Université Joseph FOURIER
Institut FOURIER
URA 188 du CNRS

FORMES MODULAIRES ET COURBES ELLIPTIQUES

d'après le cours de
DEA de Mathématiques
d' Alexeï PANCHISHKIN
1993-94

Claude MOSER

Chapitre 0.

Visite guidée: la fonction τ de Ramanujan et son contexte.

Comme son titre veut l'indiquer, ce cours traitera des formes modulaires et de leur application à l'étude des courbes elliptiques. L'idée de ce chapitre initial est de se promener un peu dans le jardin de l'arithmétique en se laissant conduire par l'exemple séduisant des propriétés de la fonction τ de Ramanujan.

Cet exemple célèbre commence par la définition d'une première forme modulaire associée à la série génératrice de la fonction τ on commence par considérer la série obtenue comme développement en série entière du produit infini

$$q\prod_{m\geq 1}(1-q^m)^{24}=\sum_{n\geq 1}\tau(n)q^n=q-24q^2+252q^3-1472q^4+\cdots$$

Posant $q=\exp(2i\pi z)$ pour z appartenant au demi-plan de Poincaré $\mathcal{H}=\{z\in\mathbf{C}\mid \mathrm{Im}(z)>0\}$, on réalise une surjection $q:\mathcal{H}\to D(0,1)\backslash\{0\}$, holomorphe sur $\mathcal{H}$, à valeurs dans le disque unité ouvert privé de son centre.

On définit la fonction $\Delta:\mathcal{H}\to\mathbf{C}$, holomorphe sur $\mathcal{H}$, par l'écriture:

$$\Delta(z)=\tilde{\Delta}(q)=q\prod_{m\geq 1}(1-q^m)^{24}$$

Cette fonction est la forme modulaire cherchée. Elle a les propriétés remarquables suivantes:

0.1 Automorphie. Le groupe SL(2,$\mathbf{Z}$) des matrices carrées d'ordre 2 à coefficients entiers rationnels et de déterminant 1 opère sur le demi-plan de Poincaré par

$$\left(\begin{pmatrix}a&b\\c&d\end{pmatrix},z\right)\mapsto\frac{az+b}{cz+d}.$$

Le groupe SL(2,$\mathbf{Z}$) est engendré par les deux matrices $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ et $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ Pour s'en rendre compte on peut utiliser l'algorithme de la division euclidienne sur le couple (a,b) et des produits par une puissance de S, laquelle est d'ordre 4.

La propriété d'automorphie s'énonce sous la forme

$$\forall\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}(2,\mathbf{Z}),\ \forall z\in\mathcal{H}\Rightarrow\Delta(\gamma\cdot z)=(cz+d)^{12}\Delta(z).$$

Remarques. Il est parfois utile de se servir de la convention d'écriture suivante. Pour tout $\gamma\in\mathrm{SL}(2,\mathbf{Z})$, et pour tout $z\in\mathcal{H}$, on a

$$\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\Rightarrow d(\gamma\cdot z)=(cz+d)^{-2}dz$$

On peut dire formellement que $\Delta(z)(dz)^6$ est invariante par l'action de SL(2,**Z**).

0.2. Multiplicativité. La fonction τ de Ramanujan est multiplicative au sens suivant [dans la formule ci-dessous et dorénavant, **P** désigne l'ensemble des nombres premiers]:

$$\begin{cases} \forall m \in \mathbf{N}^*,\ \forall n \in \mathbf{N}^*,\ (m,n)=1 \Rightarrow \tau(mn) = \tau(m)\cdot\tau(n); \\ \forall p \in \mathbf{P},\ \forall r \in \mathbf{N}^*,\ \tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1}); \\ \forall m \in \mathbf{N}^*,\ \forall n \in \mathbf{N}^*,\ \tau(mn) = \displaystyle\prod_{d|(m,n)} \tau(mn/d^2). \end{cases}$$

Cette dernière formule fut conjecturée par Ramanujan puis démontrée par Hecke. Il se peut qu'il n'existe pas de preuve "élémentaire" au sens de l'arithmétique de Gödel de cette formule. Il en est ici comme de la démonstration hautement "non-élémentaire" de la preuve de l'énoncé de Fermat que Wiles a donnée en juin 1993 [laquelle utilise des fonctions modulaires, de l'analyse p-adique, la théorie des déformations des représentations galoisiennes, de la géométrie algébrique, la théorie des faisceaux étales ...].

Une interprétation comode de la formule générale de Ramanujan à partir de la précédente repose sur l'utilisation de la série de Dirichlet formelle associée à la fonction τ:

$$L(\Delta,s) = \sum_{n\geq 1} \tau(n)n^{-s} = \prod_{p\in\mathbf{P}} \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}.$$

Cette série est analogue à la série de Dirichlet de la fonction zeta de Riemann,

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_{p\in\mathbf{P}} \left(1 - p^{-s}\right)^{-1},$$

où l'égalité résulte simplement de l'existence et de l'unicité de la décomposition primaire de tout entier naturel non nul.

De même dans le cas de la fonction τ de Ramanujan, on a l'égalité

$$\sum_{n\geq 1} \tau(n)n^{-s} = \prod_{p\in\mathbf{P}} \left(\sum_{r\geq 0} \tau(p^r)p^{-rs} \right)$$

et on vérifie l'identité résultant de la seconde formule ci-dessus:

$$\left(1 - \tau(p)p^{-s} + p^{11-2s}\right)\cdot \left(\sum_{r\geq 0} \tau(p^r)p^{-rs} \right) = 1$$

0.3. Estimations. La propriété ci-après, conjecturée initialement par Ramanujan, fut prouvée par Deligne:

$$\forall p \in \mathbf{P},\ |\tau(p)| < 2p^{11/2}.$$

Cette propriété est équivalente à la négativité stricte du discriminant du polynôme du second degré $X^2 - \tau(p)X + p^{11}$, ceci pour tout nombre premier p. Pour p fixé, soient α_p et β_p les zéros complexes conjugués de ce polynôme. La formule de multiplicativité ci-dessus implique l'identité entre fractions rationnelles et série formelle:

$$\frac{1}{(1-\tau(p)X+p^{11}X^2)}=\frac{1}{(1-\alpha_pX)(1-\beta_pX)}=\left(\sum_{r\geq 0}\tau(p^r)X^r\right).$$

On en déduit pour tout $r\geq 1$ la relation $\tau(p^r)=\sum_{j=0}^{r}\alpha_p^j\beta_p^{r-j}=\sum_{j=0}^{r}\alpha_p^{2j-r}p^{11(r-j)}$. Le module de α_p est $p^{11/2}$, ce qui implique la majoration

$$|\tau(p^r)|<(r+1)p^{11r/2}.$$

Appliquant la formule générale de Ramanujan, on obtient l'estimation

$$\forall n\in\mathbf{N}^*,\ \ |\tau(n)|<\sigma_0(n)n^{11/2}=O(n^{\frac{11}{2}+\varepsilon})$$

où $\sigma_0(n)$, le nombre des diviseurs de n, est $O(\ln(n))=O(n^\varepsilon)$ pour tout $\varepsilon>0$.

On en conclut en particulier que la série $L(\Delta,s)$ définit une fonction holomorphe dans le demi-plan $\mathrm{Re}(s)>13/2$.

0.4. Equation fonctionnelle de $L(\Delta,s)$. On définit la fonction $L^*(\Delta,s)$ par la formule $L^*(\Delta,s)=(2\pi)^{-s}\Gamma(s)L(\Delta,s)$. Cette fonction, d'une part se prolonge en une fonction holomorphe sur $\mathbf{C}$ tout entier, d'autre part satisfait à l'équation fonctionnelle $L^*(\Delta,12-s)=L^*(\Delta,s)$. Cette relation fonctionnelle peut être comparée avec l'équation fonctionnelle de la fonction $\zeta(s)$ de Riemann:

$$\zeta^*(s)=\pi^{-s/2}\Gamma(s/2)\zeta(s)=\zeta(1-s).$$

0.5. Lien avec les partitions d'entiers. On appelle partition d'un entier n une séquence croissante d'entiers naturels non nuls dont la somme est n. On désigne par $p:\mathbf{N}\to\mathbf{N}$ la fonction nombre de partitions, avec $p(0)=1$. La série génératrice de la fonction $p:\mathbf{N}\to\mathbf{N}$ est obtenue à partir d'un produit infini $\sum_{n\geq 0}p(n)X^n=\prod_{m\geq 1}(1-X^m)^{-1}$. La série entière correspondante est convergente dans le disque unité ouvert. On obtient donc une fonction holomorphe sur $\mathcal{H}$, $f:\mathcal{H}\to\mathbf{C}$ en posant

$$f(q)=\sum_{n\geq 0}p(n)q^n=\prod_{m\geq 1}(1-q^m)^{-1}.$$

On a évidemment $\tilde{\Delta}(q)=q(f(q))^{-24}$ ce qui établit le lien entre la fonction de partition et la fonction τ de Ramanujan. En utilisant les propriétés d'automorphie 0.1, Hardy et Ramanujan ont démontré l'estimation de $p(n)$

$$p(n)=\left(\frac{1}{4\sqrt{3}}+O\left(\frac{1}{\lambda(n)}\right)\right)\cdot\frac{\exp(K\cdot\lambda(n))}{\lambda(n)^2}$$

où $\lambda(n)=\sqrt{n-\frac{1}{2}}$ et $K=\pi\sqrt{2/3}$.

0.6. Congruences de Ramanujan. Pour tout nombre premier p différent de 691 on a la relation de congruence $\tau(p) \equiv 1 + p^{11} \bmod 691$, d'où on déduit d'après la relation de multiplicativité, en raisonnant par récurrence sur r, la relation de congruence

$$\tau(p^{r+1}) \equiv \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1}) \equiv \sum_{j=0}^{r+1} p^{11j} \bmod 691,$$

puis la relation de congruence plus générale:

$$\forall n \in \mathbf{Z}^+, \ \tau(n) \equiv \sum_{d|n} d^{11} \bmod 691.$$

Serre donne de cette relation de congruence une interprétation dans le cadre de la théorie de Galois. Soit $\bar{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Soient p un nombre premier différent de 691 et $\mathfrak{p}$ un idéal premier au-dessus de (p) dans l'anneau $\mathcal{O}$ des entiers de $\bar{\mathbf{Q}}$. Soient $G_\mathfrak{p}$ et $I_\mathfrak{p}$ les sous-groupes du groupe $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ respectivement définis par

$$G_\mathfrak{p} = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\} \text{ et } I_\mathfrak{p} = \{\sigma \in G \mid \forall x \in \mathcal{O}, \ \sigma x \equiv x \bmod \mathfrak{p}\}.$$

Le groupe $G_\mathfrak{p}$ s'identifie au groupe de Galois de la clôture algébrique $\bar{\mathbf{Q}}_p$ du corps $\mathbf{Q}_p$ des nombres p-adiques, tandis que le groupe $I_\mathfrak{p}$ s'identifie au groupe de Galois de la clôture algébrique du corps fini $\mathbf{F}_p$.

Serre a conjecturé, et Deligne a démontré, que pour tout nombre premier l, il existe une représentation galoisienne $\rho_l : G \to \mathrm{GL}(2, \mathbf{Z}_l)$ telle que pour tout nombre premier p différent de l, d'une part le groupe $I_\mathfrak{p}$ agit trivialement (on dit que la représentation ρ_l est non ramifiée en p), d'autre part on a $\det(\mathrm{Id} - \rho_l(Fr_p) \cdot X) = 1 + \tau(p)X + p^{11}X^2$. Dans le cas $l = 691$ on a la congruence $\rho_l(Fr_p) \equiv \begin{pmatrix} p^{11} & * \\ 0 & 1 \end{pmatrix} \bmod 691$, d'où $\tau(p) \equiv 1 + p^{11} \bmod 691$.

