{Z}e_2)/\Lambda \rightarrow \mathbf{Z}^2/\Lambda \rightarrow \mathbf{Z}^2/(\Lambda + \mathbf{Z}e_2) \rightarrow 0.$$

Le terme de gauche est cyclique (engendré par l'image de e_2). Notons d son ordre, on a $de_2 \in \Lambda$. Le terme de droite est aussi cyclique (engendré par l'image de e_1). Notons a son ordre. On a alors $ad = |\mathbf{Z}^2/\Lambda| = |\det({}^t\alpha)| = lm$ et $(ae_1 + \mathbf{Z}e_2) \cap \Lambda \neq \emptyset$. Pour tout ω_1 dans cet ensemble, (ω_1, de_2) est une base de Λ , et puisque $de_2 \in \Lambda$, on peut choisir $\omega_1 = ae_1 + be_2$ avec $0 \leq b < d$. On a donc trouvé (a, b, d) mais il reste à prouver que $(a, b, d) = l$. Pour cela notons que la transposée ${}^t\alpha$ est aussi dans $\Delta_{l,m}$, et donc que $\mathbf{Z}^2/\Lambda \simeq \mathbf{Z}/l\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$. En particulier, le noyau de la multiplication par l dans \mathbf{Z}^2/Λ est isomorphe à $(\mathbf{Z}/l\mathbf{Z})^2$, ce qui équivaut à $l\mathbf{Z}^2 \supseteq \Lambda$ et implique $l|(a, b, d)$. Réciproquement, si $\lambda := (a, b, d)$, alors $\Lambda \subseteq \lambda\mathbf{Z}^2$ et \mathbf{Z}^2/Λ contient $(\mathbf{Z}/\lambda\mathbf{Z})^2$, ce qui implique $\lambda|l$. \square

On déduit la proposition suivante :

Proposition 4.14. — *On a les égalités suivantes (où p désigne un nombre premier) :*

- (1) $T(l, m) = T(l, l)T(1, m/l) = T(1, m/l)T(l, l)$
- (2) $T(l, m)T(l', m') = T(l'l', mm')$ si $(lm, l'm') = 1$.
- (3) $T(1, p)T(1, p^r) = T(1, p^{r+1}) + \begin{cases} (p+1)T(p, p) & \text{si } r = 1 \\ pT(p, p)T(1, p^{r-1}) & \text{si } r > 1 \end{cases}$

En particulier, l'anneau $\mathbf{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$ est l'anneau des polynômes en les $T(1, p)$ et $T(p, p)$ où p parcourt les nombres premiers.

Démonstration. — (1) De manière plus générale, si z est un élément central de Δ , alors la formule de produit dans l'anneau de Hecke montre que $[\Gamma z\Gamma][\Gamma\alpha\Gamma] = [\Gamma z\alpha\Gamma] = [\Gamma\alpha\Gamma][\Gamma z\Gamma]$.

(2) Grâce au (1), on peut supposer que $l = l' = 1$. La première chose à démontrer est l'égalité ensembliste $\Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}\Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & m' \end{pmatrix}\Gamma(1) = \Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & mm' \end{pmatrix}\Gamma(1)$ (cf (4.2)). Vu le lemme précédent, cela revient à montrer que pour tous α, α' de diviseurs élémentaires respectifs $(1, m)$ et $(1, m')$, le produit a pour diviseurs élémentaires $(1, mm')$. Or on a une suite exacte

$$0 \rightarrow \alpha\mathbf{Z}^2/\alpha\alpha'\mathbf{Z}^2 \rightarrow \mathbf{Z}^2/\alpha\alpha'\mathbf{Z}^2 \rightarrow \mathbf{Z}^2/\alpha\mathbf{Z}^2 \rightarrow 0$$

qui montre que le conoyau $\text{Coker}(\alpha\alpha')$ est une extension abélienne de $\mathbf{Z}/m\mathbf{Z}$ par $\mathbf{Z}/m'\mathbf{Z}$. Mais puisque $(m, m') = 1$, une telle extension est isomorphe à $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m'\mathbf{Z} = \mathbf{Z}/mm'\mathbf{Z}$, donc les diviseurs élémentaires de $\alpha\alpha'$ sont bien $(1, mm')$.

Ceci implique que $T(1, m)T(1, m') = c.T(1, mm')$ avec c le cardinal de l'ensemble

$$C := \{(\alpha, \alpha') \in \mathcal{L}(\Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}\Gamma(1)) \times \mathcal{L}(\Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & m' \end{pmatrix}\Gamma(1)), \Gamma(1)\alpha\alpha' = \Gamma(1)\begin{pmatrix} 1 & 0 \\ 0 & mm' \end{pmatrix}\Gamma(1)\}.$$

Ici nous pouvons utiliser les systèmes de représentants donnés par le lemme précédent.

Donc si $(\alpha, \alpha') \in C$ on a $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ avec $ad = m$, $0 \leq b < d$ et $(a, b, d) = 1$

et de même $\alpha' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ avec $a'd' = m'$, $0 \leq b' < d'$ et $(a', b', d') = 1$. Alors

$\alpha\alpha' = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$. D'après la preuve du lemme précédent, on a donc $\alpha\alpha' \in \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & mm' \end{pmatrix}$ si et seulement si $aa' = 1$, $dd' = mm'$ et $mm' | (ab' + bd')$. Ceci équivaut encore $a = a' = 1$, $d = m$, $d' = m'$ et donc $mm' | (b' + bm') \Leftrightarrow b' + bm' = 0 \Leftrightarrow b = b' = 0$. On voit donc que $(\alpha, \alpha') = \left(\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & m' \end{pmatrix} \right)$ et par suite, que $c = 1$, comme voulu.

(3) Commençons par évaluer l'ensemble $\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)$. Pour cela, il faut comprendre les diviseurs élémentaires d'un produit $\alpha\alpha'$ lorsque α est de type $(1, p)$ et α' est de type $(1, p^r)$. Or, la suite exacte donnée ci-dessus nous dit que $\text{Coker}(\alpha\alpha')$ est une extension de $\mathbf{Z}/p\mathbf{Z}$ par $\mathbf{Z}/p^r\mathbf{Z}$. Il y a donc deux possibilités : soit $\text{Coker}(\alpha\alpha') \simeq \mathbf{Z}/p^{r+1}\mathbf{Z}$, soit $\text{Coker}(\alpha\alpha') \simeq \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p^r\mathbf{Z}$. Les diviseurs élémentaires de $\alpha\alpha'$ sont donc $(1, p^{r+1})$ ou (p, p^r) et on en déduit

$$\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1) = \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^{r+1} \end{pmatrix} \Gamma(1) \sqcup \Gamma(1) \begin{pmatrix} p & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1).$$

La définition du produit nous donne alors

$$T(1, p)T(1, p^r) = cT(1, p^{r+1}) + c'T(p, p^r).$$

Commençons par évaluer c . Par définition c'est le cardinal de l'ensemble

$$C := \{(\alpha, \alpha') \in \mathcal{L}(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma(1)) \times \mathcal{L}(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)), \Gamma(1)\alpha\alpha' = \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^{r+1} \end{pmatrix}\}.$$

L'ensemble de représentants fourni par le lemme précédent s'écrit ici

$$\mathcal{L}(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)) := \left\{ \begin{pmatrix} p^{r-s} & m \\ 0 & p^s \end{pmatrix}, 0 \leq s \leq r, m < p^s, (m, p^s, p^{r-s}) = 1 \right\}$$

On voit alors que $C = \left\{ \left(\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \right) \right\}$, et en particulier $c = 1$.

