Cours fondamental de M2
Formes modulaires et leurs propriétés arithmétiques

Jean-François Dat

2014-2015

Table des matières

1 Théorie analytique

1.1 Le demi-plan de Poincaré et ses quotients

Posons $\mathbb{H} := \{z \in \mathbb{C}, \Im(z) > 0\}$. C'est un ouvert connexe et simplement connexe de $\mathbb{C}$ biholomorphe au disque unité ouvert $\mathbb{D}$ par l'application $z \mapsto \frac{z-i}{z+i}$. Dans la théorie des surfaces de Riemann, on montre que, à biholomophisme près, les seules surfaces de Riemann simplement connexes sont $\mathbb{D} \simeq \mathbb{H}$, le *plan complexe* $\mathbb{C}$ et la *sphère de Riemann* $\mathbb{P}^1(\mathbb{C}) = (\mathbb{C}^2 \setminus \{0\})/\mathbb{C}^\times$.

1.1.1 *Automorphismes de* $\mathbb{H}$. L'action linéaire de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}^2$ descend en une action par biholomorphismes sur $\mathbb{P}^1(\mathbb{C})$ qui est triviale sur le centre $\mathbb{C}^\times$. Écrivons $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \coprod \{\infty\}$ où l'on a plongé $\mathbb{C}$ dans $\mathbb{P}^1(\mathbb{C})$ par $z \mapsto (1, z)\mathbb{C}^\times$. Cette coordonnée nous permet de décomposer $\mathbb{P}^1(\mathbb{C}) = \mathbb{H} \coprod \mathbb{P}^1(\mathbb{R}) \coprod \bar{\mathbb{H}}$ et on voit que le sous-groupe $\mathrm{GL}_2^+(\mathbb{R})$ des matrices à

déterminant positif respecte cette décomposition et en particulier agit sur $\mathbb{H}$. Explicitement, si $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, on a

$$\gamma z = \frac{az+b}{cz+d}, \quad \text{et } \Im(\gamma z) = \frac{\det(\gamma)}{|cz+d|^2}\Im(z).$$

THÉORÈME. – *Soit* $\mathrm{Aut}(\mathbb{H})$ *le groupe des automorphismes biholomorphes de* $\mathbb{H}$.

i) L'action décrite ci-dessus induit un isomorphisme de groupes

$$\mathrm{SL}_2(\mathbb{R})/\{\pm 1\} = \mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{H})$$

ii) L'action de $\mathrm{SL}_2(\mathbb{R})$ *sur* $\mathbb{H}$ *est transitive et le fixateur de* i *dans* $\mathrm{SL}_2(\mathbb{R})$ *est* $\mathrm{SO}_2(\mathbb{R})$. *De plus l'application* $\gamma \mapsto \gamma i$ *induit un homéomorphisme*

$$\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \xrightarrow{\sim} \mathbb{H}.$$

Dans le ii), on a muni $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ de la topologie quotient, par définition la plus fine topologie pour laquelle la projection canonique $\mathrm{SL}_2(\mathbb{R}) \longrightarrow \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ est continue.

Démonstration. Commençons par ii). Un calcul montre que $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ fixe i si et seulement si $a = d$ et $b = -c$. La condition de déterminant donne en plus $a^2 + b^2 = 1$, donc le fixateur de i dans $\mathrm{SL}_2(\mathbb{R})$ est $\mathrm{SO}_2(\mathbb{R})$. Par ailleurs, si on écrit $z = x + iy$, on constate que $z = \left[\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right] i = \begin{bmatrix} y^{-1/2} & -xy^{-1/2} \\ 0 & y^{1/2} \end{bmatrix} i$, d'où la transitivité de l'action. On en déduit que l'application du point ii) est une bijection. Comme l'action de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathbb{H}$ est visiblement continue, cette bijection est continue et il ne reste plus qu'à voir qu'elle est aussi ouverte. Pour cela il suffit de voir que si U est un ouvert de $\mathrm{SL}_2(\mathbb{R})$ alors $U.i$ est un voisinage de i dans $\mathbb{H}$, ce qui est clair par la formule $x + iy = \begin{bmatrix} y^{1/2} & -xy^{-1/2} \\ 0 & y^{-1/2} \end{bmatrix} i$. [1]

Passons au i). Un calcul montre que le noyau de l'action est bien $\{\pm 1\}$. Pour la surjectivité, soit $\gamma \in \mathrm{Aut}(\mathbb{H})$. Par le point ii), quitte à composer avec un $\alpha \in \mathrm{SL}_2(\mathbb{R})$, on peut supposer que $\gamma i = i$. Transportons cela via $\tau = \left[\begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix}\right] : z \mapsto \frac{z-i}{z+i}$. On obtient un automorphisme $\tau\gamma\tau^{-1}$ du disque unité ouvert $\mathbb{D}$ qui envoie 0 sur 0. Le lemme de Schwarz nous dit alors que $\tau\gamma\tau^{-1}$ est une homothétie $z \mapsto \zeta z$ avec $|\zeta| = 1$. On peut donc écrire $\tau\gamma\tau^{-1}(z) = \left[\begin{smallmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{smallmatrix}\right] z$ pour un $\theta \in \mathbb{R}$. Or, on calcule que $\tau^{-1}\left[\begin{smallmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{smallmatrix}\right]\tau = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$, ce qui assure que γ et $\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$ induisent le même automorphisme de $\mathbb{H}$. □

Un élément $\gamma \in \mathrm{SL}_2(\mathbb{R})$ possède 2 valeurs propres (en comptant la multiplicité) dans $\mathbb{C}$. 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 $\gamma \neq \pm 1$.

1. Lorsqu'un groupe topologique G agit continuement et transitivement sur un espace X, alors pour tout $x \in X$, l'action de X induit une bijection continue $G/G_x \longrightarrow X$. Celle-ci peut ne pas être un homéomorphisme, mais elle en est toujours un si G et X sont localement compacts.

En raisonnant sur le polynôme caractéristique on voit que (γ elliptique) $\Leftrightarrow |\operatorname{tr}(\gamma)| < 2$, que ($\gamma$ hyperbolique) $\Leftrightarrow |\operatorname{tr}(\gamma)| > 2$, et que ($\gamma$ parabolique) $\Leftrightarrow (|\operatorname{tr}(\gamma)| = 2$ 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 $\mathbb{P}^1(\mathbb{C})$.

LEMME. – *Soit* $\gamma \in \mathrm{SL}_2(\mathbb{R})$.

i) 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* $\mathrm{SL}_2(\mathbb{R})$ *à une rotation* $\left[\begin{smallmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{smallmatrix}\right] \in \mathrm{SO}_2(\mathbb{R})$.

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

iii) γ *est parabolique si et seulement si* γ *a un unique point fixe dans* $\mathbb{P}^1(\mathbb{R})$. *De plus,* γ *est conjugué dans* $\mathrm{GL}_2(\mathbb{R})$ *à une matrice de la forme* $\pm\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$.

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

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

1.1.2 *Sous-groupes discrets de* $\mathrm{SL}_2(\mathbb{R})$. Un sous-groupe Γ de $\mathrm{SL}_2(\mathbb{R})$ est dit *discret* s'il est discret pour la topologie induite. Le premier exemple est $\mathrm{SL}_2(\mathbb{Z})$, qu'on appelle *groupe modulaire* et qu'on notera aussi $\Gamma(1)$. Plus généralement, on notera pour $N \in \mathbb{N}$

$$\Gamma(N) := \operatorname{Ker}(\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})) = \{\left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right] \equiv \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right] (\mathrm{mod}\ N)\}.$$

C'est un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ appelé *sous-groupes de congruences principal* de niveau N. Dans ce cours, les groupes qui nous intéresseront particulièrement sont

$$\Gamma_1(N) := \{\left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right] \equiv \left[\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right] (\mathrm{mod}\ N)\}$$

$$\Gamma_0(N) := \{\left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right] \equiv \left[\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right] (\mathrm{mod}\ N)\}$$

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

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

PROPOSITION. – *Soit* Γ *un sous-groupe discret de* $\mathrm{SL}_2(\mathbb{R})$.

i) Pour tout $z \in \mathbb{H}$, *le fixateur* Γ_z *de* z *dans* Γ *est cyclique (et en particulier, fini).*

ii) Tout $z \in \mathbb{H}$ *admet un voisinage ouvert* U *tel que* $\forall \gamma \in \Gamma, \gamma U \cap U \neq \emptyset \Rightarrow \gamma z = z$.

iii) Deux orbites distinctes Γz et $\Gamma z'$ admettent des voisinages ouverts disjoints.

Démonstration. i) Le fixateur de z est conjugué à un sous-groupe discret de $\mathrm{SO}_2(\mathbb{R})$, donc fini. Un tel sous-groupe est cyclique (identifier $\mathrm{SO}_2(\mathbb{R})$ au cercle unité dans $\mathbb{C}^\times$).

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

ii) On applique ceci à V un voisinage compact de z. 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 z on peut trouver un voisinage ouvert U_γ de z 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.

iii) Comme ci-dessus, si V' est un voisinage compact de z', l'ensemble $\Gamma_{V,V'} := \{\gamma \in \Gamma,\ \gamma V \cap V' \neq \emptyset\}$ est fini et on en déduit U voisinage ouvert de z et U' de z' 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 Γz et $\Gamma z'$ respectivement. □

Le iii) de la proposition implique que l'espace topologique quotient $\Gamma\backslash\mathbb{H}$ est séparé. On aimerait munir ce dernier d'une structure complexe. Ceci est facile et classique lorsque Γ (ou plutôt $\Gamma/(\Gamma \cap \{\pm 1\})$ agit *librement* sur $\mathbb{H}$ (*i.e.* $\forall \gamma \in \Gamma, \forall z \in \mathbb{H}, \gamma z = z \Rightarrow \gamma = 1$). Cependant $\mathrm{PSL}_2(\mathbb{Z})$ n'agit pas librement !

1.1.3 $\Gamma\backslash\mathbb{H}$ *comme surface de Riemann.* Pour $z \in \mathbb{H}$, on note h_z le cardinal de $\Gamma_z/(\Gamma_z \cap \{\pm 1\})$. On dit que $z \in \mathbb{H}$ est un *point elliptique* de Γ si $h_z > 1$. Ainsi, Γ agit librement si et seulement si il ne possède pas de point elliptique.

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 $\mathbb{C}$ muni de son faisceau de fonctions holomorphes.

Proposition. – *Notons $\pi : \mathbb{H} \longrightarrow \Gamma\backslash\mathbb{H}$ 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 aussi $Y(\Gamma)$ cette surface de Riemann.

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

assure que $\tau\Gamma_z\tau^{-1}$ agit par rotations sur $\mathbb{D}$. Plus précisément il existe un isomorphisme de groupe $\iota : \Gamma_z \xrightarrow{\sim} \mu_{h_z}$ (racines de l'unité d'ordre h_z) tel que $\tau(\gamma z') = \iota(\gamma)\tau(z')$ pour tout $z' \in \mathbb{H}$. Pour tout rayon $r < 1$, l'ouvert $V := \tau^{-1}(D(0,r))$ est stable par Γ_z, et pour r suffisamment petit on a $\gamma V \cap V \neq \emptyset \Rightarrow \gamma \in \Gamma_z$ d'après le ii) de la proposition précédente. On a alors un diagramme commutatif

$$\begin{array}{ccc} V & \xrightarrow[\tau]{\sim} & D(0,r) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle x\mapsto x^{h_z}} \\ \pi(V) = \Gamma_z\backslash V & \xrightarrow[\bar\tau]{\sim} & \mu_{h_z}\backslash D(0,r^{h_z}) = D(0,r) \end{array}$$

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

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

1.1.4 *Pointes.* Un point x de $\mathbb{P}^1(\mathbb{R})$ 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 choisit $\tau \in \mathrm{SL}_2(\mathbb{R})$ tel que $\tau\infty = x$, alors $\tau^{-1}\Gamma_x\tau$ est un sous-groupe discret du fixateur de ∞, ce dont on déduit qu'il existe $h > 0$ tel que

$$\tau^{-1}\Gamma_x\tau.\{\pm 1\} = \{\pm\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]^m,\ m \in \mathbb{Z}\}.$$

Notons $P_\Gamma \subset \mathbb{P}^1(\mathbb{R})$ l'ensemble des pointes de Γ et $\mathbb{H}^* = \mathbb{H}^*_\Gamma := \mathbb{H} \sqcup P_\Gamma$. On munit $\mathbb{H}^*$ de la topologie engendrée par les ouverts de $\mathbb{H}$ et les ensembles de la forme $V_{\tau,r} := \tau(U_r \sqcup \{\infty\})$, où

— $r > 0$ et $U_r = \{z \in \mathbb{H}, \Im(z) > r\}$

— $\tau \in \mathrm{SL}_2(\mathbb{R})$ et $\tau.\infty \in P_\Gamma$.

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

Lemme. – *Si $x_1, x_2 \in P_\Gamma$, il existe un voisinage $V_{\tau_1,r}$ de x_1 et un voisinage $V_{\tau_2,r}$ de x_2 tels que*

$$\forall \gamma \in \Gamma,\ \gamma V_{\tau_1,r} \cap V_{\tau_2,r} \neq \emptyset \Rightarrow \gamma x_1 = x_2.$$

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 $V_{\tau_2,r} = U_r$. On a alors un $h_\infty > 0$ tel que $\Gamma_\infty.\{\pm 1\} = \{\pm\gamma_\infty^m, m \in \mathbb{Z}\}$ avec $\gamma_\infty = \left[\begin{smallmatrix} 1 & h_\infty \\ 0 & 1 \end{smallmatrix}\right]$. Notons

$x = x_1$ et fixons $\tau = \tau_1$ tel que $\tau\infty = x$, ce qui nous donne $h > 0$ 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 $\gamma\tau U_r \cap U_r \neq \emptyset$. On doit montrer que $\gamma x = \gamma\tau\infty = \infty$. En notant $c(\sigma)$ la coordonnée $(2,1)$ d'une matrice $\sigma \in \mathrm{SL}_2(\mathbb{R})$, on veut donc montrer que $c(\gamma\tau) = 0$. Vu la description de $\gamma\tau U_r$, l'hypothèse $\gamma\tau U_r \cap U_r \neq \emptyset$ implique que $r < r^{-1}c(\gamma\tau)^{-2}$, ou encore $c(\gamma\tau)^2 < r^{-2}$.

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

Pour cela, posons $\delta_{n+1} := \delta_n \left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right] \delta_n^{-1}$, qui est un élément de $\tau^{-1}\Gamma\tau$. 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 $n \to \infty$ et donc que δ_n tend vers la matrice $\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]$. Or, le groupe $\tau^{-1}\Gamma\tau$ étant discret, cela implique $\delta_n = \left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]$ pour n assez grand, donc $c(\delta_n) = 0$ et finalement $c(\delta_1) = 0$.

On laisse au lecteur les conséquences annoncées. □

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

$$\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]^{\mathbb{Z}} \backslash (U_r \sqcup \{\infty\}) \xrightarrow{\sim} D(0,\rho)$$

où $\rho = \exp(-2\pi r/h)$, ce qui munit $U_r \sqcup \{\infty\}$ d'une structure complexe. Si $x = \tau\infty$ 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

$$\begin{array}{ccc} V_{\tau,r} & \xrightarrow[\tau^{-1}]{\sim} & U_r \sqcup \{\infty\} \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle z\mapsto \exp(2i\pi z/h)} \\ \pi(V_{\tau,r}) = \Gamma_x \backslash V_{\tau,r} & \xrightarrow[\bar{\tau}^{-1}]{\sim} & D(0,\rho) \end{array}$$

ce qui munit $\pi(V_{\tau,r})$ d'une structure complexe. Concrètement, la fonction $\exp(2i\pi\tau(z)/h)$ 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.

1.1.5 *Le quotient modulaire.* Nous allons expliciter le quotient $\Gamma\backslash\mathbb{H}^*$ dans le cas du groupe modulaire $\Gamma(1)$. Selon la coutume on abrège $X(1) := X(\Gamma(1))$ et $Y(1) := Y(\Gamma(1))$.

Définition. – *Un* domaine fondamental *pour* Γ *dans* $\mathbb{H}$ *est un ouvert connexe* D *t.q.*
— $\forall\gamma \in \Gamma$, $\gamma D \cap D \neq \emptyset \Rightarrow \gamma = \pm 1$,
— $\mathbb{H} = \bigcup_{\gamma\in\Gamma} \gamma\bar{D}$ *où* $\bar{D}$ *désigne l'adhérence de* D.

Tout sous-groupe discret de $\mathrm{SL}_2(\mathbb{R})$ admet un domaine fondamental. Cela découle de l'existence d'une distance $d(z,z')$ sur $\mathbb{H}$ qui est invariante par $\mathrm{SL}_2(\mathbb{R})$. En effet, ayant choisi un z_0, on peut alors prendre

$$D = \{z \in \mathbb{H}, \forall\gamma \in \Gamma \setminus \{\pm 1\},\ d(z,z_0) < d(z,\gamma z_0)\}.$$

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

Afin d'expliciter un domaine fondamental pour $\Gamma(1)$, on notera $S := \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ et $T := \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. On a donc pour tout $z \in \mathbb{H}$

$$Sz = \frac{-1}{z} \text{ et } Tz = 1 + z,$$

et on constate aussi les relations $S^2 = 1$ et $(ST)^3 = 1$ dans $\mathrm{PSL}_2(\mathbb{R}) = \Gamma(1)/\pm 1$.

THÉORÈME. – *L'ouvert* $D := \{z \in \mathbb{H}, |z| > 1 \text{ et } |\Re(z)| < \frac{1}{2}\}$ *est un domaine fondamental pour* $\Gamma(1)$. *De plus,*

i) si $z \neq z' \in \bar{D}$ *sont* $\Gamma(1)$*-conjugués, alors* $\begin{cases} \Re z = \pm\frac{1}{2} \text{ et } z' = z \pm 1 = T^{\pm 1}z, \\ \text{ou } |z| = 1 \text{ et } z' = \frac{-1}{z} = Sz \end{cases}$

ii) le fixateur $\Gamma(1)_z$ *d'un élément* $z \in \bar{D}$ *contient strictement* $\{\pm 1\}$ *si et seulement si*

$$\begin{cases} \quad z = i, \text{ auquel cas } \Gamma(1)_i = \langle S \rangle \text{ et } \Gamma(1)_i/\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \\ \text{ou} \quad z = j := \exp(2i\pi/3), \text{ auquel cas } \Gamma(1)_j = \langle ST \rangle \text{ et } \Gamma(1)_j/\{\pm 1\} \simeq \mathbb{Z}/3\mathbb{Z} \\ \text{ou} \quad z = -1/j = \exp(2i\pi/6), \text{ auquel cas } \Gamma(1)_{j^2} = \langle TS \rangle \text{ et } \Gamma(1)_{-1/j}/\{\pm 1\} \simeq \mathbb{Z}/3\mathbb{Z} \end{cases}$$

Démonstration. Soit Γ' le sous-groupe de Γ engendré par S et T. Nous montrons d'abord que $\mathbb{H} = \bigcup_{\gamma \in \Gamma'} \gamma D$. Pour $z \in \mathbb{H}$ et $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, la formule $\Im(\gamma z) = \Im(z)/|cz+d|^2$ et le fait que c et d sont des entiers nous disent que $\gamma \mapsto \Im(\gamma z)$ atteint son maximum. Si ce maximum est atteint en $z' = \gamma_0 z$, alors $|z'| \geqslant 1$ puisque sinon on aurait $\Im(Sz') = \Im(-1/z') > \Im(z')$. Mais comme $\Im(Tz') = \Im(z')$, on peut supposer, quitte à faire agir T, que $|\Re(z')| \leqslant 1/2$.

Prouvons maintenant i) et ii). On peut supposer $\Im(z') \geqslant \Im(z)$. Si $z' = \gamma z$, cela implique $|cz + d| \leqslant 1$ et donc $c = 0, 1$ ou -1. Quitte à remplacer γ par $-\gamma$ (qui agit pareil), on peut se contenter des cas $c = 0$ ou $c = 1$. Si $c = 0$, on a $|d| = 1$ et $\gamma z = T^b z$, ce qui n'est possible que si $b = 1$ et $\Re(z) = -1/2$ ou $b = -1$ et $\Re(z) = 1/2$. Si $c = 1$, puisqu'on veut $|z+d| \leqslant 1$, 2 cas sont possibles : $d = 0$ ou ($|d| = 1$ et $z \in \{j, Sj\}$). Si $d = 0$, alors $\det\gamma = 1$ implique $b = -1$ et donc $z' = a - 1/z$. Comme $|z| = 1$, $-1/z$ est dans $\bar{D}$ donc, comme ci-dessus, on a trois cas : ($a = 0$ et $|z| = 1$) ou ($a = 1$ et $\Re(z) = -1/2$, auquel cas $z = j$)) ou ($a = -1$ et $\Re(z) = 1/2$, auquel cas $z = -1/j$). Si $d = 1$ et $z = j$, alors $a - b = 1$ donc $z' = a - 1/(1 + j) = a + j$ donc $a = 0$ ou 1. Idem pour $d = -1$ et $z = -1/j$. □

Remarque. – Géométriquement, $D \cup \{\infty\}$ est le triangle géodésique de sommets $j, -1/j$ et ∞ dans $\mathbb{H}^*$. C'est peut-être plus clair si on considère $S.D$ qui est un triangle géodésique de sommets $j, -1/j$ et 0.

COROLLAIRE. – $\mathrm{PSL}_2(\mathbb{Z})$ *est engendré par (les images de)* S *et* T.

Démonstration. Comme dans la preuve précédente, notons Γ' le groupe engendré par S et T. On a vu que $\mathbb{H} = \bigcup_{\gamma' \in \Gamma'} \gamma' \bar{D}$. Soit alors $\gamma \in \Gamma$, et choisissons $z_0 \in D$. On peut trouver $\gamma' \in \Gamma'$ tel que $\gamma'\gamma z_0 \in \bar{D}$. Mais d'après le i) on a alors $z_0 = \gamma'\gamma z_0$ et d'après le ii) on en déduit $\gamma'\gamma = \pm 1$. Donc $\Gamma(1)/\{\pm 1\}$ est engendré par les images de S et T. □

Remarque. – On peut montrer que $\langle S, T | S^2, (ST)^3 \rangle$ est une présentation de $\mathrm{PSL}_2(\mathbb{Z})$. En particulier $\mathrm{PSL}_2(\mathbb{Z})$ est isomorphe au produit libre de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

Le théorème précédent montre que $\Gamma(1)$ a deux orbites de points elliptiques, l'une d'ordre 2 et l'autre d'ordre 3.

$$\{\text{points elliptiques de } \Gamma(1) \text{ dans } \mathbb{H}\} = \Gamma(1)i \bigsqcup \Gamma(1)j.$$

Quant aux pointes, il est clair que $\infty \in P_{\Gamma(1)}$ avec $\Gamma(1)_\infty = \{\pm 1\}.\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]^{\mathbb{Z}}$. En fait, tout élément parabolique de $\mathrm{SL}_2(\mathbb{Z})$ est conjugué, *dans* $\mathrm{GL}_2(\mathbb{Q})$, à $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Donc toute pointe de $\Gamma(1)$ appartient à $\mathrm{GL}_2(\mathbb{Q}).\infty = \mathbb{P}^1(\mathbb{Q})$. En remarquant (exercice) que $\mathbb{P}^1(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Z})\infty$, on a donc

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

1.1.6 Corollaire.– *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. Nous donnons une explication topologique utilisant la classification des surfaces de Riemann compactes. Nous verrons plus tard des fonctions explicites qui réalisent les isomorphismes annoncés.

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 $\pi : \mathbb{H}^* \longrightarrow \Gamma(1)\backslash\mathbb{H}^*$ de $\bar{D}^* := \bar{D} \sqcup \{\infty\}$. Or il est clair que $\bar{D}^*$ est compact : si on a un recouvrement ouvert, l'un de ces ouverts est de la forme $(U_r \sqcup \{\infty\}) \cap \bar{D}^*$ et son complémentaire est compact dans $\bar{D}$.

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 $\bar{D}$:

— identification des demi-droites $\Re(z) = 1/2$ et $\Re(z) = -1/2$

— identification du "segment" $[i, j]$ avec le segment $[i, Sj]$.

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

1.1.7 *Sous-groupes de congruence.* Soit Γ un sous-groupe d'indice fini de $\Gamma(1)$.

Domaine fondamental. Soit $d := |\Gamma\{\pm 1\}\backslash\Gamma(1)|$. Si on choisit $\gamma_1, \cdots, \gamma_d$ tels que $\bar{\Gamma}(1) = \bigsqcup_i \bar{\Gamma}\bar{\gamma}_i$ (la barre désigne l'image dans PSL_2), alors la réunion $D' = \gamma_1 D \sqcup \cdots \sqcup \gamma_d D$ 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 $\bar{D}'$ soit connexe. Dans ce cas, l'intérieur de $\bar{D}'$ est un domaine fondamental pour Γ.

Pointes. Il est clair que $P_\Gamma \subset P_{\Gamma(1)} = \mathbb{P}^1(\mathbb{Q})$. Mais comme $\Gamma(1)_x$ est infini pour toute pointe $x \in \mathbb{P}^1(\mathbb{Q})$ et Γ d'indice fini, on a aussi Γ_x infini et x est donc une pointe. Donc $P_\Gamma = \mathbb{P}^1(\mathbb{Q})$. Par contre, en général il y a plusieurs Γ-orbites dans $\mathbb{P}^1(\mathbb{Q})$. On note n_∞ le nombre de telles orbites.

Points elliptiques. Si z est un point elliptique de Γ, il est conjugué à i ou j 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 i (ils sont d'ordre $h = 3$).

THÉORÈME. – *La surface de Riemann $X(\Gamma)$ est compacte. La projection $X(\Gamma) \longrightarrow X(1)$ 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 $X(\Gamma)$ est l'image de la réunion $\gamma_1\bar{D}^* \cup \cdots \cup \gamma_d\bar{D}^*$ qui est compact. Le fait que l'application $Y(N) \longrightarrow Y(1)$ est holomorphe découle de la définition des structures complexes, et de même pour l'holomorphie de $X(N) \longrightarrow X(1)$ 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

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

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 $f : X(\Gamma) \longrightarrow X(1)$ en $P \in X(\Gamma)$ (*i.e.*, localement autour de P, f est de la forme $z \mapsto z^{e_P}$). Dans notre cas, cela donne

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

Notons $\pi : \mathbb{H}^* \longrightarrow X(1)$ 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 j. 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, 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 $\sum_{P \mapsto \pi(i)}(e_P - 1) = (d - n_2)/2$ à la formule de Hurwitz.