0.7. Formules de Manin. En partant de la démonstration des congruences de Ramanujan décrites plus haut, et en utilisant la théorie des symboles modulaires, Manin a démontré des formules qui permettent de calculer les $\tau(n)$ beaucoup plus rapidement que par le biais du produit infini. Ces formules sont les suivantes:

$$\tau(n) = \sigma_{11}(n) - \sum_{*(n)} \left(\frac{691}{18}(\Delta^8\delta^2 - \Delta^2\delta^8) + \frac{691}{6}(\Delta^6\delta^4 - \Delta^4\delta^6) \right);$$

$$\tau(n) = \sigma_{11}(n) - \frac{691}{18} \sum_{*(n)} \Delta^2\delta^2(\Delta^2 - \delta^2)^3$$

où $\sigma_{11}(n) = \sum_{d|n} d^{11}$ et la somme ci-dessus porte sur toute les décompositions "admissibbles" $n = \Delta\Delta' + \delta\delta'$, i.e.

$$\big\{(\Delta, \delta)\big| n = \Delta\Delta' + \delta\delta',\ \Delta > \delta > 0,\ \Delta' > \delta' > 0,\ \text{ou}$$
$$\Delta | n,\ \Delta' = \frac{n}{\Delta},\ \delta' = 0,\ 0 < \frac{\delta}{\Delta} \leq \frac{1}{2}\big\}.$$

Cette formule nous donne une autre démonstration de la congruence de Ramanujan ci-dessus.

Chapitre 1.
Espaces de Formes modulaires.

Ce chapitre consiste en une première introduction à la théorie des formes modulaires, considérées comme séries de Fourier ou comme fonctions de réseaux. Il a aussi pour objet de relier ces fonctions avec les objets utilisés aujourd'hui en arithmétique. Sans trop insister pour le moment sur certaines démonstrations, on s'est attaché à donner des exemples susceptibles de motiver les études plus approfondies qui suivront.

Notations.
$\mathcal{H}$ - le demi-plan de Poincaré, ensemble des nombres complexes de partie imaginaire strictement positive.
$Z(G)$ - le centre du groupe G.
$\mathrm{GL}(2, A)$ - le groupe des matrices carrées inversibles à coefficients dans un anneau commutatif A.
$\mathrm{SL}(2, A)$ - le sous-groupe de $\mathrm{GL}(2, A)$, le noyau du déterminant.
$\mathrm{SO}(2,\mathbf{R})$ -le sous-groupe des matrices orthogonales de $SL(2, \mathbf{R})$.

1.1 Action de $\mathrm{GL}^+(2, \mathbf{R})$ sur le demi-plan de Poincaré.

On définit $\mathrm{GL}^+(2, \mathbf{R})$ comme le sous-groupe de $\mathrm{GL}(2,\mathbf{R})$ dont les éléments sont de déterminant positif. Ce groupe opère naturellement à gauche sur $\mathcal{H}$ par

$$\forall z \in \mathcal{H},\ \forall \gamma \in \mathrm{GL}^+(2, \mathbf{R}),\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \gamma \cdot z = \frac{az+b}{cz+d}$$

Cette opération est transitive. Comme espace homogène de $\mathrm{GL}^+(2, R)$, $\mathcal{H}$ s'identifie au quotient $\mathrm{GL}(2, \mathbf{R})/Z(\mathrm{SO}(2, \mathbf{R}))$.

1.1.1. Lemme. Avec les notations ci-dessus, on a les deux identités

$$\forall z \in \mathcal{H},\ \forall \gamma \in \mathrm{GL}^+(2, \mathbf{R}),\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \mathrm{Im}\,(\gamma \cdot z) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2},\ \frac{d}{dz}(\gamma \cdot z) = \frac{det(\gamma)}{(cz+d)^2}.$$

Remarque. Calcul de routine analogue à celui fait au début du chapitre 0.

A partir de l'opération à gauche définie ci-dessus, on obtient une opération à droite de $\mathrm{GL}^+(2, \mathbf{R})$ sur l'ensemble des applications de $\mathcal{H}$ dans $\mathbf{C}$ qui est donnée par la formule:

$$\forall f : \mathcal{H} \to \mathbf{C},\ \forall \gamma \in \mathrm{GL}^+(2, \mathbf{R}),\ \forall z \in \mathcal{H},\ (f \circ \gamma)(z) = f(\gamma \cdot z)$$

1.1.2. Lemme. Pour tout entier rationnel k, on définit une nouvelle action à droite de $\mathrm{GL}^+(2, \mathbf{R})$ sur l'ensemble des applications de $\mathcal{H}$ dans $\mathbf{C}$ en posant

$$\forall f : \mathcal{H} \to \mathbf{C},\ \forall \gamma \in \mathrm{GL}^+(2, \mathbf{R}),\ (f|_k\ \gamma)(z) = \frac{(\det\ \gamma)^{k/2}}{(cz+d)^k} \cdot f(\gamma \cdot z)$$

Démonstration. On commence par définir la fonction j par $j(\gamma, z) = \frac{(\det\ \gamma)^{1/2}}{cz+d}$

On a alors les identités:
$$\frac{d(\gamma \cdot z)}{dz} = j(\gamma, z)^2;$$

$$\frac{d(\gamma_1\gamma_2 \cdot z)}{dz} = j(\gamma_1\gamma_2, z)^2 = \frac{d(\gamma_1\gamma_2 \cdot z)}{d(\gamma_2 \cdot z)} \cdot \frac{d(\gamma_2 \cdot z)}{dz} = j(\gamma_1, \gamma_2 \cdot z)^2 \cdot j(\gamma_2, z)^2;$$
$$(f|_k\ \gamma)(z) = j(\gamma, z)^k \cdot f(\gamma \cdot z)$$

Pour cette raison la fonction j est appelée le **facteur d'automorphie** (associé à l'entier k).

1.1.3. Définition. Soient Γ un sous-groupe d'indice fini de $\mathrm{SL}(2, \mathbf{Z})$ et k un entier rationnel. On appelle ensemble des **formes modulaires de poids k** relativement au groupe Γ l'ensemble des applications $f : \mathcal{H} \to \mathbf{C}$ ayant les trois propriétés

(i) L'application f est holomorphe sur H;

(ii) L'application f est invariante par l'opération de Γ associée à l'entier k, induite par l'opération à droite de $\mathrm{GL}^+(2, \mathbf{R})$ sur l'ensemble des applications de H dans $\mathbf{C}$.

(iii) Pour tout $s \in \mathrm{SL}(2, \mathbf{Z})$, il existe un entier naturel $N(s)$ tel que l'application f admette un développement "régulier" de la forme $(f|_k\ s)(z) = \sum\limits_{n \geq 0} a(n, s) q^{n/N(s)}$ où, comme d'habitude, on a posé $q = \exp(2i\pi z)$.

Dans la suite on désigne cet ensemble par $\mathcal{M}(k, \Gamma)$; on l'appelle l'ensemble des formes modulaires Γ-invariantes de poids k.

Remarque. Il est clair que $\mathcal{M}(k, \Gamma)$ est un $\mathbf{C}$-espace vectoriel.

Par ailleurs, si on se place dans le cas très particulier où Γ est le groupe $\mathrm{SL}(2,\mathbf{Z})$, on obtient pour toute fonction ayant les propriétés (i) et (ii) une fonction holomorphe sur H qui est invariante par l'action usuelle de $\mathrm{SL}(2,\mathbf{Z})$. En particulier le groupe $\mathrm{SL}(2,\mathbf{Z})$ contient la matrice correspondant à la translation de vecteur 1, soit $T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, c'est-à-dire que l'application f est périodique de période 1. De ce fait elle s'écrit comme famille sommable indiciée par Z en $q = \exp(2i\pi z)$. La troisième assertion de la définition stipule que f est une série entière en q, ou encore que c'est une fonction holomorphe au voisinage de ∞, car l'application $z \to \exp(2i\pi z)$ réalise une surjection holomorphe du demi-plan de Poincaré sur le disque ouvert de centre 0 et de rayon 1 privé du point 0.

Lorsque Γ est un sous-groupe d'indice fini de $\mathrm{SL}(2,\mathbf{Z})$, il existe un plus petit entier n, diviseur de l'indice de Γ dans $\mathrm{SL}(2,\mathbf{Z})$, tel que T^n appartienne à Γ et pour tout $s \in SL(2, \mathbf{Z})$, il existe un entier $N(s)$ tel que $T^{N(s)}$ appartienne à $s\Gamma s^{-1}$. On obtient ainsi la propriété périodique de période $N(s)$.

1.1.4. Définition. Un élément de $\mathcal{M}(k,\Gamma)$ qui est nul à l'infini, c'est-à-dire dont le premier terme du développement en série entière en q est nul, est appelé une **forme parabolique de poids k** relativement à Γ. Le sous-espace vectoriel des formes paraboliques de poids k relativement à Γ est noté $\mathcal{S}(k,\Gamma)$.

On définit respectivement l'espace des formes modulaires relativement à Γ, $\mathcal{M}(\Gamma)$, et son sous-espace des formes paraboliques $\mathcal{S}(\Gamma)$ par

$$\mathcal{M}(\Gamma) = \bigoplus_{k\in\mathbf{N}} \mathcal{M}(k,\Gamma) \text{ et } \mathcal{S}(\Gamma) = \bigoplus_{k\in\mathbf{N}} \mathcal{S}(k,\Gamma)$$

Ultérieurement on démontrera le théorème de stucture suivant pour ces espaces de fonctions

1.1.5. Théorème. L'espaces $\mathcal{M}(\Gamma)$ et son sous-espace des formes paraboliques $S(\Gamma)$ ont les propriétés

(i) Pour tout couple d'entiers rationnels (k,m) on a les inclusions:
$\mathcal{M}(k,\Gamma) \bullet \mathcal{M}(m,\Gamma) \subseteq \mathcal{M}(k+m,\Gamma)$
$\mathcal{S}(k,\Gamma) \bullet \mathcal{M}(m,\Gamma) \subseteq \mathcal{S}(k+m,\Gamma)$

(ii) Pour tout sous-groupe d'indice fini Γ de SL(2,$\mathbf{Z}$) et pour tout entier rationnel k le $\mathbf{C}$-espace vectoriel $\mathcal{M}(k,\Gamma)$ est de dimension finie.

(iii) L'espace $\mathcal{M}(\Gamma)$ muni de la multiplication ordinaire des fonctions est une $\mathbf{C}$-algèbre graduée de type fini.

(iv) Dans le cas particulier où Γ est le groupe $SL(2,\mathbf{Z})$, l'algèbre graduée $\mathcal{M}(\Gamma)$ est l'algèbre $\mathbf{C}[G_4,G_6]$ où G_t $(t\in 4,6)$ est la série d'Eisenstein de poids t qui engendre $\mathcal{M}(t,\Gamma)$.

1.2. Lien entre formes modulaires et représentations

On revient à la caractérisation initiale de $\mathcal{H}$ comme quotient $\mathrm{GL}^+(2,\mathbf{R})/Z(\mathrm{SO}(2,\mathbf{R}))$. Toute matrice $g\in \mathrm{SL}(2,\mathbf{R})$ peut se décomposer sous la forme

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},\ \varepsilon\in\{-1,1\},\ \alpha>0,\ \theta\in[0,\pi[$$

On explicite cette décomposition sous la forme:

si $c=0$, alors $\varepsilon=\mathrm{sign}(a)$, $\alpha=1$, $\beta=b{\cdot}\mathrm{sign}(a)$, $\theta=0$

si $c\neq 0$, alors $\varepsilon=\mathrm{sign}(c), \alpha=(c^2+d^2)^{-1/2}$, $\theta=\mathrm{Arccos}(\varepsilon\cdot d\cdot(c^2+d^2)^{-1/2})$ et $\beta=(ac+bd)(c^2+d^2)^{-1/2}$

Si on pose $y=(c^2+d^2)^{-1}$ et $x=(ac+bd)\cdot y$, c'est-à-dire $\alpha=\sqrt{y}$ et $x=\beta\sqrt{y}$, on obtient $g\cdot i = x+iy$

Cela étant, soit f une forme modulaire de poids k relativement à un sous-groupe d'indice fini Γ de SL(2,$\mathbf{Z}$). On lui associe l'application $f^0 : \mathrm{GL}(2,\mathbf{R})\to\mathbf{C}$ définie par la formule

$$f^0(g) = \begin{cases} f(g \cdot i)j(g,i)^k & \text{si } \det(g) > 0, \\ f(g \cdot (-i))j(g,-i)^k & \text{sinon.} \end{cases}$$

Un calcul élémentaire montre qu'on a

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } \varepsilon \in \{-1, 1\} \Rightarrow g \cdot (\varepsilon i) = \frac{ad + bc + \varepsilon \cdot i \cdot \det(g)}{c^2 + d^2},$$

ce qui prouve que l'application f^0 est bien définie.

