

## CHAPITRE 2

### Formes modulaires

Une forme modulaire est une fonction analytique sur le demi-plan de Poincaré vérifiant une condition de croissance à l'infini et qui se transforme de manière particulière sous l'action du groupe  $SL_2(\mathbb{Z})$ . Nous les aborderons ici d'abord sous cet aspect, traditionnel, à la manière du livre de Serre. Comme nous le verrons, toute forme modulaire admet un développement de Fourier, dont les coefficients ont des rapports très surprenants avec l'arithmétique. De plus, lorsque l'on fixe leur *poids*, l'espace (vectoriel) des formes modulaires est de dimension finie. Cet énoncé de finitude est la source de nombreuses identités remarquables. On rapporte qu'à ce sujet Eichler aurait dit un jour que les formes modulaires constituent la 5ème opération de l'arithmétique (après l'addition, la soustraction, la multiplication et la division).

Il y a plusieurs autres points de vue importants sur la notion de forme modulaire. Comme nous le verrons, une forme modulaire peut aussi être vue comme une fonction sur l'espace des réseaux de  $\mathbb{C}$ , point de vue qui aura de nombreux avantages, notamment lorsque nous discuterons les opérateurs de Hecke. On aura alors à portée de main un troisième point de vue, le point de vue *groupe*, qui consiste à voir une forme modulaire comme une fonction sur  $GL_2(\mathbb{Z}) \backslash GL_2(\mathbb{R})$  : c'est ce point de vue qui conduit à la notion de forme automorphe, qui fera l'objet de la suite du cours.

RÉFÉRENCES : Henri Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*,

Jean-Pierre Serre, *Cours d'arithmétique*,

Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*,

D. Zagier, *Elliptic modular forms and their applications*, dans *The 1, 2, 3 of modular forms*, Springer Universitext (2008).

#### 1. Action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré et réseaux de $\mathbb{C}$

**1.1. Homographies.** Pour tout corps  $K$ , le groupe  $GL_2(K)$  agit naturellement sur  $K^2$ , et donc sur l'ensemble  $P^1(K)$  des droites vectorielles de ce dernier. On pose

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

Cet ensemble s'identifie à  $P^1(K)$  en envoyant tout élément  $z \in K$  sur la droite engendrée par  $\begin{pmatrix} z \\ 1 \end{pmatrix}$ , et le symbole  $\infty$  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  $(g, z) \mapsto gz$ .

Si  $g$  désigne l'élément  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  de  $\mathrm{GL}_2(K)$ , et si  $z \in K$ , on constate les égalités

$$(1) \quad g \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \begin{cases} (cz+d) \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix} & \text{si } cz+d \neq 0, \\ (az+b) \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } cz+d = 0. \end{cases}$$

On retrouve la formule bien connue  $gz = \frac{az+b}{cz+d}$  si  $cz+d \neq 0$ . Les bijections de  $\widehat{K}$  de cette forme sont appelées *homographies*. Elles forment donc un sous-groupe de  $\mathfrak{S}(\widehat{K})$  isomorphe à  $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^\times$  (une application linéaire préservant toutes les droites étant une homothétie). Par exemple, on a pour  $a \in K^\times$  et  $b, z \in K$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} z = az+b \text{ (homographies affines) et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z = -1/z \text{ (inversion).}$$

Pour utilisation future, mentionnons que l'élément  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  de  $\mathrm{GL}_2(K)$  étant donné, l'application  $z \mapsto cz+d, K \rightarrow K$ , sera notée  $j(g, z)$ . La formule (4) ci-dessus montre la relation dite de "cocycle" :

$$j(gg', z) = j(g, g'z)j(g', z),$$

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

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

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

appelé *demi-plan de Poincaré*, l'autre étant son conjugué complexe  $\overline{\mathbb{H}}$ . Si  $g$  est l'élément  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  de  $\mathrm{GL}_2(\mathbb{R})$ , et si  $\tau \in \mathbb{C} - \mathbb{R}$ , alors on a  $c\tau + d \neq 0$  et on constate l'égalité

$$(2) \quad \mathrm{Im} g\tau = \det g \frac{\mathrm{Im} \tau}{|c\tau + d|^2}.$$

En particulier, l'action par homographies du groupe

$$\mathrm{GL}_2(\mathbb{R})^+ := \{g \in \mathrm{GL}_2(\mathbb{R}), \det g > 0\}$$

présERVE le demi-plan de Poincaré. L'action des homographies de la forme  $a\tau + b$  avec  $a \in \mathbb{R}_{>0}$  et  $b \in \mathbb{R}$ , montre que cette action est transitive.

Ces homographies ont des propriétés géométriques remarquables, particulièrement lumineuses lorsqu'on les étudie du point de vue de la géométrie hyperbolique. Par exemple, notons  $\mathcal{C}$  l'ensemble des parties de  $\mathbb{H}$  qui sont soit de la forme  $\mathrm{Re} \tau = a$  ("droites verticales"), soit un demi-cercle de centre dans  $\mathbb{R}$  ("perpendiculaire à l'axe réel"). Deux points quelconques de  $\mathbb{H}$  appartiennent manifestement à un, et un seul, élément de  $\mathcal{C}$ . Un fait géométrique important est que  $\mathrm{GL}_2(\mathbb{R})^+$  préserve  $\mathcal{C}$ . Pour le voir, il suffit d'observer que les éléments de  $\mathcal{C}$  sont exactement les parties non vides de  $\mathbb{H}$  de la forme  $\alpha + \beta \mathrm{Re} \tau + \gamma |\tau|^2 = 0$  avec  $(\alpha, \beta, \gamma) \in \mathbb{R}^3 - \{0\}$ . La vérification de l'assertion précédente est alors un simple exercice ; il suffit même de le vérifier

pour les homographies  $\tau \mapsto \tau + \lambda$  et  $\tau \mapsto -1/\tau$  (les éléments correspondant de  $GL_2(\mathbb{R})^+/\mathbb{R}_{>0}$  engendrant ce dernier), auquel cas c'est immédiat.

**1.3. Action du sous-groupe  $\Gamma = SL_2(\mathbb{Z})$  sur  $\mathbb{H}$ .** Les éléments

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

sont dans le sous-groupe  $\Gamma := SL_2(\mathbb{Z})$  de  $GL_2(\mathbb{R})^+$ ; ils joueront un rôle très important. On a déjà vu  $S\tau = -1/\tau$  et  $T\tau = \tau + 1$ . On a aussi  $S^2 = -I_2$  et  $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ , ainsi donc que l'identité  $(ST)^3 = -I_2$ , puis  $Si = i$  et  $ST\rho = -1/(\rho + 1) = \rho$  où  $\rho = e^{2i\pi/3}$ . On pose

$$\mathcal{F} = \{\tau \in \mathbb{H}, |\operatorname{Re} \tau| \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}.$$

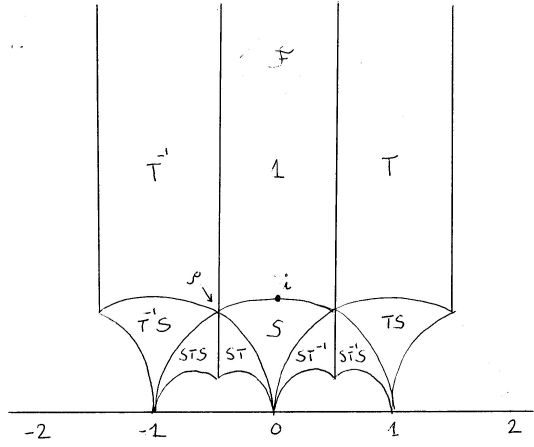


FIGURE 1. Le pavage de  $\mathbb{H}$  par la  $\Gamma$ -orbite de  $\mathcal{F}$

**Théorème 2.1.** (i) Pour tout  $\tau \in \mathbb{H}$ , l'orbite  $\Gamma\tau$  rencontre  $\mathcal{F}$ .

(ii) Si  $\tau$  et  $\tau'$  sont deux points distincts de  $\mathcal{F}$  tels que  $\Gamma\tau = \Gamma\tau'$  alors :

- soit  $\operatorname{Re} \tau = \pm \frac{1}{2}$  et  $\tau' = \tau \pm 1$ ,
- soit  $|\tau| = |\tau'| = 1$  et  $\tau' = -1/\tau$ .