Considérons maintenant la fibre $f^{-1}(\pi(j))$. 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 $P \in f^{-1}(\pi(i))$ tels que $e_P = 1$. Vu les propriétés du degré, il y a donc $\frac{d-n_3}{3}$ points $P \in f^{-1}(\pi(i))$ tels que $e_P = 3$. D'où une contribution $\sum_{P\mapsto\pi(j)}(e_P - 1) = 2(d - n_2)/3$ 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 $\sum_{P\mapsto\pi(\infty)} e_P = d$. D'où une contribution $\sum_{P\mapsto\pi(\infty)}(e_P - 1) = d - n_\infty$ à la formule de Hurwitz.

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

Remarque. – Sur la ramification aux pointes. Supposons que $x \in \mathbb{P}^1(\mathbb{R})$ 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 τ de $\Gamma(1)$, on a vu qu'une coordonnée locale autour de P est donnée par $\exp(2i\pi\tau(z)/h)$ tandis qu'une coordonnée locale autour de $\pi(z)$ est $\exp(2i\pi\tau(z))$. Dans ces coordonnées, la projection $X(\Gamma) \longrightarrow X(1)$ prend donc la forme $x \mapsto x^h$, ce qui montre que h est l'indice de ramification de cette projection au point P.

1.1.8 *Interprétation modulaire.* Le mot "modulaire" renvoie à la notion d'"espace de module", *i.e.* d'espace qui classifie certains objets. En l'occurrence, la courbe $Y(1)$ classifie les surfaces de Riemann de genre 1 à isomorphisme (ie biholomorphisme) près.

Pour expliquer cela, on utilise la notion de *tore complexe (de dimension 1)*. Par définition, c'est le quotient $\mathbb{C}/\Lambda$ de $\mathbb{C}$ par un réseau $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, muni de la structure complexe donnée par le faisceau des fonctions holomorphes invariantes par Λ, comme dans la proposition 1.1.3 (sauf qu'ici Λ agit proprement et librement, de sorte que $\mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ est un revêtement localement trivial, i.e. sans ramification). Il est clair que $\mathbb{C}/\Lambda$ est compacte et de genre 1. Inversement :

PROPOSITION. – *Toute surface de Riemann X de genre 1 est biholomorphe à un tore complexe (de dimension 1).*

Démonstration. Le théorème d'uniformisation de Riemann nous dit que le revêtement universel de X est $\mathbb{C}$ ou $\mathbb{H}$, et qu'on peut réaliser X comme quotient de son revêtement universel par un groupe y opérant librement et proprement.

Si X est de la forme $\Gamma\backslash\mathbb{H}$ pour $\Gamma \subset \mathrm{Aut}(\mathbb{H})$, alors :

— Γ doit être discret (pour agir proprement)

— Γ n'a pas de point elliptique (pour agir librement) ni de pointe (sinon on pourrait agrandir X qui est déjà compacte).

— Γ est isomorphe au groupe fondamental de X qui est $\mathbb{Z}^2$.

Le groupe Γ est donc constitué d'éléments hyperboliques qui admettent 2 droites propres communes dans $\mathbb{R}^2$ (diagonalisation simultanée). Donc, après conjugaison, Γ est un sous-groupe des matrices diagonales dans $\mathrm{SL}_2(\mathbb{R})$ (modulo ± 1), donc de $\mathbb{R}^\times$. Mais ce dernier ne possède pas de sous-groupe discret isomorphe à $\mathbb{Z}^2$. Contradiction.

Donc X est de la forme $\Gamma\backslash\mathbb{C}$. Or $\mathrm{Aut}(\mathbb{C})$ est l'ensemble des $z \mapsto az+b$ avec $a, b \in \mathbb{C}^\times \times \mathbb{C}$. Si $a \neq 1$ un tel automorphisme possède un point fixe donc n'agit pas librement. Donc

finalement Γ est un groupe discret de translations, donné par un réseau Λ comme ci-dessus, et $\Gamma\backslash\mathbb{C} = \mathbb{C}/\Lambda$. □

Remarque. – Une conséquence est que toute surface de Riemann de genre 1 peut être munie d'une structure de groupe analytique, puisque c'est le cas de $\mathbb{C}/\Lambda$.

Étudions maintenant les biholomorphismes entre deux tores complexes.

PROPOSITION. – *Toute application holomorphe $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ est de la forme $[z+\Lambda] \mapsto [\alpha z + \beta + \Lambda']$ où $\beta \in \mathbb{C}$ et $\alpha \in \mathbb{C}$ est tel que $\alpha\Lambda \subset \Lambda'$.*

Démonstration. Notons $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ et $\pi' : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda'$ les projections canoniques. Comme $\mathbb{C}$ est simplement connexe, il existe une application continue $\tilde{\varphi} : \mathbb{C} \longrightarrow \mathbb{C}$ telle que $\varphi \circ \pi = \pi' \circ \tilde{\varphi}$, et cette application est holomorphe. Pour tout $\lambda \in \Lambda$, l'application $z \mapsto \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z)$ est à valeurs dans Λ' qui est discret, et donc est constante puisque $\mathbb{C}$ est connexe. Il s'ensuit que la dérivée $\tilde{\varphi}'$ est invariante sous Λ. Celle-ci descend donc en une fonction holomorphe sur $\mathbb{C}/\Lambda$, qui n'a d'autre choix que d'être constante, de valeur $\alpha \in \mathbb{C}$. On en déduit l'existence de $\beta \in \mathbb{C}$ tel que $\tilde{\varphi}(z) = \alpha z + \beta$. □

Remarque. – Une conséquence est que toute application holomorphe entre tores complexes qui envoie 0 sur 0 *est un homomorphisme de groupes analytiques*. Il s'ensuit que, si X est une surface de Riemann compacte de genre 1 munie d'un point x, alors la structure de groupe analytique avec élément neutre x donnée par la remarque précédente est *unique*, *i.e.* ne dépend pas du biholomorphisme $\mathbb{C}/\Lambda \xrightarrow{\sim} X$ choisi, pourvu qu'il envoie 0 sur x.

Maintenant, un réseau Λ admet une base (ω_1, ω_2) comme $\mathbb{Z}$-module. Toutes les bases se déduisent l'une de l'autre par action de $\mathrm{GL}_2(\mathbb{Z})$ sur le vecteur colonne $\binom{\omega_1}{\omega_2} \in \mathbb{C}^2$. On peut ordonner la base de sorte que $\Im(\omega_1/\omega_2) > 0$. Les bases ainsi ordonnées se déduisent l'une de l'autre par action de $\mathrm{SL}_2(\mathbb{Z})$. On obtient ainsi une bijection entre l'ensemble $\mathcal{R}$ des réseaux et l'ensemble $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{V}$ des vecteurs $\binom{\omega_1}{\omega_2} \in \mathbb{C}^2$ avec $\omega_1/\omega_2 \in \mathbb{H}$ modulo action de $\mathrm{SL}_2(\mathbb{Z})$. Via cette bijection, l'action par homothétie de $\mathbb{C}^\times$ sur $\mathcal{R}$ correspond à l'action par homothétie sur $\mathcal{V}$. On vient de voir que le quotient $\mathcal{R}/\mathbb{C}^*$ s'identifie à l'ensemble $\mathcal{E}$ des classes d'isomorphisme de tores complexes. De l'autre côté, l'application $\binom{\omega_1}{\omega_2} \mapsto \omega_1/\omega_2$ induit une bijection de $\mathcal{V}/\mathbb{C}^\times$ sur $\mathbb{H}$. Au final, on obtient le résultat suivant.

PROPOSITION. – *On a des bijections*

$$\begin{array}{ccc} Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} & & \{\textit{Surf. de R. de genre 1}\}_{/\textit{biholom}} \\ {\scriptstyle z\mapsto\mathbb{Z}z\oplus\mathbb{Z}}\downarrow{\scriptstyle\sim} & & {\scriptstyle\sim}\uparrow \\ \{\textit{Réseaux de } \mathbb{C}\}_{/\textit{homothétie}} & \xrightarrow[\sim]{\Lambda\mapsto\mathbb{C}/\Lambda} & \{\textit{tores complexes}\}_{/\textit{isom}} \end{array}$$

1.2 Formes modulaires

Γ désigne toujours un sous-groupe d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$.

1.2.1 *Fonctions modulaires de poids* 0. On rappelle qu'une fonction méromorphe $X \dashrightarrow \mathbb{C}$ sur une surface de Riemann X (donc définie en dehors de ses pôles) se prolonge de manière unique en une application holomorphe $X \longrightarrow \mathbb{P}^1(\mathbb{C})$. On note $\mathcal{M}_X$ le corps des fonctions méromorphes sur X. Par exemple $\mathcal{M}_{\mathbb{P}^1(\mathbb{C})} \simeq \mathbb{C}(z)$. Un résultat spectaculaire de la théorie (dont nous n'avons pas besoin) dit que $X \mapsto \mathcal{M}_X$ 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 transcendence 1 sur $\mathbb{C}$. C'est une motivation pour étudier le corps $\mathcal{M}_{X(\Gamma)}$.

Soit φ une fonction méromorphe $X(\Gamma) \longrightarrow \mathbb{P}^1(\mathbb{C})$. Notons f la composée $\mathbb{H} \longrightarrow X(\Gamma) \xrightarrow{\varphi} \mathbb{P}^1(\mathbb{C})$. 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.*

Pour expliciter cette condition, 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 $f(z) = f(z+h)$ (autrement dit, f est invariante par une matrice $\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]$). Elle s'écrit comme une fonction méromorphe en $q = \exp(2i\pi z/h) \in \mathbb{D} \setminus \{0\}$ et admet donc un développement

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

au voisinage de $q = 0$ (donc de $z = \infty$). 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 $n << 0$. On note alors

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

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

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

$$\mathrm{ord}_{x,h}(f) := \mathrm{ord}_{\infty,h}(\tau^* f).$$

Les fonctions $f : \mathbb{H} \longrightarrow \mathbb{C}$ invariantes par Γ et méromorphes sur $\mathbb{H}$ et aux pointes sont appelées *fonctions modulaires de niveau* Γ *et poids* 0. Elles correspondent aux fonctions méromorphes sur $X(\Gamma)$.

Les fonctions $f : \mathbb{H} \longrightarrow \mathbb{C}$ invariantes par Γ et holomorphes sur $\mathbb{H}$ et aux pointes sont appelées *formes modulaires de niveau* Γ *et poids* 0. Elles correspondent aux fonctions holomorphes sur $X(\Gamma)$, et sont donc ... constantes !

1.2.2 *Formes modulaires de poids* 2. Après les fonctions méromorphes, il est naturel de regarder les *formes différentielles* méromorphes sur $X(\Gamma)$. Sur un ouvert U de $\mathbb{C}$ 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 $\mathbb{C}$, 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 $X \supseteq O \xrightarrow{\sim} U \subset \mathbb{C}$, d'une forme différentielle sur U, et ce de manière compatible avec la formule de changement de carte ci-dessus.

Soit $\pi : \mathbb{H} \longrightarrow X(\Gamma)$ 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 $\pi^*\omega = f(z)dz$. La condition d'invariance s'écrit :

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

et un calcul montre que pour $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, et en posant $j_\gamma(z) = cz + d$ on a

$$d(\gamma z) = j_\gamma(z)^{-2}dz.$$

On a donc la propriété suivante d' "automorphie" sur la fonction f

$$\forall \gamma \in \Gamma,\ f(z) = j_\gamma(z)^{-2}f(\gamma z).$$

Puisque $j_{\pm\left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]}(z)^2 = 1$, on voit que toute fonction f satisfaisant cette propriété d'automorphie est horizontalement périodique. De même, pour tout $\tau \in \mathrm{SL}_2(\mathbb{Z})$, la forme différentielle $\tau^*(f.dz) = j_\tau(z)^{-2}f(\tau z)dz$ est invariante sous $\tau^{-1}\Gamma\tau$ donc la fonction $j_\tau(z)^{-2}f(\tau z)$ est horizontalement périodique. On dit alors que f est méromorphe ou holomorphe à la pointe $\tau\infty$ si la fonction $z \mapsto j_\tau(z)^{-2}f(\tau z)$ est méromorphe ou holomorphe à l'infini. Cela ne dépend pas du choix de τ, pas plus que l'entier [2]

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

Une *fonction modulaire de niveau* Γ *et poids* 2 est une fonction sur $\mathbb{H}$ qui satisfait la propriété d'automorphie ci-dessus et est méromorphe sur $\mathbb{H}$ et aux pointes. Une telle fonction correspond donc à une forme différentielle méromorphe sur $X(\Gamma)$.

Une *forme modulaire de niveau* Γ *et poids* 2 est une fonction modulaire qui est de plus *holomorphe* sur $\mathbb{H}$ et aux pointes.

Attention. L'holomorphie de f n'est pas équivalente à celle de ω!! Pour expliquer cela, introduisons la notation $\mathrm{ord}_P(f)$ 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 $f = g(z)$ dans une coordonnée locale z au voisinage de P on a $\mathrm{ord}_P(f) = \mathrm{ord}_0(g)$. De même, si dans cette coordonnée on développe une forme différentielle méromorphe sous la forme $\omega = g(z)dz$, alors l'entier $\mathrm{ord}_0(g)$ ne dépend pas du choix de la coordonnée et se note $\mathrm{ord}_P(\omega)$. Bien sûr ω est holomorphe en P si et seulement si $\mathrm{ord}_P(\omega) \geqslant 0$.

2. on remarquera que cette définition de $\mathrm{ord}_{x,h}(f)$ est différente de la précédente (sauf si $x = \infty$), qui s'appliquait à une fonction Γ-invariante. Ici, c'est fdz qui est Γ-invariante. La notation peut paraitre ambigüe, mais l'ambiguité n'existe que pour une fonction f telle que f et fdz sont Γ-invariantes. Or une telle fonction est nulle.

LEMME. – *Soit ω une forme différentielle méromorphe sur $X(\Gamma)$ et soit f la fonction méromorphe sur $\mathbb{H}$ telle que $\pi^*\omega = f(z)dz$. Alors on a les égalités suivantes :*

i) $\mathrm{ord}_P(f) = \mathrm{ord}_{\pi(P)}(\omega)$ *si P est un point de $\mathbb{H}$ ordinaire pour Γ.*

ii) $\mathrm{ord}_P(f) = e.\mathrm{ord}_{\pi(P)}(\omega) + e - 1$ *si P est un point elliptique d'ordre e (égal à 2 ou 3).*

iii) $\mathrm{ord}_{x,h}(f) = \mathrm{ord}_{\pi(x)}(\omega) + 1$ *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 $z' = \tau(z)$ telle que π est de la forme $z' \mapsto z'^e$, avec $e = 1$ si P est ordinaire. La fonction $u = z'^e$ descend donc en une coordonnée locale autour de $\pi(P)$. Il s'ensuit que si $\omega = g(u)du$ au voisinage de $\pi(z_0)$, alors $\pi^*\omega = g(z'^e)d(z'^e) = ez'^{e-1}g(z'^e)dz'$ et donc $\mathrm{ord}_P(f) = \mathrm{ord}_P(\pi^*\omega) = \mathrm{ord}_0(z'^{e-1}g(z'^e)) = e.\mathrm{ord}_0(g) + e - 1 = e.\mathrm{ord}_{\pi(P)}(\omega) + e - 1$.

iii) Quitte à translater par un $\tau \in \mathrm{SL}_2(\mathbb{Z})$ on peut supposer que $x = \infty$. Dans ce cas, on a vu que $q = \exp(2i\pi z/h)$ est une coordonnée locale autour de $\pi(x)$. Ainsi si ω est de la forme $g(q)dq$, $\pi^*\omega$ est de la forme $2i\pi/h.g(\exp(2i\pi z/h)).\exp(2i\pi z/h)dz = f(z)dz$, de sorte que $f(z) = 2i\pi/h.q.g(q)$, et finalement $\mathrm{ord}_{\infty,h}(f) = \mathrm{ord}_0(q.g(q)) = \mathrm{ord}_0(g(q)) + 1 = \mathrm{ord}_{\pi(x)}\omega + 1$. □

Notons

— $\mathcal{M}_2(\Gamma)$ le $\mathbb{C}$-espace vectoriel des formes modulaires de niveau Γ et poids 2

— $\mathcal{S}_2(\Gamma)$ le sous-espaces des formes modulaires *paraboliques* (aussi appelées *cuspidales*, et en anglais *cusp forms*), qui par définition sont celles qui s'annulent aux pointes (ie $\mathrm{ord}_{x,h}(f) > 0$ pour chaque pointe x).

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 $a_P \in \mathbb{Z}$ est nul sauf pour un nombre fini de points. L'ensemble des diviseurs $\mathrm{Div}(X)$ est donc le groupe abélien libre de base X. Il est partiellement ordonné par la relation $\sum_P a_P[P] \leqslant \sum_P b_P[P]$ si $a_P \leqslant b_P$ pour tout P.

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

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

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

On a $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ et $\mathrm{div}(f+g) \geqslant \inf(\mathrm{div}(f), \mathrm{div}(g))$. [3] On obtient ainsi un homomorphisme de groupe $\mathcal{M}_X^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(X)$ dont l'image est notée $\mathrm{Div.pr}(X)$. Un tel diviseur est dit *principal*. Le quotient $\mathrm{Div}(X)/\mathrm{Div.pr}(X)$ s'appelle *groupe de Picard de X* et se note $\mathrm{Pic}(X)$. (C'est l'analogue du groupe des classes d'un corps de nombres).

3. 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 élements inférieurs à $\mathrm{div}(f)$ et $\mathrm{div}(g)$.

— L'application deg se factorise par $\mathrm{Pic}(X)$. En effet, si l'on considère $f \in \mathcal{M}_X^\times$ comme une application holomorphe $X \longrightarrow \mathbb{P}^1(\mathbb{C})$ dont on note e_P l'indice de ramification en un point $P \in X$, alors

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

donc son degré est nul.

— De même à toute forme différentielle méromorphe on associe

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

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

— Si $D \in \mathrm{Div}(X)$, on note

$$L(D) := \{f \in \mathcal{M}_X^\times,\ \mathrm{div}(f) + D \geqslant 0\} \sqcup \{0\}.$$

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

— Le *théorème de Riemann-Roch* affirme que

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

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

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

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

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

Revenons à $X = X(\Gamma)$ et notons $D_\pi := \sum_{P \in X(\Gamma)} (1 - 1/e_P)[P] \in \mathrm{Div}(X(\Gamma)) \otimes_{\mathbb{Z}} \mathbb{Q}$ où e_P vaut 1 pour un point ordinaire, 2 ou 3 pour un point elliptique, et $+\infty$ pour une pointe. On a donc $\deg(D_\pi) = \frac{1}{2}n_2 + \frac{2}{3}n_3 + n_\infty$.

Corollaire. – *On a les égalités*

— $\dim_{\mathbb{C}}(\mathcal{M}_2(\Gamma)) = \ell(D_\pi + K) = g - 1 + n_\infty$,

— $\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma)) = \ell(K) = g$.

Démonstration. Le lemme précédent nous dit que l'application $\omega \mapsto f$ définie par $\pi^*\omega = f(z)dz$ induit un isomorphisme

$$\{\omega,\ \mathrm{div}(\omega) + D_\pi \geqslant 0\} \sqcup \{0\} \xrightarrow{\sim} \mathcal{M}_2(\Gamma).$$

Fixons une forme différentielle méromorphe ω_0 sur $X(\Gamma)$ [4], et écrivons les autres sous la forme $\omega = g.\omega_0$, alors puisque $\mathrm{div}(\omega) = \mathrm{div}(g) + \mathrm{div}(\omega_0)$, l'application $g \mapsto g\omega_0 \mapsto f$ induit un isomorphisme

$$L(\mathrm{div}(\omega_0) + D_\pi) \xrightarrow{\sim} \mathcal{M}_2(\Gamma).$$

La même application induit l'isomorphisme

$$L(\mathrm{div}(\omega_0) + D_\pi - \sum_{P \mapsto \infty} [P]) \xrightarrow{\sim} \mathcal{S}_2(\Gamma).$$

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

$$\dim_{\mathbb{C}}(\mathcal{M}_2(\Gamma)) = \ell(\mathrm{div}(\omega_0) + \lfloor D_\pi \rfloor) = \ell(K + \lfloor D_\pi \rfloor) = \ell(K + \sum_{P \mapsto \infty} [P]).$$

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

$$\ell(K + \sum_{P \mapsto \infty} [P]) = \deg(K + \sum_{P \mapsto \infty} [P]) + 1 - g = g - 1 + n_\infty.$$

Par le même raisonnement, on obtient que

$$\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma)) = \ell(\mathrm{div}(\omega_0) + \lfloor D_\pi \rfloor - \sum_{P \mapsto \infty} [P]) = \ell(K) = g.$$

□

1.2.3 *Formes modulaires de poids $k \in \mathbb{N}$.* Pour un entier $k \in \mathbb{Z}$, on définit une action de $\mathrm{GL}_2(\mathbb{R})^+$ sur $\mathcal{M}_X$ par la formule

$$f[\gamma]_k(z) := \det(\gamma)^{k/2} j_\gamma(z)^{-k} f(\gamma z).$$

Le fait que ce soit une action, *i.e.* que $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$, découle de la formule $j_{\gamma\gamma'}(z) = j_\gamma(\gamma' z) j_{\gamma'}(z)$ que l'on vérifiera sans peine.

On espère que le paragraphe précédent rend plus naturelle la définition suivante :

Définition. – *Soit Γ un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$. Une forme modulaire de niveau Γ et poids $k \in \mathbb{N}$ est une fonction $f : \mathbb{H} \longrightarrow \mathbb{C}$ satisfaisant les propriétés suivantes :*

i) $\forall \gamma \in \Gamma$, $f[\gamma]_k = f$ (propriété d'automorphie).

ii) f est holomorphe sur $\mathbb{H}$ ainsi qu'aux pointes [5].

4. Il en existe toujours. Par exemple, sur $X(1) = \mathbb{P}^1$ on peut prendre dz (qui a $\mathrm{div}(dz) = -2[\infty]$) puis tirer en arrière dz via $X(\Gamma) \longrightarrow X(1)$

5. Comme dans le cas de poids 2, l'holomorphie à la pointe ∞ est bien définie car f est horizontalement périodique. Pour une pointe $x = \tau\infty$, $\tau \in \mathrm{SL}_2(\mathbb{Z})$, on dit que f est holomorphe ou méromorphe en x si la translatée $f[\tau]_k$, qui est aussi horizontalement périodique, l'est à l'infini. Cela ne dépend pas du choix de τ, pas plus que l'entier $\mathrm{ord}_{x,h}(f) := \mathrm{ord}_{\infty,h}(f[\tau]_k)$.

Ces fonctions forment un $\mathbb{C}$-espace vectoriel que l'on note $\mathcal{M}_k(\Gamma)$. On dit que f est parabolique (ou cuspidale, et en anglais "cusp form") si f s'annule aux pointes. L'espace des formes paraboliques est noté $\mathcal{S}_k(\Gamma)$.

On dira aussi d'une fonction satisfaisant ces propriétés avec "méromorphe" au lieu de "holomorphe" que c'est une *fonction modulaire* de niveau Γ et poids k.

Remarque. – Si k est impair et $-1 \in \Gamma$, alors $\mathcal{M}_k(\Gamma) = \mathcal{S}_k(\Gamma) = 0$ puisque $f[-1]_k = -f$.

Remarque. – Pour vérifier qu'une fonction est automorphe pour (Γ, k) il suffit de vérifier l'égalité $f[\gamma]_k = f$ pour un ensemble de générateurs de Γ. Par exemple, si $\Gamma = \Gamma(1)$ et k pair, il suffit de vérifier $f(z+1) = f(z)$ et $f(-1/z) = z^k f(z)$.

Remarque. – Si f est méromorphe et automorphe de poids k, pour vérifier que f est holomorphe aux pointes, il suffit de montrer que pour tout $\tau \in \Gamma(1)$, la fonction $\tau^* f(z)$ admet une limite lorsque $\Im(z) \to \infty$.

Remarque. – La multiplication des fonctions induit un produit $\mathcal{M}_k(\Gamma) \otimes \mathcal{M}_{k'}(\Gamma) \longrightarrow \mathcal{M}_{k+k'}(\Gamma)$, qui fait de $\mathcal{M}(\Gamma) := \bigoplus_{k\in\mathbb{N}} \mathcal{M}_k(\Gamma)$ une $\mathbb{C}$-algèbre graduée, et de $\mathcal{S}(\Gamma) := \bigoplus_{k\in\mathbb{N}} \mathcal{S}_k(\Gamma)$ un idéal de cette algèbre.

Remarque. – Lorsque $\Gamma = \Gamma(1)$, il est intéressant d'exprimer la propriété d'automorphie en termes de fonctions sur les réseaux. Une fonction sur $\mathcal{R}$ est dite homogène de poids k si

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

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

$$\{\text{Fonctions homogènes de poids } k \text{ sur } \mathcal{R}\} \leftrightarrow \{\text{Fonctions } \Gamma(1)\text{-automorphes de poids } k\}$$

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

Exemple. (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 $\Lambda^* = \Lambda \setminus \{0\}$. Cette somme converge absolument pour $k \geqslant 3$ (exercice) et, comme il se doit, est nulle si k est impair. La fonction correspondante sur $\mathbb{H}$ s'écrit

$$G_k(z) = \sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(mz+n)^k}.$$

Pour étudier l'holomorphie, choisissons $\varepsilon > 0$ suffisamment petit pour qu'il existe z_ε tel que $|z_\varepsilon| = 1-\varepsilon$ et $2\Re(z_\varepsilon) = 1+\varepsilon$. Considérons le voisinage ouvert D^ε du domaine fondamental $\bar{D}$ donné par les inégalités $|z| > (1-\varepsilon)$ et $|2\Re(z)| < 1+\varepsilon$. Pour z dans D^ε, l'inégalité

$$|mz+n|^2 = m^2 z\bar{z} + 2mn\Re(z) + n^2 \geqslant m^2(1-\varepsilon)^2 - mn(1+\varepsilon) + n^2 = |mz_\varepsilon - n|^2$$

montre que G_k converge normalement sur D^ε et y est donc holomorphe. Par automorphie, G_k est donc holomorphe sur tout $\mathbb{H}$. Pour montrer qu'elle est aussi holomorphe à la pointe ∞, il faut montrer que $G_k(z)$ possède une limite lorsque $\Im(z) \to \infty$. Par invariance sous T, on peut garder z dans $\bar{D}$, et la convergence normale nous montre que, puisque k est pair,

$$\lim_{z\in\bar{D},\Im(z)\to\infty} G_k(z) = \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} = 2\zeta(k).$$

Ainsi $G_k \in \mathcal{M}_k(\Gamma(1))$ et $G_k(\infty) = 2\zeta(k)$ (avec toujours k pair).

Exemple. (Fonction Δ) – Pour une raison qui apparaitra quand nous parlerons de courbes elliptiques, il est d'usage de poser $g_2 := 60G_4$ et $g_3 := 140G_6$. Admettant momentanément que $\zeta(4) = \frac{\pi^4}{2.3^2.5}$ et $\zeta(6) = \frac{\pi^6}{3^3.5.7}$ (cf feuille d'exercices), on constate alors que

$$\Delta := g_2^3 - 27g_3^2 \in \mathcal{S}_{12}(\Gamma(1)),$$

donnant donc un premier exemple de forme parabolique.