1.2.1. Lemme. Pour tout $f \in \mathcal{M}(k, \Gamma)$, l'application $f^0 : \mathrm{GL}(2, \mathbf{R}) \to \mathbf{C}$ satisfait à

$$\forall \gamma \in \Gamma \ f^0(\gamma \cdot g) = f^0(g); \quad \forall \theta \in \mathbf{R} \ f^0\left(g\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = \exp(-ik\theta) f^0(g).$$

Démonstration. On peut se contenter de faire la preuve pour $g \in \mathrm{GL}^+(2, \mathbf{R})$, l'autre cas étant analogue. On remarque que les relations établies dans le lemme 1.1.2 sur la fonction j sont vraies pour deux éléments quelconques de $\mathrm{GL}(2, \mathbf{R})$. En les applicant à la première formule à démontrer, on a

$$f^0(\gamma g) = f(\gamma g \cdot i) j(\gamma g, i)^k = [f|_k \gamma](g \cdot i) j(\gamma, g \cdot i)^{-k} j(\gamma g, i)^k = f(g \cdot i) j(g, i)^k = f^0(g).$$

En ce qui concerne la seconde formule, on remarque d'abord que i est invariant par l'action d'une matrice de rotation. On a donc pour tout $\theta \in \mathbf{R}$

$$j\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, i\right) = (i \cdot \sin\theta + \cos\theta)^{-1} = e^{-i\theta}.$$

1.2.2. Proposition. *Avec la notation ci-dessus, la fonction f^0 est une application de l'espace quotient $\Gamma \backslash \mathrm{GL}(2, \mathbf{R})$ à valeurs dans $\mathbf{C}$. La forme modulaire f est une forme parabolique si et seulement si la fonction f^0 est une fonction de carré intégrable sur $\Gamma \backslash \mathrm{GL}(2, \mathbf{R})$. Elle définit une représentation de GL(2,$\mathbf{R}$) engendrée par les fonctions de la forme $g \to f^0(gh)$.*

Une construction plus générale des représentations associées aux formes modulaires est liée à la notions d'idèles. On sait que $\mathbf{Z}$ est un réseau dans $\mathbf{R}$, i.e. un sous-groupe discrèt avec le groupe quotient $\mathbf{R}/\mathbf{Z}$ compact. L'anneau des idèles $\mathbf{A}$ peut être définit informellement comme un anneau minimale localement compact contenent $\mathbf{Q}$ comme un réseau. Explicitement $\mathbf{A} = \mathbf{R} \times \mathbf{A}_f$, où $\mathbf{A}_f = \hat{\mathbf{Z}} \otimes \mathbf{Q}$ l'anneau des idèles finis, $\hat{\mathbf{Z}} = \varprojlim_{n \in \mathbf{N}} \mathbf{Z}/n\mathbf{Z}$ la completion profinit de $\mathbf{Z}$, donc un anneau compact,

$$\hat{\mathbf{Z}} = \prod_{p \ premier} \mathbf{Z}_p,$$

$\mathbf{Z}_p$ l'anneau des entier p-adiques. Alors $\mathbf{A}_f$ est $\mathbf{A}$ sont localement compact, est on vérifie que $\mathbf{Q}$ est un réseau dans $\mathbf{A}$. Plus précisement, pour $v = \infty, p$, posons $\mathbf{Q}_\infty = \mathbf{R}$, et $\mathbf{Q}_p$ le corps des nombres p–adiques, alors

$$\mathbf{A} = \{x = (x_v) \mid x_v \in \mathbf{Q}_v, \text{ est } x_p \in \mathbf{Z}_p \text{ pour tout } p \text{ sauf un nombre fini,}\}$$

et $\mathbf{A}$ admèt la base des ouverts suivante: pour tout ensemble fini $S = \{\infty, p_1, \ldots, p_m\}$ et pour tout ouverts $U_v \subset \mathbf{Q}_v$ posons

$$U = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathbf{Z}_p.$$

Ensuite, on remplace $\mathbf{R}$ par $\mathbf{A}$, et $\mathrm{GL}_2(\mathbf{R})$ par $\mathrm{GL}_2(\mathbf{A})$, et on remarque que pour le sous groupe de congruence $\Gamma = \Gamma(N)$

$$\Gamma \backslash \mathrm{GL}(2, \mathbf{R}).$$

la fonction f peut être enlevée en une fonctions sur $\mathrm{GL}_2(\mathbf{Q}) \backslash \mathrm{GL}_2(\mathbf{A})$ qui engendre une représentation π_f du groupe $\mathrm{GL}_2(\mathbf{A})$ (avec l'espace de représentation engendré par les fonctions $g \mapsto \pi_f(h)(g) = f(gh)$).

L'observation-clèf du dévéloppement modern de la théorie des formes modulaires (Langlands, Piatetski–Shapiro, ...) est que la propiété de la multiplicativité de type 0.2 pour les coefficients de Fourier (normalisés) d'une forme modulaire est équivalaent au fait que la représentation correspondante π_f du groupe $\mathrm{GL}_2(\mathbf{A})$ soit *irreductible*. Dans ce cas $\pi_f = \otimes_v \pi_{f,v}$ avec $\pi_{f,v}$ certaines représentations de $\mathrm{GL}_2(\mathbf{Q}_v)$, $v = \infty, p$. Etude de certaines propriétés importants des formes modulaires ce réduit à l'étude des représentations correspondantes $\pi_{f,v}$.

1.3. Caractères de Dirichlet, Théorie de Galois et fonctions L d'Artin.

Ce paragraphe constitue d'abord un préliminaire à l'introduction des formes modulaires avec caractères introduites dans le paragraphe suivant, ensuite une courte digression sur l'arithmétique. Bien entendu son contenu sera considérablement développé par la suite.

1.3.1. Définition. Pour tout entier naturel $N \geq 2$, un **caractère modulaire** ou **caractère de Dirichlet modulo** N est un homomorphisme $\chi(\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ défini sur le groupe $(\mathbf{Z}/N\mathbf{Z})^*$ des éléments inversibles de $\mathbf{Z}/N\mathbf{Z}$ et à valeurs dans $\mathbf{C}^*$, donc dans le groupe des racines $\phi(N)$-ièmes de l'unité où ϕ est la fonction d'Euler. Par extension on nomme aussi caractère le relèvement de $\chi : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ sur $\mathbf{Z}$ nul sur les entiers non premiers avec N. Un caractère de Dirichle modulo N est dit **primitif** s'il nese factorise pas en un caractère de Dirichle modulo un diviseur propre M de N.

Dans la suite de ce paragraphe, on se fixe un entier $N \geq 2$ et on désigne par $\bar{\mathbf{Q}}$ une clôture algébrique du corps $\mathbf{Q}$ des nombres rationnels. Le corps $\mathbf{Q}^{(N)}$ des racines N-ièmes de l'unité inclus dans est une extension galoisienne de $\mathbf{Q}$ dont le groupe de Galois est isomorphe au groupe $(\mathbf{Z}/N\mathbf{Z})^*$; un isomorphisme est donné par $H_N : a \mapsto (\zeta_N \to \zeta_N^a)$, où est ζ_N une racine primitive N-ième de l'unité arbitraire. A partir de là, à tout caractère de Dirichlet $\chi : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ on associe une représentation de dimension 1 sur $\mathbf{C}$ du groupe de Galois de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}$, $\rho_\chi : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{C}^*$ donnée par $\rho_\chi = \chi \circ H_N^{-1} \circ r_N$, où, pour tout $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $r_N(\sigma)$ est la restriction de σ au corps cyclotomique $Q^{(N)}$. La plus belle illustration de cet objet est

1.3.2. Théorème de Kronecker-Weber. Soit $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{C}^*$ une représentation de dimension 1 et d'image finie du groupe de Galois de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}$. Alors il existe un et un seul caractère primitif de Dirichlet χ tel que $\rho = \rho_\chi$.

Remarque. Pour une démonstration, voir par exemple le livre de Cassels J.W. et Fröhlich A., ch. VIII.

1.3.3. Définition. Soit V un espace vectoriel complexe de dimension finie. Soit ρ : $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to V$ une représentation du groupe de Galois de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}$. Pour tout nombre premier p, soit π un idéal premier au-dessus de p dans l'anneau des entiers de $\bar{\mathbf{Q}}$, $I(\pi)$ son groupe d'inertie, $V^{I(\pi)}$ le sous-espace de V invariant par les images par ρ du groupe $I(\pi)$ et Fr_π l'automorphisme de Frobenius de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}$ associé à π. On appelle **série** L **d'Artin associée à la représentation** ρ la fonction définie comme produit infini:

$$L(s,\rho) = \prod_{p-\text{premier}} \det\bigl(id - p^{-s}\rho(Fr_\pi)|V^{I(\pi)}\bigr)^{-1}$$

1.3.4. Exemples. (i) Si la représentation ρ est la représentation triviale de dimension 1, la série L de cette représentation n'est autre que la fonction zeta de Riemann.

(ii) Si la représentation ρ est une représentation de dimension 1 et d'image finie, d'après le théorème de Kronecker-Weber, soit χ l'unique caractère de Dirichlet primitif tel que $\rho = \rho_\chi$. Alors la série L d'Artin de cette représentation est la série de Dirichlet $L(s,\chi) = \sum_{n\in\mathbf{N}} \chi(n)n^{-s}$.

On sait que si P est un ensemble de nombre premiers, la densité arithmétique de P est $\lim_{x\to\infty} \dfrac{\mathrm{Card}(P\cap[0,x])}{\pi(x)}$ où $\pi(x)$ est le nombre des nombres premiers inférieurs ou égaux à x. Un exemple d'estimation de densité est le théorème de Tchebotaref, qui généralise le théorème de la progression arithmétique de Dirichlet:

1.3.5. Théorème de Tchebotaref. Soit K un corps de nombres galoisien sur $\mathbf{Q}$ dont le groupe de Galois est G. Soient A une classe de conjugaison de G et $P(A)$ l'ensemble des nombres premiers p non ramifiés tels que les automorphismes de Frobenius des idéaux de K au-dessus de (p) appartiennent à A. Alors la densité de $P(A)$ est le quotient $\mathrm{Card}(A)/\mathrm{Card(G)}$.

Remarque. Voir par exemple [Tchebotaref, Math. Annalen 95, 1926]. Dans [Cassels & Frölich , pp.164], exposé de J.Tate, voir les ingrédients sur les automorphismes de Frobenius et la loi de réciprocité d'Artin.

Pour obtenir le théorème des nombres premiers dans une prograssion arithmétique, il suffit d'appliquer le théorème de Tchebotaref au cas du corps cyclotomique $\mathbf{Q}^{(n)}$ où n est la raison de la progression.

L'un des buts de ce cours sera de construire un analogue de ce théorème pour les représentations de dimension 2 utilisant les formes modulaires (théorème de Deligne-Serre).

1.4. Formes modulaires avec caractère

1.4.1. Définition. Soient Γ un sous-groupe d'indice fini de SL(2,**Z**), et $N \geq 2$ un entier. On note respectivement les sous-groupe de Γ

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ c \equiv 0 \bmod N \right\}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ c \equiv 0 \bmod N \ \&\ a \equiv b \equiv 1 \bmod N \right\}$$

Soient χ un caractère de Dirichlet modulo N et k un entier rationnel. On désigne par $\mathcal{M}_k(\Gamma, \chi, N)$ le sous **C**-espace vectoriel de $\mathcal{M}_k(\Gamma_1(N))$ formé des formes f telles que

$$\forall \gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix} \in \Gamma_0(N),\ f|_k\ \gamma = \chi(\gamma_{22}) \cdot f.$$

On a une définition du même type pour l'espace $\mathcal{S}_k(\Gamma, N, \chi)$ des formes paraboliques associées au caractère χ.

1.4.2. Proposition. Pour tout sous-groupe d'indice fini Γ de SL(2,**Z**), le groupe $\Gamma_1(N)$ est un sous-groupe invariant de $\Gamma_0(N)$ et le groupe quotient est isomorphe à $(\mathbf{Z}/N\mathbf{Z})^*$. On a donc une représentation linéaire naturelle de $(\mathbf{Z}/N\mathbf{Z})^*$ dans $\mathcal{M}_k(N, \chi)$ qui se décompose en produit de représentations irréductibles

1.4.3. Proposition. Pour tout entier naturel $N \geq 2$ et pour tout entier rationnel k on a les égalités suivantes sur les espaces de formes modulaires:

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(N, \chi), \qquad \mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{S}_k(N, \chi)$$

où la somme directe porte sur l'ensemble des caractères modulo N. Pour tout caractère χ modulo N, $\mathcal{S}_k(N, \chi) = \mathcal{M}_k(N, \chi) \cap \mathcal{S}_k(\Gamma_1(N))$

Remarques. Soit Γ un sous groupe d'indice fini de SL(2,**Z**) contenant $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Pour tout entier rationnel impair k on a $\mathcal{M}_k(\Gamma) = 0$. De même, pour tout caractère χ modulo N et pour tout entier rationnel k, l'espace $\mathcal{M}_k(\chi)$ est réduit à 0 si k n'est pas de la parité de χ. Ceci est conséquence immédiate des définitions.