(iii) Si  $\tau \in \mathcal{F}$  alors le stabilisateur de  $\tau$  dans  $\Gamma$  est  $\{\pm 1\}$ , sauf si  $\tau = i$  (resp.  $\tau = \rho, -\rho^2$ ), auquel cas c'est le sous-groupe engendré par  $S$  (resp.  $ST, TS$ ).

DÉMONSTRATION — Soit  $\tau \in \mathbb{H}$ . La forme quadratique  $\mathbb{R}^2 \rightarrow \mathbb{R}, (c, d) \mapsto |c\tau + d|^2$  est définie positive, elle admet donc un minimum sur  $\mathbb{Z}^2 - \{0\}$ . D'après la formule (2), il y a donc un sens à considérer l'ensemble  $E \subset \Gamma\tau$  des éléments  $\tau'$  tels que  $\operatorname{Im} \tau'$  est 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  $-1/\tau' \in \Gamma\tau$  et  $\operatorname{Im}(-1/\tau') = \frac{\operatorname{Im} \tau'}{|\tau'|^2}$ , donc  $|\tau'| \geq 1$ . Ainsi,  $\tau' \in \Gamma\tau \cap \mathcal{F}$ . Observons que cette démonstration montre en fait  $G\tau \cap \mathcal{F} \neq \emptyset$  où  $G$  désigne le sous-groupe de  $\Gamma$  engendré par  $S$  et  $T$ .

Pour montrer (ii) et (iii), 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

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

On a alors  $|c\tau + d| \leq 1$ . En particulier,  $|c \operatorname{Im} \tau| \leq 1$  et donc  $|c| \leq 1$ . Si  $c = 0$  alors  $d = a = \pm 1$  et donc  $\pm\gamma$  est une puissance de  $T$  et on est dans le premier cas du (ii). Sinon on peut supposer  $c = 1$ , quitte à remplacer  $\gamma$  par  $-\gamma$ . On voit sur le dessin que  $|\tau + d| \leq 1$  entraîne  $|\tau| = 1$ , et que l'on est dans l'un des cas suivants :

1.  $\tau \neq \rho, -\rho^2$  et  $d = 0$ . Dans ce cas,  $b = -1$  et  $\tau' = a - 1/\tau$  puis  $a = 0$  car  $|\operatorname{Re}(-1/\tau)| < 1/2$ . Ainsi,  $\gamma = S$  et  $\tau' = \tau = i$ .
2.  $\tau = \rho$  et  $d = 0, -1$ . Si  $d = 0$  on a encore  $b = -1$  et  $\tau' = a - 1/\rho = a - \rho^2$ . Cela montre que soit  $\tau' = -\rho^2, a = 0$  et  $\gamma = \pm S$ , 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.  $\square$

Soit  $\delta$  l'ensemble des  $\tau \in \mathcal{F}$  tels que l'on ait soit  $\operatorname{Re} \tau = \frac{1}{2}$ , soit  $|\tau| = 1$  et  $\operatorname{Re} \tau > 0$ . Soit  $\mathcal{F}' = \mathcal{F} - \delta$ . Les points (i) et (ii) du théorème ci-dessus montrent que pour tout  $\tau \in \mathcal{H}$ , l'orbite  $\Gamma\tau$  rencontre  $\mathcal{F}'$  en un et un seul point. On dit aussi que  $\mathcal{F}'$  est un *domaine fondamental* de l'action de  $\Gamma$  sur  $\mathbb{H}$ .

**Corollaire 2.2.**  $\Gamma$  est engendré par  $S$  et  $T$ .

DÉMONSTRATION — Il ne serait pas difficile de démontrer ce corollaire de manière directe en utilisant des opérations sur les lignes et les colonnes. Déduisons-le plutôt du théorème. Soit  $G$  le sous-groupe de  $\Gamma$  engendré par  $S$  et  $T$ . Soit  $\tau$  un point de l'intérieur de  $\mathcal{F}$ . Soit  $\gamma \in \Gamma$ . D'après la démonstration du (i) ci-dessus (dernière remarque), il existe  $g \in G$  tel que  $g^{-1}\gamma\tau \in \mathcal{F}$ . Ainsi,  $g^{-1}\gamma \in \operatorname{SL}_2(\mathbb{Z})$  fixe  $\tau$ , c'est donc  $\pm I_2$  d'après le (iii). Au final, on a  $\gamma \in G$  car  $-I_2 = S^2 \in G$ .  $\square$

## 2. Fonctions modulaires et fonctions de réseaux

**2.1. Bases et réseaux de  $\mathbb{C}$ .** (Où l'on répète d'abord légèrement différemment ce que l'on a déjà dit...) On note  $\mathcal{B}$  l'ensemble des éléments de  $\mathbb{C}^2$  de la forme  $w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$  tels que  $\{w_1, w_2\}$  est une base de  $\mathbb{C}$  vu comme  $\mathbb{R}$ -espace vectoriel ; il est bien sûr équivalent de demander  $w_2 \in \mathbb{C}^\times$  et  $w_1/w_2 \notin \mathbb{R}$ . On notera de plus  $\mathcal{B}^+ \subset \mathcal{B}$  le sous-ensemble des bases  $w$  telles que  $\operatorname{Im} w_1/w_2 > 0$  (bases *directes*).

– L'action naturelle de  $\mathbb{C}^\times$  sur  $\mathbb{C}^2$  (par homothéties) préserve évidemment  $\mathcal{B}$  et  $\mathcal{B}^+$ . Il est également évident que tout élément  $w$  de  $\mathcal{B}$  s'écrit de manière unique sous la forme  $\lambda \begin{pmatrix} \tau \\ 1 \end{pmatrix}$  avec  $\lambda \in \mathbb{C}^\times$  et  $\tau \in \mathbb{C} - \mathbb{R}$  (nécessairement  $\lambda = w_2, z = w_1/w_2$ ).

L'application  $\tau \mapsto \begin{pmatrix} \tau \\ 1 \end{pmatrix}$  induit donc des bijections

$$(3) \quad \mathbb{C} - \mathbb{R} \xrightarrow{\sim} \mathbb{C}^\times \backslash \mathcal{B} \quad \text{et} \quad \mathbb{H} \xrightarrow{\sim} \mathbb{C}^\times \backslash \mathcal{B}^+.$$

– L'action naturelle de  $\operatorname{GL}_2(\mathbb{R})$  sur  $\mathbb{C}^2$  préserve  $\mathcal{B}$  : pour  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dans  $\operatorname{GL}_2(\mathbb{R})$  on a (toujours) la (même) formule

$$(4) \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} aw_1 + bw_2 \\ cw_1 + dw_2 \end{pmatrix}$$

Cela montre que cette action de  $\mathrm{GL}_2(\mathbb{R})$  sur  $\mathcal{B}$  est simplement transitive : pour  $w, w' \in \mathcal{B}$  il existe un unique  $g \in \mathrm{GL}_2(\mathbb{R})$  avec  $w' = gw$ . Le groupe  $\mathrm{GL}_2(\mathbb{R})$  agit sur  $\mathbb{C}^2$  en commutant avec l'action de  $\mathbb{C}^\times$ , et induit donc une action sur  $\mathbb{C}^\times \backslash \mathcal{B} \xrightarrow{\sim} \mathbb{C} - \mathbb{R}$  qui n'est autre que celle étudiée au §1, par définition. La formule (2) montre que  $g \in \mathrm{GL}_2(\mathbb{R})$  préserve  $\mathcal{B}^+$  si, et seulement si,  $g \in \mathrm{GL}_2(\mathbb{R})^+$ .