1.2.4 *Pôles et zéros des fonctions modulaires.* 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 $\mathbb{C}$ est une expression de la forme $\omega = f(z)(dz)^{k'}$. Si φ est une application biholomorphe entre deux ouverts on transporte une telle forme par la formule $\varphi^*\omega = f(\varphi(z))\varphi'(z)^{k'}(dz)^{k'}$. 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

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

donnée par l'égalité $\pi^*\omega = f(z)(dz)^{k'}$. Comme pour le poids 2, on a la relation suivante entre pôles et zéros de f et ω.

$$\begin{cases} \mathrm{ord}_P(f) = e.\mathrm{ord}_{\pi(P)}(\omega) + k'(e-1) & \text{si } P \in \mathbb{H} \text{ et } e \text{ est son indice de ramification} \\ \mathrm{ord}_{x,h}(f) = \mathrm{ord}_{\pi(x)}(\omega) + k' & \text{si } x \text{ est une pointe d'ordre } h \end{cases}$$

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

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

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

Démonstration. Lorsque $k = 2k'$ est pair, les égalités ci-dessus montrent que le terme de gauche s'identifie à $\deg(\mathrm{div}(\omega)) + k'\deg(D_\pi)$. Le degré $\deg(\mathrm{div}(\omega))$ ne dépend pas de ω (puisque les autres sont de la forme $g\omega$ avec $g \in \mathcal{M}^\times_{X(\Gamma)}$). 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 $\omega_1^{k'} = f(z)^{k'}(dz)^{k'}$ sur une carte où $\omega_1 = f(z)dz$. On obtient $\deg(\mathrm{div}(\omega)) = k' \deg(\mathrm{div}(\omega_1)) = k'(2g-2)$, 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. □

Application. (Calcul de $\mathcal{M}(\Gamma(1))$) – Pour $\Gamma = \Gamma(1)$, la formule devient

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

On sait que $\mathcal{M}_k(\Gamma(1))$ est nul si k est impair. Si on fait $k = 2$, puisque chacun des $\mathrm{ord}_?(f)$ est $\geqslant 0$, on constate qu'il n'y a pas de f satisfaisant cette égalité. Donc

$$\mathcal{M}_2(\Gamma(1)) = 0.$$

Si on fait $k = 4$, on obtient que toute $f \in \mathcal{M}_4(\Gamma(1))$ possède un zéro simple en j, et ne s'annule nulle part ailleurs. Cela s'applique à G_4, et montre que f/G_4 est une forme modulaire de poids 0 donc constante, donc

$$\mathcal{M}_4(\Gamma(1)) = \mathbb{C}.G_4.$$

De même avec $k = 6$, on obtient que G_6 possède un zéro simple en i et ne s'annule nulle part ailleurs, puis que

$$\mathcal{M}_6(\Gamma(1)) = \mathbb{C}.G_6.$$

Le même raisonnement montre que $\mathcal{M}_8$ et $\mathcal{M}_{10}$ sont de dimension 1 et plus précisément

$$\mathcal{M}_8(\Gamma(1)) = \mathbb{C}.G_8 = \mathbb{C}G_4^2 \quad \text{et} \quad \mathcal{M}_{10}(\Gamma(1)) = \mathbb{C}.G_{10} = \mathbb{C}G_4G_6.$$

Enfin pour $k = 12$, toute forme *parabolique* f ne peut s'annuler en dehors de ∞, et son zéro en ∞ est d'ordre 1. Ceci s'applique à Δ, et on en déduit que

$$\mathcal{S}_{12}(\Gamma(1)) = \mathbb{C}.\Delta.$$

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

$$\mathcal{M}_k(\Gamma(1)) \xrightarrow{\sim} \mathcal{S}_{k+12}(\Gamma(1))$$

pour tout $k \in \mathbb{N}$. Par ailleurs, puisque $\mathcal{S}_k(\Gamma(1))$ est de codimension 1 dans $\mathcal{M}_k(\Gamma(1))$ (noyau de l'application $f \mapsto f(\infty)$, et puisque G_k n'est pas parabolique, on a pour $k \geqslant 12$

$$\mathcal{M}_k(\Gamma(1)) = \mathbb{C}G_k \oplus \mathcal{S}_k(\Gamma(1)).$$

Grâce aux calcul des $\mathcal{M}_k$ pour $k < 12$ on en déduit

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

En fait, on a encore mieux :

PROPOSITION. – *L'algèbre $\mathcal{M}(\Gamma(1))$ est l'algèbre des polynômes en G_4 et G_6.*

Démonstration. Il s'agit de montrer que pour $k \in 2\mathbb{N}$, la famille des $G_4^n G_6^m$ où $n, m \in \mathbb{N}$ et $4n + 6m = k$ est une base de $\mathcal{M}_k(\Gamma(1))$. On l'a déjà vérifié pour $k \leqslant 10$.

Montrons par récurrence que cette famille est génératrice pour $k \geqslant 12$. Choisissons pour cela n, m tels que $4n+6m = k$, et soit $f \in \mathcal{M}_k$. Puisque $G_4^n G_6^m$ ne s'annule pas à l'infini, il existe λ tel que $f - \lambda G_4^n G_6^m$ soit parabolique. Mais alors $f - \lambda G_4^n G_6^m = \Delta.g$ pour $g \in \mathcal{M}_{k-12}$, et par récurrence, on conclut que $f \in \mathbb{C}[G_4, G_6]$ (rappelons que $\Delta = (60)^3 G_4^3 - 27(140)^2 G_6^2$).

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 $G_4^{n_0} G_6^{m_0}$, une relation de dépendence linéaire fournit un polynôme dans $\mathbb{C}[T]$ qui annule la fonction méromorphe $G_4^3 G_6^{-2}$, laquelle devrait donc être constante, ce qui n'est pas le cas. □

Exemple. (L'invariant modulaire j) – Puisque Δ est de poids 12 avec un seul zéro simple en ∞, la fonction

$$j := 1728 \frac{g_2^3}{\Delta} = \frac{1728 g_2^3}{(g_2^3 - 27 g_3^2)}$$

est une fonction modulaire de poids 0, holomorphe sur $\mathbb{H}$ et avec un pôle d'ordre 1 en ∞. En particulier, j descend en une fonction holomorphe $\bar{j} : Y(1) = \Gamma(1)\backslash\mathbb{H} \longrightarrow \mathbb{C}$, restriction d'une application holomorphe $\bar{j} : X(1) \longrightarrow \mathbb{P}^1(\mathbb{C})$.

PROPOSITION. – *$\bar{j}$ est un isomorphisme de surfaces de Riemann. En particulier, on a*

$$\mathcal{M}_{X(1)} = \mathbb{C}(\bar{j}) \text{ et } \{\textit{Fonctions modulaires de poids } 0 \textit{ niveau } \Gamma(1)\} = \mathbb{C}(j).$$

Démonstration. Puisque $\bar{j}$ possède un unique pôle simple en ∞, elle est de degré (ou valence) 1 et par suite est un biholomorphisme $X(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$. Le reste en découle. [Alternativement, on peut utiliser la proposition ci-dessus pour voir que la fonction $\bar{j} - \lambda$ possède un unique zéro simple pour tout $\lambda \in \mathbb{C}$, puis conclure par le théorème d'inversion locale]. □

Pourquoi 1728 ? Pour avoir un résidu égal à 1 en ∞. On peut calculer que avec $q = \exp(2i\pi z)$ on a $j(z) = q^{-1} + 744 + \cdots$. Remarquons que $1728 = 2^6 3^3$.

1.2.5 *À propos des q-développements.* 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 maitrisées que maintenant. Un exercice de TD expliquera le développement

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

où les B_k sont les nombres de Bernoulli, rationnels, et $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. Un autre résultat classique dû à Jacobi, cf ci-dessous, est l'expression

$$\Delta(z) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

qui montre que, dans le développement $\frac{1}{(2\pi)^{12}}\Delta(z) = \sum_{n=1}^{\infty}\tau(n)q^n$, la fonction $n \mapsto \tau(n)$ est à valeurs entières. Cette fonction a été étudiée par Ramanujan qui a énoncé les conjectures suivantes :

i) $\tau(nm) = \tau(n)\tau(m)$ pour $(m,n) = 1$, et $\tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1})$ si p premier.

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

Nous montrerons/expliquerons plus loin comment ces conjectures ont été résolues et généralisées. Enfin, le résultat de Jacobi montre aussi que dans le developpement

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

les $c(n)$ sont entiers ! (il faut aussi utiliser le fait que $1/B_2$ est entier)

Remarque. (Sur une preuve de la formule de Jacobi) – Le but est de montrer que la fonction $f(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ est modulaire de poids 12. Elle est alors clairement parabolique, donc un multiple de Δ puisque $\mathcal{S}_{12}(\Gamma(1)) = \mathbb{C}.\Delta$, et en comparant les termes dominants on trouve le facteur $(2\pi)^{12}$. Puisque $f(z) = f(z+1)$, il suffit de prouver $f(-1/z) = z^{12}f(z)$. Chose remarquable, la dérivée logarithmique de f s'écrit

$$\frac{d}{dz}\log(f(z)) = 2i\pi\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right) =: 2i\pi E_2(z)$$

où l'on reconnait le q-développement de ce qui devrait être la série d'Eisenstein (normalisée) de poids 2, si la somme $\sum_{m,n}\frac{1}{(mz+n)^2}$ convergeait. Or, si on suit la méthode utilisée pour calculer le q-développement de G_k (cf TD), on s'aperçoit que

$$2\zeta(2)E_2(z) = \sum_{m\in\mathbb{Z}}\sum_{n\in\mathbb{Z}_m}\frac{1}{(mz+n)^2}$$

où $\mathbb{Z}_m = \mathbb{Z}$ si $m \neq 0$ et $\mathbb{Z}_m = \mathbb{Z}\setminus\{0\}$ sinon. L'ordre des sommations est crucial pour la convergence. Si on inverse le sens de sommation, on a encore convergence mais le résultat change. On peut montrer (cf livre de Serre) que

$$\sum_{m\in\mathbb{Z}}\sum_{n\in\mathbb{Z}_m}\frac{1}{(mz+n)^2} = -2i\pi/z + \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}_n}\frac{1}{(mz+n)^2}.$$

Ceci implique que $E_2(-1/z) = z^2E_2(z) + \frac{12z}{2i\pi}$, et en remontant la dérivée logarithmique on obtient $f(1/z) = z^{12}f(z)$.

1.2.6 *Dimension des espaces de formes modulaires.* Revenons au cas d'un sous-groupe de congruence Γ plus général. 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 $f(\left[\begin{smallmatrix}-1 & h\\ 0 & -1\end{smallmatrix}\right]z) = -f(z)$,

c'est-à-dire $f(z+h) = -f(z)$, alors elle est $2h$-périodique et dans son développement $f(z) = \sum_{n\in\mathbb{Z}} a_n q_{2h}^n$ où $q_{2h} = \exp(2i\pi z/2h)$, tous les a_n avec n pair sont nuls. En particulier, si elle est holomorphe à l'infini, elle s'y annule nécessairement.

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

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

ii) écrivant $x = \tau\infty$, le groupe $\tau^{-1}\Gamma_x\tau$ contient $\left[\begin{smallmatrix} -1 & h_x \\ 0 & -1 \end{smallmatrix}\right]$.

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

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

THÉORÈME. – *Pour $k > 2$ on a les formules de dimension suivantes, où l'on suppose $-1 \notin \Gamma$ lorsque k est impair.*

— $\dim_{\mathbb{C}}(\mathcal{M}_k(\Gamma)) = (k-1)(g-1) + \lfloor\frac{k}{4}\rfloor n_2 + \lfloor\frac{k}{3}\rfloor n_3 + \frac{k}{2}n_\infty^{\mathrm{reg}} + \lfloor\frac{k}{2}\rfloor n_\infty^{\mathrm{irr}}$

— $\dim_{\mathbb{C}}(\mathcal{S}_k(\Gamma)) = \dim_{\mathbb{C}}(\mathcal{M}_k(\Gamma)) - n_\infty^{\mathrm{reg}}$

Remarque. – i) Dans le cas impair (et donc $-1 \notin \Gamma$), on a $n_2 = 0$. Exercice !

ii) En utilisant la formule donnant le genre, on peut aussi écrire

$$\dim_{\mathbb{C}}(\mathcal{M}_k(\Gamma)) = \frac{kd}{12} - g + 1 + \left(\frac{k}{4} - \left\lfloor\frac{k}{4}\right\rfloor\right) n_2 + \left(\frac{k}{3} - \left\lfloor\frac{k}{3}\right\rfloor\right) n_3 + \left(\frac{k}{2} - \left\lfloor\frac{k}{2}\right\rfloor\right) n_\infty^{\mathrm{irr}}.$$

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

Démonstration. Dans le cas pair $k = 2k'$, 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 on déduit des formules

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

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

$$L(\mathrm{div}(\omega_0) + k'D_\pi) \xrightarrow{\sim} \mathcal{M}_k(\Gamma)$$

et

$$L\left(\mathrm{div}(\omega_0) + k'D_\pi - \sum_{P\mapsto\infty}[P]\right) \xrightarrow{\sim} \mathcal{S}_k(\Gamma)$$

où $D_\pi = \sum_{P\in X(\Gamma)}(1 - 1/e_P)[P]$. On en déduit que $\dim_{\mathbb{C}}(\mathcal{M}_k(\Gamma)) = \ell(k'K + \lfloor k'D_\pi\rfloor)$ avec

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

On utilise alors la formule de Riemann-Roch pour calculer $\dim \mathcal{M}_k(\Gamma)$, aidés par le fait que $\deg(k'K + \lfloor k'D_\pi\rfloor) > 2g-2$. Pour calculer la dimension de $\mathcal{S}_k(\Gamma)$ il suffit de remplacer $\mathrm{div}(\omega_0)$ par $\mathrm{div}(\omega_0) - \sum_{P\mapsto\infty}[P]$. Dans ce cas on a bien $\deg > 2g-2$ dès que $k > 2$.

Dans le cas impair, pour suivre un raisonnement similaire, il nous faut connaitre l'existence d'une fonction modulaire de poids k. *Admettons momentanément* l'existence d'une telle fonction f (à condition que $-1 \notin \Gamma$). Alors f^2 est de poids $2k$ et correspond à une k-forme différentielle méromorphe ω_0 sur $X(\Gamma)$. Vu les formules

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

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

$$L\left(\frac{1}{2}\mathrm{div}\,(\omega_0) + \frac{k}{2}D_\pi\right) \xrightarrow{\sim} \mathcal{M}_k(\Gamma)$$

et

$$L\left(\frac{1}{2}\mathrm{div}\,(\omega_0) + \frac{k}{2}D_\pi - \frac{1}{2}\sum_{P \mapsto \infty}[P]\right) \xrightarrow{\sim} \mathcal{S}_k(\Gamma).$$

Pour $\mathcal{M}_k$, il faut alors calculer la partie entière du diviseur

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

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

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

implique que $\mathrm{ord}_P(\omega_0)$ 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

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

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

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

montre que :

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

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

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

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

On obtient donc

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

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

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

Remarque. (Que se passe-t-il pour $k = 1$?) – La preuve précédente dit que (sous réserve de l'existence d'une fonction modulaire de poids 1), en notant ω_0 une forme différentielle méromorphe sur $X(\Gamma)$)

$$\dim_{\mathbb{C}}(\mathcal{M}_1(\Gamma)) = \ell\left(\frac{1}{2}\left(\mathrm{div}(\omega_0) + \sum_{P\mapsto\infty,\mathrm{reg}}[P]\right)\right).$$

Le diviseur qui apparait est bien entier malgré les apparences, et son degré est $g-1+n_\infty^{\mathrm{reg}}/2$. Lorsque $n_\infty^{\mathrm{reg}} > 2g-2$, on peut conclure que $\dim_{\mathbb{C}}(\mathcal{M}_1(\Gamma)) = n_\infty^{\mathrm{reg}}/2$. Sinon, la formule de Riemann-Roch ne permet pas de conclure, mais fournit la minoration $\dim_{\mathbb{C}}(\mathcal{M}_1(\Gamma)) \geqslant n_\infty^{\mathrm{reg}}/2$. Dans tous les cas $\dim_{\mathbb{C}}(\mathcal{S}_1(\Gamma)) = \dim_{\mathbb{C}}(\mathcal{M}_1(\Gamma)) - n_\infty^{\mathrm{reg}}/2$.

Remarque. (Existence de fonctions modulaires de poids 1) – Dans le cas k impair de la preuve précédente on a supposé l'existence de fonctions modulaires de poids k lorsque $-1 \notin \Gamma$. Il suffit bien-sûr de la prouver en poids 1. Voici un argument qui utilise le fait, que nous verrons plus tard, que pour une surface de Riemann compacte, le groupe $\mathrm{Pic}^0(X)$ des "diviseurs modulo les diviseurs principaux" de degré 0 est un groupe *divisible*.

Ainsi, si P est un point de $X(\Gamma)$, l'élement $K-(2g-2)[P]$ de $\mathrm{Pic}^0(X)$ est divisible par 2. Il s'ensuit que, si ω_0 est une forme différentielle méromorphe sur $X(\Gamma)$, il en existe une autre, ω, telle que $\mathrm{div}(\omega) = 2(\mathrm{div}(\omega_0) - (2g-2)[P])$. Soit f_2 la fonction modulaire de poids 2 et niveau Γ telle que $f_2(z)dz = \pi^*(\omega)$. Alors $\mathrm{ord}_z(f_2)$ est pair en tout point de $\mathbb{H}$ qui est simplement connexe, donc il existe une fonction $f : \mathbb{H} \longrightarrow \mathbb{C}$, méromorphe sur $\mathbb{H}$, telle que $f^2 = f_2$. Cette fonction n'est pas nécessairement automorphe de poids 1, mais il existe au moins un caractère $\chi : \Gamma \longrightarrow \{\pm 1\}$ tel que pour tout $\gamma \in \Gamma$ on a $f[\gamma]_1 = \chi(\gamma)f$. En particulier, f est automorphe de niveau $\Gamma' := \mathrm{Ker}(\chi)$, qui est un sous-groupe d'indice 2 de Γ, et par ailleurs, elle est aussi méromorphe aux pointes.

Si $\Gamma' = \Gamma$, on a gagné. Sinon, il suffit de trouver une fonction f_0 méromorphe sur $\mathbb{H}$ et aux pointes vérifiant $\forall\gamma \in \Gamma, f_0(\gamma z) = \chi(\gamma)f_0(z)$. Car alors la fonction $f_0 f$ sera modulaire de poids 1 pour Γ. Pour cela, on remarque que $X(\Gamma')$ est de degré 2 au-dessus de $X(\Gamma)$ (ici on utilise $-1 \notin \Gamma$, qui assure que l'image de Γ' dans $\mathrm{PSL}_2(\mathbb{R})$ est d'indice 2 dans celle de Γ). Donc il existe une fonction $g \in \mathcal{M}_{X(\Gamma')} \setminus \mathcal{M}_{X(\Gamma)}$. La fonction π^*g est donc modulaire de poids 0 pour Γ', mais pas pour Γ. Il s'ensuit que si $\gamma \in \Gamma \setminus \Gamma'$, la fonction $f_0(z) := \pi^*g(z) - \pi^*g(\gamma z)$ vérifie ce que l'on veut.

Exemple. (Le cas de $\Gamma(N)$, $N > 1$) – On a vu en TD que dans ce cas, $n_2 = n_3 = 0$ tandis que $n_\infty = d_N/N$ où d_N désigne le degré de $X(N) \longrightarrow X(1)$, donné par

$$d_N = [\Gamma(1) : \Gamma(N)\{\pm 1\}] = \begin{cases} \frac{1}{2}N^3 \prod_{p|N}(1-p^{-2}) & \text{si } N \neq 2 \\ 6 & \text{si } N = 2 \end{cases}$$

Ainsi, le genre vaut $g = 1+d_N/12-d_N/2N$. Par ailleurs, lorsque $-1 \notin \Gamma(N)$ (ie lorsque $N > 2$) toutes les pointes sont visiblement régulières, puisqu'une matrice $\left[\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right]$ n'appartient pas à $\Gamma(N)$. Les formules de dimension deviennent donc, pour $N > 2$,

$$\dim_{\mathbb{C}}(\mathcal{M}_k(\Gamma(N)) = \frac{k-1}{12}d_N + \frac{d_N}{2N} \quad \text{et} \quad \dim_{\mathbb{C}}(\mathcal{S}_k(\Gamma(N)) = \frac{k-1}{12}d_N - \frac{d_N}{2N}$$

1.2.7 *Séries de Poincaré.* Nous présentons ici une méthode générale pour fabriquer des formes modulaires de niveau Γ. Une idée naïve serait de partir d'une fonction quelconque f et de fabriquer la série $\varphi(z) = \sum_{\gamma\in\Gamma} f(\gamma z)/j_\gamma(z)^k$. La formule $j_{\gamma\gamma'}(z) = j_\gamma(\gamma' z)j_{\gamma'}(z)$ montre qu'une telle fonction serait bien automorphe de poids k pour Γ. Le problème est qu'une telle série ne peut pas converger car, par exemple, $j_\gamma(z) = 1$ pour une infinité de γ. Justement, pour contourner le problème, notons

$$\Gamma_\infty^+ := \{\gamma \in \Gamma, j_\gamma = 1\} = \Gamma \cap \{\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right],\ n \in \mathbb{Z}\} = \Gamma \cap \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]^{\mathbb{Z}},$$

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

Soit h tel que $\Gamma_\infty^+ = \left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right]^{\mathbb{Z}}$ (remarquons que $h = h_\infty$ si ∞ est une pointe régulière de Γ, et $h = 2h_\infty$ sinon). Des exemples typiques de fonctions f invariantes sous Γ_∞^+ sont les $f(z) = \exp(2i\pi nz/h)$, $n \in \mathbb{Z}$.

Proposition. – *La série de Poincaré de poids $k \geqslant 3$ et "caractère" $n \in \mathbb{N}$*

$$\varphi_n(z) := \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} j_\gamma(z)^{-k}\exp(2i\pi n\gamma z/h)$$

définit une forme modulaire $\varphi_n \in \mathcal{M}_k(\Gamma)$. De plus :

i) Si $n > 0$, $\varphi_n \in \mathcal{S}_k(\Gamma)$.

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

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

.

Démonstration. Pour trouver un ensemble agréable de représentants de $\Gamma_\infty^+\backslash\Gamma$, partons de l'égalité $\left[\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} a+mc & b+md \\ c & d \end{smallmatrix}\right]$. Elle nous dit que $\gamma' \in \Gamma_\infty^+\gamma \Rightarrow (a', b') \equiv (a, b) (\text{mod } h)$.

Réciproquement, si γ' vérifie $(a',b') \equiv (a,b) (\mathrm{mod}\ h)$ 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 $\gamma' \in \Gamma_\infty^+\backslash\Gamma$. Finalement, on voit qu'on obtient un ensemble de représentants de $\Gamma_\infty^+\backslash\Gamma$ en choisissant, pour tout $(c,d) \in \mathbb{Z}^2$ un élément $\gamma_{c,d} \in \Gamma$ dont la deuxième ligne est $(c\ d)$ (lorsque c'est possible !).

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

Pour $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, la formule

$$\varphi_n(\alpha z) = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} j_\gamma(\alpha z)^{-k} q_h^{n\gamma\alpha z} = j_\alpha(z)^k \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} j_{\gamma\alpha}(z)^{-k} q_h^{n\gamma\alpha z} = j_\alpha(z)^k \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma\alpha} j_\gamma(z)^{-k} q_h^{n\gamma z}.$$

montre, lorsqu'on prend $\alpha \in \Gamma$ que φ_n est bien automorphe de poids k et niveau Γ.

Puisque $j_\gamma(z)^{-k} \to 0$ lorsque $\Im(z) \to \infty$ et $\gamma \notin \Gamma(1)_\infty$, la convergence normale sur un domaine fondamental nous donne aussi pour $\alpha \in \Gamma(1)$

$$\lim_{\Im(z)\to\infty} \varphi_n[\alpha]_k(z) = \sum_{\gamma\in\Gamma_\infty^+\backslash(\Gamma\alpha\cap\Gamma(1)_\infty)} \lim_{\Im(z)\to\infty} (j_\gamma(z)^{-k}.\exp(2i\pi n\gamma z/h)).$$

La somme qui apparait ici est finie et on en déduit que $\varphi_n[\alpha]_k$ 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 $n \geqslant 0$.

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 $j_\gamma(z) = -1$ si $\gamma \in \Gamma_\infty \setminus \Gamma_\infty^+$ et $j_\gamma = 1$ pour $\gamma \in \Gamma_\infty^+$. □

Remarque. (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 $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ 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

$$\varphi_0(z) = \sum_{\gamma\in\Gamma(1)_\infty^+\backslash\Gamma(1)} j_\gamma(z)^{-k} = \sum_{\mathrm{pgcd}(c,d)=1} \frac{1}{(cz+d)^k}.$$

La ressemblance avec G_k n'est pas parfaite, mais on peut réarranger G_k comme ceci

$$G_k(z) = \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^k} = \sum_{n=1}^{\infty} \sum_{\mathrm{pgcd}(c,d)=1} \frac{1}{(cnz+dn)^k} = \sum_{n=1}^{\infty} \frac{1}{n^k} \sum_{\mathrm{pgcd}(c,d)=1} \frac{1}{(cz+d)^k}$$

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

Application. (La partie Eisenstein de $\mathcal{M}_k(\Gamma)$) – Supposons Γ distingué dans $\Gamma(1)$ avec pointes régulières. On pense par exemple à $\Gamma = \Gamma(N)$ si $N > 2$. Pour tout $\alpha \in \Gamma(1)$, la fonction $\varphi_0[\alpha]_k$ est dans $\mathcal{M}_k(\alpha^{-1}\Gamma\alpha) = \mathcal{M}_k(\Gamma)$ et s'annule 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 $j_{\sigma\gamma}(z) = j_\sigma(\gamma z)j_\gamma(z) = j_\sigma.j_\gamma(z)$ où $j_\sigma = \pm 1$ (selon que $\sigma \in \pm\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]^{\mathbb{Z}}$),

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

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 $\alpha = \left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right]$ 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"

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

Puisque E_k^x ne s'annule pas en x et s'annule aux autres pointes, la famille $(E_k^x)_{x\in\Gamma\backslash\mathbb{P}^1(\mathbb{Q})}$ est libre dans $\mathcal{M}_k(\Gamma)$. Comme on sait par ailleurs que $\dim(\mathcal{M}_k(\Gamma)) - \dim(\mathcal{S}_k(\Gamma)) = n_\infty$ (pour $k \geqslant 3$), on voit que cette famille engendre un sous-espace supplémentaire de $\mathcal{S}_k(\Gamma)$, comme dans le cas $\Gamma = \Gamma(1)$. On appelle ce sous-espace la "partie Eisenstein" de $\mathcal{M}_k(\Gamma)$.