Pour préparer l'avenir de ce cours, énonçons dès maintenant le

1.4.4. Théorème de Deligne-Serre. *Soit f une forme modulaire parabolique primitive de poids 1 asociée à un caractère χ modulo N qui soit impair. On désigne par $\sum_{n\geq 1} a(f,n)q^n$ la série de Fourier de f. Alors il existe une représentation irréductible de degré 2 $\rho_f : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ telle que la série $L(\rho_f, s)$ d'Artin coïncide avec la transformée de Mellin de la fonction f. En d'autres termes on a $L(\rho_f, s) = \sum_{n\geq 1} a(f,n)n^{-s}$. Réciproquement, soit $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ une représentation irréductible du groupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ qui soit d'image finie. Sous la condition que la conjecture d'Artin soit vraie, c'est-à-dire que la fonction L d'Artin associée soit holomorphe sur $\mathbf{C}$, il existe une forme modulaire f, parabolique de poids 1 et primitive, associée à un caractère χ telle que $\rho = \rho_f$.*

1.5. Séries théta et formes modulaires.

1.5.1. Définition. Soit m un entier strictement positif. Une forme quadratique Q à m variables sera dite entière si sa matrice est de la forme $(1/2)A$ où A est une matrice carrée symétrique d'ordre m à coefficients entiers dont les éléments diagonaux sont pairs. Etant donnée une telle forme quadratique, pour tout enier n on désigne par $A(n,Q)$ le nombre de solutions en entiers rationnels de l'équation $Q(x) = n$. On appelle alors **niveau** de Q le plus petit entier N tel que la forme quadratique de matrice $(1/2N)A^{-1}$ soit une forme quadratique entière.

1.5.2. Définition. Soient $m = 2k$ un entier strictement positif pair et Q une forme quadratique définie positive et entière à m variables. On appelle **fonction théta** associée à cette forme quadratique la fonction dont le développement en série de Fourier est de la forme $\Theta(q) = \sum_{n=0}^{\infty} A(Q,n)q^n = \sum_{x\in\mathbf{Z}^{2k}} q^{Q(x)}$ où la dernière somme porte sur tout les points du réseau $\mathbf{Z}^{2k}$.

1.5.3. Proposition. Soit Q une forme quadratique entière et définie positive de niveau N. Soient Δ le discriminant de Q et ε_Δ le symbole de Legendre associé à Δ. Alors la fonction théta de Q appartient à l'espace $\mathcal{M}_k(N,\chi)$.

Remarques. Voir par exemple [Schoeneberg].

Dans le cas $N = 1$ il est facile à démontrer cette proposition (voir [Serre, p.172]. Car le groupe $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les matrices élémentaires entières, on peut choisir $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ en tant qu'un système de générateurs de $\mathrm{SL}_2(\mathbf{Z})$. Evidemment, la série $\Theta_Q(z) = \sum_{n=0}^{\infty} A(Q,n)q^n$ est invariante par raport à T, et ce qu'il reste à vérifier dans ce cas est le fait que $\Theta_Q(Sz) = z^k\Theta_Q(z)$.

1.5.4. Exemple. Cet exemple est une illustration du théorème de Deligne-Serre. On considère la forme quadratique binaire de discriminant 23, $Q(x, y) = x^2 + 23y^2$. La fonction théta de cette forme quadratique est une forme modulaire de poids 1 associée au symbole de Legendre ε_{23}. Ecrivant le développement de Fourier de cette fonction sous la forme $\Theta(q) = \sum_{n=0}^{\infty} A(Q, n)q^n$, il résulte du théorème de Deligne-Serre qu'il existe une représentation irréductible de degré 2 $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ telle que pour tout nombre premier p et tout idéal π au dessus de (p) on ait

$$a(p) = \mathrm{Tr}(\rho_f(\mathrm{Fr}(\pi)))$$

L'anneau des entiers de $\mathbf{Q}(\sqrt{-23})$ n'est pas principal. Son groupe des classes est cyclique d'ordre 3, engendré par l'idéal premier π engendré par 2 et ω. On a dans cet anneau d'entiers $(2) = \pi\pi'$. Soit H l'extension maximale non ramifiée ou corps de classe de Hilbert de $\mathbf{Q}(\sqrt{-23})$. Le corps H est cyclique de degré 3 sur $\mathbf{Q}(\sqrt{-23})$ et admet comme groupe de Galois sur $\mathbf{Q}$ le groupe S_3. L'image de la représentation $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ est un sous-groupe de $\mathrm{GL}(2,\mathbf{C})$ isomorphe à S_3 et son noyau est $\mathrm{Gal}(\bar{\mathbf{Q}}/H)$. Le groupe image de la représentation ρ est un groupe conjugué du groupe de matrices engendré par $\left\{ \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$. Les valeurs possible des traces sont donc 2 pour les éléments dont l'image est triviale, 0 pour les éléments dont l'image est d'ordre 2 et -1 dont l'image est d'ordre 3. On a en général $a(p) \leq 2$, et $a(p) = 2$ si et seulement si l'idéal (p) est décomposé dans H en deux idéaux principaux, c'est-à-dire si et seulement si la représentation cherchée est triviale sur le Frobenius d'un idéal π au-dessus de (p).

On peut enfin montrer, par analogie avec le Théorème de Tchebotaref, que la densité arithmétique de l'ensemble des nombres premiers représentés par la forme $Q(x, y)$ est égale à $1/6$. (Et pourtant les deux premiers de ces nombres sont 59 et 101 !).

On considère la fonction $f_{23}(z) = q \prod_{m \geq 0} (1 - q^m)(1 - q^{23m})$. Cette fonction s'écrit aussi sous la forme $f_{23}(z) = \frac{1}{2}\left\{ \sum_{m,n} q^{n^2+mn+6m^2} - \sum_{m,n} q^{2n^2+mn+3m^2} \right\} = \sum_n a(n)q^n$. C'est une forme parabolique de poids 1 associée au caractère de Legendre ε_{23}.

Par ailleurs, la fonction f dont le développement de Fourier est

$$f(z) = \sum_{(x,y)\in\mathbf{Z}^2} q^{x^2+23y^2} = \sum_{n\geq 0} a(Q, n)q^n$$

n'est pas une forme parabolique puisque son terme constant est 1. Cependant on a le

1.5.5. Lemme. Avec les notations ci-dessus, pour tout nombre premier p le nombre $a(Q, p)$ est non nul si et seulement si le nombre $a(p)$ est non nul.

Démonstration. Il est clair que $a(Q, p)$ est non nul si et seulement si le nombre premier p est représenté par la forme quadratique $x^2 + 23y^2$, c'est-à-dire si et seulement si p est une norme sur $\mathbf{Q}$ d'un élément de $\mathbf{Z}[\sqrt{-23}]$. Or le discriminant -23 de $\mathbf{Q}(\sqrt{-23})$ est congru à 1 modulo 4. Une $\mathbf{Z}$-base de l'anneau des entiers de $\mathbf{Q}(\sqrt{-23})$ est donc $1, \omega$ avec $\omega = \frac{1+\sqrt{-23}}{2}$. La norme de $x + \omega y$ est alors $\frac{1}{4}\{(2x+y)^2 + 23y^2\} = x^2 + xy + 6y^2$.

Si $a(p)$ est non nul, alors p est représentable sous la forme $m^2 + mn + 6n^2$ avec m et n entier, ce qui implique m impair et n pair, $m = 2x+1$ et $n = 2y$, et p est la norme de l'entier $2x + y + y\sqrt{-23}$ et on conclut que $a(Q,p) > 0$.

Réciproquement, il suffit de montrer que si p est un nombre premier impair tel que $a(Q,p)$ soit strictement positif, alors p est représenté sur par la forme quadratique $2x^2 + xy + 3y^2$ mais ne l'est pas par la forme $s^2 + st + 6t^2$. Si p était représenté par cette dernière forme, alors p et $2p$ le seraient tous deux par la forme $2x^2 + xy + 3y^2$, ce qui impliquerait que 2 serait représenté sur par la forme $u^2 + 23v^2$. Il existerait trois nombres entiers rationnels (a, b, c) premiers entre eux dans leur ensemble tels que $2c^2 = a^2 + 23b^2$. On aurait a impair, puis b impair, $a^2 + 23b^2$ congru à 2 modulo 8 et c impair. On aurait alors $2c^2$ congru à 2 modulo 16 et $a^2 + 23b^2$ congru à 0 ou 8 modulo 16, d'où la contradiction. Une autre façon de dire la même chose est que -23 est un carré dans $\mathbf{Q}_2$, le complété de $\mathbf{Q}$ pour la valuation dyadique, donc que $\mathbf{Q}(\sqrt{-23})$ se plonge dans $\mathbf{Q}_2$, donc que 2, qui n'est pas un carré, n'est pas une norme.

1.5.6. Exemple dû à Andrianov. Considérons la forme quadratique $Q(x,y) = x^2 + y^2 + 9(z^2 + t^2)$, alors $\theta_Q \in M_2(36, 1)$,

$$r(Q,p) = \frac{4}{3}(p+1) - \frac{8}{3}\sum_{x=0}^{p-1}\left(\frac{x^3+1}{p}\right), \quad (p,6) = 1$$

Considérons la courbe elliptique $E : y^2 = x^3 + 1$; alors on a $N_p = \#E(\mathbf{Z}/p\mathbf{Z}) = p + 1 - a_p$ où

$$a_p = -\sum_{x=0}^{p-1}\left(\frac{x^3+1}{p}\right), \quad \text{et } |a_p| < 2\sqrt{p}$$

par le thérème célèbre de Hasse. La relation ci-dessus nous donne un lien entre des objets de la nature très differente: formes quadratiques entières et courbes algébriques à coefficients entiers.

1.6. Formes modulaires comme fonctions de réseaux. Soit $\Lambda \subset \mathbf{C}$ un réseau, alors $\Lambda = \langle \omega_1, \omega_2 \rangle$ pour une base $\{\omega_1, \omega_2\}$. Le réseau de type $\Lambda_z = \langle 1, z \rangle$ s'appelle standard.

Propositon. (a) Pour tout Λ il exist $\lambda \in \mathbf{C}^\times$ tel que $\Lambda = \lambda \Lambda_z$,
(b) Si $\Lambda = \langle \omega_1, \omega_2 \rangle = \langle \omega_1', \omega_2' \rangle$ alors

$$(\omega_1, \omega_2) = (\omega_1', \omega_2')\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ avec } a, b, c, d \in \mathbf{Z}, ad - bc = 1.$$

Soit $\mathcal{L}$ déigne l'ensemble des réseaux de $\mathbf{C}$.

1.6.1. Définition (fonctions de réseaux homogènes de degré k) Une application $F : \mathcal{L} \to \mathbf{C}$ s'appelle fonction de réseaux homogène de degré $-k$ si pour tout $\lambda \in \mathbf{C}^\times$ $F(\lambda\Lambda)\lambda^{-k}F(\Lambda)$. Notation: $H \in \mathcal{H}_{-k}$.

1.6.2. Définition (fonctions faiblement modulaires). Pour $k \in \mathbf{N}$ et pour un sous groupe $\Gamma \subset \Gamma(1)$ d'indice fini on défini l'espace vectoriel complex $\mathcal{M}_k^a(\Gamma)$ des fonctoins faibleent modulaires par

$$\mathcal{M}_k^a(\Gamma) = \left\{ f : H \to \mathbf{C} \mid \forall \gamma = \begin{pmatrix} a\, b \\ c\, d \end{pmatrix} \in \Gamma\ f|_k\gamma = f \right\}.$$

Propositon. *Il exist une bijection* $\mathcal{H}_{-k} \xrightarrow{\sim} \mathcal{M}_k^a(\Gamma(1))$ *donnée par la règle:*

$$F \mapsto f, \quad f(z) = F(\Lambda_z).$$

Démonstration. On vérifie d'abord que $f \in \mathrm{M}_k^a(\Gamma(1))$. On a

$$f\left(\frac{az+b}{cz+d}\right) = F\left(\left\langle \frac{az+b}{cz+d}, 1 \right\rangle\right) = F((cz+d)^{-1}\langle az+b, cz+d\rangle) =$$
$$(cz+d)^k F(\langle az+b, cz+d\rangle) = (cz+d)^k F(\Lambda_z) = (cz+d)^k f(z).$$

Maintenant pour un résau donné Λ choisissons une base $\{\omega_1, \omega_2\}$ de telle façon que $\operatorname{Im}(\omega_1/\omega_2) > 0$ et pour une $f \in \mathrm{M}_k^a(\Gamma(1))$ posons

$$F(\Lambda) = \omega_2^{-k} f\left(w_1, \omega_2, \right).$$

Cette définition implique immédiatement $F \in \mathcal{H}_{-k}$.