Un *réseau* de  $\mathbb{C}$  est par définition un sous-groupe engendré par une  $\mathbb{R}$ -base de  $\mathbb{C}$ . Si  $w \in \mathcal{B}$ , on notera  $L(w) := \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$  le réseau engendré. Si  $\mathcal{R}$  désigne l'ensemble de tous les réseaux de  $\mathbb{C}$ , on a donc une surjection canonique

$$(5) \quad \mathcal{B} \longrightarrow \mathcal{R}, \quad w \mapsto L(w).$$

Soient  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dans  $\mathrm{GL}_2(\mathbb{R})$  et  $w$  dans  $\mathcal{B}$ . On a  $L(gw) \subset L(w)$  si, et seulement si,  $aw_1 + bw_2$  et  $cw_1 + dw_2$  sont dans  $L(w)$ . Il est équivalent de demander que  $a, b, c, d$  sont dans  $\mathbb{Z}$ , i.e.  $g \in \mathrm{M}_2(\mathbb{Z})$ . En particulier,  $L(gw) = L(w)$  si, et seulement si, on a  $g$  et  $g^{-1}$  dans  $\mathrm{M}_2(\mathbb{Z})$ , i.e.  $g \in \mathrm{GL}_2(\mathbb{Z})$ . On a montré le (i) de la proposition suivante :

**Proposition 2.3.** (i) *L'application (5) induit une bijection  $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathcal{B} \xrightarrow{\sim} \mathcal{R}$ .*

(ii) *L'inclusion  $\mathcal{B}^+ \rightarrow \mathcal{B}$  induit une bijection  $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{B}^+ \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}) \backslash \mathcal{B}$ .*

DÉMONSTRATION — La surjectivité de l'application du (ii) résulte de  $\det \mathrm{GL}_2(\mathbb{Z}) = \{\pm 1\}$ , et son injectivité de  $\mathrm{SL}_2(\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{R})^+$ .  $\square$

Le groupe  $\mathbb{C}^\times$  agit naturellement sur  $\mathcal{R}$  par homothéties :  $(\lambda, L) \mapsto \lambda L$ . La projection (5) est manifestement  $\mathbb{C}^\times$ -équivariante. En mettant bout-à-bout la bijection (3) et la proposition ci-dessus on en déduit le :

**Corollaire 2.4.** *L'application  $\tau \mapsto \tau\mathbb{Z} + \mathbb{Z}$  induit une bijection  $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \xrightarrow{\sim} \mathbb{C}^\times \backslash \mathcal{R}$ .*

Étant donné que les classes d'homothétie de réseau de  $\mathbb{C}$  sont en bijection naturelle avec les classes d'isomorphisme de tores complexes de dimension 1, i.e. de courbes elliptiques complexes, on dit aussi que  $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$  s'identifie à l'espace des modules grossiers de courbes elliptiques. C'est le point de départ de nombreuses constructions en géométrie algébrique, mais qui ne seront pas abordées dans ce cours.

**2.2. Fonctions modulaires de poids  $\chi$ .** Notons  $\mathcal{F}(X)$  l'espace vectoriel des fonctions de l'ensemble  $X$  dans  $\mathbb{C}$ . Fixons un morphisme de groupes  $\chi : \mathbb{C}^\times \rightarrow \mathbb{C}^\times$  et notons  $\mathcal{F}_\chi(\mathcal{B}^+) \subset \mathcal{F}(\mathcal{B}^+)$  le sous-espace des fonctions vérifiant  $F(\lambda w) = \chi(\lambda)F(w)$  pour tout  $\lambda \in \mathbb{C}^\times$  et toute base directe  $w \in \mathcal{B}^+$ . L'application linéaire

$$(6) \quad \mathcal{F}_\chi(\mathcal{B}^+) \longrightarrow \mathcal{F}(\mathbb{H}), \quad F \mapsto (\tau \mapsto F\left(\begin{pmatrix} \tau \\ 1 \end{pmatrix}\right)),$$

est évidemment bijective, toute base directe s'écrivant de manière unique sous la forme  $\lambda \begin{pmatrix} \tau \\ 1 \end{pmatrix}$  avec  $\lambda \in \mathbb{C}^\times$  et  $\tau \in \mathbb{H}$ . Si  $f$  est une fonction sur  $\mathbb{H}$ , on notera  $f^\chi \in \mathcal{F}_\chi(\mathcal{B}^+)$  son unique antécédent par cette application.

Le groupe  $\mathrm{GL}_2(\mathbb{R})^+$  agit à droite, par translations à gauche!, sur  $\mathcal{F}(\mathcal{B}^+) : (g, F)(w) = F(gw)$ . Cette action préserve manifestement  $\mathcal{F}_\chi(\mathcal{B}^+)$ . Il en résulte une action, également à droite, de  $\mathrm{GL}_2(\mathbb{R})^+$  sur  $\mathcal{F}(\mathbb{H})$  (dépendant de  $\chi$ ), définie par transport de

structure au moyen de la bijection (6). Cette action est appelée *action de poids*  $\chi$  de  $\mathrm{GL}_2(\mathbb{R})^+$  sur  $\mathcal{F}(\mathbb{H})$ , et elle est notée  $(g, f) \mapsto f|_{\chi}g$ . Par définition, elle est donnée par la formule suivante,

$$(7) \quad (f|_{\chi}g)(\tau) := f^{\chi}\left(g\left(\begin{array}{c} \tau \\ 1 \end{array}\right)\right) = \chi(c\tau + b) f\left(\frac{a\tau + b}{c\tau + d}\right) = \chi(j(g, \tau))f(g\tau).$$

**Proposition-Définition 2.5.** *Soient  $\chi : \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times}$  un morphisme de groupes et  $f : \mathbb{H} \rightarrow \mathbb{C}$  une fonction. Les propriétés suivantes sont équivalentes :*

- (i)  $f\left(\frac{a\tau + b}{c\tau + d}\right) = \chi(c\tau + d)^{-1}f(\tau)$  pour tout  $\tau$  dans  $\mathbb{H}$  et tout  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dans  $\mathrm{SL}_2(\mathbb{Z})$ ,
- (ii)  $f|_{\chi}\gamma = f$  pour tout  $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ ,
- (iii)  $f(\tau + 1) = f(\tau)$  et  $f(-1/\tau) = \chi(\tau)^{-1}f(\tau)$  pour tout  $\tau \in \mathbb{H}$ ,
- (iv)  $f^{\chi} : \mathcal{B}^+ \rightarrow \mathbb{C}$  est invariante par  $\mathrm{SL}_2(\mathbb{Z})$ ,
- (v)  $f^{\chi}$  se factorise en une fonction  $\mathcal{R} \rightarrow \mathbb{C}$ .

Si elles sont satisfaites, on dit que  $f$  est une fonction modulaire de poids  $\chi$ .

DÉMONSTRATION — L'équivalence de (i) et (ii) est tautologique. Celle de (ii) et (iii) découle du fait que l'action de poids  $\chi$  est une action de groupes, et que  $\mathrm{SL}_2(\mathbb{Z})$  est engendré par  $S$  et  $T$ , de sorte que (ii) est équivalent à demander  $f|_{\chi}T = f$  et  $f|_{\chi}S = f$ , qui sont les deux équations données. L'équivalence entre (iv) et (ii) est tautologique, par définition de l'action de poids  $\chi$  (ou par la formule (7)). L'équivalence entre (iv) et (v) est la Proposition 2.3.  $\square$

**Définition 2.6.** *Une fonction de réseaux de poids  $\chi$  est une fonction  $F : \mathcal{R} \rightarrow \mathbb{C}$  telle que  $F(\lambda L) = \chi(\lambda)F(L)$  pour tout  $\lambda \in \mathbb{C}^*$  et tout  $L \in \mathcal{R}$ .*

**Corollaire 2.7.** *Les applications  $f \mapsto f^{\chi}$  et  $F \mapsto (\tau \mapsto F(\tau\mathbb{Z} + \mathbb{Z}))$  sont des bijections réciproques entre l'espace des fonctions modulaires de poids  $\chi$  et celui des fonctions de réseaux de poids  $\chi$ .*

**Remarque 2.8.** Pour alléger les notations, on pourra noter par le même symbole une fonction modulaire  $f$  de poids  $\chi$ , la fonction  $f^{\chi} : \mathcal{B}^+ \rightarrow \mathbb{C}$  correspondante, et la fonction de réseaux  $\mathcal{R} \rightarrow \mathbb{C}$  qui s'en déduit. Il ne peut en principe y avoir d'ambiguïté d'interprétation, puisque les arguments dans chacun des cas sont des objets mathématiques bien différents (un élément de  $\mathbb{H}$ , un élément de  $\mathcal{B}^+$ , ou un élément de  $\mathcal{R}$ ).