Pour évaluer c' on pourrait aussi expliciter l'ensemble

$$C' := \{(\alpha, \alpha') \in \mathcal{L}(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma(1)) \times \mathcal{L}(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)), \Gamma(1)\alpha\alpha' = \Gamma(1) \begin{pmatrix} p & 0 \\ 0 & p^r \end{pmatrix}\}.$$

Mais il est plus élégant d'utiliser le *degré* d'une double classe. Par définition, on pose

$$\deg([\Gamma(1)\alpha\Gamma(1)]) = |\Gamma(1) \setminus (\Gamma(1)\alpha\Gamma(1))| \quad (\text{cardinal}),$$

et on l'étend par linéarité à l'anneau de Hecke. On vérifie alors (exercice ci-dessous) que l'application $\deg : \mathbf{Z}[\Gamma(1) \setminus \Delta / \Gamma(1)] \rightarrow \mathbf{Z}$ est un homomorphisme d'anneaux. Dans notre cas, on a $\deg(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)) = p^r + p^{r-1}$, et on obtient

$$(1+p)(p^r + p^{r-1}) = c(p^{r+1} + p^r) + c' \deg(\Gamma(1) \begin{pmatrix} p & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)),$$

ce qui, compte tenu de $c = 1$ et de

$$\deg(\Gamma(1) \begin{pmatrix} p & 0 \\ 0 & p^r \end{pmatrix} \Gamma(1)) = \deg(\Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & p^{r-1} \end{pmatrix} \Gamma(1)) = \begin{cases} 1 & \text{si } r = 1 \\ p^{r-1} + p^{r-2} & \text{si } r > 1 \end{cases}$$

nous donne $c' = 1 + p$ lorsque $r = 1$ et $c' = p$ lorsque $r > 1$.

Examinons maintenant la dernière assertion. D'après (1) et (2), les $T(1, p)$ et $T(p', p')$ commutent entre eux lorsqu'on varie p et p' . D'après (3) et (2), ils engendrent $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$. Il reste alors à vérifier l'indépendance algébrique de ces éléments. Pour cela, si $1 \leq l|m$, notons $P(l, m)$ le monôme $\prod_{p|l} T(p, p)^{v_p(l)} \prod_{p|m/l} T(1, p)^{v_p(m/l)}$. Alors (2) et (3) montrent qu'en ordonnant l'ensemble des couples (l, m) selon n'importe quel ordre strict raffinant l'ordre partiel induit par la divisibilité $m|m'$, la matrice donnant les $P(l, m)$ en fonction des $T(l, m)$ est triangulaire supérieure avec des 1 sur la diagonale. Puisque les $T(l, m)$ forment une base de $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$, il s'ensuit que les $P(l, m)$ forment aussi une base. \square

Exercice 4.3.1. — Montrer que dans l'expression $[\Gamma\alpha\Gamma][\Gamma\beta\Gamma] = \sum_{\delta} c_{\delta} [\Gamma\delta\Gamma]$, on a

$$c_{\delta} = |\{(\gamma, \gamma') \in \mathcal{L}(\Gamma\alpha\Gamma) \times \mathcal{L}(\Gamma\beta\Gamma), \Gamma\gamma\gamma'\Gamma = \Gamma\delta\Gamma\}| \cdot |\Gamma \backslash (\Gamma\delta\Gamma)|^{-1}.$$

En déduire que l'application degré de la preuve précédente est bien un homomorphisme d'anneaux. Montrer aussi que l'égalité $[\Gamma\alpha\Gamma][\Gamma\beta\Gamma] = [\Gamma\alpha\beta\Gamma]$ est équivalente à ce que $\mathcal{L}(\Gamma\alpha\Gamma) \cdot \mathcal{L}(\Gamma\beta\Gamma)$ (produit dans Δ) soit un ensemble de représentants de $\Gamma \backslash (\Gamma\alpha\beta\Gamma)$.

Corollaire 4.15. — Pour $n \in \mathbf{N}$, notons $T(n) := \sum_{lm=n} T(l, m)$ (en particulier on a $T(p) = T(1, p)$). Alors on a les formules :

- (1) $T(nm) = T(n)T(m)$ si $(n, m) = 1$,
- (2) $T(p^{r+1}) = T(p)T(p^r) - pT(p, p)T(p^{r-1})$,

et, de manière équivalente, la formule générale $T(n)T(m) = \sum_{l|(m, n)} lT(l, l)T(mn/l^2)$.

Démonstration. — Exercice. \square

4.4. Action sur les formes modulaires de niveau $\Gamma(1)$. — Rappelons que l'action de poids k de $\mathrm{SL}_2(\mathbf{R})$ sur $M_k(\Gamma(1))$ est induite par l'action de poids k du groupe $G = \mathrm{GL}_2(\mathbf{Q})_+$ donnée par $f[\gamma]_k(\tau) = \det(\gamma)^{k/2} j(\gamma, \tau)^{-k} f(\gamma\tau)$. Néanmoins, pour obtenir des formules rationnelles, et même entières, il est préférable de normaliser cette action différemment en posant

$$f[\gamma]'_k(\tau) = \det(\gamma)^{k-1} j(\gamma, \tau)^{-k} f(\gamma\tau) = \det(\gamma)^{k/2-1} f[\gamma]_k(\tau).$$

De même on pose $f[\Gamma(1)\alpha\Gamma(1)]'_k = \sum_i f[\alpha_i]'_k$ si $\Gamma(1)\alpha\Gamma(1) = \sqcup_i \Gamma(1)\alpha_i$ et on étend cette action à l'anneau de Hecke $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$ par linéarité. Voici des formules explicites.

Lemme 4.16. — Pour $n \geq 1$ et $f \in M_k(\Gamma(1))$, on a

$$f[T(n)]'_k(\tau) = n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} d^{-k} f((a\tau + b)/d).$$

Si $f(\tau) = \sum_{m \in \mathbf{N}} a(m)q^m$ est son q -développement en ∞ (avec $q = \exp(2i\pi\tau)$), alors

$$f[T(n)]'_k(\tau) = \sum_{m \in \mathbf{N}} \left(\sum_{d|(m,n)} d^{k-1} a(mn/d^2) \right) q^m.$$

Démonstration. — Par définition, si $\mathcal{L} \subset \Delta$ est n'importe quel ensemble de représentants des $\Gamma(1)$ -classes à gauche dans $\Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)$, on a

$$f[T(l, m)]'_k(\tau) = \sum_{\gamma \in \mathcal{L}} \det(\gamma)^{k-1} j(\gamma, \tau)^{-k} f(\gamma\tau).$$

En prenant l'ensemble

$$\mathcal{L} = \mathcal{L}(\Gamma(1) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma(1)) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, ad = lm, 0 \leq b < d, (a, b, d) = l \right\}$$

fourni par le lemme précédent, on voit que $f[T(l, m)]'_k(\tau)$ est donné par une somme similaire à celle de l'énoncé, restreinte aux indices (a, b, d) tels que $(a, b, d) = l$. En sommant sur les (l, m) tels que $lm = n$, on obtient la première formule de l'énoncé.

La seconde découle de la première et des deux égalités

$$f((a\tau + b)/d) = \sum_{m \in \mathbf{N}} a(m) e^{2i\pi mb/d} q^{ma/d}, \text{ et } \sum_{b=0}^{d-1} e^{2i\pi mb/d} = \begin{cases} d & \text{si } d|m \\ 0 & \text{sinon.} \end{cases}$$

□

On retrouve donc les formules du premier paragraphe.

4.5. Formalisme général. — Deux sous-groupes Γ_1, Γ_2 d'un groupe G sont dits *commensurables* si $\Gamma_1 \cap \Gamma_2$ est d'indice fini dans Γ_1 et Γ_2 . On obtient ainsi une relation d'équivalence sur les sous-groupes de G (exercice : prouver la transitivité). Un sous-groupe Γ sera appelé *sous-groupe de Hecke* de G si pour tout $\alpha \in G$, Γ et $\alpha\Gamma\alpha^{-1}$ sont commensurables. Dans ce cas tout sous-groupe Γ' commensurable avec Γ est un sous-groupe de Hecke.

Exemple 4.17. — Dans $G = \text{GL}_2(\mathbf{Q})$, les sous-groupes d'indice fini de $\text{SL}_2(\mathbf{Z})$ sont des sous-groupes de Hecke. Pour le voir, il suffit de montrer que si $\alpha \in \text{GL}_2(\mathbf{Q})$, alors $\alpha\Gamma(1)\alpha^{-1} \cap \Gamma(1)$ est d'indice fini dans $\Gamma(1)$. Quitte à multiplier α par un scalaire, on peut supposer que $\alpha \in \text{M}_2(\mathbf{Z})$. Soit alors N son déterminant. On a $N\alpha^{-1} \in \text{M}_2(\mathbf{Z})$ (c'est la transposée de la comatrice de α) donc $\alpha^{-1}(N\text{M}_2(\mathbf{Z}))\alpha \subset \text{M}_2(\mathbf{Z})$, donc $\alpha^{-1}\Gamma(N)\alpha \subset \text{M}_2(\mathbf{Z})$. Comme $\alpha^{-1}\Gamma(N)\alpha$ est un groupe, on a $\alpha^{-1}\Gamma(N)\alpha \subset \text{GL}_2(\mathbf{Z})$, et comme $\det(\alpha^{-1}\gamma\alpha) = \det(\gamma)$, on a $\alpha^{-1}\Gamma(N)\alpha \subset \text{SL}_2(\mathbf{Z})$, et finalement $\Gamma(N) \subset \alpha\Gamma(1)\alpha^{-1} \cap \Gamma(1)$.