Exemple. (Séries d'Eisenstein pour $\Gamma(N)$.) – Lorsque $\Gamma = \Gamma(N)$, $N > 2$, deux pointes $x = r/t$ et $x' = r'/t'$ (où pgcd$= 1$ et $t, t' > 0$) sont équivalentes si et seulement si $(r, t) \equiv \pm(r', t')[N]$ (exercice). On calcule alors que

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

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 $\overline{v} \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ d'ordre N. On peut alors poser

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

et un calcul similaire au cas $\Gamma(1)$ montre la formule

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

1.2.8 *Produit scalaire de Petersson.* On rappelle que $\mathbb{H}$ possède une mesure invariante sous $\mathrm{SL}_2(\mathbb{R})$, dite "mesure de Poincaré", et donnée par $d\mu(z) = \frac{1}{y^2}dx.dy = \frac{i}{2\Im(z)^2}dz.d\bar{z}$.

Si $f : \mathbb{H} \longrightarrow \mathbb{C}$ est une fonction continue et bornée, alors pour tout $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, l'intégrale $\int_D f(\alpha z)d\mu(z)$ de f sur le domaine fondamental $D = \{z, |\Re(z)| \leqslant 1/2, |z| \geqslant 1\}$ converge absolument.

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

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

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

$$\int_{X(\Gamma)} f.d\mu = \int_{D_\Gamma} f(z)d\mu(z).$$

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 $V_\Gamma = d_\Gamma V_{\Gamma(1)}$ et on peut calculer[6] $V_{\Gamma(1)} = \pi/3$.

Soit maintenant $f, g \in \mathcal{M}_k(\Gamma)$. La relation $\Im(\gamma z) = \Im(z)|j_\gamma(z)|^{-2}$ montre que la fonction $h(z) := \Im(z)^k f(z)\overline{g(z)}$ est invariante par Γ.

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

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

Définition. – *Pour $f \in \mathcal{S}_k(\Gamma)$, $g \in \mathcal{M}_k(\Gamma)$, on appelle*

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

le produit scalaire de Petersson de f et g.

La restriction à $\mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma)$ 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. – *Soit $f \in \mathcal{S}_k(\Gamma)$ de développement $f(z) = \sum_{n=1}^\infty a_n q_h^n$ avec $q_h = \exp(2i\pi z/h)$ et h la largeur de la pointe ∞. Alors pour toute série de Poincaré φ_n on a*

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

6. Plus généralement, on peut montrer que l'aire d'un triangle géodésique dans $\mathbb{H} \cup \mathbb{P}^1(\mathbb{R})$ 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. En joignant les séries d'Eisenstein, on obtient :

COROLLAIRE. – *$\mathcal{S}_k(\Gamma)$ est engendré par les φ_n, $n > 0$. De plus, pour Γ distingué, la partie Eisenstein $\mathcal{E}_k(\Gamma)$ est orthogonale à $\mathcal{S}_k(\Gamma)$ et on a $\mathcal{M}_k(\Gamma) = \mathcal{S}_k(\Gamma) \oplus \mathcal{E}_k(\Gamma)$.*

Démonstration (du théorème). Vu l'absolue convergence de la série définissant φ_n on peut écrire (en notant D_Γ un domaine fondamental pour Γ)

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

Pour la deuxième ligne on utilise $\Im(z) = \Im(\gamma z)|j_\gamma(z)|^2$, pour la troisième ligne on utilise $1 = j_{\gamma^{-1}\gamma}(z) = j_{\gamma^{-1}}(\gamma z) j_\gamma(z)$ et pour la quatrième on utilise l'automorphie de f. Maintenant, on remarque que $\bigsqcup_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} \gamma D_\Gamma$ 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 $D_h = \{z, 0 \leqslant \Re(z) \leqslant h\}$. On peut donc écrire

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

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

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

et des intégrations par parties montrent la formule annoncée. □

1.3 Opérateurs de Hecke

1.3.1 *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. – Dans $G = \mathrm{GL}_2(\mathbb{Q})$, les sous-groupes d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ sont des sous-groupes de Hecke. Pour le voir, il suffit de montrer que si $\alpha \in \mathrm{GL}_2(\mathbb{Q})$, 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 $\alpha \in \mathrm{M}_2(\mathbb{Z})$. Soit alors N son déterminant. On a $N\alpha^{-1} \in \mathrm{M}_2(\mathbb{Z})$ (c'est la transposée de la comatrice de α) donc $\alpha^{-1}(N\mathrm{M}_2(\mathbb{Z}))\alpha \subset \mathrm{M}_2(\mathbb{Z})$, donc $\alpha^{-1}\Gamma(N)\alpha \subset \mathrm{M}_2(\mathbb{Z})$. Comme $\alpha^{-1}\Gamma(N)\alpha$ est un groupe, on a $\alpha^{-1}\Gamma(N)\alpha \subset \mathrm{GL}_2(\mathbb{Z})$, et comme $\det(\alpha^{-1}\gamma\alpha) = \det(\gamma)$, on a $\alpha^{-1}\Gamma(N)\alpha \subset \mathrm{SL}_2(\mathbb{Z})$, et finalement $\Gamma(N) \subset \alpha\Gamma(1)\alpha^{-1} \cap \Gamma(1)$.

Soit 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 [7] $\mathbb{Z}[\Gamma_1\backslash G/\Gamma_2]$ aux invariants $\mathbb{Z}[\Gamma_1\backslash G]^{\Gamma_2}$. Considérons alors l'application

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[\Gamma_2\backslash G], \mathbb{Z}[\Gamma_1\backslash G]) & \to & \mathbb{Z}[\Gamma_1\backslash G/\Gamma_2] \\ \varphi & \mapsto & \varphi([\Gamma_2.1]) \end{array} .$$

Le Hom désigne les homomorphismes de $\mathbb{Z}[G]$-modules (à droite). Comme $\mathbb{Z}[\Gamma_2\backslash G]$ est engendré, en tant que $\mathbb{Z}[G]$-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 $\mathbb{Z}[\Gamma_1\backslash G]$, que l'on peut donc identifier à un élément de $\mathbb{Z}[\Gamma_1\backslash G/\Gamma_2]$. 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

$$[\Gamma_1\alpha\Gamma_2] : \quad \begin{array}{rcl} \mathbb{Z}[\Gamma_2\backslash G] & \to & \mathbb{Z}[\Gamma_1\backslash G] \\ [\Gamma_2 g] & \mapsto & \displaystyle\sum_{\Gamma_1\gamma \in \Gamma_1\backslash(\Gamma_1\alpha\Gamma_2)} [\Gamma_1\gamma g] \end{array} .$$

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"

$$\mathbb{Z}[\Gamma_1\backslash G/\Gamma_2] \otimes \mathbb{Z}[\Gamma_2\backslash G/\Gamma_3] \longrightarrow \mathbb{Z}[\Gamma_1\backslash G/\Gamma_3]$$

qui est explicitement donnée, sur les bases canoniques, par la formule

$$[\Gamma_1\alpha\Gamma_2].[\Gamma_2\beta\Gamma_3] = \sum_{\delta} c_\delta.[\Gamma_1\delta\Gamma_3]$$

7. Pour un ensemble X, $\mathbb{Z}[X]$ désigne le $\mathbb{Z}$-module libre de base $\{[x], x \in X\}$

où $c_\delta \in \mathbb{N}$ 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. – $c_\delta \neq 0$ 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 $\mathbb{Z}[\Gamma\backslash G/\Gamma]$ appelé *anneau de Hecke de* (G, Γ), ainsi qu'un isomorphisme d'anneaux

$$\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[\Gamma\backslash G]) \xrightarrow{\sim} \mathbb{Z}[\Gamma\backslash G/\Gamma].$$

Si $\Delta \subset G$ est un sous-ensemble stable par multiplication et contenant Γ, on note $\mathbb{Z}[\Gamma\backslash\Delta/\Gamma]$ le sous-module de $\mathbb{Z}[\Gamma\backslash G/\Gamma]$ engendré par les $[\Gamma\delta\Gamma]$, $\delta \in \Delta$. Vu la formule donnant le produit, c'est un *sous-anneau* de $\mathbb{Z}[\Gamma\backslash G/\Gamma]$.

Maintenant, donnons-nous un $\mathbb{C}$-espace vectoriel V (ou un $\mathbb{Z}$-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

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[\Gamma\backslash G], V) & \to & V^\Gamma \\ \varphi & \mapsto & \varphi([\Gamma.1]) \end{array}$$

est un isomorphisme de $\mathbb{C}$-espaces vectoriels. On en déduit, par composition avec $[\Gamma_1\alpha\Gamma_2]$, une application linéaire $V^{\Gamma_1} \longrightarrow V^{\Gamma_2}$ 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 $\mathbb{Z}[\Gamma\backslash G/\Gamma]$-module à droite sur V^Γ.

Exemple. – Prenons V l'espace des fonctions $\mathbb{H} \longrightarrow \mathbb{C}$ sur lequel $G = \mathrm{GL}_2(\mathbb{Q})_+$ agit par l'action de poids $k \geqslant 0$ donnée par $f[\gamma]_k(z) := \det(\gamma)^{k/2} j_\gamma(z)^{-k} f(\gamma z)$ L'espace V^Γ contient les sous-espaces $\mathcal{M}_k(\Gamma)$ et $\mathcal{S}_k(\Gamma)$. 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 $\mathcal{M}_k(\Gamma_1)$ dans $\mathcal{M}_k(\Gamma_2)$ et $\mathcal{S}_k(\Gamma_1)$ dans $\mathcal{S}_k(\Gamma_2)$. En particulier, on a une action à droite de $\mathbb{Z}[\Gamma\backslash G/\Gamma]$ sur $\mathcal{M}_k(\Gamma)$ et $\mathcal{S}_k(\Gamma)$.

1.3.2 *L'anneau de Hecke en niveau* $\Gamma(1)$. Soit $\Delta = \Delta(1) = \mathrm{M}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})_+$. Il est clair que Δ est stable par produit et contient $\Gamma(1)$. Nous allons décrire l'anneau $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$.

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

LEMME. – *Notons $\Delta_{l,m}$ l'ensemble des matrices $\alpha \in \Delta$ de diviseurs élémentaires (l,m).*

i) $\Delta_{l,m} = \Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)$

ii) l'ensemble $\mathcal{L}(\Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)) := \{\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right],\ ad = lm, 0 \leqslant b < d \text{ et } (a,b,d) = l\}$ *est un ensemble de représentants des $\Gamma(1)$-classes à gauche dans $\Delta_{l,m}$*

Démonstration. i) Supposons $\alpha = \gamma_1\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\gamma_2$ avec $\gamma_1, \gamma_2 \in \Gamma(1)$. Alors $\alpha(\mathbb{Z}^2) = \gamma_1(l\mathbb{Z} \oplus m\mathbb{Z})$. Donc l'automorphisme γ_1 de $\mathbb{Z}^2$ induit un isomorphisme $\mathbb{Z}^2/(l\mathbb{Z} \oplus m\mathbb{Z}) \xrightarrow{\sim} \mathrm{Coker}(\alpha)$ qui montre que $\mathrm{Coker}(\alpha)$ 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 $\mathbb{Z}^2$ telle que $(l\omega_1, m\omega_2)$ soit une base de $\alpha(\mathbb{Z}^2)$. Soit γ_1 la matrice de passage de la base canonique (e_1, e_2) de $\mathbb{Z}^2$ à (ω_1, ω_2), et soit γ_2 la matrice de passage de la base $(l\omega_1, m\omega_2)$ de $\alpha(\mathbb{Z}^2)$ à la base $(\alpha(e_1), \alpha(e_2)$ de $\alpha(\mathbb{Z})^2$. Alors on a $\alpha = \gamma_1\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\gamma_2$. A priori on a seulement $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbb{Z})$, mais quitte à changer γ_1 par $\gamma_1\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ et γ_2 par $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]\gamma_2$, on voit que $\alpha \in \Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)$.

ii) On utilise la remarque suivante :

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

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 $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] \in \Gamma(1)\alpha$ si et seulement si le réseau $\Lambda := {}^t\alpha(\mathbb{Z}^2)$ 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 $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right] \in \Gamma(1)\alpha$ vérifiant $0 \leqslant b < d$. Pour prouver l'existence, considérons la suite exacte

$$0 \longrightarrow (\Lambda + \mathbb{Z}e_2)/\Lambda \longrightarrow \mathbb{Z}^2/\Lambda \longrightarrow \mathbb{Z}^2/(\Lambda + \mathbb{Z}e_2) \longrightarrow 0.$$

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 $ad = |\mathbb{Z}^2/\Lambda| = |\det({}^t\alpha)| = lm$ et $(ae_1 + \mathbb{Z}e_2) \cap \Lambda \neq \emptyset$. 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 $0 \leqslant b < d$. 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 $\mathbb{Z}^2/\Lambda \simeq \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. En particulier, le noyau de la multiplication par l dans $\mathbb{Z}^2/\Lambda$ est isomorphe à $(\mathbb{Z}/l\mathbb{Z})^2$, ce qui équivaut à $l\mathbb{Z}^2 \supseteq \Lambda$ et implique $l|(a,b,d)$. Réciproquement, si $\lambda := (a,b,d)$, alors $\Lambda \subseteq \lambda\mathbb{Z}^2$ et $\mathbb{Z}^2/\Lambda$ contient $(\mathbb{Z}/\lambda\mathbb{Z})^2$, ce qui implique $\lambda|l$. □

Notons $T(l,m) := [\Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)]$. D'après le lemme, les $T(l,m)$, $1 \leqslant l|m$, forment une base de $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$. Voici la table de multiplication dans cette base.

PROPOSITION. – *On a les égalités suivantes (où p désigne un nombre premier) :*

i) $T(l,m) = T(l,l)T(1,m/l) = T(1,m/l)T(l,l)$

ii) $T(l,m)T(l',m') = T(ll',mm')$ *si* $(lm, l'm') = 1$.

iii) $T(1,p)T(1,p^r) = T(1,p^{r+1}) + \begin{cases} (p+1)T(p,p) & si\ r = 1 \\ pT(p,p)T(1,p^{r-1}) & si\ r > 1 \end{cases}$

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

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

ii) Grâce au i), on peut supposer que $l = l' = 1$. La première chose à démontrer est l'égalité ensembliste $\Gamma(1)\left[\begin{smallmatrix}1&0\\0&m\end{smallmatrix}\right]\Gamma(1)\left[\begin{smallmatrix}1&0\\0&m'\end{smallmatrix}\right]\Gamma(1) = \Gamma(1)\left[\begin{smallmatrix}1&0\\0&mm'\end{smallmatrix}\right]\Gamma(1)$ (cf la remarque sur le produit de doubles classes). 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

$$0 \longrightarrow \alpha\mathbb{Z}^2/\alpha\alpha'\mathbb{Z}^2 \longrightarrow \mathbb{Z}^2/\alpha\alpha'\mathbb{Z}^2 \longrightarrow \mathbb{Z}^2/\alpha\mathbb{Z}^2 \longrightarrow 0$$

qui montre que le conoyau $\mathrm{Coker}(\alpha\alpha')$ est une extension abélienne de $\mathbb{Z}/m\mathbb{Z}$ par $\mathbb{Z}/m'\mathbb{Z}$. Mais puisque $(m,m') = 1$, une telle extension est isomorphe à $\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/m'\mathbb{Z} = \mathbb{Z}/mm'\mathbb{Z}$, 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

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

Ici nous pouvons utiliser les systèmes de représentants donnés par le lemme précédent. Donc si $(\alpha,\alpha') \in C$ on a $\alpha = \left[\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right]$ avec $ad = m$, $0 \leqslant b < d$ et $(a,b,d) = 1$ et de même $\alpha' = \left[\begin{smallmatrix}a'&b'\\0&d'\end{smallmatrix}\right]$ avec $a'b' = m'$, $0 \leqslant b' < d'$ et $(a',b',d') = 1$. Alors $\alpha\alpha' = \left[\begin{smallmatrix}aa'&ab'+bd'\\0&dd'\end{smallmatrix}\right]$. D'après la preuve du lemme précédent, on a donc $\alpha\alpha' \in \Gamma(1)\left[\begin{smallmatrix}1&0\\0&mm'\end{smallmatrix}\right]$ si et seulement si $aa' = 1$, $dd' = mm'$ et $mm'|(ab'+bd')$. Ceci équivaut encore $a = a' = 1$, $d = m$, $d' = m'$ (puisque $(m,m') = 1$) et donc $mm'|(b'+bm') \Leftrightarrow b'+bm' = 0 \Leftrightarrow b = b' = 0$. On voit donc que $(\alpha,\alpha') = (\left[\begin{smallmatrix}1&0\\0&m\end{smallmatrix}\right], \left[\begin{smallmatrix}1&0\\0&m'\end{smallmatrix}\right])$ et par suite, que $c = 1$, comme voulu.

iii) Commençons par évaluer l'ensemble $\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^r\end{smallmatrix}\right]\Gamma(1)$. 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 $\mathrm{Coker}(\alpha\alpha')$ est une extension de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^r\mathbb{Z}$. Il y a donc deux possibilités : soit $\mathrm{Coker}(\alpha\alpha') \simeq \mathbb{Z}/p^{r+1}\mathbb{Z}$, soit $\mathrm{Coker}(\alpha\alpha') \simeq \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^r\mathbb{Z}$. Les diviseurs élémentaires de $\alpha\alpha'$ sont donc $(1,p^{r+1})$ ou (p,p^r) et on en déduit

$$\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^r\end{smallmatrix}\right]\Gamma(1) = \Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^{r+1}\end{smallmatrix}\right]\Gamma(1) \bigsqcup \Gamma(1)\left[\begin{smallmatrix}p&0\\0&p^r\end{smallmatrix}\right]\Gamma(1).$$

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

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

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

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

On voit alors que $C=\{(\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right],\left[\begin{smallmatrix}1&0\\0&p^r\end{smallmatrix}\right])\}$, et en particulier $c=1$.

Pour évaluer c' on pourrait aussi expliciter l'ensemble

$$C' := \{(\alpha,\alpha')\in\mathcal{L}(\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\Gamma(1))\times\mathcal{L}(\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^r\end{smallmatrix}\right]\Gamma(1)),\Gamma(1)\alpha\alpha'=\Gamma(1)\left[\begin{smallmatrix}p&0\\0&p^r\end{smallmatrix}\right]\}.$$

Mais il est plus élégant d'utiliser le *degré* d'une double classe. Par définition, on pose

$$\deg([\Gamma\alpha\Gamma]) = |\Gamma\backslash(\Gamma\alpha\Gamma)| \quad \text{(cardinal)},$$

et on l'étend par linéarité à l'anneau de Hecke. On vérifie alors (exercice ci-dessous) que l'application $\deg : \mathbb{Z}[\Gamma\backslash G/\Gamma]\longrightarrow\mathbb{Z}$ est un homomorphisme d'anneaux. Dans notre cas, on a $\deg(\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^r\end{smallmatrix}\right]\Gamma(1)) = p^r+p^{r-1}$, et on obtient

$$(1+p)(p^r+p^{r-1}) = c(p^{r+1}+p^r) + c'\deg(\Gamma(1)\left[\begin{smallmatrix}p&0\\0&p^r\end{smallmatrix}\right]\Gamma(1)),$$

ce qui, compte tenu de $c=1$ et de

$$\deg(\Gamma(1)\left[\begin{smallmatrix}p&0\\0&p^r\end{smallmatrix}\right]\Gamma(1)) = \deg(\Gamma(1)\left[\begin{smallmatrix}1&0\\0&p^{r-1}\end{smallmatrix}\right]\Gamma(1) = \begin{cases}1 & \text{si } r=1\\ p^{r-1}+p^{r-2} & \text{si } r>1\end{cases}$$

nous donne $c'=1+p$ lorsque $r=1$ et $c'=p$ lorsque $r>1$.

Examinons maintenant la dernière assertion. D'après i) et ii), les $T(1,p)$ et $T(p',p')$ commutent entre eux lorqu'on varie p et p'. D'après iii) et ii), ils engendrent $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$. Il reste alors à vérifier l'indépendence algébrique de ces éléments. Pour cela, si $1\leqslant l|m$, 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 ii) et iii) 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 $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1))$, il s'ensuit que les $P(l,m)$ forment aussi une base. □

Exercice. – Montrer que dans l'expression $[\Gamma\alpha\Gamma][\Gamma\beta\Gamma]=\sum_\delta c_\delta[\Gamma\delta\Gamma]$, on a

$$c_\delta = |\{(\gamma,\gamma')\in\mathcal{L}(\Gamma\alpha\Gamma)\times\mathcal{L}(\Gamma\beta\Gamma),\ \Gamma\gamma\gamma'\Gamma=\Gamma\delta\Gamma\}|.|\Gamma\backslash(\Gamma\delta\Gamma)|^{-1}.$$

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 $\mathcal{L}(\Gamma\alpha\Gamma).\mathcal{L}(\Gamma\beta\Gamma)$ (produit dans Δ) soit un ensemble de représentants de $\Gamma\backslash(\Gamma\alpha\beta\Gamma)$.

Corollaire. – *Pour $n\in\mathbb{N}$, notons $T(n):=\sum_{lm=n}T(l,m)$ (en particulier on a $T(p)=T(1,p)$). Alors on a les formules :*

i) $T(nm)=T(n)T(m)$ *si* $(n,m)=1$,

ii) $T(p^{r+1})=T(p)T(p^r)-pT(p,p)T(p^{r-1})$,

et, de manière équivalente, la formule générale $T(n)T(m)=\sum_{l|(m,n)}lT(l,l)T(mn/l^2)$.

Démonstration. Exercice. □

1.3.3 *Action sur les formes modulaires de niveau 1.* On a déjà remarqué que l'action de $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$ sur les fonctions automorphes de poids k pour $\Gamma(1)$ préserve $\mathcal{M}_k(\Gamma(1))$ et $\mathcal{S}_k(\Gamma(1))$. Rappelons que cette action est induite par l'action de poids k du groupe $G = \mathrm{GL}_2(\mathbb{Q})_+$ donnée par $f[\gamma]_k(z) = \det(\gamma)^{k/2} j_\gamma(z)^{-k} f(\gamma z)$. Néanmoins, pour obtenir des formules rationnelles, et même entières, il est préférable de normaliser cette action différemment en posant

$$f[\gamma]'_k(z) = \det(\gamma)^{k-1} j_\gamma(z)^{-k} f(\gamma z) = \det(\gamma)^{k/2-1} f[\gamma]_k(z).$$

On a alors de même $[\Gamma(1)\alpha\Gamma(1)]'_k = \det(\alpha)^{k/2-1}[\Gamma(1)\alpha\Gamma(1)]_k$. Voici des formules explicites.

LEMME. – *Pour $n \geqslant 1$ et $f \in \mathcal{M}_k(\Gamma(1))$, on a*

$$f[T(n)]'_k(z) = n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} d^{-k} f((az+b)/d).$$

Si $f(z) = \sum_{m\in\mathbb{N}} a(m)q^m$ est son q-développement en ∞ (avec $q = \exp(2i\pi z)$), alors

$$f[T(n)]'_k(z) = \sum_{m\in\mathbb{N}} \left(\sum_{d|(m,n)} d^{k-1} a(mn/d^2) \right) q^m.$$

Démonstration. Par définition, si $\mathcal{L} \subset \Delta$ est n'importe quel ensemble de représentants des $\Gamma(1)$-classes à gauche dans $\Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)$, on a

$$f[T(l,m)]'_k(z) = \sum_{\gamma\in\mathcal{L}} \det(\gamma)^{k-1} j_\gamma(z)^{-k} f(\gamma z).$$

En prenant l'ensemble

$$\mathcal{L} = \mathcal{L}(\Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma(1)) = \{\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right],\ ad = lm, 0 \leqslant b < d, (a,b,d) = l\}$$

fourni par le lemme précédent, on voit que $f[T(l,m)]'_k(z)$ 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

$$f((az+b)/d) = \sum_{m\in\mathbb{N}} a(m) e^{2i\pi mb/d} q^{ma/d}, \text{ et } \sum_{b=0}^{d-1} e^{2i\pi mb/d} = \begin{cases} d & \text{si } d|m \\ 0 & \text{sinon.} \end{cases}$$

□

Nous allons maintenant montrer que les $T(n)$ sont auto-adjoints pour le produit de Petersson. Nous aurons besoin du lemme suivant.

LEMME. – *Soit $\alpha \in \Delta$ et Γ d'indice fini dans $\Gamma(1) \cap \alpha^{-1}\Gamma(1)\alpha$. Alors pour $f, g \in \mathcal{S}_k(\alpha\Gamma\alpha^{-1})$, on a $f[\alpha]_k, g[\alpha]_k \in \mathcal{S}_k(\Gamma)$ et*

$$\langle f[\alpha]_k, g[\alpha]_k\rangle_\Gamma = \langle f, g\rangle_{\alpha\Gamma\alpha^{-1}}.$$

Démonstration. Le fait que $f[\alpha]_k, g[\alpha]_k \in \mathcal{S}_k(\Gamma)$ est évident. Soit $h(z) := \Im(z)^k f(z)\overline{g(z)}$. La formule $\Im(\alpha z) = \det(\alpha)|j_\alpha(z)|^{-2}\Im(z)$ montre que $h(\alpha z) = \Im(z)^k f[\alpha]_k(z)\overline{g[\alpha]_k(z)}$. On a donc

$$\langle f[\alpha]_k, g[\alpha]_k\rangle_\Gamma = \frac{1}{V_\Gamma}\int_{D_\Gamma} h(\alpha z)d\mu(z) = \frac{1}{V_\Gamma}\int_{\alpha D_\Gamma} h(z)d\mu(z) = \langle f, g\rangle_{\alpha\Gamma\alpha^{-1}}.$$

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 $d\mu(z)$ sous $\mathrm{GL}_2(\mathbb{R})_+$, 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. □

PROPOSITION. – *Pour $f, g \in \mathcal{S}_k(\Gamma(1))$ on a $\langle f[T(n)]'_k, g\rangle_{\Gamma(1)} = \langle f, g[T(n)]'_k\rangle_{\Gamma(1)}$.*

Démonstration. Il suffit bien sûr de prouver la même formule pour $[T(l,m)]_k$. 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 $\left[\begin{smallmatrix} l & 0 \\ 0 & m\end{smallmatrix}\right]$ sur $\left[\begin{smallmatrix} m & 0 \\ 0 & l\end{smallmatrix}\right]$, 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 $\Gamma(1) \cap \left[\begin{smallmatrix} l & 0 \\ 0 & m\end{smallmatrix}\right]^{-1}\Gamma(1)\left[\begin{smallmatrix} l & 0 \\ 0 & m\end{smallmatrix}\right]$. 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,

$$\begin{aligned}
& \langle f[T(l,m)]_k, g\rangle_{\Gamma(1)} = \langle f[T(l,m)]_k, g\rangle_\Gamma \\
= \; & \sum_{\alpha\in\tilde{\mathcal{L}}}\langle f[\alpha]_k, g\rangle_\Gamma = \sum_{\alpha\in\tilde{\mathcal{L}}}\langle f[\alpha]_k, g\rangle_{\Gamma(1)\cap\alpha^{-1}\Gamma(1)\alpha} \\
= \; & \sum_{\alpha\in\tilde{\mathcal{L}}}\langle f, g[\alpha^{-1}]_k\rangle_{\alpha\Gamma(1)\alpha^{-1}\cap\Gamma(1)} = \sum_{\alpha\in\tilde{\mathcal{L}}}\langle f, g[\alpha^*]_k\rangle_\Gamma \\
= \; & \langle f, g[T(l,m)]_k\rangle_\Gamma = \langle f, g[T(l,m)]_k\rangle_{\Gamma(1)}.
\end{aligned}$$

□

COROLLAIRE. – *L'espace $\mathcal{S}_k(\Gamma(1))$ 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 $f(z) = \sum_{n>0} a(n)q^n$ est une forme propre et de valeurs propres $(\lambda(n))_{n\in\mathbb{N}^*}$, alors*

$$\forall n \in \mathbb{N}^*, a(n) = a(1)\lambda(n).$$

En particulier, si f est normalisée de sorte que $a(1) = 1$, on a les propriétés :

$$\begin{cases} a(nm) = a(n)a(m) \text{ si } (n,m) = 1 \\ a(p^{r+1}) = a(p)a(p^r) - p^{k-1}a(p^{r-1}) \text{ pour } p \text{ premier}, r \geqslant 1. \end{cases}$$

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 $\mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)]$ qui permet une diagonalisation simultanée.