Les caractères continus  $\chi : \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times}$  joueront par la suite un rôle naturellement plus important. Ceux sont ceux de la forme  $\lambda \mapsto \lambda^k|\lambda|^s$ , avec  $k \in \mathbb{Z}$  et  $s \in \mathbb{C}$  (exercice!). Lorsque  $\chi$  est le caractère  $\lambda \mapsto \lambda^{-k}$  (noter le signe  $-$ ), où  $k \in \mathbb{Z}$  est fixé, on utilisera l'expression *de poids*  $k$  à la place de *poids*  $\chi$ , et l'on note traditionnellement  $f|_k g$  pour  $f|_{\chi}g$ . Par exemple, une fonction modulaire de poids 0 (i.e. de poids  $\chi = 1$ ) est simplement une fonction sur  $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ .

**Exemple 2.9.** Soient  $k \in \mathbb{Z}$  et  $s \in \mathbb{C}$  tels que  $k + \operatorname{Re} s > 2$ . La série d'Eisenstein

$$G_{k;s}(L) = \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^k |\lambda|^s}$$

est absolument convergente, et définit une fonction modulaire de poids  $\lambda \mapsto \lambda^{-k} |\lambda|^{-s}$ . Vue comme fonction de  $\tau \in \mathbb{H}$ , on a  $G_{k;s}(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{(n\tau + m)^k |n\tau + m|^s}$ .

L'assertion de convergence absolue de  $G_{k;s}(L)$  sera justifiée en détail un peu plus loin. Le reste s'en déduit immédiatement.

**Exemple 2.10.** La fonction covol :  $\mathcal{R} \rightarrow \mathbb{R}_{>0}$ , où  $\operatorname{covol}(L)$  désigne le covolume du réseau  $L$  étant pris dans la  $\mathbb{R}$ -base  $1, i$ , est modulaire de poids  $\lambda \mapsto |\lambda|^2$ . Comme fonction sur  $\mathcal{B}$ , c'est  $w \mapsto |\det_{i,1}(w_1, w_2)|$ . Comme fonction sur  $\mathbb{H}$ , c'est la fonction  $\tau \mapsto \left| \det \begin{bmatrix} \operatorname{Im} \tau & 0 \\ \operatorname{Re} \tau & \operatorname{Im} \tau \end{bmatrix} \right| = \operatorname{Im} \tau$  (c'est aussi ce qui dit la formule (2) !).

**Exemple 2.11.** Si  $f$  est (une fonction) modulaire de poids  $\chi$ , et si  $f'$  est modulaire de poids  $\chi'$ , alors  $ff'$  est modulaire de poids  $\chi\chi'$ . De plus,  $|f|$  est modulaire de poids  $|\chi|$ . Si  $|\chi|$  est le caractère  $\lambda \mapsto |\lambda|^{-s}$  avec  $s \in \mathbb{R}$ , alors  $|f| \cdot \operatorname{covol}^{s/2}$  est modulaire de poids 0, i.e.  $|f(\tau)|(\operatorname{Im} \tau)^{s/2}$  définit une fonction  $\operatorname{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \rightarrow \mathbb{R}_{\geq 0}$ .

### 3. Formes modulaires

Notons  $\mathcal{O}(\mathbb{H}) \subset \mathcal{F}(\mathbb{H})$  le sous-espace des fonctions holomorphes. Si  $k \in \mathbb{Z}$ , l'action de poids  $k$  de  $\operatorname{GL}_2(\mathbb{R})^+$  sur  $\mathcal{F}(\mathbb{H})$  préserve manifestement  $\mathcal{O}(\mathbb{H})$ .

**Définition 2.12.** Une forme modulaire de poids  $k \in \mathbb{Z}$  est une fonction  $f : \mathbb{H} \rightarrow \mathbb{C}$  qui est une fonction modulaire de poids<sup>1</sup>  $k$ , telle que :

- (i)  $f$  est holomorphe,
- (ii)  $f(\tau)$  admet une limite finie quand  $\operatorname{Im} \tau \rightarrow +\infty$ , notée  $f(\infty)$ .

L'ensemble des formes modulaires de poids  $k$  est un sous-espace de  $\mathcal{O}(\mathbb{H})$ . Suivant Serre, nous le noterons  $M_k$ . La relation  $f|_k - \mathbf{I}_2 = (-1)^k f$  montre que si  $f \in M_k$  alors  $f = (-1)^k f$ , de sorte que  $M_k = 0$  si  $k$  est impair. Les fonctions constantes sont modulaires de poids 0 : nous verrons plus loin que ce sont les seules. Un premier exemple intéressant de forme modulaire est donné par les séries d'Eisenstein (Exemple 2.9), vues ici comme fonction de  $\tau$ . Si  $k$  est un entier  $\geq 3$ , on pose  $G_k = G_{k;0}$ .

**Proposition 2.13.** On suppose que  $k$  est pair  $\geq 4$ . Alors on a  $G_k \in M_k$  et  $G_k(\infty) = 2\zeta(k)$ . En particulier  $G_k \neq 0$ .

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

$$|\mu\tau + \nu| \geq C \sup(|\mu|, |\nu|).$$

1. ... ce qui signifie donc que l'on a  $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$  pour tout  $\tau$  dans  $\mathbb{H}$  et tout  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dans  $\operatorname{SL}_2(\mathbb{Z})$ .

Soient  $\tau \in \mathcal{D}_{A,B}$  et  $(\mu, \nu) \in \mathbb{R}^2$ . D'une part, on a  $|\mu\tau + \nu| \geq |\operatorname{Im}(\mu\tau + \nu)| > A|\mu|$ . D'autre part, on constate sur un dessin qu'il existe  $\delta > 0$  tel que  $|\lambda\tau + 1| > \delta$  pour tout  $\lambda \in \mathbb{R}$  et tout  $\tau \in \mathcal{D}_{A,B}$ . Ainsi, pour  $\nu \neq 0$  on a  $|\mu\tau + \nu| = |\nu| \left| \frac{\mu}{\nu}\tau + 1 \right| \geq \delta|\nu|$ . En conclusion,  $C = \min(A, \delta)$  convient.

Si  $s \geq 1$ , il y a exactement  $4 \cdot 2s = 8s$  couples  $(m, n) \in \mathbb{Z}^2$  tels que  $\sup(|m|, |n|) = s$ . On en déduit la majoration

$$\sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{|m\tau + n|^k} \leq \frac{1}{C^k} \sum_{s \geq 1} \frac{8s}{s^k}$$

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 de  $\tau$ . Nous avons déjà justifié dans l'exemple 2.9 que la convergence absolue de la série définissant  $G_k$  implique sa modularité de poids  $k$ . On peut le re-justifier directement : les bijections  $(m, n) \mapsto (m, n + m)$  et  $(m, n) \mapsto (n, -m)$  de  $\mathbb{Z}^2 - \{0\}$  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  $\operatorname{Im} \tau$  vers l'infini quand  $\tau \in \mathcal{D}_{1,1}$ . 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  $G_k(\tau) \rightarrow 2\zeta(k)$ . On conclut par 1-périodicité de  $G_k$ .  $\square$

Si  $k \geq 4$  est pair, on pose  $E_k = \frac{1}{2\zeta(k)} G_k \in M_k$  (série d'Eisenstein "normalisée"), de sorte que l'on ait  $E_k(\infty) = 1$ . Bien entendu, cette définition a un sens puisque  $\zeta(k) \neq 0$ . L'application  $M_k \rightarrow \mathbb{C}$ ,  $f \mapsto f(\infty)$ , est une application linéaire. Son noyau, noté  $S_k$ , est le sous-espace des formes modulaires *paraboliques* ("cuspidal" en anglais). Si  $k \geq 4$ , il est donc engendré par les éléments de la forme  $f - f(\infty)E_k$ .