Soient Γ_1, Γ_2 deux sous-groupes de Hecke commensurables de G . Alors les orbites de Γ_2 agissant à droite sur $\Gamma_1 \backslash G$ sont *finies*. En effet, on a une bijection

$$(\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2) \backslash \Gamma_2 \xrightarrow{\sim} \Gamma_1 \backslash (\Gamma_1\alpha\Gamma_2)$$

donnée par $(\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2)\gamma \mapsto \Gamma_1\alpha\gamma$. Cela permet d'identifier $\mathbf{Z}[\Gamma_1 \backslash G / \Gamma_2]$ aux invariants $\mathbf{Z}[\Gamma_1 \backslash G]^{\Gamma_2}$. Considérons alors l'application

$$\begin{aligned} \text{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[\Gamma_2 \backslash G], \mathbf{Z}[\Gamma_1 \backslash G]) &\rightarrow \mathbf{Z}[\Gamma_1 \backslash G / \Gamma_2] \\ \varphi &\mapsto \varphi([\Gamma_2.1]) \end{aligned} .$$

Le Hom désigne les homomorphismes de $\mathbf{Z}[G]$ -modules (à droite). Comme $\mathbf{Z}[\Gamma_2 \backslash G]$ est engendré, en tant que $\mathbf{Z}[G]$ -module, par $[\Gamma_2.1]$, un tel homomorphisme est entièrement déterminé par sa valeur $\varphi([\Gamma_2.1])$, laquelle doit être un élément Γ_2 -invariant de $\mathbf{Z}[\Gamma_1 \backslash G]$, que l'on peut donc identifier à un élément de $\mathbf{Z}[\Gamma_1 \backslash G / \Gamma_2]$. Réciproquement, la donnée d'un tel élément détermine un φ , *i.e.* l'application ci-dessus est donc bijective. Explicitement, l'action de $[\Gamma_1\alpha\Gamma_2]$ est donnée par

$$[\Gamma_1\alpha\Gamma_2] : \begin{array}{ccc} \mathbf{Z}[\Gamma_2 \backslash G] & \rightarrow & \mathbf{Z}[\Gamma_1 \backslash G] \\ [\Gamma_2g] & \mapsto & \sum_{\Gamma_1\gamma \in \Gamma_1 \backslash (\Gamma_1\alpha\Gamma_2)} [\Gamma_1\gamma g] \end{array} .$$

La notation en indice signifie concrètement que l'on peut sommer sur γ décrivant n'importe quel ensemble $\mathcal{L}(\Gamma_1\alpha\Gamma_2)$ de représentants dans G de l'ensemble quotient $\Gamma_1 \backslash (\Gamma_1\alpha\Gamma_2)$, le résultat étant clairement indépendant du choix de ces représentants.

Si Γ_3 est un troisième sous-groupe commensurable à Γ_1 (et donc à Γ_2), la composition des homomorphismes nous fournit une application "produit"

$$\mathbf{Z}[\Gamma_1 \backslash G / \Gamma_2] \otimes \mathbf{Z}[\Gamma_2 \backslash G / \Gamma_3] \rightarrow \mathbf{Z}[\Gamma_1 \backslash G / \Gamma_3]$$

qui est explicitement donnée, sur les bases canoniques, par la formule

$$[\Gamma_1\alpha\Gamma_2].[\Gamma_2\beta\Gamma_3] = \sum_{\delta} c_{\delta}.[\Gamma_1\delta\Gamma_3]$$

où $c_{\delta} \in \mathbf{N}$ est le cardinal de l'ensemble suivant

$$\{(\Gamma_1\gamma, \gamma') \in \Gamma_1 \backslash (\Gamma_1\alpha\Gamma_2) \times \mathcal{L}(\Gamma_2\beta\Gamma_3), \Gamma_1\gamma\gamma' = \Gamma_1\delta\} .$$

Dans cet ensemble, on a noté $\mathcal{L}(\Gamma_2\beta\Gamma_3)$ un ensemble de représentants, dans G , de $\Gamma_2 \backslash (\Gamma_2\beta\Gamma_3)$. L'ensemble décrit dépend du choix de ces représentants, mais le cardinal n'en dépend pas, puisque c'est le coefficient de $[\Gamma_1\delta\Gamma_3]$ dans l'expression du produit décrit ci-dessus. [Exercice : vérifier directement que le cardinal ne dépend pas du choix de représentants].

Remarque 4.18. — $c_{\delta} \neq 0$ si et seulement si $\Gamma_1\delta\Gamma_3 \subset \Gamma_1\alpha\Gamma_2\beta\Gamma_3$.

Lorsqu'on fait $\Gamma_1 = \Gamma_2 = \Gamma_3 =: \Gamma$, on a ainsi obtenu une structure d'anneau sur $\mathbf{Z}[\Gamma \backslash G / \Gamma]$ appelé *anneau de Hecke de (G, Γ)* , ainsi qu'un isomorphisme d'anneaux

$$\text{End}_{\mathbf{Z}[G]}(\mathbf{Z}[\Gamma \backslash G]) \xrightarrow{\sim} \mathbf{Z}[\Gamma \backslash G / \Gamma] .$$

Si $\Delta \subset G$ est un sous-ensemble stable par multiplication et contenant Γ , on note $\mathbf{Z}[\Gamma \backslash \Delta / \Gamma]$ le sous-module de $\mathbf{Z}[\Gamma \backslash G / \Gamma]$ engendré par les $[\Gamma \delta \Gamma]$, $\delta \in \Delta$. Vu la formule donnant le produit, c'est un *sous-anneau* de $\mathbf{Z}[\Gamma \backslash G / \Gamma]$.

Maintenant, donnons-nous un \mathbf{C} -espace vectoriel V (ou un \mathbf{Z} -module) muni d'une action linéaire à droite de G , que l'on note $(v, g) \mapsto v.g$. Pour la même raison que plus haut, l'application suivante

$$\begin{aligned} \text{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[\Gamma \backslash G], V) &\rightarrow V^\Gamma \\ \varphi &\mapsto \varphi([\Gamma.1]) \end{aligned}$$

est un isomorphisme de \mathbf{C} -espaces vectoriels. On en déduit, par composition avec $[\Gamma_1 \alpha \Gamma_2]$, une application linéaire $V^{\Gamma_1} \rightarrow V^{\Gamma_2}$ qui est explicitement donnée par

$$\forall v \in V^{\Gamma_1}, v.[\Gamma_1 \alpha \Gamma_2] = \sum_{\Gamma_1 \gamma \in \Gamma_1 \backslash (\Gamma_1 \alpha \Gamma_2)} v\gamma.$$

[Exercice : vérifier directement que le membre de droite est bien invariant par Γ_2 .] Par définition, ces applications sont compatibles au "produit", et en particulier, lorsque $\Gamma_2 = \Gamma_1 = \Gamma$, on obtient une structure de $\mathbf{Z}[\Gamma \backslash G / \Gamma]$ -module à droite sur V^Γ .

Exemple 4.19. — Prenons V l'espace des fonctions $\mathbb{H} \rightarrow \mathbf{C}$ sur lequel $G = \text{GL}_2(\mathbf{Q})_+$ agit par l'action de poids $k \geq 0$ donnée par $f[\gamma]_k(\tau) := \det(\gamma)^{k/2} j(\gamma, \tau)^{-k} f(\gamma\tau)$. L'espace V^Γ contient les sous-espaces $M_k(\Gamma)$ et $S_k(\Gamma)$. La formule $f.[\Gamma_1 \alpha \Gamma_2]_k = \sum_{\gamma \in \mathcal{L}(\Gamma_1 \alpha \Gamma_2)} f[\gamma]_k$ montre (exercice) que $[\Gamma_1 \alpha \Gamma_2]_k$ respecte l'holomorphie sur \mathbb{H} et aux pointes, et donc envoie $M_k(\Gamma_1)$ dans $M_k(\Gamma_2)$ et $S_k(\Gamma_1)$ dans $S_k(\Gamma_2)$. En particulier, on a une action à droite de $\mathbf{Z}[\Gamma \backslash G / \Gamma]$ sur $M_k(\Gamma)$ et $S_k(\Gamma)$.