Pour $f \in \mathcal{M}_k(\Gamma(1))$, on a vu que le terme en q dans le q-développement de $f[T(n)'_k](z)$ 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 $\lambda : \mathbb{Z}[\Gamma(1)\backslash\Delta/\Gamma(1)] \longrightarrow \mathbb{C}$, donc vérifient les égalités.

$$\begin{cases} \lambda(nm) = \lambda(n)\lambda(m) \text{ si } (n,m) = 1 \\ \lambda(p^{r+1}) = \lambda(p)\lambda(p^r) - p\lambda(T(p,p))a(p^{r-1}) \text{ pour } p \text{ premier}, r \geqslant 1. \end{cases}$$

Il reste donc à calculer $\lambda(T(p,p))$, mais $f[T(p,p)]'_k(z) = \det \left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]^{k-1} j_{\left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]}(z)^{-1} f(z) = p^{2k-2}p^{-k}f(z)$, donc $\lambda(T(p,p)) = p^{k-2}$. □

Remarque. – La formule $a(n) = \lambda(n)a(1)$ montre que pour une forme parabolique propre (donc non nulle, comme tout vecteur propre) on a toujours $a(1) \neq 0$, de sorte que f est un multiple d'une forme propre normalisée.

Exemple. – L'espace $\mathcal{S}_{12}(\Gamma(1))$ est de dimension 1, donc Δ est vecteur propre des opérateurs de Hecke. On en déduit les propriétés de multiplicativité de la fonction τ conjecturées par Ramanujan.

Remarque. – La seconde conjecture de Ramanujan, sur la taille des $\tau(n)$ se généralise ainsi : *si $f \in \mathcal{S}_k(\Gamma(1))$ 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. (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 $Re(s) > (k+1)/2$.

1.3.4 *L'anneau de Hecke en niveau* $\Gamma_0(N)$. Nous allons décrire l'anneau de Hecke $\mathcal{H}_0(N) := \mathbb{Z}[\Gamma_0(N)\backslash\Delta_0(N)/\Gamma_0(N)]$ où $\Delta_0(N) := \{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Delta,\ c \equiv 0[N] \text{ et } (a,N) = 1\}$. 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. – *Notons* $\Delta_0(N)_{l,m}$ *l'ensemble des* $\alpha \in \Delta_0(N)$ *d'invariants* (l,m).

i) $\Delta_0(N)_{l,m} = \Gamma_0(N)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma_0(N)$.

ii) l'ensemble $\mathcal{L}_0(N)_{l,m} := \{\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right],\ (a,N) = 1, ad = lm, 0 \leqslant b < d \text{ et } (a,b,d) = l\}$ *est un ensemble de représentants des* $\Gamma_0(N)$*-classes à gauche dans* $\Delta_0(N)_{l,m}$.

Démonstration. i) 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 $\mathbb{Z}^2$ telle que :

— $(l\omega_1, m\omega_2)$ soit une base de $\alpha(\mathbb{Z}^2)$

— $\omega_1 \in (\mathbb{Z} \oplus N\mathbb{Z})$ (pour que la matrice de passage γ_1 soit dans $\Gamma_0(N)$).

— $\alpha(e_1) \in (l\mathbb{Z}\omega_1 \oplus Nm\mathbb{Z}\omega_2)$ (pour que la matrice de passage γ_2 soit dans $\Gamma_0(N)$).

On peut montrer que toute base (ω_1, ω_2) de $\mathbb{Z}^2$ telle que $(l\omega_1, mN\omega_2)$ soit une base de $\alpha(\mathbb{Z} \oplus N\mathbb{Z})$ convient (exercice ou cf Miake 4.5.1).

ii) 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 $\gamma \in \Gamma_0(N)$. □

Notons encore $T(l,m) := [\Gamma_0(N)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]\Gamma_0(N)]$. D'après le lemme, les $T(l,m)$, pour $1 \leqslant l|m$ et $(l,N) = 1$, forment une base de $\mathcal{H}_0(N)$. Voici la table de multiplication dans cette base.

PROPOSITION. – *On a les égalités suivantes (où* p *désigne un nombre premier) :*

i) $T(l,m) = T(l,l)T(1,m/l) = T(1,m/l)T(l,l)$

ii) $T(l,m)T(l',m') = T(ll',mm')$ *si* $(lm, l'm') = 1$.

iii) Si $p \nmid N$, $T(1,p)T(1,p^r) = T(1,p^{r+1}) + \begin{cases} (p+1)T(p,p) & \text{si } r = 1 \\ pT(p,p)T(1,p^{r-1}) & \text{si } r > 1 \end{cases}$

iv) Si $p|N$, $T(1,p)T(1,p^r) = T(1,p^{r+1})$.

En particulier, l'anneau $\mathbb{Z}[\Gamma_0(N)\backslash\Delta_0(N)/\Gamma_0(N)]$ *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 $\Gamma(1)$. □

COROLLAIRE. – *Pour* $n \in \mathbb{N}$, *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 :*

i) $T(nm) = T(n)T(m)$ *si* $(n,m) = 1$,

ii) $T(p^{r+1}) = T(p)T(p^r) - pT(p,p)T(p^{r-1})$, *si* $p \nmid N$

iii) $T(p^{r+1}) = T(p)T(p^r)$ *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. □

1.3.5 *Action sur le formes modulaires en niveau* $\Gamma_1(N)$. Bien-sûr, l'anneau de Hecke $\mathcal{H}_0(N)$ agit naturellement sur $\mathcal{M}_k(\Gamma_0(N))$. Mais en fait, il agit aussi sur les formes modulaires en niveau $\Gamma_1(N)$, une fois qu'on les a "coupées en morceaux". Le point de départ pour cela est le fait que $\Gamma_1(N)$ est distingué dans $\Gamma_0(N)$ avec un quotient abélien fini. Cela nous permet de décomposer

$$\begin{array}{ll} \mathcal{M}_k(\Gamma_1(N)) & = \bigoplus_\chi \mathcal{M}_k(N,\chi) \\ f & = \sum_\chi f_\chi \qquad \text{avec } f_\chi = [\Gamma_0(N):\Gamma_1(N)]^{-1} \sum_{\gamma\in\Gamma_0(N)/\Gamma_1(N)} \chi^{-1}(\gamma).f[\gamma]_k. \end{array}$$

où χ décrit les caractères (=homomorphismes) $\Gamma_0(N)/\Gamma_1(N) \longrightarrow \mathbb{C}^\times$ et

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)),\ f[\gamma]_k = \chi(\gamma)f,\ \forall\gamma \in \Gamma_0(N)\}\,.$$

En d'autres termes, $\mathcal{M}_k(N,\chi)$ 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 $\chi : \Delta_0(N) \longrightarrow \mathbb{C}^\times$. 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 $\mathcal{M}_k(N,\chi)$ 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

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N) \mapsto d(\mathrm{mod}\ N) \in (\mathbb{Z}/N\mathbb{Z})^\times$$

induit un isomorphisme $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$. Ainsi les caractères de $\Gamma_0(N)/\Gamma_1(N)$ sont de la forme $\chi(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]) = \psi(d) = \psi(a)^{-1} = \overline{\psi}(a)$ où ψ décrit les caractères de Dirichlet modulo N. On peut donc prolonger χ à $\Delta_0(N)$ par la formule $\chi(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]) = \overline{\psi}(a)$ (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* $\Gamma_0(N)$ *et le caractère de Dirichlet correspondant, et même la fonction* $\mathbb{Z} \longrightarrow \mathbb{C}$ *correspondante qui envoie* n *sur* $\chi(n)$ *si* $(n,N) = 1$ *et sur* 0 *sinon.*

Lemme. – *Pour* $n \geqslant 1$ *et* $f \in \mathcal{M}_k(N,\chi)$, *on a*

$$f[T(n)]_k^\chi(z) = n^{k-1}\sum_{ad=n}\sum_{b=0}^{d-1} \chi(a)d^{-k}f((az+b)/d).$$

Si $f(z) = \sum_{m\in\mathbb{N}} a(m)q^m$ est son q-développement en ∞ (avec $q = \exp(2i\pi z)$), alors

$$f[T(n)]_k^\chi(z) = \sum_{m\in\mathbb{N}} \left(\sum_{d|(m,n)} \chi(d) d^{k-1} a(mn/d^2) \right) q^m.$$

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 $\chi(d)$. □

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. – Vérifier que la somme $\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{S}_k(N, \chi)$ est une somme orthogonale pour le produit de Petersson sur $\mathcal{S}_k(\Gamma_1(N))$.

Proposition. – *Supposons $(n, N) = 1$. Alors pour $f, g \in \mathcal{S}_k(N, \chi)$ 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, $[T(n)]_k^\chi$ est un opérateur normal sur $\mathcal{S}_k(N, \chi)$.

Démonstration. Il suffit de prouver l'analogue pour $[T(l, m)]_k^\chi$ 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 $\left[\begin{smallmatrix} m & 0 \\ 0 & l \end{smallmatrix}\right]$ 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 $\Gamma_1(N) \cap \left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]^{-1}\Gamma_1(N)\left[\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right]$ et on écrit

$$\begin{aligned}
& \langle f[T(l,m)]_k^\chi, g\rangle_{\Gamma_1(N)} = \langle f[T(l,m)]_k^\chi, g\rangle_\Gamma \\
= \;& \sum_{\alpha\in\tilde{\mathcal{L}}} \langle f[\alpha]_k^\chi, g\rangle_\Gamma = \sum_{\alpha\in\tilde{\mathcal{L}}} \chi^{-1}(\alpha)\langle f[\alpha]_k, g\rangle_{\Gamma_1(N)\cap\alpha^{-1}\Gamma_1(N)\alpha} \\
= \;& \sum_{\alpha\in\tilde{\mathcal{L}}} \chi^{-1}(\alpha)\langle f, g[\alpha^{-1}]_k\rangle_{\alpha\Gamma_1(N)\alpha^{-1}\cap\Gamma_1(N)} = \sum_{\alpha\in\tilde{\mathcal{L}}} \chi^{-1}(\alpha)\overline{\chi(\alpha^*)}\langle f, g[\alpha^*]_k^\chi\rangle_\Gamma \\
= \;& \overline{\chi}(\det(\alpha))\langle f, g[T(l,m)]_k^\chi\rangle_\Gamma = \overline{\chi}(lm)\langle f, g[T(l,m)]_k^\chi\rangle_{\Gamma(1)}.
\end{aligned}$$

(Noter que $\chi^{-1} = \overline{\chi}$.) □

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. – *L'espace $\mathcal{S}_k(N, \chi)$ 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 $f(z)=\sum_{n>0}a(n)q^n$ 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 :

$$\begin{cases} a(nm)=a(n)a(m) \text{ si } (n,m)=1 \text{ et } (n,N)=1 \\ a(p^{r+1})=a(p)a(p^r)-\chi(p)p^{k-1}a(p^{r-1}) \text{ pour } p \text{ premier} \nmid N, r\geqslant 1. \end{cases}$$

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 $\chi(p)p^{k-2}$. □

Maintenant se posent deux problèmes qui n'apparaissaient pas en niveau $\Gamma(1)$.

Problème. – 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. – 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.

1.3.6 *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 $\mathcal{S}_k(N,\chi)[\lambda']$ le sous-espace propre associé à ce système. Comme les $T(p)$ pour $p|N$ commutent aux $T(n)$, ils stabilisent $\mathcal{S}_k(N,\chi)[\lambda']$. 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 $\lambda(n)$, $n\in\mathbb{N}$. 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 $\mathcal{S}_k(N,\chi)[\lambda']$ 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.* $\mathcal{S}_k(N,\chi)[\lambda']$ 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. – *i) Soit $l > 1$ un diviseur de N et $f \in \mathcal{S}_k(\Gamma_1(N/l))$. Alors la fonction $i_l f : z \mapsto f(lz)$ est dans $\mathcal{S}_k(\Gamma_1(N))$ et vérifie $a_n(i_l f) = 0$ pour $(n, N) = 1$.*

ii) Réciproquement, si $f \in \mathcal{S}_k(\Gamma_1(N))$ vérifie $a_n(f) = 0$ pour $(n, N) = 1$, alors il existe des formes $f_l \in \mathcal{S}_k(\Gamma_1(N/l))$ pour $l > 1$ diviseur de N telles que $f = \sum_{l|N} i_l f_l$.

Démonstration. i) Remarquons que $f(lz) = l^{1-k}.f[\left(\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right)]'_k(z)$ qui est une fonction automorphe 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 $\mathcal{S}_k(\Gamma_1(N))$. De plus, son q-développement s'écrit $f(lz) = \sum_{n\in\mathbb{N}} a_n(f)q^{ln}$, de sorte que $a_n(i_l f) = 0$ si $l \nmid n$. En particulier, $a_n(i_l f) = 0$ si $(n, N) = 1$.

ii) La réciproque est plus difficile et fait l'objet d'une feuille de TD. □

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 $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ de $\mathcal{S}_k(\Gamma_1(N))$ engendré par toutes les fonctions de la forme $f(lz)$ où :

— $f \in \mathcal{S}_k(\Gamma_1(M))$ 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 $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ comme l'orthogonal de $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ pour le produit de Petersson.

LEMME. – *i) $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$ et $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ sont stables sous l'action de $\Gamma_0(N)$ de poids k, et en particulier se décomposent*

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \bigoplus_{\chi\in\widehat{\mathbb{Z}/N\mathbb{Z}}^\times} \mathcal{S}_k(N,\chi)^{\text{old}} \text{ et } \mathcal{S}_k(\Gamma_1(N))^{\text{new}} = \bigoplus_{\chi\in\widehat{\mathbb{Z}/N\mathbb{Z}}^\times} \mathcal{S}_k(N,\chi)^{\text{new}}.$$

De plus on a, en notant m_χ le conducteur de χ,

$$\mathcal{S}_k(N,\chi)^{\text{old}} = \sum_{\substack{m_\chi|M|N, M\neq N \\ l|(N/M)}} i_l(\mathcal{S}_k(M,\chi)) = \sum_{\substack{m_\chi|M|N, M\neq N \\ l|(N/M)}} i_l(\mathcal{S}_k(M,\chi)^{\text{new}}).$$

ii) Soit $m_\chi|M|N$ et l un diviseur premier ou unité de N/M. Alors pour p premier on a

$$[T(p)]_k^{\chi,N} \circ i_l = \begin{cases} i_l \circ [T(p)]_k^{\chi,M} & \text{si } l \neq p \\ i_1 & \text{si } l = p \end{cases}$$

iii) L'application $f \mapsto f[w_N]_k$, où $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ induit une involution de $\mathcal{S}_k(\Gamma_1(N))$ qui envoie $\mathcal{S}_k(N,\chi)$ dans $\mathcal{S}_k(N,\overline{\chi})$. De plus on a

$$[w_N]_k \circ i_l = l^{-1}.(i_1 \circ [w_{N/l}]_k)$$

de sorte que $[w_N]_k$ stabilise $\mathcal{S}_k(\Gamma_1(N))^{\text{old}}$.

Démonstration. i) Soit $f \in \mathcal{S}_k(\Gamma_1(N/l))$ et $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N)$ (donc $l|c$). On a

$$(i_l f)\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]_k = l^{1-k}.f\left[\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right]_k\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]_k = l^{1-k}.f\left[\begin{smallmatrix} a & bl \\ c/l & d \end{smallmatrix}\right]_k\left[\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right]_k = i_l(f\left[\begin{smallmatrix} a & bl \\ c/l & d \end{smallmatrix}\right]_k)$$

où l'on remarque que $f\left[\begin{smallmatrix} a & bl \\ c/l & d \end{smallmatrix}\right]_k \in \mathcal{S}_k(\Gamma_1(N/l))$ puisque $\left[\begin{smallmatrix} a & bl \\ c/l & d \end{smallmatrix}\right] \in \Gamma_0(N/l)$. Ceci montre que $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{old}}$ 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 $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$ est aussi stable par $\Gamma_0(N)$.

Par ailleurs, si χ est un caractère de Dirichlet module 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 $f \in \mathcal{S}_k(N,\chi)^{\mathrm{old}}$ sous la forme $f = \sum_j i_{l_j} f_j$ avec $f_j \in \mathcal{S}_k(M_j,\chi_j)$ et $l_j|(N/M_j)$, alors on a aussi $f = \sum_{j,\chi_j=\chi} i_{l_j} f_j$.

ii) Soit $f \in \mathcal{S}_k(M,\chi)$. La formule décrivant l'action de $T(p)$ sur les q-développements montre que

$$a_n(i_l(f[T(p)]_k^{\chi,M}) = \begin{cases} 0 & \text{si } l \nmid n \\ \sum_{d|(n/l,p)} \chi(d) d^{k-1} a_{np/ld^2}(f) & \text{si } l|n \end{cases}$$

$$a_n((i_l f)[T(p)]_k^{\chi,N}) = \sum_{d|(n,p)} \chi(d) d^{k-1} a_{np/d^2}(i_l f) \text{ avec } a_{np/d^2}(i_l f) = \begin{cases} 0 & \text{si } l \nmid np/d^2 \\ a_{np/ld^2}(f) & \text{si } l|np/d^2 \end{cases}$$

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 $a_n((i_p f)[T(p)]_k^{\chi,N}) = a_{np}(i_p(f)) = a_p(f) = a_p(i_1 f)$.

iii) Si $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{M}_2(\mathbb{Z})$ on calcule que $w_N\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]w_N^{-1} = \begin{bmatrix} d & -c/N \\ -bN & a \end{bmatrix}$. 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 automorphes 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 ${}^{w_N}\chi(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]) = \chi(w_N\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]w_N^{-1}) = \chi(a) = \overline{\chi}(d) = \bar{\chi}(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right])$, donc ${}^{w_N}\chi = \overline{\chi}$. Il est alors clair que $f \mapsto f[w_N]_k$ envoie $\mathcal{S}_k(N,\chi)$ dans $\mathcal{S}_k(N,{}^{w_N}\chi) = \mathcal{S}_k(N,\overline{\chi})$.

Finalement, on calcule $[w_N]_k \circ i_l$ avec la formule explicite $f[w_N]_k(z) = N^{-1}z^{-k}f(\frac{-1}{Nz})$. □

Remarque. – D'après le i), si χ est primitif (i.e. $m_\chi = N$), alors $\mathcal{S}_k(N,\chi) = \mathcal{S}_k(N,\chi)^{\mathrm{new}}$.

Corollaire. – *$\mathcal{S}_k(N,\chi)^{\mathrm{old}}$ et $\mathcal{S}_k(N,\chi)^{\mathrm{new}}$ sont stables sous l'action de $\mathcal{H}_0(N)$ sur $\mathcal{S}_k(N,\chi)$.*

Démonstration. D'après le ii) du lemme, $\mathcal{S}_k(N,\chi)^{\mathrm{old}}$ 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 $\mathcal{S}_k(N,\chi)^{\mathrm{new}}$ est stable par *les adjoints* des $T(p)$. Pour $p \nmid N$, l'adjoint de $T(p)$ est $\overline{\chi}(p)T(p)$, donc $T(p)$ stabilise $\mathcal{S}_k(N,\chi)^{\mathrm{new}}$. Pour $p|N$, il faut un autre argument !

Rappelons-nous que dans ce cas $\mathcal{L}_0(N)_{1,p} = \{\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right], 0 \leqslant j < p\}$ et on a donc $f[T(p)]_k^{\chi} = \sum_{j=0}^{p-1} f\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]_k$. 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 $f \mapsto \sum_{j=0}^{p-1} f\left[\begin{smallmatrix} p & j \\ 0 & 1 \end{smallmatrix}\right]_k$. Cet opérateur n'est autre que $w_N \circ [T(p)]_k^{\overline{\chi}} \circ w_N^{-1}$. D'après ii) et iii) du lemme, $T(p)^*$ stabilise donc $\mathcal{S}_k(N,\chi)^{\text{old}}$, et par adjonction, $T(p)$ stabilise $\mathcal{S}_k(N,\chi)^{\text{new}}$, comme voulu. □

On peut maintenant faire marcher notre argument basé sur la multiplicité 1 d'un système de valeurs propres partiel.

COROLLAIRE. – *L'espace des formes nouvelles $\mathcal{S}_k(N,\chi)^{\text{new}}$ admet une base orthogonale constituée de formes propres pour* tous *les $T(n)$, $n \in \mathbb{N}$. 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 $\mathcal{S}_k(N,\chi)^{\text{new}}[\lambda']$ 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 ii) du théorème précédent nous dit qu'une telle f est ancienne. Contradiction. □

Une forme $f \in \mathcal{S}_k(\Gamma_1(N))$ nouvelle, propre et normalisée est appelée *forme primitive de conducteur N*. Les formes primitives forment une base de $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$. Le i) 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. – *L'ensemble $\{f(lz), f \in \mathcal{S}_k(\Gamma_1(M))$ primitive et $Ml|N\}$ est une base de $\mathcal{S}_k(\Gamma_1(N))$.*

2 Théorie géometrico-arithmétique

2.1 Liens entre formes modulaires et représentations Galoisiennes

Notre but est d'expliquer autant que possible quelques liens entre formes modulaires et représentations Galoisiennes. Ces liens sont apparus lorsque les mathématiciens ont réalisé que chacune de ces notions donnait lieu à des fonctions L dont les propriétés, prouvés ou conjecturales, se ressemblaient beaucoup.

2.1.1 *Représentations Galoisiennes.* Le groupe de Galois absolu de $\mathbb{Q}$ est un objet d'étude fondamental en théorie des nombres. Comme tout groupe, un bon moyen de l'approcher est d'étudier ses représentations linéaires. On s'intéresse donc aux représentations *continues*

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_n(C)$$

où C désigne un corps local de caractéristique 0 (ou éventuellement la clôture algébrique d'un tel corps). Ici, le groupe $\text{GL}_n(C)$ est muni de la topologie qui fait de lui un ouvert de $\text{M}_n(C)$ qui est un espace vectoriel de dimension finie sur le corps local C. Le groupe

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est lui muni de la topologie qui fait des $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, K extension finie de $\mathbb{Q}$, une base de voisinages ouverts de l'unité. C'est aussi la topologie produit lorsqu'on écrit

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \left\{ (\gamma_K)_K \in \prod_{[K:\mathbb{Q}]<\infty} \mathrm{Gal}(K/\mathbb{Q}),\ (\gamma_K)_{|K'} = \gamma_{K'} \text{ si } K' \subset K \right\},$$

ce qui montre que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est "profini" (limite projective de groupes fini) et donc compact. On a alors la dichotomie suivante :

i) Si $C = \mathbb{C}$ (ou $\mathbb{R}$), ρ est continue si et seulement si elle se factorise par un groupe de Galois fini $\mathrm{Gal}(K/\mathbb{Q})$. Ces représentations sont appelées *représentations d'Artin.*

ii) Si C est une extension du corps $\mathbb{Q}_\ell$ (complété de $\mathbb{Q}$ pour la valeur absolue ℓ-adique), alors la continuité de ρ est équivalente aux propriétés suivantes :
   — ρ est à valeurs dans $\mathrm{GL}_2(\mathcal{O}_C)$, après éventuelle conjugaison dans $\mathrm{GL}_2(C)$.
   — Pour tout n, la représentation ρ modulo ℓ^n se factorise par le groupe de Galois d'une extension finie de $\mathbb{Q}$.
   Ces représentations sont souvent simplement appelées *représentations ℓ-adiques.*

Exemple. ($n = 1$: *caractères cyclotomiques.*) – Soit N un entier, μ_N le groupe des racines N-èmes de 1 dans $\overline{\mathbb{Q}}$ et $\zeta_N \in \mu_N$ une racine primitive. On rappelle que l'application $\sigma \mapsto n_\sigma$ où $\sigma(\zeta_N) = \zeta_N^{n_\sigma}$ définit un isomorphisme $\varepsilon_N : \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$. Ainsi tout *caractère de Dirichlet* χ modulo N définit un caractère continu

$$\chi \circ \varepsilon_N : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \longrightarrow \mathrm{GL}_1(\mathbb{C}).$$

Par ailleurs, la collection des ε_{ℓ^n}, $n \in \mathbb{N}$, définit à la limite un isomorphisme $\varepsilon_{\ell^\infty} : \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times$, que l'on peut donc voir comme un caractère continu

$$\varepsilon_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \longrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell).$$

Le théorème de Kronecker-Weber nous dit qu'on a ainsi construit toutes les représentations continues de dimension 1 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Exemple. ($n = 2$: *courbes elliptiques*) – Soit E une courbe elliptique sur $\mathbb{Q}$ (nous ferons quelques rappels plus tard). Alors on sait que le sous-groupe des points de N-torsion $E(\overline{\mathbb{Q}})[N]$ est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^2$. Comme il est aussi visiblement muni d'une action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ compatible au produit dans E et comme les points de N-torsion sont définis sur une extension finie de $\mathbb{Q}$, on obtient une représentation continue

$$\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

L'accouplement de Weil nous dit que le déterminant de $\rho_{E,N}$ est donné par ε_N.