De même façon on définit

$$\mathcal{L}_1(N) = \left\{(\Lambda, P \bmod \Lambda) \mid P \bmod \Lambda \in \mathbf{C}/\Lambda, \mathrm{ord}(P \bmod \Lambda) = N\right\},$$
$$\mathcal{L}_0(N) = \left\{(\Lambda, \langle P \bmod \Lambda\rangle) \mid P \bmod \Lambda \in \mathbf{C}/\Lambda, \#\langle P \bmod \Lambda\rangle = N\right\},$$
$$\mathcal{L}(N) = \left\{(\Lambda, P \bmod \Lambda, Q \bmod \Lambda) \mid P, Q \bmod \Lambda \in \mathbf{C}/\Lambda,\right.$$
$$\left.\langle P \bmod \Lambda\rangle \oplus \langle Q \bmod \Lambda\rangle = N^{-1}\Lambda/\Lambda \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^2\right\}.$$

Proposition (exercise). *Il y a des ismorphismes naturels:*

(a)

$$\mathcal{H}_{-k}(\mathcal{L}(N)) \xrightarrow{\sim} \mathcal{M}_k^a(\Gamma(N)),$$

(b)

$$\mathcal{H}_{-k}(\mathcal{L}_1(N)) \xrightarrow{\sim} \mathcal{M}_k^a(\Gamma_1(N)),$$

(c)

$$\mathcal{H}_{-k}(\mathcal{L}_0(N)) \xrightarrow{\sim} \mathcal{M}_k^a(\Gamma_0(N)).$$

Démonstration est analogue à la précedante. On pose $F \mapsto f$ où

(a)

$$f(z) = F((\Lambda_z, \langle \frac{1}{N} \bmod \Lambda_z\rangle),$$

(b)

$$f(z) = F((\Lambda_z, \frac{1}{N} \bmod \Lambda_z),$$

(c)

$$f(z) = F(\left(\Lambda_z, \frac{1}{N} \bmod \Lambda_z, \frac{z}{N} \bmod \Lambda_z\right)).$$

1.7. Séries d'Eisenstein et et leur développements de Fourier. Soit $k > 2$. Pour un réseau $\Lambda \subset \mathbf{C}$ posons

$$G_k(\Lambda) = \sum_{l \in \Lambda} l^{-k} = \sum_{m,n}{}'(m\omega_1 + n\omega_2)^{-k}, \quad \Lambda = \langle \omega_1, \omega_2 \rangle,$$

1.7.1. Proposition. *(a) On a*

$$G_k(z) = \sum_{m,n}{}'(mz+n)^{-k} \in \mathcal{M}_k(\Gamma(1));$$

(b)

$$G_k(z) = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right],$$

où $q = e(z) = \exp(2\pi i z)$, B_k sont les nombres de Bernoullli définis parle développement suivant

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

(Table numérique:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = B_5 = \cdots = 0,\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},$$
$$B_8 = -\frac{5}{66},\ B_{12} = \frac{691}{2730}\ B_{14} = -\frac{7}{6},\ B_{16} = \frac{3617}{510}\ B_{18} = -\frac{43867}{798}\ ,\ldots).$$

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

$$G_k(z) = \frac{(2\pi i)^k}{(k-1)!}\left[-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right].$$

Exemples.

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in \mathcal{M}_4(\mathrm{SL}(2,\mathbf{Z}),$$

$$E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n \in \mathcal{M}_6(\mathrm{SL}(2,\mathbf{Z}),$$

$$E_8(z) = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n \in \mathcal{M}_8(\mathrm{SL}(2,\mathbf{Z}),$$

$$E_{10}(z) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n \in \mathcal{M}_{10}(\mathrm{SL}(2,\mathbf{Z}),$$

$$E_{12}(z) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n \in \mathcal{M}_{12}(\mathrm{SL}(2,\mathbf{Z}),$$

$$E_{14}(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n \in \mathcal{M}_{14}(\mathrm{SL}(2,\mathbf{Z}).$$

Démonstration. L'automorphie est claire car $G_k(\lambda\Lambda) = \lambda^{-k}G_k(\Lambda)$ donc $G_k \in \mathcal{H}_{-k}$ est une fonction de réseaux homogène de degré $-k$. Pour trouver le développement de Fourier on utilise la décomposition classique du sin en produit

$$\sin(\pi a) = \pi a\prod_{n=1}^{\infty}\left(1 - \frac{a^2}{n^2}\right). \tag{7.1}$$

La dérivée logarithmiue de (7.1) nous donne

$$\pi\mathrm{ctg}\pi a = \frac{1}{a} + \sum_{n=1}^{\infty}\left(\frac{1}{a+n} - \frac{1}{a-n}\right). \tag{7.2}$$

Remarquons

$$\pi i\frac{e^{\pi ia} + e^{-\pi ia}}{e^{\pi ia} - e^{-\pi ia}} = \pi i + \frac{2\pi i}{e^{2\pi ia} - 1} = \pi i - 2\pi i\sum_{n=1}^{\infty}e^{2\pi ina} \tag{7.3}$$

et posons $x = 2\pi ia$; ceci implique

$$\frac{x}{2} + \frac{x}{e^x - 1} = 1 + \sum_{n=1}^{\infty}\frac{2x^2}{x^2 - (2\pi in)^2}$$

ou

$$\sum_{k=0}^{\infty}B_k\frac{x^k}{k!} + \frac{x}{2} = 1 - \sum_{n=1}^{\infty}\frac{2\left(\frac{x}{2\pi in}\right)^2}{-\left(\frac{x}{2\pi in}\right)^2 + 1} =$$

$$1 - 2\sum_{n=1}^{\infty}\sum_{k=2k'\geq 2}\left(\frac{x}{2\pi in}\right)^k = 1 - 2\sum_{k=2k'\geq 2}\frac{\zeta(k)}{(2\pi i)^k}x^k.$$

Ceci implique immédiatement

$$\zeta(k) = -\frac{(2\pi i)^k}{2}\frac{B_k}{k!}, \tag{7.4}$$

en particulier,

$$\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}.$$

Pour démontrer (b) on effectue l'intégration des deux parties de (7.3) par raport à a $(k-1)$ fois:

$$-(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} e^{2\pi ina} = (-1)^{k-1}(k-1)! \sum_{n\in\mathbf{Z}} (a+n)^{-k}, \quad (k \in 2\mathbf{Z}, k \geq 2). \tag{7.5}$$

Posons $a = mz$ alors

$$\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi inmz} = \sum_{n\in\mathbf{Z}} (mz+n)^{-k}. \tag{7.6}$$

Si maintenant $k > 2$ on peut effectuer la sommation pa rapport à m de 1 à ∞. Comme résultat on ait

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}\sum_{n=-\infty}^{\infty} (mz+n)^{-k} = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{m,d=1}^{\infty} d^{k-1} q^{md}\right]. \tag{7.7}$$

Remarquons que la série double dans (7.7) est absolument convergente pour $k > 2$ mais la séries (7.7) a un sens aussi pour $k = 2$ comme une série réitérative avec la convergence conditionnelle. On finie la démonsration en substituant (7.4) dans (7.7).

1.7.2. Théorème. *Soit* $\Delta(z) = q \prod_{m\geq 1} (1-q^m)^{24}$. *Alors on a*

$$\Delta(-z^{-1}) = z^{12}\Delta(z).$$

Démonstration. Posons

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

On a

$$\frac{d}{dz}\log(\Delta(z)) = \frac{d}{dz}\log q + 24\sum_{m=1}^{\infty}\frac{d}{dz}\log(1-q^m) =$$

$$2\pi i(1 - 24\sum_{m=1}^{\infty} mq(1-q^m)^{-1}) = 2\pi i E_2(z), \quad \frac{dq}{dz} = 2\pi i q.$$

Il est suffit d'établir

1.7.3. Proposition.

$$z^{-2}E_2(-z^{-1}) = E_2(z) + \frac{12}{2\pi iz}. \tag{7.8}$$

Démonstration da la proposition. On utilise la série (7.7) avec $k = 2$ qui converge conditionelement:

$$E_2(z) = \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \left(\sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} (mz+n)^{-2} \right) =$$

$$1 + \frac{3}{\pi^2} \sum_{m\neq 0} \left(\sum_{n=-\infty}^{\infty} (mz+n)^{-2} \right) = 1 + \frac{6}{\pi^2} \sum_{m=1}^{\infty} \left(\sum_{n=-\infty}^{\infty} (mz+n)^{-2} \right).$$

Pour tout m fixé on a

$$\sum_{n=-\infty}^{\infty} (mz+n)^{-2} = 1 - \frac{4}{B_2} \sum_{d=1}^{\infty} dq^{md} = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Maintenant on substitue

$$z^{-2}E_2(-z^{-1}) = \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \left(\sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} (-m+nz)^2 \right) = 1 + \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \sum_{m\neq 0} (mz+n)^{-2}.$$

Si l'on pose $a_{m,n} = (mz+n)^{-2}$, la démonstraton ce réduite à l'égalité

$$-\sum_m \sum_n a_{m,n} + \sum_n \sum_m a_{m,n} = \frac{12}{2\pi iz}.$$

Pour la démontrer on introduit le terme correctif suivant

$$b_{m,n}(z) = \frac{1}{(mz+n-1)(mz+n)} = \frac{1}{(mz+n-1)} - \frac{1}{(mz+n)} \tag{7.9}$$

Alors on obtient la série modifiée

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \left((mz+n)^{-2} - b_{m,n}(z) \right) \tag{7.10}$$

qui déjà converge absolument car

$$(mz+n)^{-2} - ((mz+n-1)(mz+n))^{-1} = (mz+n)^{-2}(mz+n-1)^{-1}.$$

D'autre part

$$\tilde{E}_2(z) =$$

$$1 + \frac{3}{\pi^2} \sum_{m \neq 0} \left(\sum_{n=-\infty}^{\infty} (mz+n)^{-2} \right) + \frac{3}{\pi^2} \sum_{m \neq 0} \sum_{n=-\infty}^{\infty} \left(\frac{1}{(mz+n)} - \frac{1}{(mz+n-1)} \right),$$

et la dernière somme ce téléscope vers zéro, donc

$$\tilde{E}_2(z) = E_2(z).$$

Il est possible de changer l'ordre de sommation dans (7.10) grâce à la convergence absolue, d'où

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \sum_{m \neq 0} \left((mz+n)^{-2} - b_{m,n}(z) \right) =$$

$$z^{-2} E_2(-z^{-1}) - \frac{3}{\pi^2} \sum_{n=-\infty}^{\infty} \left(\sum_{m \neq 0} b_{m,n} \right).$$

Il reste à évaluer la dernière somme:

$$\sum_{n=-\infty}^{\infty} \left(\sum_{m \neq 0} b_{m,n} \right) = \lim_{N \to \infty} \sum_{n=-N+1}^{n=N} \left(\sum_{m \neq 0} b_{m,n} \right).$$

Mais

$$\sum_{m \neq 0} (mz-n)^{-2} = \frac{1}{z^2} \sum_{m \neq 0} (n/z-m)^{-2} = -\frac{1}{n^2} - \frac{4\pi^2}{z^2} \sum_{d=1}^{\infty} d e^{-2\pi i n d(1/z)}$$

donc pour tout z la somme externe converge absolument, et la ce transforme en

$$\sum_{m \neq 0} \left(\sum_{n=-N+1}^{n=N} b_{m,n} \right) = \sum_{m \neq 0} \left(\frac{1}{(mz-N)} - \frac{1}{(mz+N)} \right) =$$

$$\frac{2}{z} \sum_{m=1}^{\infty} \left(\frac{1}{(-N/z+m)} + \frac{1}{(-N/z-m)} \right) = \frac{2}{z} \left(\pi \mathrm{ctg} \left(-\frac{\pi N}{z} \right) + \frac{z}{N} \right) \to -\frac{2\pi i}{z}$$

quand $N \to \infty$, $z \in \mathcal{H}$, entraînant proposition 1.7.3 et théorème 1.7.2.