4.6. L'anneau de Hecke en niveau $\Gamma_0(N)$. — Nous allons décrire l'anneau de Hecke $\mathcal{H}_0(N) := \mathbf{Z}[\Gamma_0(N) \backslash \Delta_0(N) / \Gamma_0(N)]$ où $\Delta_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta, c \equiv 0[N] \text{ et } (a, N) = 1 \right\}$. L'invariant principal d'une matrice $\alpha \in \Delta_0(N)$ est toujours le couple (l, m) des diviseurs élémentaires de son conoyau. La condition $\alpha \in \Delta_0(N)$ impose que $(l, N) = 1$.

Lemme 4.20. — Notons $\Delta_0(N)_{l,m}$ l'ensemble des $\alpha \in \Delta_0(N)$ d'invariants (l, m) .

$$(1) \Delta_0(N)_{l,m} = \Gamma_0(N) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma_0(N).$$

$$(2) \text{l'ensemble } \mathcal{L}_0(N)_{l,m} := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, (a, N) = 1, ad = lm, 0 \leq b < d \text{ et } (a, b, d) = l \right\}$$

est un ensemble de représentants des $\Gamma_0(N)$ -classes à gauche dans $\Delta_0(N)_{l,m}$.

Démonstration. — (1) La différence avec le cas $\Gamma(1)$ est la suivante. Partant de $\alpha \in \Delta_0(N)$ on doit trouver une base (ω_1, ω_2) de \mathbf{Z}^2 telle que :

- $(l\omega_1, m\omega_2)$ soit une base de $\alpha(\mathbf{Z}^2)$
- $\omega_1 \in (\mathbf{Z} \oplus N\mathbf{Z})$ (pour que la matrice de passage γ_1 soit dans $\Gamma_0(N)$).
- $\alpha(e_1) \in (l\mathbf{Z}\omega_1 \oplus Nm\mathbf{Z}\omega_2)$ (pour que la matrice de passage γ_2 soit dans $\Gamma_0(N)$).

On peut montrer que toute base (ω_1, ω_2) de \mathbf{Z}^2 telle que $(l\omega_1, mN\omega_2)$ soit une base de $\alpha(\mathbf{Z} \oplus N\mathbf{Z})$ convient (exercice ou cf Miake 4.5.1).

(2) On procède comme dans le cas $\Gamma(1)$ en remarquant que pour $\alpha, \alpha' \in \Delta_0(N)$, si $\alpha' = \gamma\alpha$ pour un $\gamma \in \Gamma(1)$, alors $\gamma \in \Gamma_0(N)$. \square

Notons encore $T(l, m) := [\Gamma_0(N) \begin{pmatrix} l & 0 \\ 0 & m \end{pmatrix} \Gamma_0(N)]$. D'après le lemme, les $T(l, m)$, pour $1 \leq l|m$ et $(l, N) = 1$, forment une base de $\mathcal{H}_0(N)$. Voici la table de multiplication dans cette base.

Proposition 4.21. — *On a les égalités suivantes (où p désigne un nombre premier) :*

- (1) $T(l, m) = T(l, l)T(1, m/l) = T(1, m/l)T(l, l)$
- (2) $T(l, m)T(l', m') = T(ll', mm')$ si $(lm, l'm') = 1$.
- (3) Si $p \nmid N$, $T(1, p)T(1, p^r) = T(1, p^{r+1}) + \begin{cases} (p+1)T(p, p) & \text{si } r = 1 \\ pT(p, p)T(1, p^{r-1}) & \text{si } r > 1 \end{cases}$
- (4) Si $p|N$, $T(1, p)T(1, p^r) = T(1, p^{r+1})$.

En particulier, l'anneau $\mathbf{Z}[\Gamma_0(N) \backslash \Delta_0(N) / \Gamma_0(N)]$ est l'anneau des polynômes en les $T(1, p)$, p premier et les $T(p', p')$, p' premier ne divisant pas N .

Démonstration. — A partir du lemme précédent, et notamment des ensembles $\mathcal{L}_0(N)_{l,m}$, on peut suivre le même raisonnement que dans le cas $\Gamma(1)$. \square

Corollaire 4.22. — *Pour $n \in \mathbf{N}$, notons $T(n) := \sum_{lm=n, (l,N)=1} T(l, m)$ (en particulier on a $T(p) = T(1, p)$). Alors on a les formules :*

- (1) $T(nm) = T(n)T(m)$ si $(n, m) = 1$,
- (2) $T(p^{r+1}) = T(p)T(p^r) - pT(p, p)T(p^{r-1})$, si $p \nmid N$
- (3) $T(p^{r+1}) = T(p)T(p^r)$ si $p|N$.

et, de manière équivalente, la formule générale

$$T(n)T(m) = \sum_{\substack{l|(m,n) \\ (l,N)=1}} lT(l, l)T(mn/l^2).$$

Démonstration. — Exercice. \square

4.7. Action sur les formes modulaires en niveau $\Gamma_1(N)$. — Bien-sûr, l'anneau de Hecke $\mathcal{H}_0(N)$ agit naturellement sur $M_k(\Gamma_0(N))$. Mais en fait, il agit aussi sur les formes modulaires en niveau $\Gamma_1(N)$, une fois qu'on les a "coupées en morceaux". On rappelle qu'on avait une décomposition :

$$\begin{aligned} M_k(\Gamma_1(N)) &= \bigoplus_{\chi} M_k(\Gamma_0(N), \chi) \\ f &= \sum_{\chi} f_{\chi} \end{aligned} \quad \text{avec } f_{\chi} = [\Gamma_0(N) : \Gamma_1(N)]^{-1} \sum_{\gamma \in \Gamma_0(N)/\Gamma_1(N)} \chi^{-1}(\gamma) \cdot f[\gamma]_k.$$

où χ décrit les caractères de Dirichlet $\Gamma_0(N)/\Gamma_1(N) \rightarrow \mathbf{C}^{\times}$. et

$$M_k(\Gamma_0(N), \chi) = \{f \in M_k(\Gamma_1(N)), f[\gamma]_k = \chi(\gamma)f, \forall \gamma \in \Gamma_0(N)\}.$$

En d'autres termes, $M_k(\Gamma_0(N), \chi)$ consiste en des fonctions invariantes sous $\Gamma_0(N)$ pour l'action de poids k et tordue par χ donnée par $f[\gamma]_k^\chi := \chi^{-1}(\gamma)f[\gamma]_k$. Le point clef, expliqué ci-dessous, est que le caractère χ se prolonge en une application multiplicative $\chi : \Delta_0(N) \rightarrow \mathbf{C}^\times$. Ceci permet de tordre l'action de $\Delta_0(N)$ par la même formule $f[\alpha]_k^\chi := \chi(\alpha)^{-1}f[\alpha]_k'$ et de faire agir $\mathcal{H}_0(N)$ sur $M_k(\Gamma_0(N), \chi)$ par la formule habituelle

$$f[\Gamma_0(N)\alpha\Gamma_0(N)]_k^\chi := \sum_{\alpha' \in \Gamma_0(N) \backslash (\Gamma_0(N)\alpha\Gamma_0(N))} f[\alpha']_k^\chi = \sum_{\alpha' \in \Gamma_0(N) \backslash (\Gamma_0(N)\alpha\Gamma_0(N))} \chi(\alpha')^{-1}f[\alpha']_k'.$$

Pour voir que χ se prolonge à $\Delta_0(N)$, on remarque que l'application

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mapsto d \pmod{N} \in (\mathbf{Z}/N\mathbf{Z})^\times$$

induit un isomorphisme $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^\times$. Ainsi les caractères de $\Gamma_0(N)/\Gamma_1(N)$ sont de la forme $\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \psi(d) = \psi(a)^{-1} = \bar{\psi}(a)$ où ψ décrit les caractères de Dirichlet modulo N . On peut donc prolonger χ à $\Delta_0(N)$ par la formule $\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \bar{\psi}(a)$ (mais pas $\psi(d)$ car d n'est pas nécessairement premier à N !).