**Corollaire 2.14.** *Pour tout entier pair  $k \geq 4$ , on a  $M_k = S_k \oplus \mathbb{C}E_k$ .*

#### 4. $q$ -développement d'une forme modulaire

Observons que si  $z \in \mathbb{C}$  alors  $|e^{2i\pi z}| = e^{-2\pi \operatorname{Im} z}$ . Soit  $D = \{z \in \mathbb{C}, |z| < 1\}$ . On considère l'application

$$q : \mathbb{H} \longrightarrow D - \{0\}, \quad \tau \mapsto e^{2i\pi\tau}.$$

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

Soit  $f : \mathbb{H} \rightarrow \mathbb{C}$  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  $\{\tau \in \mathbb{H}, |\operatorname{Re}(\tau - \tau_0)| < 1/2\}$  de  $\tau_0$  dans  $\mathbb{H}$ , et le voisinage ouvert  $D - \mathbb{R}_{\leq 0} e^{2i\pi\tau_0}$  de  $e^{2i\pi\tau_0}$  dans  $D$  (un inverse s'obtient en considérant une branche du logarithme complexe). Si  $f$  est holomorphe il y a donc équivalence entre :

- $f(\tau)$  admet une limite quand  $\operatorname{Im} \tau \rightarrow \infty$ ,
- $|f(\tau)|$  est bornée sur  $\{\tau \in \mathbb{H}, \operatorname{Im} \tau > 1\}$ ,



- $|\widetilde{f}(q)|$  est bornée au voisinage de  $q = 0$ ,
- $\widetilde{f}$  se prolonge en une fonction holomorphe sur tout  $D$ ,
- $\widetilde{f}$  admet un développement en série entière en 0 de rayon de convergence  $\geq 1$ .

(L'implication assertion 3  $\Rightarrow$  assertion 4 est le lemme de prolongement de Riemann). Cela justifie à la proposition-définition suivante.

**Proposition-Définition 2.15.** *Soit  $f \in M_k$ . La forme  $f$  admet un unique développement*

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

avec  $a_n(f) \in \mathbb{C}$  pour tout entier  $n \geq 0$ , normalement convergent sur toute partie de  $\mathbb{H}$  de la forme  $\text{Im } \tau > A$ ,  $A \in \mathbb{R}_{>0}$ . 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  $a_0(f) = f(\infty)$ .

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.

## 5. Détermination de l'espace $M_k$

**5.1. Un théorème de structure.** Observons que si  $f \in M_k$  et  $g \in M_{k'}$  alors  $fg \in M_{k+k'}$ . On peut donc fabriquer tout un tas de formes modulaires à l'aide des séries d'Eisenstein. Par exemple, si  $r$  et  $s$  sont des entiers  $\geq 0$  alors  $E_4^r E_6^s \in M_{4r+6s}$ .

**Théorème 2.16.** *Soit  $k \in \mathbb{Z}$ . L'espace  $M_k$  admet pour base les  $E_4^r E_6^s$ , avec  $(r, s) \in \mathbb{N}^2$  vérifiant  $4r + 6s = k$ .*

(La finitude même de  $\dim M_k$  est assez surprenante !)

Observons d'abord que si  $f \in M_k$  alors  $f(i) = f|_k S(i) = i^{-k} f(i)$ . Ainsi,  $f(i) = 0$  si  $k \not\equiv 0 \pmod{4}$ . De même  $f(\rho) = 0$  si  $k \not\equiv 0 \pmod{6}$ . En particulier,  $E_6(i) = 0$  et  $E_4(\rho) = 0$ . Nous démontrerons  $E_4(i) \neq 0$  dans la section suivante (pouvez-vous le démontrer directement ?) et que la famille de l'énoncé est génératrice : admettons-le pour l'instant. Vérifions ici qu'elle est libre. On procède par récurrence sur  $k \geq 0$ , le cas  $k = 0$  étant trivial. Supposons donc pour  $k \geq 0$  donné que l'on ait une relation de dépendance linéaire

$$\sum_{4r+6s=k} \lambda_{r,s} E_4^r E_6^s = 0.$$

Si  $k$  est multiple de 4, l'évaluation en  $\tau = i$  de cette formule donne  $\lambda_{k/4,0} = 0$  (car on a  $E_4(i) \neq 0$ ). Dans tous les cas, on a donc " $\lambda_{r,s} \neq 0$  implique  $s \neq 0$ ". Ainsi, soit tous les  $\lambda_{r,s}$  sont nuls, soit on a  $k \geq 6$  et on peut simplifier l'égalité ci-dessus par  $E_6$  (l'anneau des fonctions holomorphes sur  $\mathbb{H}$  étant intègre...), puis conclure par récurrence sur  $k$ .  $\square$

**Définition 2.17.** *(Fonction  $\Delta$  de Jacobi) La fonction  $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$  est une forme modulaire parabolique de poids 12.*

L'apparition du facteur 1728 sera expliquée plus loin. D'après ce que nous avons dit ci-dessus,  $\Delta \neq 0$  car  $\Delta(i) = \frac{1}{1728} E_4(i)^3$ .

**5.2. Sur les zéros des formes modulaires.** Soient  $f \in M_k$  et  $P \in \mathbb{H}$ . On note  $v_P(f)$  l'ordre d'annulation de  $f$  au point  $P$  et  $e_P$  le cardinal du stabilisateur de  $P$  dans  $\mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$ . Ces deux quantités, des entiers  $\geq 0$ , ne dépendent que de la  $\Gamma$ -orbite de  $P$  (pour  $v_P(f)$ , cela vient de la non annulation des  $j(\gamma, \tau)$  quand  $\gamma \in \Gamma$  et  $\tau \in \mathbb{H}$ ). De plus, d'après le Théorème 2.1 (iii) on a  $e_i = 2$ ,  $e_\rho = 3$ , et si  $P$  n'est pas dans l'orbite de  $i$  ou  $\rho$  alors  $e_P = 1$ . On note aussi  $v_\infty(f)$  l'ordre d'annulation de  $\tilde{f}$  en 0.

**Proposition 2.18.** (Formule  $k/12$ ) Soient  $k \in \mathbb{Z}$  et  $f \in M_k$  non nulle. On a la relation

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

Il fait partie de l'énoncé que la somme de gauche est en fait une somme finie (nécessairement  $\geq 0$ ). Le lecteur préférant voir d'abord comment utiliser cette formule, et par exemple terminer la démonstration du théorème 2.16, peut commencer par lire la sous-section suivante.

DÉMONSTRATION — Soit  $f \in M_k$  non nulle. Rappelons que la  $\Gamma$ -orbite de tout zéro de  $f$  rencontre le domaine  $\mathcal{F}$ . Si  $r$  est un réel  $> 0$  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'admet pas de zéro dans  $\Omega_r$ . 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 des  $\Gamma$ -orbites de points constituées de zéros de  $f$  est fini (et donc que la somme apparaissant dans la formule  $k/12$  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  $\lambda$  (resp.  $\mu$ ). 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 (i.e  $i, \rho, -\rho^2$ , l'un des  $\lambda, \lambda + 1$ , ou l'un des  $\mu, -1/\mu$ ). Nous noterons  $\gamma_{XY}$  le chemin portion de  $\mathcal{C}$  allant de  $X$  à  $Y$  (dans ce sens). Le chemin  $\gamma_{D'E}$  est par définition le chemin  $T\gamma_{AB}^{\mathrm{opp}}$ . De même, on a choisi  $\gamma_{C'D} = S\gamma_{B'C}^{\mathrm{opp}}$ . Enfin, on suppose que  $\gamma_{EA}$  est de partie imaginaire  $r$  suffisamment grande de sorte qu'aucun zéro de  $f$  ne soit de partie imaginaire  $> r$ . L'existence d'un tel contour est justifiée par le paragraphe précédent (zéros isolés).