Chapitre 2. Méthodes analytiques dans la théorie des formes modulaires

2.1. Structure des espaces des formes modulaires de niveau 1 (voir [Serre, pp.127–178]).

2.1.1. Domaine fondamentale du groupe modulaire. Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a

$$S(z) = -z^{-1}, \; T(z) = z+1.$$

Soit d'aure part, D le sous–ensemble de $\mathcal{H}$ formé dea points z tels que $|z| >\geq 1$ et $|\mathrm{Re}\,(z)| \leq 1/2$. Nous allons voir que D est un *domain fondamental* pour l'action de $\Gamma(1) = \mathrm{SL}(2,\mathbf{Z})$ sur $\mathcal{H}$, i.e. l'application naturelle $D \to \Gamma(1)\backslash\mathcal{H}$ est surjective, et sa restriction à l'intérieur de D est injective. En même temps on va voir que S et T engendrent $\Gamma(1) = \mathrm{SL}(2,\mathbf{Z})$.

Théorème. *1) Pour tout $z \in \mathcal{H}$ il existe $\gamma \in \Gamma(1)$ tel que $\gamma(z) \in D$.*
2) Supposons que deux points distincts $z, z' \in D$ soient congrus modulo $\Gamma(1)$. On a alors, soit $\mathrm{Re}\,(z) = \pm 1/2$ et $z = z' + 1$, soit $|z| = 1$ et $z' = -1/z$.
3) Soit $z \in D$, et soit $St(z) = \{\gamma \in \Gamma(1) \mid \gamma(z) = z\}$ le stabilisateur de z dans $\Gamma(1)$. On a $St(z) = \{\pm 1\}$ sauf dans les trois cas suivants:
$z = i$, auquel cas $St(z)$ est le groupe d'ordre 4 engendré par S;
$z = \rho = e^{2\pi i/3}$, auquel cas $St(z)$ est le groupe d'ordre 6 engendré par $ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$;
$z = -\overline{\rho} = e^{\pi i/3}$, auquel cas $St(z)$ est le groupe d'ordre 6 engendré par $TS = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

2.1.2. Théorème (génerateurs du groupe modulaire). *Les matrices S et T engendrent $\Gamma(1)$*

Démontration des théorèmes 2.1.1 et 2.1.2. Soit Γ' le sous–groupe de $\Gamma(1)$ engendré par S et T, et soit $z \in \mathcal{H}$. On va voir qu'il existe $\gamma' \in \Gamma'$ tel que $\gamma' \in D$ (ce qui démontrera l'assertion 1) de Théorème 1.2.1. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément e Γ', on a

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

comme c et d sont entiers, le nombre des couples (c,d) tels que $|cz+d|$ sont inférieur à un nombre donné est fini. On en conclut qu'il exist $\gamma \in \Gamma'$ tel que $\mathrm{Im}\,(\gamma(z)$ soit maximum. Il existe d'autre part un entier n tel que $T^n\gamma(z)$ ait une partie réele comprise entre $-1/2$ et $1/2$. L'élément $z' = T^n\gamma(z)$ appartient à D; en effet, il suffit de vour que $|z'| \geq 1$; mais si l'on avait $|z'| < 1$ l'élément $S(z')$ aurait une partie imaginaire strictement plus grande que $\mathrm{Im}\,(z')$, ce qui est impossible. L'élément $\gamma' = T^n\gamma$ répond donc à la question.

Prouvons maintemant les assertions 2) et 3) du théorème. Soient $z \in D$ et $\gamma \in Ga(1)$ tels que $\gamma(z) \in D$. Qitte à remplacer (z,γ) par $(\gamma(z),\gamma^{-1})$ on peut suposer que $\mathrm{Im}\,(g(z)) \geq \mathrm{Im}\,(z)$, i.e. que $|cz+d|$ est ≤ 1. Ceci est évidemment impossible si $|c| \geq 2$. Restent donc les cas $c = 0, 1, -1$. Si $c = 0$, on a $d = \pm 1$ et γ est une translations par $\pm b$. Comme $\mathrm{Re}\,(z)$ et $\mathrm{Re}\,(\gamma(z))$ sont deux compris entre $-1/2$ et $1/2$, cela entraîne, soit $b = 0$ et $\gamma = \pm 1$, soit $b = \pm 1$, auquel cas l'on des nombres $\mathrm{Re}\,(z)$ et $\mathrm{Re}\,(\gamma(z))$ doit être égal à $1/2$, l'autre $-1/2$. Si $c = 1$, le fait que $|z+d|$ soit ≤ 1 entraîne $d = 0$, sauf si $z = \rho$ (resp. $z = -\overline{\rho}$) auquel cas on peut avoir $d = 0, 1$ (resp. $d = 0, -1$). Le cas $d = 0$ donne $\gamma(z) = a - (1/z)$ et la première partie de la discusion montre que $a = 0$ sauf si $\mathrm{Re}\,(z) = \pm 1/2$, i.e. si $z = \rho$ ou $-\overline{\rho}$, auquel cas on peut prendre $a = 0, -1$ ou $a = 0, 1$. Le cas $z = \rho$, $d = 1$ donne $\gamma(z) = a - 1/(1+\rho) = 1 + \rho$, d'où $a = 0, 1$; on traite de même le cas $c = 1$ en changement les signes de a, b, c, d (ce qui ne change pas la transformation definit par γ. Ceci achève la vérification des assertions 2) et 3).

Il nous reste à prouver que $\Gamma' = \Gamma(1)$. Soit γ un élément de $\Gamma(1)$. Chosissons un point z_0 intérieur à D (par exemple $z_0 = 2i$), et soit $z = \gamma(z_0)$. On a vu plus haut qu'il existe $\gamma' \in \Gamma'$ tel que $\gamma'(z) \in D$. Les points z_0 et $\gamma'(z)$ sont congrus modulo $\Gamma(1)$, et l'un d'eux est intérieur à D. D'après 2) et 3) il en résulte que ces points sont confondues et que $\gamma'\gamma = \pm 1$. On a donc bien que $\gamma \in \Gamma'$ ce qui achève la démonstration.

2.1.3. Classification des éléments de $\mathrm{SL}(2,\mathbf{R})$**.** Nous appellons une classification géométrique des éléments de $\mathrm{SL}(2,\mathbf{R})$. (a) On apelle $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *elliptique*, si la forme normale de Jordan de γ est de type $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{smallmatrix}\right)$ avec $|\lambda| = 1, \lambda \neq \pm 1$. Cette condition est équivalante au fait que $|a+d| < 2$, où à la condition que la transformation $z \mapsto \gamma(z)$ a une seul point fixé dans $\mathcal{H}$ (et deux points complex–conjugués dans $\mathbf{C}$).
(b) On apelle $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *parabolique*, si la forme normale de Jordan de γ est de type $\pm\left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right)$ avec $\mu \neq 0$. Cette condition est équivalante au fait que $|a+d| = 2$, où à la condition que la transformation $z \mapsto \gamma(z)$ a une seul point fixé dans $\overline{\mathbf{C}} = \mathbf{C} \cup \infty$ qui appartient à $\overline{\mathbf{R}} = \mathbf{R} \cup \infty$.
(c) On apelle $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *hyperbolique*, si la forme normale de Jordan de γ est de type $\left(\begin{smallmatrix} mu & o \\ 0 & mu^{-1} \end{smallmatrix}\right)$ avec $\mu \neq \pm 1, \mu \in \mathbf{R}$. Cette condition est équivalante au fait que $|a+d| > 2$, où à la condition que la transformation $z \mapsto \gamma(z)$ a deux points fixés dans $\mathbf{R} =$.

Exemple. S, ST, TS sont elliptiques, T^n sont paraboliques, $\left(\begin{smallmatrix} 6 & 1 \\ 5 & 1 \end{smallmatrix}\right)$ est hyperbolique.

Théorème 2.1.1 facilement implique que tout élément elliptique de $\Gamma(1)$ est conjugué dans $\Gamma(1)$ soit à $\pm S$, soit à $\pm ST$, tout élément hyperbolique de $\Gamma(1)$ est conjugué dans $\Gamma(1)$ à $\pm T^n$.

Soit f une fonction méromorphe sur $\mathcal{H}$, non identifiquement nulle, et soit p un point de $\mathcal{H}$. Nous appellerons ordre de f en p, et nous noterons $v_p(f)$, l'entier n tel que $f/(z-p)^n$ soit holomorphe et non nul en p.

Lorsque f est une fonction modulaire de poids k, l'identité

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

montre que $v_p(f) = v_{\gamma(p)}(f)$ pour tout $\gamma \in Ga = \Gamma(1)$; en autre termes $v_p(f)$ ne dépend que de l'image de p dans $\Gamma\backslash H$. On peut de plus définir $v_\infty(f)$ comme l'ordre pour $q = 0$ de la fonction $\tilde{f}(q) = f(z)$ asociée à f. Posons $e_p = 2$ (resp.$e_p = 3$) si p est congru modulo Γ à i (resp. à ρ), et $e_p = 1$.

2.1.4. Proposition (sur le degré du diviseur d'une forme modulaire pour $\mathrm{SL}(2,\mathbf{Z})$**).** *Soit f une fonction modulaire de poids k par rapport à $\Gamma(1)$, non identiquement nulle. On a*

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

[On peut aussi écrire cette formule sous la forme

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in \Gamma(1)\backslash\mathcal{H}} {}^{*\prime} v_p(f) = \frac{k}{12},$$

où le signe $\sum_{p\in\Gamma(1)\backslash\mathcal{H}}{}^{*\prime}$ indique que la sommation porte sur les points de $\Gamma(1)\backslash\mathcal{H}$ ditincts des classes de i et de ρ].

Une démonstration simple utlise la structure naturelle de surface de Riemann sur $\Gamma(1)\backslash\overline{\mathcal{H}}$, où $\overline{\mathcal{H}} = \mathcal{H}\cup\mathbf{Q}\cup\infty$ (voir §2).

2.1.5. Théoreme (sur la fonction Δ de Ramanujan et les séries d'Eisenstein) *(i) On a $\mathcal{M}_k(\Gamma(1)) = 0$ pour $k < 0$ et $k = 2$.*

(ii) Pour $k = 0, 4, 6, 8, 10$ $\mathcal{M}_k(\Gamma(1))$ est un espace de dimension 1 admettant pour base $1, E_4, E_6, E_8, E_{10}$; on a $\mathcal{S}_k(\Gamma(1)) = 0$.

(iii) La multiplication par Δ définit un isomorphisme de $\mathcal{M}_{k-12}(\Gamma(1))$ sur $\mathcal{S}_k(\Gamma(1))$.

2.1.6. Téorème (dimension des espaces des formes modulaires pour $\mathrm{SL}(2,\mathbf{Z})$**).** *(a)*

$$\dim\mathcal{M}_k(\Gamma(1)) = \begin{cases} \left[\frac{k}{12}\right], & k\equiv 2(\mathrm{mod}12),\ k\geq 0,\\ 0, & k\equiv 1(\mathrm{mod}2),\\ \left[\frac{k}{12}\right]+1, & k\not\equiv 2(\mathrm{mod}12),\ k\geq 0,\ k\in 2\mathbf{Z}.\end{cases}$$

$$\dim\mathcal{S}_k(\Gamma(1)) = \begin{cases} \left[\frac{k}{12}\right]-1, & k\equiv 2(\mathrm{mod}12),\ k\geq 12,\\ 0, & k\equiv 1(\mathrm{mod}2),\\ \left[\frac{k}{12}\right], & k\not\equiv 2(\mathrm{mod}12),\ k\geq 0,\ k\in 2\mathbf{Z}.\end{cases}$$

(b) Les produits

$$\{E_4^\alpha E_6^\beta \mid 4\alpha + 6\beta = k\}$$

forment une base de $\mathcal{M}_k(\Gamma(1))$

Démonstraion est immédiate de 1.2.5.

Corollaire. *On a l'identité*

$$\Delta(z) = \frac{1}{1728}(E_4^3 - E_6^3).$$

En effet $\Delta(z)\in\mathcal{S}_{12}(\Gamma(1))$, et par 1.2.6 $\dim Sc_{12}(\Gamma(1)) = 1$, et il reste à remarquer que la fonction $\frac{1}{1728}(E_4^3 - E_6^3)$ aussi appartient à $\mathcal{S}_{12}(\Gamma(1))$, et que toutes les deux fonctions ont le coefficient de q égale à 1.