Dorénavant, nous ferons l'abus de noter par la même lettre χ un caractère de Dirichlet et le caractère de $\Gamma_0(N)$ correspondant, et même la fonction $\mathbf{Z} \rightarrow \mathbf{C}$ correspondante qui envoie n sur $\chi(n)$ si $(n, N) = 1$ et sur 0 sinon.

Lemme 4.23. — Pour $n \geq 1$ et $f \in M_k(\Gamma_0(N), \chi)$, on a

$$f[T(n)]_k^\chi(\tau) = n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} \chi(a)d^{-k}f((a\tau + b)/d).$$

Si $f(\tau) = \sum_{m \in \mathbf{N}} a(m)q^m$ est son q -développement en ∞ (avec $q = \exp(2i\pi\tau)$), alors

$$f[T(n)]_k^\chi(\tau) = \sum_{m \in \mathbf{N}} \left(\sum_{d|(m,n)} \chi(d)d^{k-1}a(mn/d^2) \right) q^m.$$

Démonstration. — Même calcul que pour $\Gamma(1)$. Dans la première formule, on n'oubliera pas que $\chi(a) = 0$ si $(a, N) \neq 1$, idem dans la seconde ligne pour $\chi(d)$. \square

4.8. Les opérateurs de Hecke et le produit de Petersson. — Dans le chapitre précédent nous avons trouvé une base de la partie d'Eisenstein $\mathcal{E}_k(\Gamma) := M_k(\Gamma)/S_k(\Gamma)$. Par contre on avait juste trouvé un ensemble de générateurs de $S_k(\Gamma)$. Dans cette section nous allons voir qu'il existe une base (non explicite) de l'espace que formes paraboliques avec des bonnes propriétés.

4.8.1. Niveau $\Gamma(1)$. — Nous allons maintenant montrer que dans le cas de niveau $\Gamma(1)$ les $T(n)$ sont auto-adjoints pour le produit de Petersson. Nous aurons besoin du lemme suivant.

Lemme 4.24. — Soit $\alpha \in \Delta$ et Γ d'indice fini dans $\Gamma(1) \cap \alpha^{-1}\Gamma(1)\alpha$. Alors pour $f, g \in S_k(\alpha\Gamma\alpha^{-1})$, on a $f[\alpha]_k, g[\alpha]_k \in S_k(\Gamma)$ et

$$\langle f[\alpha]_k, g[\alpha]_k \rangle_\Gamma = \langle f, g \rangle_{\alpha\Gamma\alpha^{-1}}.$$

Démonstration. — Le fait que $f[\alpha]_k, g[\alpha]_k \in S_k(\Gamma)$ est évident. Soit $h(\tau) := \text{Im}(\tau)^k f(\tau)\overline{g(\tau)}$. La formule $\text{Im}(\alpha\tau) = \det(\alpha)|j_\alpha(\tau)|^{-2}\text{Im}(\tau)$ montre que $h(\alpha\tau) = \text{Im}(\tau)^k f[\alpha]_k(\tau)\overline{g[\alpha]_k(\tau)}$. On a donc

$$\langle f[\alpha]_k, g[\alpha]_k \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{D_\Gamma} h(\alpha\tau) d\mu(\tau) = \frac{1}{V_\Gamma} \int_{\alpha D_\Gamma} h(\tau) d\mu(\tau) = \langle f, g \rangle_{\alpha\Gamma\alpha^{-1}}.$$

Ici, D_Γ est un domaine fondamental pour Γ dans \mathbb{H} . La première égalité vient de la définition du produit de Petersson, la seconde de l'invariance de $d\mu(\tau)$ sous $\text{GL}_2(\mathbf{R})_+$, et la troisième du fait que αD_Γ est un domaine fondamental pour $\alpha\Gamma\alpha^{-1}$, de volume égal à celui de D_Γ . \square

Proposition 4.25. — Pour $f, g \in S_k(\Gamma(1))$ on a $\langle [T(n)]'_k f, g \rangle_{\Gamma(1)} = \langle f, [T(n)]'_k g \rangle_{\Gamma(1)}$.

Démonstration. — Il suffit bien sûr de prouver la même formule pour l'action de poids k de $T(l, m)$. Montrons d'abord qu'il existe un système de représentants commun aux $\Gamma(1)$ -classes à gauche et à droite dans $\Delta_{l, m}$. Partons d'un ensemble \mathcal{L} de représentants des classes à gauche. Puisque $\Delta_{l, m}$ est stable par transposition, ${}^t\mathcal{L}$ est un ensemble de représentants des classes à droite. Pour chaque $\alpha \in \mathcal{L}$ il existe $\gamma_\alpha, \delta_\alpha \in \Gamma(1)$ tels que ${}^t\alpha = \gamma_\alpha \alpha \delta_\alpha$. Posons alors $\tilde{\alpha} := \gamma_\alpha \alpha = {}^t\alpha \delta_\alpha^{-1}$. On a donc $\Gamma(1)\tilde{\alpha} = \Gamma(1)\alpha$ et $\tilde{\alpha}\Gamma(1) = {}^t\alpha\Gamma(1)$. L'ensemble $\tilde{\mathcal{L}} = \{\tilde{\alpha}, \alpha \in \mathcal{L}\}$ fait donc l'affaire.

Considérons maintenant l'anti-involution de Δ donnée par $\alpha^* := \det(\alpha)\alpha^{-1}$. Puisqu'elle stabilise $\Gamma(1)$ et envoie $\begin{bmatrix} l & 0 \\ 0 & m \end{bmatrix}$ sur $\begin{bmatrix} m & 0 \\ 0 & l \end{bmatrix}$, elle stabilise aussi $\Delta_{l, m}$. Puisque $\tilde{\mathcal{L}}$ est un ensemble de représentants des $\Gamma(1)$ -classes à droite dans $\Delta_{l, m}$, $\tilde{\mathcal{L}}^*$ est un ensemble de représentants des classes à gauche. Enfin, pour tout $\alpha \in \Delta$ on a $f[\alpha^{-1}]'_k = f[\alpha^*]'_k$.

Choisissons maintenant Γ distingué dans $\Gamma(1)$ et contenu dans $\Gamma(1) \cap \begin{bmatrix} l & 0 \\ 0 & m \end{bmatrix}^{-1}\Gamma(1)\begin{bmatrix} l & 0 \\ 0 & m \end{bmatrix}$. Ainsi Γ est contenu dans tous les $\alpha\Gamma(1)\alpha^{-1}$ et $\alpha^{-1}\Gamma(1)\alpha$ pour $\alpha \in \tilde{\mathcal{L}}$. On a alors, d'après le lemme précédent,

$$\begin{aligned} & \langle f[T(l, m)]'_k, g \rangle_{\Gamma(1)} = \langle f[T(l, m)]'_k, g \rangle_\Gamma \\ &= \sum_{\alpha \in \tilde{\mathcal{L}}} \langle f[\alpha]'_k, g \rangle_\Gamma = \sum_{\alpha \in \tilde{\mathcal{L}}} \langle f[\alpha]'_k, g \rangle_{\Gamma(1) \cap \alpha^{-1}\Gamma(1)\alpha} \\ &= \sum_{\alpha \in \tilde{\mathcal{L}}} \langle f, g[\alpha^{-1}]'_k \rangle_{\alpha\Gamma(1)\alpha^{-1} \cap \Gamma(1)} = \sum_{\alpha \in \tilde{\mathcal{L}}} \langle f, g[\alpha^*]'_k \rangle_\Gamma \\ &= \langle f, g[T(l, m)]'_k \rangle_\Gamma = \langle f, g[T(l, m)]'_k \rangle_{\Gamma(1)}. \end{aligned}$$

\square

Corollaire 4.26. — L'espace $S_k(\Gamma(1))$ admet une base orthogonale formée de formes qui sont des vecteurs propres pour tous les $T(n)$ (et même pour tous les $T(l, m)$). De plus, si $f(\tau) = \sum_{n>0} a(n)q^n$ est une forme propre et de valeurs propres $(\lambda(n))_{n \in \mathbf{N}^*}$, alors

$$\forall n \in \mathbf{N}^*, a(n) = a(1)\lambda(n).$$

En particulier, si f est normalisée de sorte que $a(1) = 1$, on a les propriétés :

$$\begin{cases} a(nm) = a(n)a(m) \text{ si } (n, m) = 1 \\ a(p^{r+1}) = a(p)a(p^r) - p^{k-1}a(p^{r-1}) \text{ pour } p \text{ premier, } r \geq 1. \end{cases}$$

Démonstration. — L'existence d'une base orthogonale de formes propres découle de la diagonalisabilité des $T(l, m)$ (qui sont auto-adjoints), et de la commutativité de $\mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)]$ qui permet une diagonalisation simultanée.