La formule des résidus appliquée à la 1-forme méromorphe  $\frac{df}{f} = \frac{f'(\tau)}{f(\tau)}d\tau$  s'écrit donc

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

la somme portant sur les  $\Gamma$ -orbites de zéros de  $f$  ne contenant ni  $i$  ni  $\rho$ . Examinons maintenant les contributions des diverses portions du contour. Les fonctions  $f$  et  $f'$  étant  $T$ -invariantes on observe d'abord

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

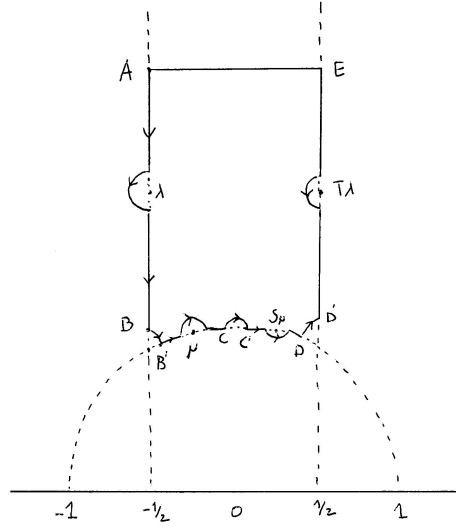


FIGURE 2. Le chemin d'intégration dans la démonstration de la formule  $k/12$

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

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

En effet, la première égalité est un simple changement de variables (réelles!), et la seconde est le théorème des résidus appliqué à  $\tilde{f}$ , sachant que par hypothèse 0 est le seul zéro éventuel de  $\tilde{f}$  dans le disque de  $D$  bordé par  $\omega$ . De plus, par modularité de  $f$  on a  $\frac{f'}{f} = -\frac{k}{\tau} + \frac{(f \circ S)'}{f \circ S}$ , 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 rappelons-le  $S\gamma_{B'C} = \gamma_{C'D}^{\text{opp}}$ . Lorsque le point  $B'$  tend vers  $\rho$ ,  $C$  tend vers  $i$ , et lorsque les portions de cercles autour des points notés  $\mu$  sont de rayon tendant vers 0, alors l'intégrale de chemin  $\frac{1}{i} \int_{\gamma_{B'C}} \frac{d\tau}{\tau}$  tend vers l'angle orienté défini par  $\rho$ , 0 et  $i$ , i.e.  $-(\frac{2\pi}{3} - \frac{2\pi}{4}) = -\frac{\pi}{6}$ . De même, lorsque  $B$  et  $B'$  tendent vers  $\rho$  alors l'intégrale de chemin  $\frac{1}{i} \int_{\gamma_{BB'}} \frac{f'(\tau)}{f(\tau)} d\tau$  tend vers l'angle orienté  $\widehat{B\rho B'} = -\frac{\pi}{3}$  multiplié par  $v_{\rho}(f)$ . Un argument similaire vaut en  $-1/\bar{\rho} = \rho + 1$ . 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 en mettant toutes ces identités bout à bout.  $\square$

**5.3. Conséquences de la formule  $k/12$ .** La première conséquence évidente de la formule  $k/12$  est l'annulation  $M_k = 0$  si  $k < 0$ . De plus, on a  $S_k = 0$  si  $k < 12$ , car  $v_{\infty}(f) \geq 1$  si  $f \in S_k - \{0\}$ . En particulier, on a donc  $M_0 = \mathbb{C}1$  (les constantes).

Séparant les orbites de  $i$  et  $\rho$  des autres, la formule  $k/12$  s'écrit aussi

$$(8) \quad v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_P v_P(f) = \frac{k}{12},$$

la somme portant sur les  $\Gamma$ -orbites de points de  $\mathbb{H}$  distinctes de  $\Gamma i$  et  $\Gamma \rho$ . En particulier on a  $M_2 = 0$  car chaque terme de gauche est soit  $> 1/6$ , soit nul. On a donc montré le :

**Corollaire 2.19.** (i) Si  $k < 12$  alors  $S_k = 0$ .

(ii) Si  $k < 0$  ou  $k = 2$  alors  $M_k = 0$ .

(iii)  $M_0 = \mathbb{C}1$  et si  $k = 4, 6, 8, 10$  alors  $M_k = \mathbb{C}E_k$ .

Appliquons la formule (8) à  $k = 4$  et  $f = E_4$ . Dans ce cas on a  $\frac{k}{12} = \frac{1}{3}$ , mais l'annulation évidente  $E_4(\rho) = 0$  entraîne  $\frac{1}{3}v_\rho(f) \geq 1/3$ . Ainsi, la seule  $\Gamma$ -orbite de points qui sont des zéros de  $E_4$  est celle de  $\rho$ . En particulier, cela démontre la non-nullité annoncée

$$E_4(i) \neq 0,$$

puis  $\Delta \neq 0$  car on a  $\Delta(i) = \frac{1}{1728}E_4(i)^3$ .

Appliquant maintenant (8) à  $k = 12$  et  $f = \Delta$ , on en déduit que  $\Delta$  ne s'annule pas sur  $\mathbb{H}$  et que l'inégalité  $v_\infty(\Delta) \geq 1$  est une égalité. En particulier, si  $k$  est quelconque et si  $f \in S_k$  alors la fonction  $\frac{f}{\Delta}$  est une forme modulaire de poids  $k - 12$ . On a démontré le corollaire suivant.

**Corollaire 2.20.** (i) La fonction  $\Delta$  ne s'annule pas sur  $\mathbb{H}$  et l'on a  $v_\infty(\Delta) = 1$ .

(ii) Si  $k \in \mathbb{Z}$  alors  $S_k = \Delta M_{k-12}$ . En particulier,  $S_{12} = \mathbb{C}\Delta$  est de dimension 1.

Démontrons enfin que  $M_k$  est engendré par les  $E_4^r E_6^s$ , où  $r, s$  sont des entiers  $\geq 0$  tels que  $4r + 6s = k$ . D'après le corollaire 2.19, on peut supposer  $k \geq 4$ . On procède par récurrence sur  $k$ . Observons que  $k$  étant pair  $\geq 4$ , il existe des entiers positifs  $r, s$  tels que  $k = 4r + 6s$  : on a soit  $k \equiv 0 \pmod{4}$ , soit  $k \equiv 6 \pmod{4}$  et  $k \geq 6$ . Un tel couple  $(r, s)$  étant fixé, observons que pour tout  $f \in M_k$  alors  $f - f(\infty)E_4^r E_6^s \in S_k$ . Mais  $S_k = \Delta M_{k-12}$  d'après le corollaire 2.20, et  $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ . Cela termine la démonstration, ainsi donc que celle du théorème 2.16.  $\square$

Les corollaires 2.19 et 2.20 entraînent également immédiatement le corollaire suivant :

**Corollaire 2.21.** Supposons  $k \geq 0$  pair. La dimension de  $S_k$  vaut  $[k/12]$  si  $k \not\equiv 2 \pmod{12}$ ,  $[k/12] - 1$  sinon.

**Remarque 2.22.** Comme  $\Delta$  ne s'annule pas sur  $\mathbb{H}$ , la fonction  $j := \frac{E_4^3}{\Delta}$  ("invariant modulaire") est une fonction modulaire de poids 0, manifestement holomorphe sur  $\mathbb{H}$ . En revanche,  $|j(\tau)|$  tends vers  $+\infty$  lorsque  $\text{Im}(\tau)$  tend vers l'infini. Ainsi, si l'on avait omise la condition de limite (ii) dans la définition des formes modulaires, l'espace  $M_0$  aurait été de dimension infinie, à cause des polynômes en  $j$ . De même, tous les  $M_k$  avec  $k$  pairs auraient été de dimension infinie (considérer  $j^m \frac{E_4^{k+12r}}{\Delta^r}$  avec  $r$  assez grand et  $m$  quelconque).

## 6. Quelques $q$ -développements

**6.1. Séries d'Eisenstein.** Si  $k \in \mathbb{Z}$  et  $n \geq 1$  est un entier, on pose  $\sigma_k(n) = \sum_{d|n} d^k$ . On rappelle que les nombres de Bernoulli sont définis par la série formelle  $\frac{t}{e^t-1} = \sum_{n \geq 0} \frac{B_n}{n!} t^n$ . L'identité suivante est essentiellement due à Euler.