En considérant le système projectif des $E(\overline{\mathbb{Q}})[\ell^n]$ où les applications de transition sont données par la multiplication par ℓ, on obtient à la limite une représentation continue

$$\rho_{E,\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Exemple. (*Cohomologie ℓ-adique.*) – Plus généralement, pour une variété algébrique X définie sur $\mathbb{Q}$, Grothendieck a défini des groupes de "cohomologie étale" $H^i_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}/N\mathbb{Z})$ sur lesquels le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit. En prenant la limite projective sur n des $H^i_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell^n\mathbb{Z})$ et en inversant ℓ, on obtient un espace vectoriel $H^i_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ de dimension finie sur $\mathbb{Q}_\ell$ et muni d'une action linéaire continue de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. De telles représentations ℓ-adiques sont dites "d'origine géométrique". Ici, l'usage des coefficients ℓ-adiques est crucial : Serre a remarqué qu'il n'existe pas de théorie cohomologique Galois équivariante à coefficients complexes.

Représentations locales. Soit p un nombre premier. Fixons une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. Tout plongement $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ induit, par restriction des automorphismes, un plongement $\iota_* : G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Comme tout autre ι' est de la forme $\iota\circ\gamma$ pour un $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, le plongement ${\iota'}_*$ est conjugué à ι_* sous γ, et par conséquent les deux restrictions $\rho\circ\iota_*$ et $\rho\circ{\iota'}_*$ de ρ à $G_{\mathbb{Q}_p}$ sont conjuguées sous $\rho(\gamma)$, et donc équivalentes. On note simplement $\rho_{|G_{\mathbb{Q}_p}}$ la (classe d'équivalence de) représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ ainsi obtenue.

Ramification. Notons $|.|_p$ l'unique extension à $\overline{\mathbb{Q}}_p$ de la valeur absolue p-adique. L'action de $G_{\mathbb{Q}_p}$ sur $\overline{\mathbb{Q}}_p$ préserve la valeur absolue $|.|_p$ et en particulier stabilise l'anneau des entiers $\overline{\mathbb{Z}}_p = \{x \in \overline{\mathbb{Q}}_p, |x|_p \leqslant 1\}$ et son idéal maximal $\overline{\mathfrak{m}}_p := \{x \in \overline{\mathbb{Q}}_p, |x|_p < 1\}$. Ainsi $G_{\mathbb{Q}_p}$ agit par automorphismes de corps sur le quotient $\overline{\mathbb{Z}}_p/\overline{\mathfrak{m}}_p = \overline{\mathbb{F}}_p$, d'où un morphisme

$$G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$

dont on note $I_{\mathbb{Q}_p}$ le noyau, appelé *sous-groupe d'inertie* de $G_{\mathbb{Q}_p}$. On dit alors que la représentation ρ est *non ramifiée en p* (ou encore que $\rho_{|G_{\mathbb{Q}_p}}$ est non ramifiée) si $\rho_{|I_{\mathbb{Q}_p}}$ est triviale, c'est-à-dire si $I_{\mathbb{Q}_p}$ agit par l'identité sur l'espace $V = C^n$ de la représentation ρ.

Exercice. – p est non ramifié dans ρ si et seulement si ρ se factorise par $\mathrm{Gal}(\overline{\mathbb{Q}}^{(p')}/\mathbb{Q})$ où $\overline{\mathbb{Q}}^{(p')}$ est le sous-corps maximal de $\overline{\mathbb{Q}}$ dans lequel p n'est pas ramifié. [Indication : cela revient à vérifier que $\overline{\mathbb{Q}}^{(p')}$ est le sous-corps fixé par le sous-groupe engendré par tous les $\iota_*(I_{\mathbb{Q}_p})$, où ι décrit les plongements $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$].

Nous ne considèrerons que des représentations qui n'ont qu'un nombre fini de premiers ramifiés. Cette condition est automatique pour les représentations d'Artin, car si par exemple ρ se factorise par $\mathrm{Gal}(K/\mathbb{Q})$, alors tout p non ramifié dans K est non ramifié pour ρ. Par contre, cette condition n'est pas automatique pour les représentations ℓ-adiques. Pour un entier N, nous dirons que ρ *est non ramifiée en dehors de N* si les seuls premiers ramifiés dans ρ sont des diviseurs de N. Cela équivaut à demander que ρ se factorise par $\mathrm{Gal}(\overline{\mathbb{Q}}^{(N)}/\mathbb{Q})$ où $\overline{\mathbb{Q}}^{(N)}$ désigne le sous-corps de $\overline{\mathbb{Q}}$ maximal dans lequel les seuls premiers ramifiés sont les diviseurs de N.

Polynômes caractéristiques de Frobenius. On sait que le morphisme $G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{F}_p}$ est surjectif. Soit σ_p n'importe quel élément de $G_{\mathbb{Q}_p}$ s'envoyant sur le Frobenius $(x \mapsto x^p) \in G_{\mathbb{F}_p}$.

Alors σ_p normalise $I_{\mathbb{Q}_p}$ donc stabilise les $I_{\mathbb{Q}_p}$-invariants $V^{I_{\mathbb{Q}_p}}$ dans l'espace $V = C^n$ de la représentation ρ. On pose alors

$$\Phi_{\rho,p}(X) := \det\left((\mathrm{id} - X\rho(\sigma_p))|V^{I_{\mathbb{Q}_p}}\right) \in C[X]$$

le polynôme caractéristique (ou presque) de $\rho(\sigma_p)$ agissant sur ces $I_{\mathbb{Q}_p}$-invariants. Celui-ci est indépendant du choix de σ_p puisque tout autre choix appartient à $\sigma_p.I_{\mathbb{Q}_p}$.

On voit sur la définition que $\Phi_p(X)$ est de degré au plus n, et que que p est ramifié si et seulement si $\Phi_p(X)$ est de degré $< n$.

2.1.2 *Représentations d'Artin et formes de poids* 1. La possibilité d'une correspondance entre formes modulaires et représentations Galoisiennes se voit plus facilement sur les représentations d'Artin. Dans ce cas, les polynômes $\Phi_p(X)$ sont à coefficients complexes bornés indépendamment de p. En effet, puisque ρ se factorise par un groupe fini, les valeurs propres de $\rho(\sigma_p)$ sont des racines de l'unité et donc $|\operatorname{tr}(\wedge^i\rho(\sigma_p))| \leqslant \binom{n}{i}$. Il s'ensuit que le produit Eulerien

$$L(s,\rho) = \prod_p \Phi_p(p^{-s})^{-1}$$

converge pour $\Re(s) > 1$.

Exercice. – Supposons $n = 1$. Si ρ est la représentation triviale, on a $L(s,\rho) = \zeta(s)$. Plus généralement, si $\rho = \chi \circ \varepsilon_N$ pour un caractère de Dirichlet *primitif* χ modulo N, on a $L(s,\rho) = L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$.

Exemple. – Soit K une extension finie de $\mathbb{Q}$, et X l'ensemble fini des plongements de K dans $\overline{\mathbb{Q}}$. Le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur X et donc agit linéairement sur l'espace vectoriel $\mathbb{C}^X$. D'où une représentation d'Artin ρ de dimension $n = [K : \mathbb{Q}]$. On montre alors (excellent exercice) que $L(s,\rho) = \zeta_K(s) = \prod_{\mathfrak{p}\in\mathrm{Max}(\mathcal{O}_K)}(1 - (N\mathfrak{p})^{-s})^{-1} = \sum_{\mathfrak{a}} |N\mathfrak{a}|^{-s}$ (la fonction ζ du corps K). Ici $\mathfrak{a}$ décrit les idéaux non nuls de $\mathcal{O}_K$.

Remarque. – Si $\rho = \rho_1 \oplus \rho_2$, alors $L(s,\rho) = L(s,\rho_1)L(s,\rho_2)$.

Le théorème de Cebotarev nous dit que tout élément d'un groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ fini est une substitution de Frobenius [8] pour un p non ramifié dans K (et même pour une infinité de tels p). Ainsi, puisqu'une représentation complexe d'un groupe fini est déterminée par son caractère, une représentation d'Artin ρ est uniquement déterminée par les $\operatorname{tr}(\rho(\sigma_p))$ pour les premiers p où ρ est non ramifiée. Comme on peut retrouver $\operatorname{tr}(\rho(\sigma_p)) = b_p$ dans le développement $L(s,\rho) = \sum_{n=1}^{\infty} b_n n^{-s}$, elle est donc *a fortiori* déterminée par sa fonction $L(s,\rho)$.

Artin a montré que $L(s,\rho)$ admet un prolongement méromorphe à $s \in \mathbb{C}$ et satisfait une certaine équation fonctionnelle du même type que celle satisfaite par ζ, $L(s,\chi)$ ou ζ_K par exemple. Il a ensuite conjecturé que ce prolongement $L(s,\rho)$ est *holomorphe si et*

8. i.e. un élément de la forme $\iota_*(\sigma_p)_{|K}$ pour un plongement ι et un relèvement du Frobenius σ_p comme ci-dessus

seulement si ρ n'a pas de vecteurs fixes sous $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Cette conjecture est toujours un problème ouvert.

Lorsque ρ est de dimension 2, l'équation fonctionnelle de $L(s,\rho)$ est semblable à celle satisfaite par la fonction $L(s,f)$ d'une forme primitive *de poids* 1. De plus, Hecke avait prouvé l'holomorphie de $L(s,f)$. Le spectaculaire théorème suivant a été conjecturé par Langlands, qui y voyait une raison profonde à la conjecture d'Artin.

THÉORÈME. (Deligne-Serre) – *Soit $f \in \mathcal{S}_1(N,\chi)$ une forme primitive. Il existe une unique représentation d'Artin ρ_f de dimension 2 telle que $L(s,f) = L(s,\rho_f)$.*

Remarque. – L'égalité $L(s,f) = L(s,\rho_f)$ est équivalente à l'égalité de tous les facteurs locaux

$$\forall p,\ 1 - a_p(f)p^{-s} + \chi(p)p^{-2s} = \Phi_p(p^{-s}),$$

et donc aux égalités

$$\begin{gathered}\forall p \nmid N,\ a_p(f) = \mathrm{tr}(\rho(\sigma_p)) \text{ et } \chi(p) = \det(\rho(\sigma_p)) \\ \text{et } \forall p|N,\ a_p(f) = \mathrm{tr}(\rho(\sigma_p)|V^{I_p}).\end{gathered}$$

En particulier, on voit que ρ_f est non ramifiée en dehors de N et ramifiée en tout premier divisant N. En fait, comme on l'a vu ci-dessus, la représentation ρ_f est entièrement déterminée par les égalités

$$\mathrm{tr}(\rho(\sigma_p)) = a_p(f) \text{ pour } p \nmid N.$$

Dans leur preuve, Deligne et Serre construisent ρ_f satisfaisant l'égalité des facteurs locaux en $p \nmid N$, puis montrent que les égalités en les facteur locaux en $p|N$ découlent des équations fonctionnelles pour chacune des fonctions L.

Remarque. – Comme $L(s,f)$ n'est pas le produit de deux fonctions L de Dirichlet, la représentation ρ_f est irréductible. Par ailleurs, son déterminant est manifestement $\det(\rho_f) = \chi \circ \varepsilon_N$. En particulier, on voit que la *conjugaison complexe*[9] σ_∞ a pour déterminant $\det(\rho(\sigma_\infty)) = \chi(-1) = -1$. Cette dernière égalité est une condition nécessaire pour avoir $\mathcal{S}_1(N,\chi) \neq 0$.

De manière remarquable, ce résultat enrichit les deux mondes :

— D'une part, il implique la conjecture de Ramanujan-Petersson pour f de poids 1, qui prédisait $|a_p(f)| \leqslant 2$.

— D'autre part, il implique la conjecture d'Artin pour les représentations ρ_f. D'ailleurs, la forme moderne donnée par Langlands à la *conjecture d'Artin est que toute représentation irréductible de dimension* 2 *est de la forme* ρ_f. Notons que pour les représentations *réductibles* de dimension 2, donc de la forme $\rho = (\chi \circ \varepsilon_N) \oplus (\chi' \circ \varepsilon_{N'})$, on sait construire une série d'Eisenstein telle que $L(s,f) = L(s,\chi)L(s,\chi')$.

9. On peut supposer que $\overline{\mathbb{Q}}$ est plongé dans $\mathbb{C}$ pour simplifier. Sinon, une conjugaison complexe n'est définie qu'à conjugaison près, et joue le rôle de substitution de Frobenius pour la valeur absolue archimédienne.

Nous n'allons pas expliquer la preuve de Deligne et Serre, mais nous signalons que, bien que le théorème concerne des objets "plus simples" (représentations d'Artin), sa preuve utilise la construction de représentations Galoisiennes associées à des formes de poids $k > 1$, qui comme nous allons le voir, sont ℓ-adiques.

2.1.3 *Représentations ℓ-adiques et formes de poids $k \geqslant 2$..*

THÉORÈME. (Deligne, Shimura) – *Soit $f \in \mathcal{S}_k(N, \chi)$ une forme primitive de poids k, niveau N, et nebentypus χ.*

i) Le corps K_f engendré sur $\mathbb{Q}$ par les valeurs propres $\lambda(n)$, $n \in \mathbb{N}$ est de degré fini sur $\mathbb{Q}$, et les $\lambda(n)$ sont des entiers algébriques.

ii) Soit $\mathfrak{l}$ un idéal maximal de $\mathcal{O}_{K_f}$ au dessus d'un premier ℓ. Notons $K_{f,\mathfrak{l}}$ le complété de K_f pour la valeur absolue associée à $\mathfrak{l}$. C'est donc une extension finie de $\mathbb{Q}_\ell$. Alors il existe une unique (à conjugaison près) représentation continue

$$\rho_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{l}})$$

telle que pour tout $p \nmid \ell N$ on a l'égalité

$$(*)_p \qquad \Phi_{p,\rho_{f,\mathfrak{l}}}(X) = 1 - \lambda(p)X + \chi(p)p^{k-1}X^2.$$

De plus, $\rho_{f,\mathfrak{l}}$ est irréductible, son déterminant est le caractère $(\chi \circ \varepsilon_N).\varepsilon_{\ell^\infty}^{k-1}$, et l'égalité $(*)_p$ est vraie pour tout $p \neq \ell$.

Remarque. (Sur l'unicité) – La représentation $\rho_{f,\mathfrak{l}}$, si elle existe, est visiblement non ramifiée en $p \nmid \ell N$ (et ramifiée en $p|\ell N$). Comme dans le cas des représentations d'Artin, le théorème de Cebotarev assure que $\rho_{f,\mathfrak{l}}$ est déterminée, à semi-simplification près, par les égalités $(*)_p$ en chaque $p \nmid \ell N$, et même simplement par les égalités $\mathrm{tr}(\rho(\sigma_p)) = \lambda(p)$ pour $p \nmid \ell N$. Mais puisque $\rho_{f,\mathfrak{l}}$ est irréductible, elle est complètement déterminée par ces égalités.

Remarque. (Sur le déterminant) – Notons que $\chi \circ \varepsilon_N$ est bien à valeurs dans $K_{f,\mathfrak{l}}$, et même dans K_f, par construction. De même $\varepsilon_{\ell^\infty}$ est à valeurs dans $\mathbb{Z}_\ell^\times \subset K_{f,\mathfrak{l}}^\times$. Maintenant l'égalité entre $\det(\rho_{f,\mathfrak{l}})$ (admettant que $\rho_{f,\mathfrak{l}}$ existe) et le caractère annoncé est vraie au moins en toutes les substitutions de Frobenius en les $p \nmid \ell N$ d'après $(*)_p$, et donc en tout élément de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ d'après Cebotarev.

Remarque. (Sur l'égalité $(*)_p$ pour $p|N$, $p \neq \ell$) – Comme dans le cas de poids 1, ces égalités aux premiers ramifiés découlent des équations fonctionnelles satisfaites par les fonctions L de chaque côté. Sauf qu'il n'est pas clair a priori que $\rho_{f,\mathfrak{l}}$ admette une fonction L raisonnable (ce n'est pas une représentation complexe !). En fait, la construction même de $\rho_{f,\mathfrak{l}}$ via la cohomologie étale ℓ-adique, jointe aux propriétés non triviales de celle-ci, permet de lui associer une telle fonction L.

Remarque. (Et en $p = \ell$?) – Ce qui se passe en $p = \ell$ est assez mystérieux, et pourtant crucial dans les applications arithmétiques. Afin d'expliquer la particularité de ce cas, remarquons que l'on peut interpréter l'égalité $(*)_p$ lorsque $p \nmid \ell N$ comme une description

complète de la restriction $\rho_{|G_{\mathbb{Q}_p}}$. Mais lorsque $p|N$, on est dans la situation bizarre où on sait que $\rho_{|G_{\mathbb{Q}_p}}$ est bien déterminée (à cause de Cebotarev), mais on ne sait pas la "lire" sur f. Même lorsque $p \neq \ell$, l'égalité $(*)_p$ ne suffit pas à décrire $\rho_{|G_{\mathbb{Q}_p}}$. Néanmoins dans ce cas, on comprend bien depuis Langlands comment décrire complètement $\rho_{|G_{\mathbb{Q}_p}}$, à partir de la *représentation automorphe* associée à f. C'est l'objet de la "correspondance de Langlands locale". Mais lorsque $p = \ell$, même la représentation automorphe associée à f est insuffisante pour décrire $\rho_{|G_{\mathbb{Q}_\ell}}$. C'est l'objet du récent "programme de Langlands p-adique" d'essayer de comprendre ce qui se passe, l'outil principal étant la "théorie de Hodge p-adique".

Remarque. (Sur les conséquences du théorème) – Comme dans le cas de poids 1, ce théorème permet de prouver la conjecture de Ramanujan-Petersson. Sauf que les estimées du côté Galoisien sont beaucoup plus difficiles ! Là encore, elles découlent de la construction via la cohomologie étale, et des conjectures de Weil démontrées par Deligne sur la taille du nombre de points des variétés sur les corps finis !

Remarque. (Sur la réciproque) – Comme dans le cas des représentations d'Artin, il existe une réciproque conjecturale à ce théorème. Une première version, dûe à Langlands, prédit que toute représentation irréductible de dimension 2 "d'origine géométrique" (i.e. apparaissant comme sous-quotient de la cohomologie d'une variété algébrique sur $\mathbb{Q}$) provient d'une forme modulaire. Ceci contient déjà la "conjecture de modularité pour les courbes elliptiques", promue par Shimura, Taniyama et Weil, dont un cas particulier prouvé par Wiles a permis de boucler la preuve du théorème de Fermat. Une version encore plus spectaculaire a été énoncée par Fontaine et Mazur, où l'hypothèse "d'origine géométrique" est remplacée par une condition liée à la théorie de Hodge ℓ-adique, dont l'énoncé nous mènerait trop loin. Cette conjecture (en poids $\geqslant 2$) a connu des progrès récents spectaculaires, et seuls quelques cas résistent. MAIS... ce n'est que le cas $n = 2$ d'une conjecture encore plus générale, reliant représentations Galoisiennes et "représentations automorphes", et qui elle, est encore loin d'être comprise...

2.1.4 *Stratégie de la preuve.* La première idée est d'exhiber un sous-groupe abélien libre de type fini H et générateur du $\mathbb{C}$-espace vectoriel $\mathcal{S}_k(N, \chi)$ qui soit stable par l'action de l'anneau de Hecke $\mathcal{H}_0(N)$. Le théorème de Cayley-Hamilton nous dit alors que les valeurs propres d'un opérateur de Hecke sont des zéros de son polynôme caractéristique en tant qu'endomorphisme de H, lequel est monique à coefficients entiers, ce qui prouve le i) du théorème. Dans le cas $k = 2$ et $\chi = 1_N$, nous pourrons prendre pour H l'homologie singulière $H_1(X_0(N), \mathbb{Z})$. En général, il faut prendre l'homologie "à coefficients dans un système local" dépendant de k.

La deuxième idée consiste à montrer d'abord que $X_0(N)$ possède un modèle canonique comme courbe algébrique sur $\mathbb{Q}$, puis à essayer d'en déduire une action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur l'homologie H. C'est cette deuxième étape qui est techniquement très difficile, et qui d'ailleurs ne fonctionne pas bien. Ce que l'on parvient à faire, c'est définir une action Galoisienne sur l'homologie à coefficients $\mathbb{Z}/\ell^n\mathbb{Z}$, et donc, en prenant la limite, sur l'homologie $H_{\mathbb{Z}_\ell}$ à coefficients dans $\mathbb{Z}_\ell$.

À ce point, on dispose d'un $\mathbb{Z}_\ell$-module libre de type fini muni d'une action de $\mathcal{H}_0(N)$

et de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Il faut alors montrer que l'action Galoisienne ρ est non ramifiée en tout $p \nmid \ell N$, puis montrer qu'une substitution de Frobenius σ_p en un tel p satisfait l'équation polynomiale (appelée relation de congruence d'Eichler-Shimura)

$$1 - T(p).\rho(\sigma_p) + pT(p,p).\rho(\sigma_p)^2 = 0.$$

À partir de là, il reste à montrer que l'espace $H_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} K_{f,\mathfrak{l}}[\lambda]$ (sous-espace propre pour tous les T_p) est de dimension 2 sur $K_{f,\mathfrak{l}}$. C'est la représentation cherchée.

Dorénavant nous supposons $k = 2$ et $\chi = 1_N$. Nous partons donc de $f \in \mathcal{S}_2(\Gamma_0(N))$. Nous allons essayer de mener à bien la stratégie ci-dessus dans ce cas, en profitant de l'isomorphisme

$$\mathcal{S}_2(\Gamma_0(N)) \xrightarrow{\sim} \Omega^1(X_0(N)) := \{\textit{formes différentielles holomorphes } \omega \textit{ sur } X_0(N)\}.$$

2.2 Algébricité des valeurs propres de Hecke

2.2.1 *Jacobienne, homologie, théorème d'Abel.* Soit X une surface de Riemann compacte de genre g. Si $\omega \in \Omega^1(X)$ est une forme différentielle holomorphe, on peut l'intégrer le long de tout chemin continu $c : [0,1] \longrightarrow X$. Le théorème des résidus et l'holomorphie de ω assurent que si c' est homotope à c alors $\int_{c'} \omega = \int_c \omega$. Fixons un point $x_0 \in X$. En se restreignant aux lacets basés en x_0 on obtient un homomorphisme de groupes

$$\pi_1(X, x_0)_{\mathrm{ab}} = H_1(X, \mathbb{Z}) \longrightarrow \Omega^1(X)^*.$$

Avec un peu de topologie algébrique, on voit que le groupe abélien $H_1(X,\mathbb{Z})$ est libre de rang $2g$, engendré par les lacets longitudinaux $c_1, \cdots, c_g$ et les lacets latitudinaux $c'_1, \cdots, c'_g$ autour des g "trous" de X. Avec un peu de théorie de Hodge, on montre que la famille $\{\int_{c_i}, i = 1, \cdots, g\} \cup \{\int_{c'_i}, i = 1, \cdots, g\}$ est une $\mathbb{R}$-base de $\Omega^1(X)^*$. En particulier $H^1(X,\mathbb{Z})$ est un réseau co-compact du $\mathbb{C}$-espace vectoriel $\Omega^1(X)^*$ et le quotient

$$J(X) := \Omega^1(X)^*/H_1(X,\mathbb{Z})$$

est naturellement une variété complexe compacte de dimension g, munie d'une structure de groupe analytique abélien (on parle de "tore complexe").

Si maintenant c est un chemin de x_0 à x, l'image de l'élément $\int_c \in \Omega^1(X)^*$ dans $J(X)$ ne dépend que de x et on peut la noter simplement $\int_{x_0}^x$. Considérons alors l'application

$$\mathrm{Div}^0(X) \longrightarrow J(X),\ \sum_x n_x[x] \mapsto \sum_x n_x \int_{x_0}^x.$$

Le *théorème d'Abel-Jacobi* affirme que cette application induit un isomorphisme de groupes [10]

$$\mathrm{Pic}^0(X) \xrightarrow{\sim} J(X).$$

Nous allons montrer que, lorsque $X = X_0(N)$, tous ces objets sont munis d'une action naturelle des opérateurs de Hecke T_p compatible avec l'application d'Abel-Jacobi et avec l'isomorphisme $\mathcal{S}_2(\Gamma_0(N)) \simeq \Omega^1(\Gamma_0(N))$.

10. Ce qui confirme le fait utilisé précédemment que le groupe $\mathrm{Pic}^0(X)$ est divisible.

2.2.2 *Fonctorialité.* Soit $\pi : X \longrightarrow Y$ un morphisme non constant de surfaces de Riemann compactes. Il induit deux homomorphismes

$$\pi_* : \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}^0(Y) \text{ et } \pi^* : \mathrm{Pic}^0(Y) \longrightarrow \mathrm{Pic}^0(X)$$

définis par $\pi_*([x]) := [\pi(x)]$ et $\pi^*([y]) = \sum_{x\in\pi^{-1}(y)} e_x[x]$, où e_x désigne l'indice de ramification de π en x. Ces définitions sur Div préservent clairement Div^0. Il faut voir qu'elles préservent aussi les diviseurs principaux. Pour cela on remarque que $\pi^*(\mathrm{div}(f)) = \mathrm{div}(f \circ \pi)$ tandis que $\pi_*(\mathrm{div}(f)) = \mathrm{div}(N(f))$ où N désigne la norme de l'extension $\mathbb{C}(X)/\mathbb{C}(Y)$ (concrètement, on a $N(f)(y) = \prod_{x\in\pi^{-1}(y)} f(x)^{e_x}$).

Il induit aussi deux applications $\mathbb{C}$-linéaires

$$\pi_* : \Omega^1(X) \longrightarrow \Omega^1(Y) \text{ et } \pi^* : \Omega^1(Y) \longrightarrow \Omega^1(X).$$

On a déjà rencontré π^*, qui est simplement défini en coordonnées locales $u = \pi(z)$ par $\pi^*(f(u)du) = f(\pi(z))\pi'(z)dz$. Définir π_* est un peu plus délicat. On commence par définir $\pi_*(\omega)$ sur l'ouvert $Y' \subset Y$ au-dessus duquel π est non ramifié. Pour $y \in Y'$, on choisit un voisinage V de y tel que $\pi^{-1}(V) = \bigsqcup_{x\in\pi^{-1}(y)} U_x$ avec $\pi_{|U_x} : U_x \xrightarrow{\sim} V$. On pose alors $\pi_*(\omega)_{|V} := \sum_x (\pi_{|U_x})^{-1*}(\omega_{|U_x})$. Il faut ensuite voir que ceci se prolonge de manière holomorphe à Y. En raisonnant au voisinage d'un point de ramification on se ramène au cas où π est de la forme $z \mapsto u = z^e$ sur un disque épointé D^* en 0. On calcule alors que $\pi_*(\sum_{n\in\mathbb{N}} a_n z^n dz)_{|D^*} = \sum_{m\in\mathbb{N}} a_{e(m+1)-1} u^m du$ qui se prolonge visiblement de manière holomorphe en 0.