2.1.7. Application: une démonstration de la congruence de Ramanujan

$$\tau(n)\equiv\sigma_{11}(n) \bmod 691.$$

En effet,

$$E_6^2(z) = \left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)^2 \in\mathbf{Z}[[q]],$$

donc on peut développer $E_6^2(z)$ sur la base E_{12}, Δ de l'espace $\mathcal{M}_{12}(\Gamma(1))$ de dimension 2: $E_6^2 = E_{12} + \alpha\Gamma$, où

$$1 - 1008q + \ldots = 1 + \frac{65520}{691}q + \ldots + \alpha q + \ldots,$$

et $\ldots = \mathcal{O}(q^2)$. Alors

$$\alpha = -1008 - \frac{65520}{691} = \frac{a}{691} \quad \text{avec } a \equiv -65520(\mathrm{mod} 691),$$

et le développement implique

$$\frac{65520}{691}\sigma_{11}(n) + \frac{a}{691}\tau(n) \in \mathbf{Z}, \quad \text{où} \quad 65520(\sigma_{11}(n) - \tau(n)) \equiv 0(\mathrm{mod} 691),$$

d'où la congruence.

2.2. Formes modulaires pour sous–groupes de congruence de $\mathrm{SL}_2(\mathbf{Z})$

2.2.1. Exemples des formes modulaires de niveau supérieur. Nous avons déjà renconteré certaines exemples des formes modulaires pour sous–groupes de congruences de $\mathrm{SL}_2(\mathbf{Z})$. La fonction

$$f_{23}(z) = q \prod_{m=1}^{\infty} (1-q^m)(1-q^{23m}) =$$

$$\frac{1}{2}\left\{ \sum_{m,n} q^{m^2+mn+6n^2} - \sum_{m,n} q^{2m^2+mn+3n^2} \right\} \in \mathcal{S}_1(23, \varepsilon_{-23})$$

provient une exemple d'une forme parabolique sur $\Gamma_0(23)$ avec le caractère de Dirichlet $\varepsilon_{-23}(d) = \left(\frac{-23}{d}\right)$. En effet, soit f la partie droite, alors $f \in \mathcal{S}_1(23, \varepsilon_{-23})$ par le théorème de Hecke–Schöneberg. On voit que $f_{23}(z)^{24} = \Delta(z)\Delta(23z)$. Considérons la fraction $f^{24}/f_{23}^{24} = f^{24}/\Delta(z)\Delta(23z)$, qui est une fonction holomorphe sur $\Gamma_0(23)\backslash H$. Nous allons voir que

$$X_{\Gamma_0(23)} = \Gamma_0(23)\backslash H \cup \{0\} \cup \{\infty\}$$

a une structure naturelle de surface de Riemann compact. D'autre part, il est clair que la fonction $\Delta(z)\Delta(23z)$ a un zéro d'ordre 24 en ∞ et en 0 car elle est invariante par rapport a l'involution $\left(\begin{smallmatrix} 0 & -1 \\ 23 & 0 \end{smallmatrix}\right)$. Ceci implique que $f^{24}/\Delta(z)\Delta(23z)$ est holomorphe partout sur $X_{\Gamma_0(23)}$ d'ou elle est une constante. Comaraison des coefficients de q complete la démonstration.

2.2.2. Séries d'Eisenstein de niveau supèrieur. La théorie de séries d'Eisenstein peut être étendue sur les sous–groupes de congruence (voir Hecke, Mathematische Werke, S.461–486).

Pour un réseau $\Lambda = \langle \omega_1, \omega_2 \rangle$, une base $\langle P, Q \rangle$ du groupe $\Lambda_N = N_{-1}\Lambda/\Lambda \cong (\mathbf{Z}/N\mathbf{Z})^2$, et pour une paire $a_1, a_2 \bmod N$ posons

$$G_k^{a_1,a_2,N}(\Lambda, P, Q) = \sum_{l \in \Lambda + a_2 P + a_2 Q} l^{-k},$$

où $k \geq 3$. Alors la série définit une forme modulaire suivante pour le sous–groupe de congruence principal $\Gamma(N)$ de niveau N et de poids k:

$$G_k(z; a_1, a_2, N) = \sum_{\substack{m_1 \equiv a_1 \bmod N \\ m_2 \equiv a_2 \bmod N}} (m_1 z + m_2)^{-k} = N^k G_k^{a_1,a_2,N}(\Lambda_z, \frac{1}{z}, \frac{1}{N}),$$

oú $\Lambda_z = \langle 1, z \rangle$.

En effet, cette série converge absolument, satisfait la propriété d'automorphie par rapport à $\Gamma(N)$ et admet le développement de Fourier suivant:

$$G_k(z; a_1, a_2, N) = \delta\left(\frac{a_1}{N}\right) \sum_{m_2 \equiv a_2 \bmod N} m_2^{-k} + \frac{(-2\pi i)^k}{N^k (k-1)!} \sum_{\substack{mm_1 > 0 \\ m_1 \equiv a_1 \bmod N}} m^{k-1} \mathrm{sgn} m \zeta_N^{a_2 m} q^{mm_1/N},$$

oú $\zeta_N = \exp(2\pi i/N)$.

Cette formule est facilement impliquée par le développment

$$\sum_{n \in \mathbf{Z}} (mz+n)^{-k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n m z} \quad (k \geq 2, m \neq 0)$$

que nous avons déjà unilisé plus haut. D'un autre côté, pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ on a

$$G_k(z; a_1, a_2, N)|_k \gamma = (cz+d)^{-k} G_k(\gamma(z); a_1, a_2, N) = G_k(z; a_1', a_2', N)$$

avec

$$(a_1', a_2') = (a_1, a_2) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod N.$$

Cela signifie que toutes les condition de la définition des formes modulares de poids k sur $\gamma(n)$ sont satisfées.

De même façon on peut on peut construire des séries analogues sur les groupes $\Gamma_1(N)$ et $\Gamma_0(N)$ (aussi avec un caractère de Dirichlet $\chi \bmod N$ quelconque):

$$G_k^{a,N}(\Lambda, P) = \sum_{l \in \Lambda + aP} l^{-k},$$

$$G_k^{\chi,N}(\Lambda, P) = \sum_{a \bmod N} \overline{\chi}(a) G_k^{a,N}(\Lambda, P)),$$

$$G_k^{a,N}(\Lambda, \langle P \rangle) = \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^*} G_k^{a,N}(\Lambda, P)$$

Exercise. Trouver les développements de Fourier des séries

$$G_k(a, N, z) = N^k G_k^{a,N}(\Lambda_z, \frac{1}{N})$$

$$G_k(\chi, N, z) = N^k G_k^{\chi,N}(\Lambda_z, \frac{1}{N}).$$

2.2.3. Surfaces de Riemann: exemples liés aux séries d'Eisenstein et aux réseaux complexes

Pour obtenir une déscription de la structure de l'algèbre des formes modulaires par rapport à un sous–groupe de congruence Γde $\mathrm{SL}(2,\mathbf{Z})$ il faut de nouveau considèré le domaine fondamentale $\Gamma\backslash H$. Cependant, la structure de $\Gamma\backslash H$ est en général plus complqué que celle de $\mathrm{SL}(2,\mathbf{Z})\backslash H$. Pour la mieux comprendre il faut fournir $\Gamma\backslash H$ avec une structure d'une surface de Riemann, c'est à dire, d'une variété complexe de dimension 1.

Nous donnons quelques examples et proprétés de surfaces de Riemann: Exemples connus de surfaces de Riemann sont:

(a) la sphère de Riemann S^2, pour laquelle le structure de surface de Riemann est donnée par la projection stereographique, qui identifie S^2 avec le plan projectif $\mathbf{CP}^1 = \mathbf{C}\cup\infty$

(b) le torus complexe $\mathbf{C}/\Lambda$, $\Lambda = \langle\omega_1,\omega_2\rangle$ est un réseau de $\mathbf{C}$. On peut fournir $\mathbf{C}/\Lambda$ avec la structure d'une courbe projective complexe à la manière suivante.

Considèrons la fonctions $\wp$ de Weierstrass

$$\wp(u) = \wp(u,\Lambda) = \frac{1}{u^2} + \sum_{l\in\Lambda}{}' \left(\frac{1}{(u-l)^2} - \frac{1}{l^2}\right)$$

(le prime signifie que $l \neq 0$); c'est une fonction méromorphe double périodique sur $\mathbf{C}$ avec les pôles doulble dans les points $u = l$. Pour sa dérivé on a

$$\wp'(u) = \wp'(u,\Lambda) = -2\sum_{l\in\Lambda} \frac{1}{(u-l)^3}.$$

Il est facile de voir que les développments de Laurant de $\wp(u)$ et de $\wp'(u)$ sont

$$\begin{aligned}
\wp(u) &= u^{-2} + \sum_{n=2}^{\infty}(2n-1)G_{2n}(\Lambda)u^{2n-2} = u^{-2} + 3G_4u^2 + 5G_6u^4 + \mathcal{O}(u^6) \\
\wp'(u) &= -2u^{-3} + \sum_{n=2}^{\infty}(2n-1)(2n-2)G_{2n}(\Lambda)u^{2n-3} \\
&= -2u^{-3} + 6G_4u + 20G_6u^3 + \mathcal{O}(u^5)
\end{aligned}$$

D'où on obtient la relation suivant

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3,$$

où

$$g_2 = 60\sum_{l\in\Lambda}{}'\frac{1}{l^4}, \qquad g_3 = 140\sum_{l\in\Lambda}{}'\frac{1}{l^6}.$$

(La fonction $\wp'(u)^2 - 4\wp^3 + 60G_4\wp + 140G_6$ est identiquement nul car son développement de Laurant en 0 contient ne que des puissances positives de u:

$$\begin{aligned}
\wp(u) &= u^{-2} + 3G_4u^2 + 5G_6u^4 + \mathcal{O}(u^6),\\
\wp^3(u) &= u^{-6} + 9G_4u^{-2} + 15G_6 + \mathcal{O}(u^2)\\
\wp'(u) &= -2u^{-3} + 6G_4u + 20G_6u^3 + \mathcal{O}(u^5),\\
\wp'^2(u) &= 4u^6 - 24G_4u^{-2} - 80G_6 + \mathcal{O}(u^2)
\end{aligned}$$

et cette fonction est une fonction double périodique sur $\mathbf{C}$ qui s'annule à l'origine, c'est à dire elle est la constante 0).

(c) Domaine fondamental de $\mathrm{SL}_2(\mathbf{Z})$**.** Nous avons vu que

$$\Delta(z) = \frac{1}{1728}(E_4^3 - E_6^2) = (2\pi)^{-12}(g_2^3 - 27g_3^2).$$

Posons

$$j(z) = \frac{g_2^3}{g_2^3 - 27g_3^2}, \quad \overline{\Gamma\backslash H} = \Gamma\backslash H \cup \{i\infty\}.$$

Alors $j(z)$ provient un isomorphisme $\overline{\Gamma\backslash H} \xrightarrow{\sim} \overline{\mathbf{C}} = S^1 = \mathbf{C} \cup \infty$.

Dans le paragraph suivant nous allons fournir $\overline{\Gamma\backslash H}$ avec une structure de surface de Riemann compacte. Ceci nous permetra de déterminer les dimensions des espaces des formes modulaires sur sous–groupes de congruence.

2.3. Surface de Riemann associée à un sous-groupe de congruence

2.3.1. Eléments elliptiques, paraboliques et hyperboliques d'un sous–groupe de $\mathrm{SL}(2,\mathbf{R})$**.** Soit $\Gamma \subset \mathrm{SL}_2(\mathbf{R})$ un sous-groupe discrèt.

Définition.

(a) On appelle $s \in H$ elliptique pour Γ s'il existe $\gamma \neq \pm 1$ tel que $\gamma(s) = s$; notation:

$$Ell(\Gamma) = \{s \in H \ |s \text{ elliptique } pour \ \Gamma\};$$

(b) On appelle $s \in \mathbf{R} \cup \{\infty\}$ parabolique pour Γ s'il existe $\gamma \neq \pm 1$ tel que $\gamma(s) = s$; notation:

$$Par(\Gamma) = \{s \in \mathbf{R} \cup \{i\infty\} \ |s \text{ parabolique } pour \ \Gamma\};$$

(c) On appelle $s \in \mathbf{R}$ hypérbolique pour Γ s'il existe $\mathbf{g}$ $a \neq \pm 1$ tel que $\gamma(s) = s$; notation:

$$Hyp(\Gamma) = \{s \in \mathbf{R} \ |s \text{ hyperbolique } pour \ \Gamma\}$$

Exercise. Trouver tous les éléments elliptiques, paraboliques et hyperboliques de $\Gamma = \Gamma(1) = \mathrm{SL}_2(\mathbf{Z})$. (Montrer que $Ell(\Gamma) = \{\gamma(i), \gamma(j) | \gamma \in \mathrm{SL}_2(\mathbf{Z})\}$, $Par(\Gamma) = \mathbf{Q} \cup i\infty$).