Pour $f \in M_k(\Gamma(1))$, on a vu que le terme en q dans le q -développement de $f[T(n)]'_k(\tau)$ est $a(n)$. Le terme en q de $\lambda(n)f$ est $a(1)\lambda(n)$ d'où l'égalité $a(n) = a(1)\lambda(n)$.

Enfin lorsque $a(1) = 1$, les formules annoncées sont équivalentes aux mêmes formules pour $\lambda(n)$. Or les $\lambda(n)$ sont les valeurs en $T(n)$ d'un homomorphisme d'algèbres $\lambda : \mathbf{Z}[\Gamma(1) \backslash \Delta / \Gamma(1)] \rightarrow \mathbf{C}$, donc vérifient les égalités.

$$\begin{cases} \lambda(nm) = \lambda(n)\lambda(m) \text{ si } (n, m) = 1 \\ \lambda(p^{r+1}) = \lambda(p)\lambda(p^r) - p\lambda(T(p, p))a(p^{r-1}) \text{ pour } p \text{ premier, } r \geq 1. \end{cases}$$

Il reste donc à calculer $\lambda(T(p, p))$, mais $f[T(p, p)]'_k(\tau) = \det \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}^{k-1} j\left(\begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}, \tau\right)^{-1} f(\tau) = p^{2k-2} p^{-k} f(\tau)$, donc $\lambda(T(p, p)) = p^{k-2}$. \square

Remarque 4.27. — La seconde conjecture de Ramanujan, sur la taille des $\tau(n)$ se généralise ainsi : si $f \in S_k(\Gamma(1))$ est une forme propre et normalisée, alors $a(n) = o(n^{(k-1)/2+\varepsilon})$ pour tout $\varepsilon > 0$. Cette conjecture, dite "de Ramanujan-Petersson", équivaut (cf TD) à ce que les racines u_p, v_p du polynôme $X^2 - a(p)X + p^{k-1}$ soient conjuguées complexes (et donc de module $p^{(k-1)/2}$). Des travaux de Shimura ont montré comment cette conjecture était impliquée par les "conjectures de Weil" sur la taille du nombre de points rationnels de certaines variétés sur des corps finis, lesquelles conjectures de Weil ont finalement été démontrées par Deligne à l'aide de la cohomologie étale de Grothendieck.

Remarque 4.28 (cf TD). — Pour une forme parabolique propre et normalisée, la somme de Dirichlet $L(f, s) = \sum a(n)n^{-s}$ converge pour $Re(s) > k/2$ et admet un produit Eulerien

$$L(s, f) = \prod_p \frac{1}{1 - a(p)p^{-s} + p^{k-1-2s}}.$$

La conjecture de Ramanujan-Petersson implique la convergence pour $Re(s) > (k+1)/2$.

4.8.2. Niveau $\Gamma_1(N)$. — Venons-en aux propriétés d'adjonction des $T(n)$ pour le produit de Petersson. Ici se produit un vrai changement par rapport à $\Gamma(1)$. Commençons par un exercice.

Exercice 4.8.1. — Vérifier que la somme $S_k(\Gamma_1(N)) = \bigoplus_{\chi} S_k(\Gamma_0(N), \chi)$ est une somme orthogonale pour le produit de Petersson sur $S_k(\Gamma_1(N))$.

Proposition 4.29. — Supposons $(n, N) = 1$. Alors pour $f, g \in S_k(\Gamma_0(N), \chi)$ on a

$$\langle f[T(n)]_k^{\chi}, g \rangle_{\Gamma_1(N)} = \bar{\chi}(n) \langle f, g[T(n)]_k^{\chi} \rangle_{\Gamma_1(N)}.$$

En particulier, $T(n)$ est un opérateur normal sur $S_k(\Gamma_0(N), \chi)$.

Démonstration. — Il suffit de prouver l'analogie pour $T(l, m)$ sous l'hypothèse que $(lm, N) = 1$. Pour cela on utilise la même involution $\alpha \mapsto \alpha^* = \det(\alpha)\alpha^{-1}$ que dans le cas $\Gamma(1)$. Le point clef est que, sous l'hypothèse $(lm, N) = 1$, la matrice $\begin{pmatrix} m & 0 \\ 0 & l \end{pmatrix}$ est encore dans $\Delta_0(N)$, et donc $\Delta_0(N)_{l,m}$ est stable par l'involution $*$, puisque $\Gamma_0(N)$ l'est. Cela permet de montrer l'existence d'un système de représentants $\tilde{\mathcal{L}}$ commun aux classes à gauche et à droite (noter que la transposée ne fonctionne pas ici). Puis on fait le même calcul que pour $\Gamma(1)$; on choisit Γ distingué contenu dans $\Gamma_1(N) \cap \begin{bmatrix} l & 0 \\ 0 & m \end{bmatrix}^{-1} \Gamma_1(N) \begin{bmatrix} l & 0 \\ 0 & m \end{bmatrix}$ et on écrit

$$\begin{aligned} & \langle f[T(l, m)]_k^{\chi}, g \rangle_{\Gamma_1(N)} = \langle f[T(l, m)]_k^{\chi}, g \rangle_{\Gamma} \\ &= \sum_{\alpha \in \tilde{\mathcal{L}}} \langle f[\alpha]_k^{\chi}, g \rangle_{\Gamma} = \sum_{\alpha \in \tilde{\mathcal{L}}} \chi^{-1}(\alpha) \langle f[\alpha]_k, g \rangle_{\Gamma_1(N) \cap \alpha^{-1} \Gamma_1(N) \alpha} \\ &= \sum_{\alpha \in \tilde{\mathcal{L}}} \chi^{-1}(\alpha) \langle f, g[\alpha^{-1}]_k \rangle_{\alpha \Gamma_1(N) \alpha^{-1} \cap \Gamma_1(N)} = \sum_{\alpha \in \tilde{\mathcal{L}}} \chi^{-1}(\alpha) \overline{\chi(\alpha^*)} \langle f, g[\alpha^*]_k^{\chi} \rangle_{\Gamma} \\ &= \bar{\chi}(\det(\alpha)) \langle f, g[T(l, m)]_k^{\chi} \rangle_{\Gamma} = \bar{\chi}(lm) \langle f, g[T(l, m)]_k^{\chi} \rangle_{\Gamma(1)}. \end{aligned}$$

(Noter que $\chi^{-1} = \bar{\chi}$.) □

Le point nouveau, ici, est que les $T(p)$ pour $p|N$ ne sont pas normaux en général, donc on n'a pas d'argument général pour les diagonaliser. On peut donc seulement diagonaliser simultanément les $T(n)$ pour $(n, N) = 1$.

Corollaire 4.30. — L'espace $S_k(\Gamma_0(N), \chi)$ admet une base orthogonale formée de formes qui sont des vecteurs propres pour tous les $T(n)$ avec $(n, N) = 1$ (et même pour tous les $T(l, m)$ avec $(lm, N) = 1$). De plus, si $f(\tau) = \sum_{n>0} a(n)q^n$ est une forme propre et de valeurs propres $(\lambda(n))_{(n, N)=1}$, alors

$$\forall n \text{ t.q. } (n, N) = 1, a(n) = a(1)\lambda(n).$$

En particulier, si f est normalisée de sorte que $a(1) = 1$, on a les propriétés :

$$\begin{cases} a(nm) = a(n)a(m) \text{ si } (n, m) = 1 \text{ et } (n, N) = 1 \\ a(p^{r+1}) = a(p)a(p^r) - \chi(p)p^{k-1}a(p^{r-1}) \text{ pour } p \text{ premier } \nmid N, r \geq 1. \end{cases}$$

Démonstration. — Même preuve que dans le cas $\Gamma(1)$ sauf deux points. Pour la première propriété de multiplicativité, on utilise $a(nm) = a(m)\lambda(n)$, qui découle de la formule donnant le terme en q^m dans le développement de Fourier de $f[T(n)]_k^\chi$. Pour la seconde, on a besoin de la valeur propre de $[T(p, p)]_k^\chi$ qui est maintenant $\chi(p)p^{k-2}$. \square

Maintenant se posent deux problèmes qui n'apparaissent pas en niveau $\Gamma(1)$.