**Proposition 2.23.** *Soit  $k$  un entier pair  $\geq 4$ . On a  $E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 0} \sigma_{k-1}(n) q^n$ .*

DÉMONSTRATION — Rappelons qu'Euler a démontré que pour tout  $z \in \mathbb{C} - \mathbb{Z}$ , on a

$$(9) \quad \frac{\pi}{\tan \pi z} = \frac{1}{z} + \sum_{n \in \mathbb{Z} - \{0\}} \left( \frac{1}{z-n} + \frac{1}{n} \right)$$

Justifions brièvement cette identité. Notons  $g(z)$  la série de fonctions de droite et posons  $f(z) = \frac{\pi}{\tan \pi z}$ . Si  $|z| \leq r$  et  $|n| > r$  alors l'inégalité

$$\left| \frac{1}{z-n} + \frac{1}{n} \right| = \frac{|z|}{|n||z-n|} \leq \frac{r}{|n|(|n|-r)}$$

montre que la série de fonctions méromorphes  $g(z)$  converge normalement sur tout compact de  $\mathbb{C}$ . C'est donc une fonction méromorphe sur  $\mathbb{C}$ , holomorphe sur  $\mathbb{C} - \mathbb{Z}$ , dont les pôles en les entiers sont simples de résidu 1. La fonction  $f$  a les mêmes propriétés que  $g$ , de sorte que  $f - g$  est holomorphe sur  $\mathbb{C}$ . Mais  $f$  et  $g$ , et donc  $f - g$ , sont 1-périodiques et impaires (c'est un exercice pour  $g$ ). Pour en déduire que  $f - g$  est nulle il suffit d'après Liouville de montrer que  $f$  et  $g$  restent bornées quand  $\text{Im} \tau \rightarrow \infty$ . C'est clair pour  $f$ . Pour  $g$ , on observe que  $qg(\tau) \rightarrow 0$  quand  $\text{Im}(\tau) \rightarrow +\infty$ , d'où l'on tire que  $\tilde{g}$  est holomorphe en 0 (lemme de prolongement de Riemann), ce qui conclut.

Si  $\tau \in \mathbb{H}$  on a le développement évident  $\frac{\pi}{\tan \pi \tau} = i\pi \frac{q+1}{q-1} = i\pi - 2i\pi \sum_{n \geq 0} q^n$ . Soit  $k \geq 2$ . En dérivant  $k-1$  fois par rapport à  $\tau$  la formule d'Euler, on trouve l'identité

$$\sum_{n \in \mathbb{Z}} \frac{1}{(\tau+n)^k} = \frac{(-2i\pi)^k}{(k-1)!} \sum_{n \geq 0} n^{k-1} q^n.$$

Supposons  $k$  pair  $\geq 4$ . On applique cette identité à  $m\tau$  pour tout  $m$  entier  $\geq 1$ , ce qui a pour effet de remplacer  $q$  par  $q^m$ , et on fait la somme (la convergence absolue du terme de droite ayant déjà été vérifiée). On en déduit, pour  $k \geq 4$  pair :

$$\frac{1}{2} G_k(\tau) - \zeta(k) = \frac{(2i\pi)^k}{(k-1)!} \sum_{n \geq 0} \sigma_{k-1}(n) q^n.$$

Pour conclure, on utilise une identité fameuse due à Euler :

$$\zeta(k) = -\frac{(2i\pi)^k}{2k!} B_k.$$

En fait, cette formule est aussi conséquence de l'identité (9). En effet, cette dernière dérivée  $k-1$  fois s'écrit

$$\left( \frac{2i\pi}{e^{2i\pi z} - 1} - \frac{1}{z} \right)^{(k-1)} = (-1)^{k-1} (k-1)! \sum_{n \neq 0} \frac{1}{(z+n)^k}.$$

Par définition des nombres de Bernoulli on a  $\frac{2i\pi}{e^{2i\pi z} - 1} - \frac{1}{z} = \sum_{n \geq 1} (2i\pi)^n \frac{B_n}{n!} z^{n-1}$  au voisinage de  $z = 0$ . On conclut par évaluation en  $z = 0$ .  $\square$

Observons que le  $q$ -développement de  $E_k$  est à coefficients dans  $\mathbb{Q}$ . Mieux,  $E_4$  et  $E_6$  sont à coefficients entiers, comme le montre le tableau suivant.

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

**Corollaire 2.24.** *Soit  $M_k(\mathbb{Z}) \subset M_k$  le sous-groupe constitué des formes modulaires dont tous les coefficients de Fourier sont dans  $\mathbb{Z}$ . Alors  $M_k(\mathbb{Z})$  est libre de rang  $\dim M_k$ , et engendré sur  $\mathbb{Z}$  par une  $\mathbb{C}$ -base de  $M_k$ .*

DÉMONSTRATION — Soit  $N$  un entier  $> k/12$ . L'application linéaire  $u : M_k \rightarrow \mathbb{C}^{N+1}$ ,  $f \mapsto (a_n(f))_{n=0}^N$ , est injective, car si  $f$  non nulle est dans  $\ker u$  alors on a  $v_\infty(f) > k/12$ , ce qui contredit la formule  $k/12$ . En particulier, le groupe  $M_k(\mathbb{Z})$  se plonge dans  $\mathbb{Z}^{N+1}$  : il est donc libre de type fini sur  $\mathbb{Z}$ . Comme toute famille  $\mathbb{Z}$ -libre dans  $\mathbb{Z}^r$  est  $\mathbb{C}$ -libre dans  $\mathbb{C}^r$ , toute famille  $\mathbb{Z}$ -libre de  $M_k(\mathbb{Z})$  est  $\mathbb{C}$ -libre dans  $M_k$  (appliquer  $u$ ). Ainsi le  $\mathbb{Z}$ -rang de  $M_k(\mathbb{Z})$  est  $\leq \dim M_k$ . Mais  $E_4^r E_6^s$  est dans  $M_{4k+6s}(\mathbb{Z})$  d'après l'observation ci-dessus, donc on conclut par le Théorème 2.16.  $\square$

**6.2. La magie des formes modulaires.** En guise d'exemple, considérons  $E_4^2$ . C'est un élément de  $M_8 = \mathbb{C} E_8$  (Corollaire 2.19). Comme  $E_4^2(\infty) = E_8(\infty) = 1$ , on a nécessairement

$$E_4^2 = E_8.$$

Cette identité est tout à fait non triviale ! En effet, une fois les coefficients de Fourier égalisés elle s'écrit

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m) \sigma_3(n-m), \quad \forall n \geq 1.$$

Par exemple,  $1 + 2^7 = 129 = 1 + 2^3 + 120$ . Cette méthode de raisonnement a de nombreuses autres applications.

**6.3. La fonction  $\Delta$ .** La formule  $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ , combinée aux  $q$ -développements de  $E_4$  et  $E_6$ , permet d'exprimer les coefficients de Fourier de  $\Delta$ . On trouve (en notant  $1728 = 3 \cdot 240 + 2 \cdot 504$ )

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \dots$$

**Théorème 2.25.** (Jacobi)  $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$ .

Avant de discuter la démonstration de cet énoncé, faisons quelques remarques de nature historique. Les coefficients de Fourier  $a_n(\Delta)$  de  $\Delta$  sont notés  $\tau(n)$  : c'est la fonction  $\tau$  de Ramanujan. Elle possède une riche histoire. En 1916, Ramanujan avait notamment conjecturé par inspection les deux propriétés suivantes :

- (a) si  $m$  et  $n$  sont premiers entre eux, alors  $\tau(mn) = \tau(m)\tau(n)$ ,
- (b) si  $p$  est premier, et si  $n \geq 1$  alors  $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ ,

(c) si  $p$  est premier, on a  $|\tau(p)| \leq 2p^{11/2}$ .