Enfin, on a aussi des applications

$$\pi_* : H_1(X,\mathbb{Z}) \longrightarrow H_1(Y,\mathbb{Z}) \text{ et } \pi^* : H_1(Y,\mathbb{Z}) \longrightarrow H_1(X,\mathbb{Z}).$$

L'application π_* est simplement la composition $c \mapsto \pi \circ c$ des lacets, et comme ci-dessus, l'application π^* est plus délicate. Partant d'un lacet c tracé sur Y et basé en y, on commence par le déformer pour qu'il évite le lieu de ramification. Puisque π est un isomorphisme local, pour chaque $x \in \pi^{-1}(y)$, il existe un unique chemin c_x relevant c et tel que $c_x(0) = x$. On obtient alors une permutation $x \mapsto c_x(1)$ de la fibre $\pi^{-1}(x)$. Si $x_0 \mapsto x_1 \mapsto \cdots \mapsto x_r$ est une orbite de cette permutation, alors la concaténation des c_{x_i} est un lacet tracé sur X. On définit $\pi^*(c)$ comme l'image de la somme des lacets associés à chaque orbite. On vérifie alors sur les définitions le lemme suivant.

Lemme. – *Pour un lacet c tracé sur Y et $\omega \in \Omega^1(X)$, on a $\int_{\pi^* c} \omega = \int_c \pi_*\omega$. Pour un lacet c tracé sur X et $\omega \in \Omega^1(Y)$, on a $\int_{\pi_* c} \omega = \int_c \pi^*\omega$.*

Ce lemme implique que les adjoints respectifs de π^* et π_* sur les Ω^1 induisent des morphismes

$$\pi_* : J(X) \longrightarrow J(Y) \text{ et } \pi^* : J(Y) \longrightarrow J(X).$$

Toujours sur les définitions, on vérifie aussi :

Lemme. – *Les applications d'Abel-Jacobi $\mathrm{Pic}^0 \longrightarrow J$ sont compatibles avec π_* et π^*.*

Enfin, la situation qui nous intéresse est la suivante.

LEMME. – *Supposons que $X = X(\Gamma)$ et $Y = X(\Gamma')$ avec $\Gamma \subset \Gamma'$, et notons π_Γ, resp $\pi_{\Gamma'}$ la projection de $\mathbb{H}^*$ sur $X(\Gamma)$, resp. sur $X(\Gamma')$. Alors les diagrammes suivants sont commutatifs*

$$\begin{array}{ccc} \Omega^1(X(\Gamma)) & \xrightarrow[\pi_\Gamma^*]{\sim} & \mathcal{S}_2(\Gamma) \\ {\scriptstyle \pi^*}\uparrow & & \uparrow{\scriptstyle f\mapsto f} \\ \Omega^1(X(\Gamma')) & \xrightarrow[\pi_{\Gamma'}^*]{\sim} & \mathcal{S}_2(\Gamma') \end{array} \quad et \quad \begin{array}{ccc} \Omega^1(X(\Gamma)) & \xrightarrow[\pi_\Gamma^*]{\sim} & \mathcal{S}_2(\Gamma) \\ {\scriptstyle \pi_*}\downarrow & & \downarrow{\scriptstyle f\mapsto \sum_{\gamma'\in\Gamma\backslash\Gamma'} f[\gamma']_2} \\ \Omega^1(X(\Gamma')) & \xrightarrow[\pi_{\Gamma'}^*]{\sim} & \mathcal{S}_2(\Gamma') \end{array}$$

Démonstration. Dans les diagrammes, la notation π_Γ^* est légèrement abusive, mais est là pour rappeler que l'isomorphisme $\Omega^1(X(\Gamma)) \xrightarrow{\sim} \mathcal{S}_2(\Gamma)$ est défini par $\omega \mapsto f$ où $\pi_\Gamma^*(\omega) = f(z)dz$. A partir de là, la commutativité du premier diagrammes est évidente puisque $\pi_{\Gamma'}^* = (\pi \circ \pi_\Gamma)^* = \pi_\Gamma^* \circ \pi^*$.

Pour voir la commutativité du second, partons de $\omega \in \Omega^1(X(\Gamma))$ et notons $g \in \mathcal{S}_2(\Gamma')$ telle que $\pi_{\Gamma'}^*\pi_*\omega = g(z)dz$. On veut montrer que $g = \sum_{\gamma'\in\Gamma\backslash\Gamma'} f[\gamma']_2$. Il suffit de le prouver sur l'ouvert dense des points ordinaires (i.e. hors des lieux de ramification de π, π_Γ et $\pi_{\Gamma'}$). Soit alors $y \in X(\Gamma')$ point ordinaire et $z \in \pi_{\Gamma'}^{-1}(y)$. Comme $\pi_{\Gamma'}$ est un isomorphisme local au-dessus d'un voisinage de y, il existe des voisinages V_y de y et O_z de z tels que $\pi_{\Gamma'}$ induise $O_z \xrightarrow{\sim} V_y$ et $\pi_{\Gamma'}^{-1}(V_y) = \bigsqcup_{\gamma'\in\Gamma'} \gamma' O_z$. Alors si on choisit un ensemble $\mathcal{L}$ de représentants de $\Gamma\backslash\Gamma'$, on voit que $\pi^{-1}(y) = \{\pi_\Gamma(\gamma' z),\ \gamma' \in \mathcal{L}\}$ et $\pi^{-1}(V_y) = \bigsqcup_{\gamma'\in\mathcal{L}} \pi_\Gamma(\gamma' O_z)$ avec, pour chaque γ', π qui induit un isomorphisme $\pi_\Gamma(\gamma' O_z) \xrightarrow{\sim} V_y$. De plus, puisque $\pi \circ \pi_\Gamma = \pi_{\Gamma'}$, l'inverse de cet isomorphisme vérifie

$$(*) :\ (\pi_{|\pi_\Gamma(\gamma' O_z)})^{-1} \circ \pi_{\Gamma'} = \pi_\Gamma \circ \gamma'.$$

Maintenant, par définition, on a

$$\pi_*(\omega)_{|V_y} \quad = \quad \sum_{\gamma'\in\mathcal{L}} (\pi_{|\pi_\Gamma(\gamma' O_z)})^{-1^*}(\omega_{|\pi_\Gamma(\gamma' O_z)})$$

Donc d'après $(*)$,

$$(\pi_{\Gamma'}^*(\pi_*\omega))_{|O_z} = \sum_{\gamma'\in\mathcal{L}} \gamma'^* \pi_\Gamma^*(\omega_{|\pi_\Gamma(\gamma' O_z)}),$$

et finalement

$$(g(z)dz)_{|O_z} = \sum_{\gamma'\in\mathcal{L}} \gamma'^*((f(z)dz)_{|\gamma' O_z}) = \left(\sum_{\gamma'\in\mathcal{L}} \gamma'^*(f(z)dz)\right)_{|O_z}$$

Mais $\gamma'^*(f(z)dz) = f(\gamma' z)d(\gamma' z) = f[\gamma']_2(z)dz$. □

2.2.3 *Correspondances.* Une correspondance C entre deux S.R. compactes X et X' est un diagramme

$$X \xleftarrow{\pi} Y \xrightarrow{\pi'} X'$$

dans lequel π et π' sont des morphismes non constants entre surfaces de Riemann compactes. D'après le paragraphe précédent, la correspondance C induit des homomorphismes

$$C_* := \pi'_* \circ \pi^* : \begin{cases} \Omega^1(X) \longrightarrow \Omega^1(X') \\ \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}^0(X') \\ H_1(X,\mathbb{Z}) \longrightarrow H_1(X',\mathbb{Z}) \\ J(X) \longrightarrow J(X') \end{cases}$$

compatibles avec l'accouplement d'intégration entre H_1 et Ω^1 et l'application d'Abel-Jacobi.

La situation qui nous intéresse est la suivante. Soit $X = X(\Gamma)$ pour $\Gamma \subset \Gamma(1)$ un sous-groupe de congruence, et soit $\Gamma\alpha\Gamma$ une double classe dans Δ. On lui associe la correspondance $C_{\Gamma\alpha\Gamma}$:

$$X(\Gamma) \xleftarrow{\pi^\alpha} X(\alpha^{-1}\Gamma\alpha \cap \Gamma) \xrightarrow{\pi} X(\Gamma)$$

où π^α est la composée $X(\alpha^{-1}\Gamma\alpha \cap \Gamma) \xrightarrow{\sim} X(\Gamma \cap \alpha\Gamma\alpha^{-1}) \longrightarrow X(\Gamma)$ et où le premier isomorphisme est induit par $\alpha : \mathbb{H}^* \to \mathbb{H}^*$.

Lemme. – *Le diagramme suivant est commutatif.*

$$\begin{array}{ccc} \Omega^1(X(\Gamma)) & \xrightarrow[\pi_\Gamma^*]{\sim} & \mathcal{S}_2(\Gamma) \\ {\scriptstyle C_{\Gamma\alpha\Gamma,*}}\downarrow & & \downarrow{\scriptstyle [\Gamma\alpha\Gamma]_2} \\ \Omega^1(X(\Gamma)) & \xrightarrow[\pi_\Gamma^*]{\sim} & \mathcal{S}_2(\Gamma) \end{array}$$

Démonstration. D'après le lemme précédent, l'action de $C_{\Gamma\alpha\Gamma,*}$ sur $\Omega^1(X(\Gamma))$ correspond à l'action suivante sur $\mathcal{S}_2(\Gamma)$

$$f \mapsto \sum_{\gamma \in (\alpha^{-1}\Gamma\alpha\cap\Gamma)\backslash\Gamma} (f[\alpha]_2)[\gamma]_2 = \sum_{\delta \in \Gamma\backslash(\Gamma\alpha\Gamma)} f[\delta]_2 = f[\Gamma\alpha\Gamma]_2,$$

c'est à dire à l'action de l'opérateur de Hecke $[\Gamma\alpha\Gamma]$. □

On pourrait montrer directement que l'action des $C_{\Gamma\alpha\Gamma}$ définit une action de l'anneau de Hecke $\mathbb{Z}[\Gamma\backslash\Delta/\Gamma]$ sur chacun des objets $\mathrm{Pic}^0(X(\Gamma))$, $H_1(X(\Gamma),\mathbb{Z})$ etc, du paragraphe précédent. Cependant, on peut maintenant le déduire du fait que c'est vrai sur Ω^1 par le lemme, donc sur $\Omega^{1,*}$ par passage au dual, donc sur H_1 puisque l'action y est la restricition de celle sur $\Omega^{1,*}$, et donc finalement sur J et Pic^0.

Corollaire. – *L'image* $\mathbb{T}_\Gamma$ *de* $\mathbb{Z}[\Gamma\backslash\Delta/\Gamma]$ *dans* $\mathrm{End}_{\mathbb{C}}(\mathcal{S}_2(\Gamma))$ *est un* $\mathbb{Z}$*-module de type fini.*

Démonstration. Il suffit de voir que l'image de l'anneau de Hecke dans le dual $\Omega^1(X(\Gamma))^*$ est un $\mathbb{Z}$-module de type fini. Or, l'anneau de Hecke stabilise le réseau $H_1(X,\mathbb{Z})$ donc son image est contenue dans $\mathrm{End}_{\mathbb{Z}}(H_1(X,\mathbb{Z}))$ qui est de type fini sur $\mathbb{Z}$. □

Nous spécialisons maintenant notre discussion à $\Gamma = \Gamma_0(N)$ et l'action de l'anneau de Hecke $\mathcal{H}_0(N)$. On notera $\mathbb{T}_0(N)$ son image dans $\mathrm{End}_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N)))$, qui est un anneau *commutatif*.

On rappelle qu'un système de valeurs propres $(\lambda(n)_{n\in\mathbb{N}})$ des $T(n)$ agissant sur $\mathcal{S}_2(\Gamma_0(N))$ est déterminé par les $\lambda(p)$, p premier, et détermine un *caractère* (ie un homomorphisme d'anneaux) $\lambda : \mathcal{H}_0(N) \longrightarrow \mathbb{C}$. Ce caractère se factorise par $\mathbb{T}_0(N)$ qui, par le corollaire, est de type fini comme module sur $\mathbb{Z}$. Il s'ensuit que $\mathrm{Im}(\lambda)$ est un ordre dans un corps de nombres K_λ. En d'autres termes :

Corollaire. – *Soit $f \in \mathcal{S}_2(\Gamma_0(N))$ une forme propre et normalisée pour tous les $T(n)$, $n \in \mathbb{N}$. Alors le corps K_f engendré par les coefficients $a_n(f)$, $n \in \mathbb{N}$ du q-développement de f est un corps de nombres, et les $a_n(f)$ y sont des entiers algébriques.*

Pour la suite, il est utile de comparer les systèmes de valeurs propres de $\mathcal{H}_0(N)$ dans $\mathcal{S}_2(\Gamma_0(N))$ avec ceux apparaissant dans $H_1(X_0(N),\mathbb{C})$. On utilise la notation $V[\lambda]$ pour désigner l'espace propre associé à λ sur V, *i.e.*

$$V[\lambda] = \{v \in V, \forall T \in \mathcal{H}_0(N),\, Tv = \lambda(T)v\}.$$

On utilise aussi la notation V_λ pour désigner l'espace propre généralisé associé à λ sur V, *i.e.*

$$V_\lambda = \{v \in V, \forall T \in \mathcal{H}_0(N),\, (T-\lambda(T))^n v = 0 \text{ pour } n >> 0\}.$$

Proposition. – *Pour tout caractère $\lambda : \mathcal{H}_0(N) \longrightarrow \mathbb{C}$ on a*

$$\dim_{\mathbb{C}}(H_1(X,\mathbb{C})_\lambda) = 2\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))_\lambda),$$

$$\textit{et } \dim_{\mathbb{C}}(H_1(X,\mathbb{C})[\lambda]) > \dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))[\lambda]) \textit{ si non nul.}$$

Démonstration. On a $\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))_\lambda) = \dim_{\mathbb{C}}(\Omega^1(X_0(N))_\lambda) = \dim_{\mathbb{C}}(\Omega^1(X_0(N))^*_\lambda)$. Pour voir la dernière égalité, on peut prendre une base B de $\Omega^1(X_0(N))$ dans laquelle $\mathcal{H}_0(N)$ agit de manière triangulaire (triangularisation simultanée d'une famille d'endomorphismes commutants 2 à 2). La dimension de $\Omega^1(X_0(N))_\lambda$ est alors le nombre d'occurences de λ sur la diagonale. Mais dans la base duale B^* de $\Omega^1(X_0(N))^*$, $\mathcal{H}_0(N)$ agit par des matrices triangulaires inférieures et on lit aussi la dimension de $\Omega^1(X_0(N))^*_\lambda$ sur la diagonale, qui est la même que dans B.

Par ailleurs, on sait que $H_1(X,\mathbb{Z})$ est un réseau cocompact de $\Omega^1(X_0(N))^*$, et donc l'inclusion $H_1(X,\mathbb{Z}) \hookrightarrow \Omega^1(X_0(N))^*$ induit un isomorphisme $\mathbb{R}$-linéaire

$$H_1(X,\mathbb{R}) \xrightarrow{\sim} \Omega^1(X_0(N))^*$$

et par suite un isomorphisme $\mathbb{C}$-linéaire

$$H_1(X,\mathbb{C}) \xrightarrow{\sim} \Omega^1(X_0(N))^* \oplus \overline{\Omega^1(X_0(N))^*}$$

où la notation $\overline{V}$ désigne le "conjugué" d'un espace vectoriel complexe, *i.e.* le même espace mais avec l'action de $\mathbb{C}$ conjuguée : $\forall z \in \mathbb{C}, \forall v \in \overline{V}, z \cdot v := \overline{z}v$. Bien-sûr, $\mathcal{H}_0(N)$ agit encore sur $\overline{\Omega^1(X_0(N))^*}$, et le problème est maintenant de montrer que pour tout caractère λ, on a

$$\dim_{\mathbb{C}}(\Omega^1(X_0(N))^*_\lambda) = \dim_{\mathbb{C}}(\overline{\Omega^1(X_0(N))^*}_\lambda),$$

ou encore

$$\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))_\lambda) = \dim_{\mathbb{C}}(\overline{\mathcal{S}_2(\Gamma_0(N))^*}_\lambda).$$

Remarquons que le produit hermitien de Petersson fournit un isomorphisme $\mathcal{S}_2(\Gamma_0(N)) \xrightarrow{\sim} \overline{\mathcal{S}_2(\Gamma_0(N))^*}$ par la formule $g \mapsto (f \mapsto \langle f, g\rangle)$. Mais les $T(n)$ ne sont pas tous auto-adjoints pour ce produit (seulement si $(n, N) = 1$), donc cet isomorphisme n'est pas "entièrement" compatible avec l'action de $\mathcal{H}_0(N)$. Cependant, on a aussi vu que l'adjoint de $[T(p)]_2$ est $[T(p)]_2^* = [w_N]_2 \circ [T(p)]_2 \circ [w_N^{-1}]_2$ lorsque $p|N$. Cette formule est en fait valable pour tout p car, lorsque $p \nmid N$, $[T(p)]_2$ commute à $[w_N]_2$. Il s'ensuit que l'isomorphisme

$$\mathcal{S}_2(\Gamma_0(N)) \xrightarrow{\sim} \overline{\mathcal{S}_2(\Gamma_0(N))^*},\ g \mapsto \varphi_g : (f \mapsto \langle f[w_N^{-1}]_2, g\rangle)$$

est compatible à l'action de $\mathcal{H}_0(N)$ (i.e. on a $\varphi_{g[T]_2}(f) = \varphi_g(f[T]_2)$), et par conséquent

$$\dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))_\lambda) = \dim_{\mathbb{C}}(\overline{\mathcal{S}_2(\Gamma_0(N))^*}_\lambda)$$

$$\text{et } \dim_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N))[\lambda]) = \dim_{\mathbb{C}}(\overline{\mathcal{S}_2(\Gamma_0(N))^*}[\lambda])$$

pour tout caractère $\lambda : \mathcal{H}_0(N) \longrightarrow \mathbb{C}$. On a donc prouvé l'égalité annoncée. L'inégalité s'ensuit aussi puisque, si $\dim(\Omega^1(X_0(N))[\lambda]) \neq 0$ alors $\dim(\Omega^1(X_0(N))^*_\lambda) \neq 0$ donc aussi $\dim(\Omega^1(X_0(N))^*[\lambda]) \neq 0$. □

Corollaire. – *Soit $f \in \mathcal{S}_2(\Gamma_0(N))$ primitive et λ le système de valeurs propres associé. Alors*

$$\dim_{\mathbb{C}}(H_1(X_0(N), \mathbb{C})[\lambda]) = \dim_{K_f}(H_1(X_0(N), K_f)[\lambda]) = 2.$$

Démonstration. On a vu dans ce cas que $\mathcal{S}_2(\Gamma_0(N))[\lambda] = \mathcal{S}_2(\Gamma_0(N))_\lambda$ est de dimension 1. D'après la proposition on a donc $\dim_{\mathbb{C}}(H_1(X_0(N), \mathbb{C})[\lambda]) \leqslant \dim_{\mathbb{C}}(H_1(X_0(N), \mathbb{C})_\lambda) = 2$ et aussi $\dim_{\mathbb{C}}(H_1(X_0(N), \mathbb{C})[\lambda]) > 1$. On a donc $\dim_{\mathbb{C}}(H_1(X_0(N), \mathbb{C})[\lambda]) = 2$. Comme λ est à valeurs dans le sous-corps $K_f \subset \mathbb{C}$, on a aussi $\dim_{K_f}(H_1(X_0(N), K_f)[\lambda]) = 2$. □

Continuons avec f comme dans le corollaire. Soit maintenant ℓ un premier et $\mathfrak{l} \in \mathrm{Max}(\mathcal{O}_{K_f})$ au-dessus de ℓ. Posons

$$V_f := H_1(X, K_{f,\mathfrak{l}})[\lambda].$$

Cet espace de dimension 2 sur $K_{f,\mathfrak{l}}$ est l'espace de la représentation Galoisienne que nous cherchons. Pour définir cette représentation, on utilisera le lien suivant avec Pic^0.

$$H_1(X, K_{f,\mathfrak{l}}) = \left(\varprojlim_m \mathrm{Pic}^0(X_0(N))[\ell^m]\right) \otimes_{\mathbb{Z}_\ell} K_{f,\mathfrak{l}}.$$

En effet, si on désigne par $\mathrm{Pic}^0(X)[N]$ le noyau de la multiplication par N dans Pic^0, le théorème d'Abel-Jacobi identifie $\mathrm{Pic}^0(X)[N]$ avec $N^{-1}H_1(X,\mathbb{Z})/H_1(X,\mathbb{Z}) \simeq H_1(X,\mathbb{Z}) \otimes (\mathbb{Z}/N\mathbb{Z})$, ce qui en passant à la limite projective fournit un isomorphisme

$$\lim_{\longleftarrow m} \mathrm{Pic}^0(X)[\ell^m] \simeq H_1(X,\mathbb{Z}) \otimes \mathbb{Z}_\ell = H_1(X,\mathbb{Z}_\ell).$$

On voit ainsi qu'il nous faut maintenant définir une action de Galois sur $\mathrm{Pic}^0(X_0(N)))$. Pour cela, nous devons d'abord trouver un modèle "canonique" de $X_0(N)$ comme courbe algébrique sur $\mathbb{Q}$.

2.3 Le modèle canonique de $X_0(N)$

On sait que toute surface de Riemann compacte peut être définie par des équations algébriques. Formalisons un peu ce que cela signifie.

2.3.1 *Variétés algébriques.* Soit k un corps. Une variété algébrique X sur k est un k-schéma de type fini intègre. C'est donc un espace annelé localement isomorphe au spectre d'une k-algèbre de type fini intègre. Un morphisme de variétés est un morphisme d'espaces annelés.

Une variété est *projective* si elle est isomorphe à une sous-variété fermée de $\mathbb{P}^n$ (définie par des polynômes homogènes). Une variété possède un unique point générique dont l'anneau local est le corps des fonctions rationnelles $k(X)$ de X. La *dimension* de X (au sens de la longueur d'une chaîne maximale de fermés irréductibles) est égale au degré de transcendence de $k(X)$ sur k.

Une *courbe* C sur k est une variété de dimension 1. Si k est parfait, on dit que C est *lisse* sur k si ses anneaux locaux sont des anneaux de valuation discrète. On peut montrer que toute courbe "propre" (ou "complète") est en fait projective. Un des premiers résultats de la théorie des courbes algébriques est que la correspondance

$$C \mapsto k(C)$$

établit une anti-équivalence de catégories entre courbes algébriques sur k (avec morphismes non constants) et corps de degré de transcendence 1 et finiment engendrés sur k. Voici comment on peut reconstruire une courbe C_K à partir d'un tel corps K. On prend pour espace

$$|C_K| = \{\eta\} \cup \{\text{anneaux de valuation discrète } k \subset V \subset K \text{ t.q. } \mathrm{Frac}(V) = K\},$$

où η sera le point générique. Un ensemble est déclaré ouvert s'il est le complémentaire dans C_K d'un sous-ensemble fini, mais contient η. Pour un ouvert U on pose $\mathcal{O}_{C_K}(U) = \bigcap_{V \in U} V \subset K$. On montre que c'est une algèbre de type fini sur k et un anneau de Dedekind. Le pré-faisceau $U \mapsto \mathcal{O}_{C_K}(U)$ est un faisceau qui définit donc une structure d'espace annelé sur C_K, et on vérifie que la structure induite sur U est celle de $\mathrm{Spec}(\mathcal{O}_{C_K}(U))$. Ainsi C_K est une courbe, dont on vérifie facilement qu'elle est complète.

2.3.2 *Algébrisation des tores complexes de dimension* 1. L'algébrisation d'une surface de Riemann compacte peut se faire de manière pragmatique en prenant la courbe algébrique lisse complète associée à son corps de fonctions. Mais dans le cas des tores $\mathbb{C}/\Lambda$, on peut exhiber des équations dépendant holomorphiquement de Λ. Considérons la série de la variable $x \in \mathbb{C}$

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

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 $\wp_\Lambda$ de Weierstrass en $x \in \mathbb{C}$

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

elle aussi Λ-périodique et méromorphe, mais avec des pôles d'ordre 2 en $\omega \in \Lambda$. Ainsi $\wp_\Lambda$ et $\wp'_\Lambda$ descendent en des fonctions méromorphes sur $\mathbb{C}/\Lambda$. En raisonnant sur les pôles possibles d'une fonction méromorphe générale sur $\mathbb{C}/\Lambda$, on montre que $\mathcal{M}_{\mathbb{C}/\Lambda} = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$. Avec le même genre d'idées, on montre que la fonction

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

est holomorphe, donc constante, puis nulle. Ceci donne une présentation du corps $\mathcal{M}_{\mathbb{C}/\Lambda}$ et montre que l'application

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

est un isomorphisme de $\mathbb{C}/\Lambda$ sur la surface de Riemann associée à la courbe elliptique d'équation $y^2 = 4x^3 - g_2x - g_3$. Notons que lorsqu'on fait varier Λ sous la forme $\Lambda = \Lambda_z = z\mathbb{Z} \oplus \mathbb{Z}$ avec $z \in \mathbb{H}$, on obtient une famille analytique de courbes elliptiques sur $\mathbb{H}$, tracée sur $\mathbb{H} \times \mathbb{P}^2(\mathbb{C})$, d'équation non-homogène $y^2 = 4x^3 - g_2(z) - g_3(z)$. Le discriminant de cette famille est la forme modulaire $\Delta \in \mathcal{S}_{12}(\Gamma(1))$ et son invariant j est la fonction modulaire j.

On se rappelle que $Y(1)$ paramétrise les tores complexes à isomorphisme près. On peut naturellement se demander si la famille précédente "descend" en une famille de courbes elliptiques sur $Y(1)$. On aimerait même que cette famille dépende algébriquement de la coordonnée j que l'on a sur $Y(1)$ et que la courbe E_j soit d'invariant j... Mais cela est un peu trop demander, à cause des points elliptiques, qui correspondent à des courbes ayant "trop d'automorphismes".

Restreignons-donc la famille ci-dessus au lieu ordinaire. Remarquons que c'est le lieu où $g_2 \neq 0$ et $g_3 \neq 0$ et c'est aussi le lieu où $j \neq 0, 1728$. On peut alors faire un changement de variable $(x, y) = ((g_3/g_2)x', (g_3/g_2)^{3/2}y'))$ pour mettre la famille ainsi restreinte sous la forme $E_z : y^2 = 4x^3 - \frac{27j(z)}{j(z)-1728}x - \frac{27j(z)}{j(z)-1728}$, ce qui descend manifestement en une famille

algébrique de courbes elliptiques d'équation $E_j : y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}$ sur la droite affine de coordonnée j et privée des points $j = 0, 1728$.