Problème 4.8.2. — *Pour une forme propre comme dans le corollaire, on n'a qu'une factorisation partielle de la fonction L .*

$$L(s, f) = \prod_{p \nmid N} \frac{1}{1 - a(p)p^{-s} + \chi(p)p^{k-1-2s}} \cdot \left(\sum_{n'} a(n')n'^{-s} \right)$$

où n' décrit les entiers dont tous les facteurs premiers divisent N . Ce n'est pas satisfaisant, et nous devons donc travailler plus pour gagner plus.

Problème 4.8.3. — *Si f est comme dans le corollaire, rien n'empêche $a(1)$ d'être nul ! Dans ce cas, on a même $a(n) = 0$ pour tout n tel que $(n, N) = 1$, et on n'a rien appris sur la fonction L de f .*

4.9. Formes anciennes, formes nouvelles, formes primitives. — En fait, ces deux problèmes sont liés. Pour le voir, fixons un système de valeurs propres $\lambda' = (\lambda(n))_{(n, N)=1}$ et notons $S_k(\Gamma_0(N), \chi)[\lambda']$ le sous-espace propre associé à ce système. Comme les $T(p)$ pour $p|N$ commutent aux $T(n)$, ils stabilisent $S_k(\Gamma_0(N), \chi)[\lambda']$. Si cet espace est par aventure de dimension 1, alors chaque $T(p)$ agit par un scalaire $\lambda(p)$ et l'espace est donc propre pour tous les $\lambda(n)$, $n \in \mathbf{N}$. Dans ce cas la fonction L a bien un produit Eulerien de la forme attendue

$$L(s, f) = \prod_{p \nmid N} \frac{1}{1 - a(p)p^{-s} + \chi(p)p^{k-1-2s}} \prod_{p|N} \frac{1}{1 - a(p)p^{-s}} = \prod_p \frac{1}{1 - a(p)p^{-s} + \chi(p)p^{k-1-2s}}$$

(on se rappelle que $\chi(p) = 0$ si $p|N$.)

Si maintenant l'espace $S_k(\Gamma_0(N), \chi)[\lambda']$ est de dimension > 1 , alors il n'y a pas d'argument *a priori* pour diagonaliser les $T(p)$, $p|N$. Néanmoins, on remarque que, justement dans ce cas, la forme linéaire $f \mapsto a_1(f) = a(1)$ a un noyau non nul, *i.e.* $S_k(\Gamma_0(N), \chi)[\lambda']$ contient des formes non nulles telles que $a(n) = 0$ pour tout n premier à N .

Le résultat suivant explique d'où viennent de telles formes.

Théorème 4.31. — (1) *Soit $l > 1$ un diviseur de N et $f \in S_k(\Gamma_1(N/l))$. Alors la fonction $i_l f : \tau \mapsto f(l\tau)$ est dans $S_k(\Gamma_1(N))$ et vérifie $a_n(i_l f) = 0$ pour $(n, N) = 1$.*

(2) *Réciproquement, si $f \in S_k(\Gamma_1(N))$ vérifie $a_n(f) = 0$ pour $(n, N) = 1$, alors il existe des formes $f_l \in S_k(\Gamma_1(N/l))$ pour $l > 1$ diviseur de N telles que $f = \sum_{l|N} i_l f_l$.*

Démonstration. — (1) Remarquons que $f(l\tau) = l^{1-k} \cdot f\left[\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right]'_k(\tau)$ qui est une fonction faiblement modulaire de poids k pour le groupe $\left[\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right]^{-1} \Gamma_1(N/l) \left[\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right] \cap \Gamma(1)$ qui contient $\Gamma_1(N)$. Elle est aussi clairement holomorphe et s'annule aux pointes, donc $i_l f$ appartient

bien à $S_k(\Gamma_1(N))$. De plus, son q -développement s'écrit $f(l\tau) = \sum_{n \in \mathbf{N}} a_n(f)q^{ln}$, de sorte que $a_n(i_l f) = 0$ si $l \nmid n$. En particulier, $a_n(i_l f) = 0$ si $(n, N) = 1$.

(2) La réciproque est plus difficile et fera l'objet d'une feuille de TD. \square

Ce résultat suggère que la source de nos problèmes se trouve dans les formes modulaires qui proviennent des "niveaux plus bas". Il nous invite donc à considérer le sous-espace $S_k(\Gamma_1(N))^{\text{old}}$ de $S_k(\Gamma_1(N))$ engendré par toutes les fonctions de la forme $f(l\tau)$ où :

- $f \in S_k(\Gamma_1(M))$ pour un diviseur $M|N$ strict.
- $l|(N/M)$ (et $l = 1$ est permis).

Et même si ce n'est pas encore évident, il est très opportun de définir $S_k(\Gamma_1(N))^{\text{new}}$ comme l'orthogonal de $S_k(\Gamma_1(N))^{\text{old}}$ pour le produit de Petersson.

Lemme 4.32. — (1) $S_k(\Gamma_1(N))^{\text{old}}$ et $S_k(\Gamma_1(N))^{\text{new}}$ sont stables sous l'action de $\Gamma_0(N)$ de poids k , et en particulier se décomposent

$$S_k(\Gamma_1(N))^{\text{old}} = \bigoplus_{\chi \in \widehat{\mathbf{Z}/N\mathbf{Z}^\times}} S_k(\Gamma_0(N), \chi)^{\text{old}} \text{ et } S_k(\Gamma_1(N))^{\text{new}} = \bigoplus_{\chi \in \widehat{\mathbf{Z}/N\mathbf{Z}^\times}} S_k(\Gamma_0(N), \chi)^{\text{new}}.$$

De plus on a, en notant m_χ le conducteur de χ ,

$$S_k(\Gamma_0(N), \chi)^{\text{old}} = \sum_{\substack{m_\chi | M | N, M \neq N \\ l | (N/M)}} i_l(S_k(M, \chi)) = \sum_{\substack{m_\chi | M | N, M \neq N \\ l | (N/M)}} i_l(S_k(M, \chi)^{\text{new}}).$$

(2) Soit $m_\chi | M | N$ et l un diviseur premier ou unité de N/M . Alors pour p premier on a

$$[T(p)]_k^{\chi, N} \circ i_l = \begin{cases} i_l \circ [T(p)]_k^{\chi, M} & \text{si } l \neq p \\ i_1 & \text{si } l = p \end{cases}$$

(3) L'application $f \mapsto f[w_N]_k$, où $w_N = \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ induit une involution de $S_k(\Gamma_1(N))$ qui envoie $S_k(\Gamma_0(N), \chi)$ dans $S_k(\Gamma_0(N), \bar{\chi})$. De plus on a

$$[w_N]_k \circ i_l = l^{-1} \cdot (i_1 \circ [w_{N/l}]_k)$$

de sorte que $[w_N]_k$ stabilise $S_k(\Gamma_1(N))^{\text{old}}$.

Démonstration. — (1) Soit $f \in S_k(\Gamma_1(N/l))$ et $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ (donc $l|c$). On a

$$(i_l f) \left[\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right]_k = l^{1-k} \cdot f \left[\begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \right]_k \left[\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right]_k = l^{1-k} \cdot f \left[\begin{bmatrix} a & bl \\ c/l & d \end{bmatrix} \right]_k \left[\begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \right]_k = i_l(f \left[\begin{bmatrix} a & bl \\ c/l & d \end{bmatrix} \right]_k)$$

où l'on remarque que $f \left[\begin{bmatrix} a & bl \\ c/l & d \end{bmatrix} \right]_k \in S_k(\Gamma_1(N/l))$ puisque $\begin{bmatrix} a & bl \\ c/l & d \end{bmatrix} \in \Gamma_0(N/l)$. Ceci montre que $S_k(\Gamma_1(N))^{\text{old}}$ est stable par $\Gamma_0(N)$. Par adjonction de $[\alpha]_k$ et $[\alpha^{-1}]_k$ pour $\alpha \in \Gamma(1)$ (cf lemme plus haut), on en déduit que l'orthogonal $S_k(\Gamma_1(N))^{\text{new}}$ est aussi stable par $\Gamma_0(N)$.