Par exemple, on a bien  $\tau(6) = -6048 = -24 \cdot 252 = \tau(2)\tau(3)$  et  $\tau(4) = -1472 = (-24)^2 - 2^{11} = \tau(2)^2 - 2^{11}$ . Ces conjectures ont eu une influence considérable sur la théorie des nombres, et se sont avérées très loin d'être anecdotiques, peut-être en dépit de leur apparence. Les deux premières ont été démontrées par [Mordell](#)<sup>2</sup>. Ce sont des conséquences simples de l'égalité  $\dim S_{12} = 1$  démontrée ici et de l'existence de certains opérateurs agissant sur les espaces de formes modulaires ; ces opérateurs seront étudiés plus tard de manière systématique par Hecke et feront l'objet du prochain cours (de sorte que nous démontrerons (a) et (b)). La troisième, maintenant un théorème fameux de Deligne, s'est avérée être une manifestation des célèbres conjectures de Weil, elles-même démontrées aussi par Deligne, donnant des estimées précises "à la Hasse" sur le nombre des solutions  $(x_1, \dots, x_d)$  dans  $(\mathbb{Z}/p\mathbb{Z})^d$  d'une équation de la forme  $P(X_1, \dots, X_d) = 0$  avec  $P \in (\mathbb{Z}/p\mathbb{Z})[X_1, \dots, X_d]$  un polynôme. Le lien entre les formes modulaires et ces conjectures avait d'ailleurs déjà été suspecté avant Deligne par des mathématiciens comme Eichler, Shimura, Kuga et Sato. Les conjectures de Weil, furent l'une des motivations principale de la refonte de la géométrie algébrique initiée par Grothendieck et son école dans les années 60, elles ont été complètement démontrées par Deligne. Nous n'aborderons pas du tout la démonstration de Deligne dans ce cours. En revanche, nous verrons que (c) est un cas très particulier d'une conjecture extrêmement générale (est très largement ouverte) en théorie des formes automorphes.

DÉMONSTRATION — (du Théorème 2.25) Comme  $S_{12} = \mathbb{C}\Delta$ , il suffit de montrer que la fonction sur  $\mathbb{H}$  définie par  $f(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24}$  est dans  $S_{12}$ . C'est manifestement une fonction holomorphe vérifiant  $f(\tau + 1) = f(\tau)$  et  $f(\tau) \rightarrow 0$  quand  $\text{Im } \tau$  tend vers  $+\infty$ , de sorte qu'il suffirait de vérifier  $f(-1/\tau) = \tau^{12} f(\tau)$ . Considérons en fait l'identité générale à démontrer, à savoir que pour  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dans  $\text{SL}_2(\mathbb{Z})$  on a

$$(10) \quad j(\gamma, \tau)^{-12} f(\gamma\tau) = f(\tau).$$

Étant donnée l'écriture en produit de  $f$  on va s'intéresser à la dérivée logarithmique de cette identité. La théorie des fonctions holomorphes (voir par exemple le livre de H. Cartan Ch. V §3 Thm. 2, p. 161) montre que la dérivée logarithmique de  $f$  est la somme des dérivées logarithmiques de chacun des termes du produit. Celle de  $q$  est  $2i\pi q$ , et celle de  $1 - q^n$  est  $-2i\pi \sum_{m \geq 1} nq^{nm}$ . On a donc  $f'(\tau)/f(\tau) = 2i\pi E_2$  où  $E_2$  est la fonction sur  $\mathbb{H}$  définie par

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

La notation est bien "compatible" avec celle des  $E_k$  pour  $k > 2$ . Mieux, l'argument d'Euler donné dans la proposition 2.23 montre que l'on a

$$(11) \quad 2\zeta(2) E_2(\tau) = \sum_{n \in \mathbb{Z} - \{0\}} \frac{1}{n^2} + 2 \sum_{m \geq 1} \left( \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^2} \right)$$

(la somme n'est plus absolument convergente, et doit être effectuée dans l'ordre indiqué). D'autre part, la dérivée logarithmique de  $\tau \mapsto j(\gamma, \tau) = c\tau + d$  est la

<sup>2</sup> On Mr. Ramanujan's Empirical Expansions, Proceedings of the Cambridge Philosophical Society, Mathematical and physical sciences (1917).

fonction  $-cj(\gamma, \tau)^{-1}$ , et celle de  $\tau \mapsto \gamma\tau$  est  $j(\gamma, \tau)^{-2}$ . Ainsi, la dérivée logarithmique de l'équation (10) à prouver s'écrit après division par  $2i\pi$

$$(12) \quad -\frac{12}{2i\pi} cj(\gamma, \tau)^{-1} + j(\gamma, \tau)^{-2}E_2(\gamma\tau) = E_2(\tau).$$

Esquissons maintenant seulement la démonstration de cette identité donnée par Zagier (référence citée §2.3), qu'il attribue à Hecke (voir aussi le cours d'arithmétique de Serre pour démonstration directe pour  $\gamma = S$ , ce qui suffira pour prouver le théorème). On regarde la série d'Eisenstein  $G_{2,s}$ , avec disons  $s$  réel  $> 0$ , introduite dans l'Exemple 2.9. Zagier démontre d'abord que pour tout réseau  $L$ , la fonction  $s \rightarrow G_{2,s}(L)$  admet une limite quand  $s \rightarrow 0$  (c'est en fait un cas particulier du fameux prolongement méromorphe à  $\mathbb{C}$  des séries d'Eisenstein valable pour tout  $k, s$ ), que nous noterons  $G_2$ . L'argument de régularisation donné par Zagier (avec pour point de départ l'identité (11)) montre que  $G_2$  est relié à  $E_2$  par la formule suivante pour  $G_2$

$$(13) \quad \frac{1}{2\zeta(2)}G_2(\tau) = E_2(\tau) - \frac{6}{2\pi} \frac{1}{\text{Im } \tau}.$$

Comme  $G_{2,s}$  est modulaire de poids  $\lambda^{-2}|\lambda|^{-s}$ , la fonction  $G_2$  est modulaire de poids 2, par passage à la limite. Ainsi,  $G_2$  n'est pas holomorphe, mais une fonction modulaire de poids 2, alors que la fonction  $E_2$  est holomorphe, mais pas modulaire (comme il se doit!). L'équation (12) résulte alors de l'identité (13) et de l'identité  $(G_2)_{|2\gamma} = G_2$ , modulo le calcul immédiat suivant

$$\frac{6}{2\pi} \left( \left( \frac{1}{\text{Im } \tau} \right)_{|2\gamma} - \frac{1}{\text{Im } \tau} \right) = \frac{12}{2i\pi} cj(\gamma, \tau)^{-1}.$$

On pourra noter que comme  $\text{Im } \tau$  est modulaire de poids  $\chi(\lambda) = |\lambda|^2 = \lambda\bar{\lambda}$ , on a

$$\left( \frac{1}{\text{Im } \tau} \right)_{|2\gamma} = \chi(j(\gamma, \tau))j(\gamma, \tau)^{-2} \left( \frac{1}{\text{Im } \tau} \right)_{|x\gamma} = \frac{\overline{j(\gamma, \tau)}}{j(\gamma, \tau)} \frac{1}{\text{Im } \tau}.$$

(sans calcul!), et conclure par  $\overline{j(\gamma, \tau)} - j(\gamma, \tau) = -2i \text{Im } j(\gamma, \tau) = \frac{2}{i} c \text{Im } \tau$ .

Au final, nous avons démontré qu'il existe une constante  $C_\gamma \in \mathbb{C}^\times$  telle que  $f_{|12\gamma} = C_\gamma f$  : c'est l'information que l'on obtient en disant que la dérivée logarithmique de (10) est nulle. Autrement dit,  $f$  est vecteur propre de  $\Gamma$  pour l'action de poids 12, de "système de valeurs propres les  $C_\gamma$ ". Il en résulte que  $\gamma \rightarrow C_\gamma, \text{SL}_2(\mathbb{Z}) \rightarrow \mathbb{C}^\times$ , est un morphisme de groupes. Pour voir qu'il est trivial, il suffit de vérifier  $C_T = 1$  et  $C_S = 1$ , une remarque que l'on avait déjà faite au début. Mais  $C_T = 1$  est évident car  $f(\tau + 1) = f(\tau)$ . Enfin, si l'on contemple l'équation

$$\tau^{-12} f(1/\tau) = C_S f(\tau),$$

on a pour  $\tau = i$  l'identité  $f(i) = C_S f(i)$ . Il ne reste qu'à observer que l'on a  $f(i) \neq 0$ , ce qui c'est évident ; on constate même sur la formule définissant  $f$  que  $f(iy)$  est un réel  $> 0$  pour tout  $y \in \mathbb{R}_{>0}$ .  $\square$