Comme on sait qu'une courbe elliptique est définie sur $\mathbb{Q}$ si et seulement si son invariant j est rationnel, on a justifié ainsi de choisir, comme modèle $X(1)_{\mathbb{Q}}$ de $X(1)$ sur $\mathbb{Q}$, la droite projective $\mathbb{P}^1$ de corps des fonctions $\mathbb{Q}(j)$.

2.3.3 *Algébrisation et modèle rationnel de $X_0(N)$.* Nous allons décrire le corps des fonctions méromorphes de $X_0(N)$. On sait que j définit une fonction méromorphe $j \in \mathcal{M}_{X_0(N)}$. Par un calcul déjà vu, la fonction méromorphe $j_N(z) = j(Nz) = j([\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]z)$ est aussi modulaire de niveau $\Gamma_0(N)$.

THÉORÈME. – *On a $\mathcal{M}_{X_0(N)} = \mathbb{C}(j, j_N)$. De plus, il existe un polynôme symétrique $f_N \in \mathbb{Z}[X, Y]$ tel que $f_N(X, Y) = 0$. Enfin, $f_p(X, Y) \equiv (Y - X^p)(Y^p - X)(mod\ p)$.*

Démonstration. Rappelons que l'on connait déjà le degré de $\mathcal{M}_{X_0(N)}$ sur $\mathcal{M}_{X(1)} = \mathbb{Q}(j)$ qui est égal à $[\Gamma(1) : \Gamma_0(N)]$. Choisissons un ensemble $\mathcal{L}$ de représentants de $\Gamma_0(N)\backslash\Gamma(1)$. Tout $\alpha \in \Gamma(1)$ induit une permutation $\gamma \mapsto \gamma_\alpha$ déterminée par $\Gamma_0(N)\gamma\alpha = \Gamma_0(N)\gamma_\alpha$.

Pour toute fonction $f \in \mathcal{M}_{\Gamma_0(N)}$, considérons le polynôme

$$P_f(Y) := \prod_{\gamma\in\mathcal{L}}(Y - f(\gamma z)) = \sum_{i=0}^{|\mathcal{L}|} a_i(z)Y^i.$$

Ses coefficients $a_i(z)$ sont des polynômes symmétriques en les $f(\gamma z)$, $\gamma \in \mathcal{L}$. On a donc $a_i(\alpha z) = a_i(z)$ pour tout $\alpha \in \Gamma(1)$, *i.e.* $a_i(z) \in \mathcal{M}_{\Gamma(1)} = \mathbb{C}(j)$, et ainsi $P_f \in \mathbb{C}(j)[Y]$.

D'un autre côté, considérons le polynôme minimal $Q_f(Y) = \sum_{j=0}^{r} b_j(z)Y^j$ de f sur $\mathbb{C}(j)$ (donc $b_j \in \mathbb{C}(j)$). Comme b_j est invariant par tout $\alpha \in \Gamma(1)$, on voit que les fonctions $f(\gamma z)$, $\gamma \in \mathcal{L}$, sont aussi des racines de ce polynôme. Ainsi, Q_f divise P_f dans $\mathbb{C}(j)[Y]$.

Appliquons ceci à la fonction j_N. Remarquons d'abord que les fonctions $j_N(\gamma z)$, $\gamma \in \mathcal{L}$ sont deux à deux distinctes. En effet, si $j(N\gamma z) = j(N\gamma' z)$ on sait qu'il existe $\alpha \in \Gamma(1)$ tel que $N\gamma z = \alpha N\gamma' z$ pour tout z. En prenant z dont le fixateur dans $\Gamma(1)$ est $\{\pm 1\}$ (i.e. z ordinaire), on obtient $[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]\gamma = \pm\alpha[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]\gamma'$ donc $\gamma\gamma'^{-1} = [\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]^{-1} \pm \alpha[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]$ et en particulier $\gamma\gamma'^{-1} \in \Gamma(1) \cap [\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}]^{-1}\Gamma(1)[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}] = \Gamma_0(N)$, donc $\gamma = \gamma'$. Il s'ensuit que le polynôme minimal Q_{j_N} de j_N sur $\mathbb{C}(j)$ est égal au polynôme

$$P_{j_N}(Y) = \prod_{\gamma\in\mathcal{L}}(Y - j_N(\gamma z)) \in \mathbb{C}(j)[Y].$$

Puisque son degré est égal à $[\mathcal{M}_{X_0(N)} : \mathbb{C}(j)]$, on en déduit $\mathcal{M}_{X_0(N)} = \mathbb{C}(j, j_N)$.

Maintenant, les coefficients de $P_{j_N}(Y)$ sont à la fois des fonctions rationnelles en j et des fonctions holomorphes en z. Mais puisque $j : \mathbb{H} \longrightarrow \mathbb{C}$ est surjective, cela implique que ces coefficients sont polynomiaux en j (sinon ils auraient des pôles en tant que fonctions de z). Ainsi $P_{j_N}(Y) = f_N(j, Y)$ pour un unique polynôme $f_N(X, Y) \in \mathbb{C}[X, Y]$.

Montrons la symétrie de $f_N(X, Y)$ en X, Y. On remarque qu'en changeant z en $-1/Nz$, on obtient $f_N(j(-1/Nz), j(-1/z)) = 0$, mais par $[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}]$ invariance de j, on a $j(-1/Nz) =$

$j(Nz)$ et $j(-1/z) = j(z)$, donc $f_N(j_N, j) = 0$. Comme $f_N(X,Y)$ est irréductible dans $\mathbb{C}(X)[Y]$, cela implique que $f_N(Y,X)$ est un multiple de $f_N(X,Y)$ dans $\mathbb{C}(X)[Y]$ et en fait aussi dans $\mathbb{C}[X,Y]$. Donc $f_N(Y,X) = C(X,Y)f_N(X,Y)$, ce qui implique $C(X,Y)C(Y,X) = 1$, puis $C(X,Y) = \pm 1$, mais -1 est impossible car implique $f_N(X,X) = 0$, donc $(X-Y)|f_N(X,Y)$ ce qui contredit l'irréductibilité.

Montrons que $f_N(X,Y) \in \mathbb{Q}[X,Y]$. Écrivons pour cela $f_N(X,Y) = \sum c_{i,j}X^iY^j$ avec $c_{i,j} \in \mathbb{C}$ et $c_{i,|\mathcal{L}|} = \delta_{i,0}$ (polynôme minimal, donc monique en Y). Si dans l'équation $f_N(j, j_N) = 0$ on substitue le q-développement de j, qui est à coefficients dans $\mathbb{Z}$, on obtient un système d'équations linéaires à coefficients dans $\mathbb{Z}$ qui *détermine* les $c_{m,n}$ (par unicité du polynôme minimal). Ce système a une solution dans $\mathbb{C}$ donc aussi dans $\mathbb{Q}$. Tous les $c_{m,n}$ sont donc dans $\mathbb{Q}$, et $f_N(X,Y) \in \mathbb{Q}[X,Y]$ comme voulu.

Avant de continuer, nous aurons besoin du lemme suivant.

Lemme. – *Considérons le morphisme d'anneaux*

$$\mathbb{C}[X,Y] \longrightarrow \mathbb{C}[[q]][q^{-1}][Y],\ f(X,Y) \mapsto f(j,Y),$$

où j est envoyé sur son q-développement $j(z) = q^{-1} + \sum_{n\in\mathbb{N}} c_n q^n$. Si $\mathcal{I}$ est un sous-groupe additif stable par multiplication de $\mathbb{C}$, alors

$$f(j,Y) \in \mathcal{I}[[q]][q^{-1}][Y] \Rightarrow f(X,Y) \in \mathcal{I}[X,Y].$$

Démonstration. Ecrivons $f(X,Y) = \sum_i a_i(X)Y^i$, puis $a_i(X) = \sum_k a_{ik}X^k$. Le coefficient de $q^{-k}Y^i$ dans $f(j,Y)$ appartient à $a_{ik} + \mathbb{Z}[a_{i,k'}]_{k'>k}$. Supposons que $f(X,Y) \notin \mathcal{I}[X,Y]$ et soit $a_{ik} \notin \mathcal{I}$ avec k maximal. Alors le coefficient de $q^{-k}Y^i$ dans $f(j,Y)$ est dans $a_{ik} + \mathcal{I}$ donc n'est pas dans $\mathcal{I}$. Contradiction. □

Maintenant, du fait que le q-développement de j est à coefficients entiers, on déduit que pour tout $\gamma \in \mathcal{L}$, $j_N(\gamma z)$ a un q_N-développement à coefficients dans $\mathbb{Z}[e^{2i\pi/N}]$. Pour cela, on utilise le lemme 1.3.2 qui nous dit que $\Gamma(1)\left[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right]\gamma$ contient une (unique) matrice $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ telle que $ad = N$ et $b < d$. On a alors $j_N(\gamma z) = j(\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]z)$, et on utilise le q-developpement de j pour constater que le q_N-développement de $j_N(\gamma z)$ est comme annoncé. Il s'ensuit que $f_N(j,Y) \in \mathbb{Z}[e^{2i\pi/N}][[q]][q^{-1}][Y]$ et, par le lemme, que $f_N(X,Y) \in \mathbb{Z}[e^{2i\pi/N}][X,Y]$. Joint au fait que $f_N(X,Y) \in \mathbb{Q}[X,Y]$, on en déduit que

$$f_N(X,Y) \in \mathbb{Z}[X,Y].$$

Finalement, supposons $N = p$. En se rappelant l'ensemble $\mathcal{L}(\Gamma(1)\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]\Gamma(1)$ de 1.3.2, on voit que

$$f_N(j,Y) = (Y - j(pz)) \prod_{m=0}^{p-1} \left(Y - j(\frac{z+m}{p})\right).$$

On a vu que le q_p développement de $j(\frac{z+m}{p})$ est dans $\mathbb{Z}[e^{2i\pi/p}]$. En fait, tous ces développements sont congrus modulo l'idéal $\mathfrak{p} = (1 - e^{2i\pi/p})$ de $\mathbb{Z}[e^{2i\pi/p}]$, et donc en particulier congrus

à celui de $j_{p^{-1}}(z) = j(z/p)$. En d'autres termes, on a dans l'anneau $\mathbb{Z}[e^{2i\pi/p}][[q_p]][q_p^{-1}][Y]$ la congruence

$$f_N(j, Y) \equiv (Y - j_p)\,(Y - j_{p^{-1}})^p \mod \mathfrak{p}.$$

Comme les deux côtés sont dans l'anneau $\mathbb{Z}[[q_p]][q_p^{-1}][Y]$, on a aussi la même congruence modulo p dans ce dernier anneau. Or, on a aussi les congruences $j_p \equiv j^p$ et $(j_{p^{-1}})^p \equiv j$ modulo (p) dans l'anneau $\mathbb{Z}[[q_p]][q_p^{-1}]$. On en déduit la congruence $f_N(j, Y) \equiv (Y - j^p)(Y^p - j)$ dans l'anneau $\mathbb{Z}[[q_p]][q_p^{-1}][Y]$, et puisque ces deux éléments vivent dans $\mathbb{Z}[[q][q^{-1}][Y]$, on a simplement

$$(f_N(j, Y) - (Y - j^p)(Y^p - j)) \in p\mathbb{Z}[[q][q^{-1}][Y].$$

Il s'agit maintenant d'en déduire que

$$f_N(X, Y) - (Y - X^p)(Y^p - X) \in p\mathbb{Z}[X, Y].$$

Mais cela découle du lemme ci-dessus avec $\mathcal{I} = p\mathbb{Z}$. □

Ceci nous suggère un joli modèle sur $\mathbb{Q}$:

Définition. – *On définit la courbe modulaire $X_0(N)_{\mathbb{Q}}$ sur $\mathbb{Q}$ comme la courbe algébrique complète dont le corps des fonctions rationnelles est*

$$\mathbb{Q}(j, j_N) := \mathbb{Q}(j)[j_N]/((f_N(j, j_N)).$$

Avec cette définition, on retrouve $X_0(N)$ comme S.R. associée à la courbe algébrique complexe obtenue par extension des scalaires de $X_0(N)_{\mathbb{Q}}$ de $\mathbb{Q}$ à $\mathbb{C}$. On voit aussi que la projection $X_0(N) \longrightarrow X(1)$ provient d'un morphisme de variétés $X_0(N)_{\mathbb{Q}} \longrightarrow X(1)_{\mathbb{Q}}$.

2.3.4 *L'action de Galois sur* $\mathrm{Pic}^0(X_0(N))[\ell^m]$. Soit $X_0(N)_{\overline{\mathbb{Q}}}$ l'extension des scalaires de $X_0(N)_{\mathbb{Q}}$ à $\overline{\mathbb{Q}}$. On définit la notion de diviseur exactement comme dans le cas des S.R. Un diviseur est donc une somme $\sum_P a_P[P]$ de points fermés de $X_0(N)_{\overline{\mathbb{Q}}}$. De même on a la notion de diviseur principal (grâce au fait que les anneaux locaux sont de valuation discrète, ce qui permet de définir $\mathrm{ord}_P(f)$ pour f fonction rationnelle), puis la notion de Pic et Pic^0.

On peut associer à toute courbe lisse complète C sur un corps k sa variété Jacobienne, qui est une variété abélienne dont les points à valeurs dans $\overline{k}$ s'identifient à $\mathrm{Pic}^0(C_{\overline{k}})$. Les seules conséquences qui nous intéressent de ce fait général, mais difficile, sont les suivantes :

i) on a $\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}}) \subset \mathrm{Pic}^0(X_0(N))$,

ii) pour tout entier M, on a $\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}})[M] = \mathrm{Pic}^0(X_0(N))[M]$.

Autrement dit, les points de torsion de Pic^0, a priori complexes, sont "définis" sur $\overline{\mathbb{Q}}$. Mais, ce que nous avons gagné maintenant, c'est une action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur ces points de torsion. En effet, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur les points fermés de $X_0(N)_{\overline{\mathbb{Q}}}$, donc sur les diviseurs, préserve clairement les diviseurs principaux, et donc agit sur $\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}})$. Cette action est compatible avec la loi de groupe, donc elle stabilise les points de M-torsion.

Il nous faut maintenant vérifier que cette action de Galois est compatible avec l'action de l'anneau de Hecke.

2.3.5 *Modèle rationnel des correspondances de Hecke.* Rappelons que l'action de $T(p)$ est celle de la double classe $\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\Gamma_0(N)$. Géométriquement, on a vu que l'action sur $\mathrm{Pic}^0(X_0(N))$ est celle induite par la correspondance

$$X_0(N) \xleftarrow{\pi^p} X_0(N,p) \xrightarrow{\pi} X_0(N)$$

où $X_0(N,p) = X(\Gamma_0(N) \cap \left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]^{-1}\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right])$, π est la projection canonique, et π^p est la compositition de la projection canonique avec l'action de $\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]$ qui induit un isomorphisme $X(\Gamma_0(N) \cap \left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]^{-1}\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]) \xrightarrow{\sim} X(\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]^{-1} \cap \Gamma_0(N))$. On sait que le corps des fonctions de $X_0(N)$ est $\mathbb{C}(j, j_N)$. On en déduit que celui de $X(\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]^{-1}\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right])$ est $\mathbb{C}(j_{p^{-1}}, j_{Np^{-1}})$ (noter que $j_{p^{-1}} = j\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]_0$ est modulaire pour $\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]^{-1}\Gamma_0(N)\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]$), puis par composition des corps, que $\mathcal{M}_{X_0(N,p)} = \mathbb{C}(j, j_N, j_{p^{-1}}, j_{Np^{-1}})$. On constate alors que, en termes de corps de fonctions, la correspondance précédente est donnée par

$$\mathbb{C}(j, j_N) \xrightarrow{\iota^p} \mathbb{C}(j, j_N, j_{p^{-1}}, j_{Np^{-1}}) \xleftarrow{\iota} \mathbb{C}(j, j_N)$$

où ι est l'inclusion canonique donnée par $j \mapsto j$ et $j_N \mapsto j_N$ tandis que ι^p est donnée par $j \mapsto j_{p^{-1}}$ et $j_N \mapsto j_{Np^{-1}}$. Mais il est maintenant clair que les mêmes applications induisent un diagramme

$$\mathbb{Q}(j, j_N) \xrightarrow{\iota^p} \mathbb{Q}(j, j_N, j_{p^{-1}}, j_{Np^{-1}}) \xleftarrow{\iota} \mathbb{Q}(j, j_N)$$

qui définit un modèle sur $\mathbb{Q}$ de la correspondance $T(p)$, c'est à dire une correspondance algébrique

$$X_0(N)_{\mathbb{Q}} \xleftarrow{\pi^p} X_0(N,p)_{\mathbb{Q}} \xrightarrow{\pi} X_0(N)_{\mathbb{Q}}$$

qui redonne la précédente après extension des scalaires et passage aux S.R. Ainsi l'action de $T(p)$ sur $\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}}$ est induite par la même formule $\pi_* \circ \pi^{p,*}$ qu'au niveau des S.R., laquelle commute maintenant clairement à l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

2.4 Relations d'Eichler-Shimura

Pour terminer la construction de la représentation ρ_f associée à $f \in \mathcal{S}_2(\Gamma_0(N))$, nous devons comparer l'action de $T(p)$ à celle d'une substitution de Frobenius σ_p, au moins pour tous les premiers p en dehors d'un nombre fini. Le théorème que nous avons en vue est le suivant :

2.4.1 Théorème.– *Pour p premier ne divisant pas ℓN, l'action de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *sur le groupe* $\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}})[\ell^m]$ *est non ramifiée et pour toute substitution de Frobenius σ_p en p, on a l'égalité*

$$T(p) = \sigma_p + p\sigma_p^{-1}$$

dans $\mathrm{End}(\mathrm{Pic}^0(X_0(N)_{\overline{\mathbb{Q}}})[\ell^m])$.

La preuve utilise la réduction modulo p de la courbe modulaire $X_0(N)$ et utilise quelques faits généraux sur les Jacobiennes.

2.4.2 *Courbes sur $\mathbb{F}_p$.* Soit C une courbe propre et lisse sur $\mathbb{F}_p$, telle que son extension $C_{\overline{\mathbb{F}}_p}$ soit encore une courbe propre et lisse (la seule chose qui peut manquer est la connexité ; en d'autres termes, on veut que la clôture algébrique de $\mathbb{F}_p$ dans $\mathbb{F}_p(C)$ soit $\mathbb{F}_p$). Comme précédemment, on peut considérer $\mathrm{Pic}^0(C_{\overline{\mathbb{F}}_p})$, qui est muni d'une action de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, et s'identifie aux $\overline{\mathbb{F}}_p$-points de la variété Jacobienne de C. Nous noterons σ_p le générateur habituel $x \mapsto x^p$ de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

On dispose sur le corps $\mathbb{F}_p(C)$ de l'endomorphisme de Frobenius $F^* : f \mapsto f^p$. Celui-ci, par extension des scalaires induit un endomorphisme $\mathrm{id} \otimes F^*$ de l'anneau $\overline{\mathbb{F}}_p \otimes_{\mathbb{F}_p} \mathbb{F}_p(C)$ qui s'étend à son corps de fractions $\overline{\mathbb{F}}_p(C)$ et est appelé "Frobenius géométrique". Attention, ce dernier n'est plus donné par $f \mapsto f^p$ (le "Frobenius absolu"), puisqu'il est $\overline{\mathbb{F}}_p$-linéaire. Nous avons plutôt une factorisation

$$(\mathrm{id} \otimes F^*)(\sigma_p \otimes \mathrm{id}) = \text{ Frobenius absolu sur } \overline{\mathbb{F}}_p(C).$$

Nous noterons par $F : C_{\overline{\mathbb{F}}_p} \longrightarrow C_{\overline{\mathbb{F}}_p}$ l'"endomorphisme de Frobenius géométrique" obtenu par dualité corps/courbe. Au niveau des points fermés de $C_{\overline{\mathbb{F}}_p}$, le Frobenius absolu agit trivialement et donc le Frobenius relatif agit comme le générateur σ_p du groupe de Galois. Concrètement, si C est plongée dans $\mathbb{P}^r_{\overline{\mathbb{F}}_p}$, on a $F([x_0, \cdots, x_r]) = [x_0^p, \cdots, x_r^p]$. Par contre, bien que F induise une permutation des points fermés, ce n'est pas un automorphisme ; il est ramifié (et même inséparable) de degré p en tout point.

L'endomorphisme F induit, comme tout morphisme de courbes algébriques non constant, deux endomorphismes

$$F_* \text{ et } F^* \in \mathrm{End}\,(\mathrm{Pic}^0(C_{\overline{\mathbb{F}}_p})).$$

Par ce qui précède, on peut comparer leur action à celle de Galois :

$$F_* = \sigma_p \text{ et } F^* = p\sigma_p^{-1}.$$

2.4.3 *Réduction des courbes.* Soit C une courbe lisse projective sur $\mathbb{Q}$ et p un premier. Un modèle $\mathcal{C}$ de C sur le localisé $\mathbb{Z}_{(p)}$ est un schéma plat sur $\mathbb{Z}_{(p)}$ tel que $\mathcal{C}_{\mathbb{Q}} := \mathcal{C} \times_{\mathrm{Spec}(\mathbb{Z}_{(p)})} \mathrm{Spec}(\mathbb{Q}) \simeq C$. On dit que c'est un bon modèle si la réduction $\mathcal{C}_{\mathbb{F}_p} := \mathcal{C} \times_{\mathrm{Spec}(\mathbb{Z}_{(p)})} \mathrm{Spec}(\mathbb{F}_p)$ est une courbe lisse. Concrètement, pour trouver un modèle, on peut définir C dans $\mathbb{P}^r$ par des polynômes homogènes à coefficients dans $\mathbb{Z}_{(p)}$. La réduction $\mathcal{C}_{\mathbb{F}_p}$ est alors définie par les même polynômes vus modulo p. Mais trouver un bon modèle est plus difficile. Parfois il n'en existe pas. On dit que C a bonne réduction s'il en existe un.

Dans ce cas, l'application de réduction $\mathbb{P}^r(\mathbb{Q}) \longrightarrow \mathbb{P}^r(\mathbb{F}_p)$ (noter qu'on peut chasser les dénominateurs en coordonnées homogènes) induit une application des $\mathbb{Q}$-points de C sur les $\mathbb{F}_p$-points de $\mathcal{C}_{\mathbb{F}_p}$. Plus généralement, si $\mathfrak{p}$ est un idéal maximal de $\overline{\mathbb{Z}}$ au-dessus de p, alors la réduction modulo $\mathfrak{p}$ induit une application

$$C(\overline{\mathbb{Q}}) \longrightarrow \mathcal{C}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p).$$

Cette application se prolonge par linéarité aux diviseurs. On peut alors montrer les propriétés suivantes (toujours sous l'hypothèse de bonne réduction) :

i) L'application de réduction mod $\mathfrak{p}$ induit un épimorphisme $\mathrm{Pic}^0(C_{\overline{\mathbb{Q}}}) \longrightarrow \mathrm{Pic}^0(C_{\overline{\mathbb{F}}_p})$.

ii) Pour $\ell \neq p$, elle induit un isomorphisme $\mathrm{Pic}^0(C_{\overline{\mathbb{Q}}})[\ell^m] \xrightarrow{\sim} \mathrm{Pic}^0(C_{\overline{\mathbb{F}}_p})[\ell^m]$.

2.4.4 *Réduction de la courbe modulaire $X_0(N)_{\mathbb{Q}}$.* On peut montrer que $X_0(N)$ a bonne réduction en tout $p \nmid N$. Cela semble difficile à voir sur l'équation "modulaire" $f_N(X,Y)$ qu'on a obtenue. On le montre plutôt en utilisant une interprétation modulaire de $X_0(N)$ comme paramétrisant des courbes elliptiques munies de sous-groupes d'ordre p. Comme nous n'avons pas le temps de discuter cela, on se contentera de remarquer qu'une courbe sur $\mathbb{Q}$ a toujours bonne réduction en dehors d'un nombre fini de premiers. Soit p un tel premier. Alors le corps des fonctions de la réduction $X_0(N)_{\mathbb{F}_p}$ peut être défini sur $\mathbb{F}_p(j)$ par la même équation $f_N(X,Y)$ réduite modulo p, i.e. $\mathbb{F}_p(X_0(N)_{\mathbb{F}_p}) = \mathbb{F}_p(j)[Y]/(f_N(j,Y))$.

On veut comprendre $T(p)$ en termes de F_* et F^*. La correspondance $T(p)$ fait intervenir $X_0(N,p)$, qui malheureusement n'a pas bonne réduction en p. Cependant, l'équation f_p qui lie $j(z)$ et $j(p^{-1}z)$ a une réduction intéressante donnée par le théorème 2.3.3.

Faisons $N = 1$ pour simplifier la discussion et essayons de comprendre la correspondance

$$X(1)_{\mathbb{F}_p} \xleftarrow{\pi^p} X_0(1,p)_{\mathbb{F}_p} \xrightarrow{\pi} X(1)_{\mathbb{F}_p}$$

au moins génériquement, c'est-à-dire sur les anneaux totaux de fractions. D'après le théorème 2.3.3 on a "dualement"

$$\mathbb{F}_p(j) \longrightarrow \mathbb{F}_p(j)[Y]/(Y^p - j)(Y - j^p) \longleftarrow \mathbb{F}_p(j).$$

ou encore

$$\mathbb{F}_p(j) \longrightarrow \mathbb{F}_p(j)[Y]/(Y^p - j) \times \mathbb{F}_p(j)/(Y - j^p) \longleftarrow \mathbb{F}_p(j).$$

et finalement

$$\mathbb{F}_p(j) \longrightarrow \mathbb{F}_p(j^{1/p}) \times \mathbb{F}_p(j) \longleftarrow \mathbb{F}_p(j).$$

Dans ce diagramme la flèche de droite envoie j sur (j,j), alors que la flèche de gauche envoie j sur $(Y,Y) = (j^{1/p}, j^p)$. Un diagramme similaire pour $X_0(N)$ montre que, génériquement, la correspondance est de la forme :

$$X_0(N)_{\mathbb{F}_p} \xleftarrow{\mathrm{id} \cup F} X_0(N)_{\mathbb{F}_p} \bigcup X_0(N)_{\mathbb{F}_p} \xrightarrow{F \cup \mathrm{id}} X_0(N)_{\mathbb{F}_p}.$$

Ici par génériquement, on entend que la situation est vraiment comme décrit (avec union disjointe), au-dessus d'un ouvert de $X_0(N)_{\mathbb{F}_p}$. Mais la réduction de $X_0(N,p)$ "en entier" est une réunion non-disjointe de deux copies de $X_0(N)_{\mathbb{F}_p}$.

Nous admettrons que cette situation générique suffit à montrer que la correspondance $T(p)$ coincide avec $(F \cup \mathrm{id})_* \circ (\mathrm{id} \cup F)^* = F + F^*$, ce qui finit de prouver (ou plutôt d'expliquer) la relation d'Eichler-Shimura.