Par ailleurs, si χ est un caractère de Dirichlet modulo M et l un diviseur de N/M , la formule ci-dessus montre aussi que $i_l(S_k(M, \chi)) \subset S_k(N, \chi)$, d'où l'inclusion \supseteq dans l'égalité annoncée. Cela montre l'autre inclusion aussi. En effet si on écrit $f \in S_k(\Gamma_0(N), \chi)^{\text{old}}$ sous la forme $f = \sum_j i_{l_j} f_j$ avec $f_j \in S_k(M_j, \chi_j)$ et $l_j | (N/M_j)$, alors on a aussi $f = \sum_{j, \chi_j = \chi} i_{l_j} f_j$.

(2) Soit $f \in S_k(M, \chi)$. La formule décrivant l'action de $T(p)$ sur les q -développements montre que

$$a_n(i_l(f[T(p)]_k^{\chi, M})) = \begin{cases} 0 & \text{si } l \nmid n \\ \sum_{d|(n/l, p)} \chi(d) d^{k-1} a_{np/d^2}(f) & \text{si } l|n \end{cases}$$

$$a_n((i_l f)[T(p)]_k^{\chi, N}) = \sum_{d|(n, p)} \chi(d) d^{k-1} a_{np/d^2}(i_l f) \text{ avec } a_{np/d^2}(i_l f) = \begin{cases} 0 & \text{si } l \nmid np/d^2 \\ a_{np/d^2}(f) & \text{si } l|np/d^2 \end{cases}$$

Supposons d'abord $l \neq p$. Dans ce cas, on a $l|(np/d^2) \Leftrightarrow l|n$ et $(n, p) = (n/l, p)$, et on trouve que $a_n((i_l f)[T(p)]_k^{\chi, N}) = a_n(i_l(f[T(p)]_k^{\chi, M}))$ comme voulu.

Supposons maintenant $l = p$. Alors en particulier $p|N$ et $\chi(p) = 0$. La formule ci-dessus se simplifie en $a_n((i_p f)[T(p)]_k^{\chi, N}) = a_{np}(i_p(f)) = a_p(f) = a_p(i_1 f)$.

(3) Si $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{Z})$ on calcule que $w_N \begin{bmatrix} a & b \\ c & d \end{bmatrix} w_N^{-1} = \begin{bmatrix} d & -c/N \\ -bN & a \end{bmatrix}$. On voit donc que la conjugaison par w_N induit une involution de $\Gamma_1(N)$ et de $\Gamma_0(N)$. L'application $f \mapsto f[w_N]_k'$ induit donc une involution sur les fonctions faiblement modulaires de poids k et niveau $\Gamma_1(N)$, qui préserve visiblement les formes modulaires et les formes paraboliques. La conjugaison par w_N sur $\Gamma_0(N)$ induit aussi une involution $\chi \mapsto {}^{w_N}\chi$ sur les caractères de $\Gamma_0(N)$ et on a ${}^{w_N}\chi(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \chi(w_N \begin{bmatrix} a & b \\ c & d \end{bmatrix} w_N^{-1}) = \chi(a) = \bar{\chi}(d) = \bar{\chi}(\begin{bmatrix} a & b \\ c & d \end{bmatrix})$, donc ${}^{w_N}\chi = \bar{\chi}$. Il est alors clair que $f \mapsto f[w_N]_k$ envoie $S_k(\Gamma_0(N), \chi)$ dans $S_k(\Gamma_0(N), {}^{w_N}\chi) = S_k(\Gamma_0(N), \bar{\chi})$.

Finalement, on calcule $[w_N]_k \circ i_l$ avec la formule explicite $f[w_N]_k(\tau) = N^{-1} \tau^{-k} f(\frac{-1}{N\tau})$. \square

Remarque 4.33. — D'après le (1), si χ est primitif (i.e. $m_\chi = N$), alors $S_k(\Gamma_0(N), \chi) = S_k(\Gamma_0(N), \chi)^{\text{new}}$.

Corollaire 4.34. — $S_k(\Gamma_0(N), \chi)^{\text{old}}$ et $S_k(\Gamma_0(N), \chi)^{\text{new}}$ sont stables sous l'action de $\mathcal{H}_0(N)$ sur $S_k(\Gamma_0(N), \chi)$.

Démonstration. — D'après le (2) du lemme, $S_k(\Gamma_0(N), \chi)^{\text{old}}$ est stable par tous les $T(p)$. Comme il est aussi clairement stable par les $T(p, p)$, $p \nmid N$, il est stable par $\mathcal{H}_0(N)$. Il s'ensuit que $S_k(\Gamma_0(N), \chi)^{\text{new}}$ est stable par les adjoints des $T(p)$. Pour $p \nmid N$, l'adjoint de $T(p)$ est $\bar{\chi}(p)T(p)$, donc $T(p)$ stabilise $S_k(\Gamma_0(N), \chi)^{\text{new}}$. Pour $p|N$, il faut un autre argument!

Rappelons-nous que dans ce cas $\mathcal{L}_0(N)_{1, p} = \{ \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}, 0 \leq j < p \}$ et on a donc $f[T(p)]_k^\chi = \sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k$. Le calcul utilisé pour montrer que $T(p)$ est normal si $p \nmid N$ montre pour tout p que l'adjoint $T(p)^*$ de $T(p)$ est $f \mapsto \sum_{j=0}^{p-1} f[\begin{bmatrix} p & j \\ 0 & 1 \end{bmatrix}]_k$. Cet opérateur n'est autre que $w_N \circ T(p) \circ w_N^{-1}$. D'après (2) et (3) du lemme, $T(p)^*$ stabilise donc $S_k(\Gamma_0(N), \chi)^{\text{old}}$, et par adjonction, $T(p)$ stabilise $S_k(\Gamma_0(N), \chi)^{\text{new}}$, comme voulu. \square

On peut maintenant faire marcher notre argument basé sur la multiplicité 1 d'un système de valeurs propres partiel.

Corollaire 4.35. — *L'espace des formes nouvelles $S_k(\Gamma_0(N), \chi)^{\text{new}}$ admet une base orthogonale constituée de formes propres pour tous les $T(n)$, $n \in \mathbf{N}$. De plus, la multiplicité d'un système de valeurs propres est 1.*

Démonstration. — Par un argument déjà donnée, il suffit de montrer que la multiplicité d'un système de valeurs propres $\lambda' = (\lambda(n))_{(n,N)=1}$ est 1, i.e. que $S_k(\Gamma_0(N), \chi)^{\text{new}}[\lambda']$ est de dimension 1. Or on a vu que si tel n'est pas le cas, cet espace propre contient une forme non nulle telle que $a_1(f) = 0$ et donc $a_n(f) = 0$ pour $(n, N) = 1$. Mais le (2) du théorème précédent nous dit qu'une telle f est ancienne. Contradiction. \square

Une forme $f \in S_k(\Gamma_1(N))$ nouvelle, propre et normalisée est appelée *forme primitive de conducteur N* . Les formes primitives forment une base de $S_k(\Gamma_1(N))^{\text{new}}$. Le (1) du lemme montre comment toutes les formes de niveau $\Gamma_1(N)$ sont obtenues à partir des formes primitives de niveau $\Gamma_1(M)$, $M|N$. En fait on peut démontrer (nous ne le ferons pas) le théorème suivant.

Théorème 4.36. — *L'ensemble $\{f(l\tau), f \in S_k(\Gamma_1(M)) \text{ primitive et } M|N\}$ est une base de $S_k(\Gamma_1(N))$.*

Références

- [1] Chenevier, Introduction aux formes modulaires, notes à http://gaetan.chenevier.perso.math.cnrs.fr/coursENS/notes_chenevier.pdf
- [2] Dat, photocopié disponible à <http://webusers.imj-prg.fr/~jean-francois.dat/enseignement/FM/FM.pdf>
- [3] Diamond-Shurman, *A first course in modular forms*, Springer.
- [4] Koblitz, *Introduction to elliptic curves and modular forms*, Springer
- [5] Miyake, *Modular Forms*, Springer
- [6] Serre, *Cours d'arithmétique*, Presse Universitaire de France.
- [7] Shimura, *Introduction to the arithmetic theory of Automorphic functions*, Princeton university Press.

ALBERTO MÍNGUEZ, Institut de Mathématiques de Jussieu, Université Paris 6. 4, place Jussieu. 75005, Paris, France. URL: <http://webusers.imj-prg.fr/~alberto.minguez/>
E-mail : alberto.minguez@imj-prg.fr