Plus généralement, pour tout $\Gamma \subset \mathrm{SL}_2(\mathbf{Z})$ d'indice fini on a $Par(\Gamma) = \mathbf{Q} \cup i\infty$.

Posons $\Gamma_s = \{\gamma \in \Gamma | \gamma(s) = s\}$ le stabilisateur de s dans Γ.

Soit $\Gamma \subset \mathrm{SL}_2(\mathbf{Z})$ d'indice fini. Posons $\overline{H} = H \cup \mathbf{Q} \cup i\infty = H \cup Par(\Gamma)$.

On a topoligie naturelle sur $\overline{H}$, ceci permit de définir l'espace topologique $\overline{\Gamma \backslash H}$. Pour cette topologie sur $\overline{H}$ une base de voisinages d'un point parabolique s est donnée par les ensembles $\{s\} \cup D$, où D est un disque ouvert dans H tangent à la droite réele au point s.

2.3.2. Structure complexe sur $\overline{\Gamma \backslash H}$**.** Pour fournir $\overline{\Gamma \backslash H}$ avec structure d'une surface de Riemann remarquons que pour tout $v \in \overline{H}$ il existe un voisinage U avec fermeture compact tel que

$$\Gamma_v = \{\gamma \in \Gamma \ |\gamma(U) \cap U = \emptyset\}$$

c'est dire, $\gamma(U) \cap U \neq \emptyset \Rightarrow g(v) = v$.

Ceci implique qu'on a l'inclusion

$$\Gamma_v \backslash U \hookrightarrow \overline{\Gamma \backslash H},$$

et $\Gamma_v \backslash U$ est un voisinage du point $\varphi(v)$ où φ la projection naturelle $\varphi : \overline{H} \to \overline{\Gamma \backslash H}$.

Si le point $v \in H$ est ni elliptique ni parabolique on a que Γ_v ne contient que 1 et possiblement –1. Donc on a un homeomorphisme $\varphi : U \to \Gamma_v \backslash U$.

Supposons que v est elliptique et posons $\overline{\Gamma}_v = \Gamma_v \cdot \{\pm 1\}/\{\pm 1\}$. Soit λ l'isomorphisme holomorphe de H sur le disc D tel que $\lambda(v) = 0$. Si l'ordre de $\overline{\Gamma}_v$ est égal à n, le groupe $\lambda \overline{\Gamma}_v \lambda^{-1}$ est formé par les transformations

$$w \mapsto \zeta^k w, \quad k = 0, 1, \cdots, n-1, \quad \zeta = e^{2\pi i/n}.$$

Dans ce cas là on définit la structure complexe en v par $p(\varphi(z)) = \lambda(z)^n$. Il est clair que p est un homeomorphisme sur un ouvert de $\mathbf{C}$.

Soit finalement s un point parabolique de Γ et ρ un élément de $\mathrm{SL}_2(\mathbf{R})$ tel que $\rho(s) = \infty$. Alors

$$\rho\Gamma\rho^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \ | m \in \mathbf{Z} \right\}$$

pour un nombre $h > 0$.

On définit alors un homeomorphisme p de $\Gamma_s \backslash U$ dans $\mathbf{C}$ par

$$p(\varphi(z)) = \exp[2\pi i \rho(z)/h]$$

qui provient la structure complexe cherchée au voisinage de s.

Soit X et X' deux surfaces de Riemann compactes et $f : X' \to X$ une application holomorphe. Alors f soit constante soit surjective. Dans le cas où f est surjective on dit que f est un revêtement. Si $z_0 \in X'$, $w_0 = f(z_0) \in X$ et u, t – des paramètres locaux aux points z_0, w_0 respectivement, on apelle l'indice de ramification $e = e(w_0)$de f en w_0 au-dessus de z_0 le nombre $e = v_{z_0}(t(f(z)))$, i.e.

$$t(f(z)) = a_e u(z)^e + a_{e+1} u(z)^{e+1} + \cdots, \quad a_e \neq 0,$$

dans un voisinage de z_0. Il n'y a qu'un nombre fini des image réciproques d'un point w_0 fixé; si $e_1, \cdots, e_h$ sont les indices de ramification correspondantes, leur somme $n = e_1 + \cdots + e_h$ ne depend pas de point w_0 et est appellé le degré du revêtement f.

2.3.3. Théorème (formule de Hurwitz) *Soit $g = g(X)$, $g' = g'(X)$ les genres de X, X'. Alors*

$$2g' - 2 = n(2g - 2) + \sum_{z \in X'} (e_z - 1).$$

2.3.4. Le revêtement défini par un sous–groupe d'indice fini et sa ramification.

Considérons le revêtement

$$X_{\Gamma'} \longrightarrow X_\Gamma, \quad \overline{\Gamma' \backslash H} \to \overline{\Gamma \backslash H}$$

pour un sous-groupe $\Gamma' \subset \Gamma$ d'indice fini. Soit

$$\overline{\Gamma} = \Gamma \cdot \{\pm 1\}/\{\pm 1\}, \quad \overline{\Gamma'} = \Gamma' \cdot \{\pm 1\}/\{\pm 1\}$$

les images dans $\mathrm{PSL}_2(\mathbf{R}) = \mathrm{SL}_2(\mathbf{R})/\{\pm 1\}$, alors $n = [\overline{\Gamma} : \overline{\Gamma'}]$. Pour tout $z \in \overline{H}$ considérons le diagramm suivant:

$$\begin{array}{cccccc} & \overline{H} & \xrightarrow{id} & \overline{H} & \\ \varphi' & \downarrow & & \downarrow & \varphi \\ & \overline{\Gamma' \backslash H} & \xrightarrow{f} & \overline{\Gamma \backslash H} & \end{array}$$

les projections naturelles. Soit $z \in \overline{H}$, $p = \varphi(z)$ et $f^{-1}(p) = \{q_1, \cdots, q_h\}$. Choisissons des points w_k tels que $q_k = \varphi'(w_k)$.

2.3.5. Proposition (Le genre d'une courbe modulaire). *L'indice de ramification* e_k *de* f *en* q_k *est égale à* $[\overline{\Gamma}_{w_k} : \overline{\Gamma'}_{w_k}]$. *Si* $w_k = \sigma_k(z)$ *pour* $\sigma_k \in \overline{\Gamma}$ *on a:*

$$e_k = [\overline{\Gamma_z} : \sigma_k^{-1}\overline{\Gamma'}\sigma_k \cap \overline{\Gamma_z}]$$

et $\overline{\Gamma} = \cup_{k=1^h}\overline{\Gamma'}\sigma_k\overline{\Gamma_z}$ *(la réunion disjoint). En particulière, si* Γ' *est distingué on a* $e_1 = \cdots = e_h$ *et* $[\overline{\Gamma} : \overline{\Gamma}'] = e_1 h$.

Les surfaces de Riemann $X_\Gamma = \overline{\Gamma\backslash H}$ sont compactes et alors ils admetent une structure d'une courbe algébrique notée aussi par X_Γ. On appelle X_Γ courbe modulaire. Par example $X_{\Gamma(1)} = \overline{\mathrm{SL}_2(\mathbf{Z})\backslash H}$ a une structure canonique de la droite projective complexe $\mathbf{CP}^1$ fournie par l'invariant $J(z) = \frac{1728E_4^3}{E_4^3 - E_6^2}$. On voit donc que $g(X_{\Gamma(1)}) = 0$.

En utilisant la description de la ramification si-dessus on va trouver tout d'abord les genres des courbes modulaires (voir Shimura, Ch.1, §1.6).

Proposition. *Le genre* $g = g_\Gamma = g(X_\Gamma)$ *est donné par la formule*

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Démonstration utilise la formule de Hurwitz.

Soit $e_1, \ldots, e_t$ les indices de ramification des points w_k de $\overline{\Gamma\backslash H}$ au-dessus de $\varphi_\Gamma(j)$, $j = e^{2\pi i/3}$. Alors $\mu = e_1 + \ldots e_t$ ou $e_3 = 1$ ou 3. Le nombre d'indices k avec $e_k = 1$ est égal à ν_3 car $e_k = [\overline{\Gamma(1)}_j : \overline{\Gamma}_{w_k}]$. Posons $t = \nu_3 + \nu_3'$ alors $\mu = \nu_3 + \nu_3'$. Ceci implique

$$\sum_{k=1}^{t}(e_k - 1) = \mu - t = 2\nu_3' = \frac{2(\mu - \nu_3)}{3}$$

Par analogie,

$$\sum_{P\ au-dessus\ de\ \varphi(i)} (e_P - 1) = \frac{\mu - \nu_2}{2}$$

$$\sum_{P\ au-dessus\ de\ \varphi(\infty)} (e_P - 1) = \mu - \nu_\infty.$$

Il reste de substituer ces données dans la formule Hurwitz.

On utilise souvent la notation $X(N) = \overline{\Gamma(N)\backslash H}$, $X_0(N) = \overline{\Gamma_0(N)\backslash H)}$, $X_1(N) = \overline{\Gamma_1(N)\backslash H)}$.

2.3.6. Le genre de $X(N)$.

Soit $\Gamma(N)$ le sous groupe de congruence principal de niveau N donc $\mathrm{SL}_2(\mathbf{Z}) = \Gamma(1)$. Pour un revêtement

$$\overline{\Gamma\backslash H} \longrightarrow \overline{\Gamma(1)\backslash H}$$

on va déterminer les indices de ramification. On a vu que le degré du revêtement est égal à $\mu = [\overline{\Gamma(1)} : \overline{\Gamma}]$. On va noter par φ_Γ la projection naturelle de $\overline{H}$ sur $\overline{\Gamma\backslash H}$. Si z un point elliptique de $\Gamma(1)$ on a $|\overline{\Gamma(1)}_z| = 2$ ou 3.

Par contre, si $N > 1$ on a $||\overline{\Gamma(N)}_z| = 1$. En effet, Nous avons déjà vu que tout élément elliptique de $\Gamma(1)$ est conjugé à un des éléments suivants:

$$\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \pm\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Mais aucun de ces éléments est conjugé avec 1_2 modulo N. Le fait que $\Gamma(N)$ est ditingué implique l'affirmation.

Posons $\nu_2 = \nu_2(\Gamma)$, $\nu_3 = \nu_3(\Gamma)$ pour le nombre de point elliptiques d'ordre 2 (resp. 3) sur X_Γ, et soit ν_∞ le nombre des points paraboliques. Soit $\mu = [\overline{\Gamma(1)} : \overline{\Gamma}]$.

Soit $\Gamma = \Gamma(N)$, $N > 1$. Alors $\nu_2 = \nu_3 = 0$, $\nu_\infty = \mu/N$. C'est un sous-groupe distingué, et il suffit de verifier que $e_s = N$ pour $s \in \overline{H}$ tel que $\varphi_{\Gamma(N)}(s) = i\infty$. Mais $\Gamma(N)_s = \{\pm\left(\begin{smallmatrix} 1 & Nb \\ 0 & 1 \end{smallmatrix}\right) | b \in \mathbf{Z}\}$ d'où le résultat. Alors

$$g_N = g(\Gamma(N)) = 1 + \frac{\mu \cdot (N-6)}{12N} \quad (N > 1).$$

On a déjà vu que

$$\mu = \frac{N^3}{2}\prod_{p|N}(1 - p^{-2}) \textit{ pour } N > 3 \textit{ et } \mu = 6 \textit{ pour } N = 2.$$

Exercise. Montrer que les points paraboliques $s = a/b$, $s' = a'/b'$ du groupe $\Gamma(N)$ sont $\Gamma(N)$–équivalent si et seulement si

$$\begin{pmatrix} a \\ b \end{pmatrix} \equiv \pm\begin{pmatrix} a' \\ b' \end{pmatrix} \bmod N$$

2.3.7. Le genre de $X_0(N)$. Considérons maintenant le sous–groupe $\Gamma_0(N)$. On a $\mu = N\prod_{p|N}(1 + p^{-1}) = \sharp\mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$. La ramification est donnée par la

Proposition. *Pour $\Gamma = \Gamma_0(N)$ on a*

$$\nu_2 = \begin{cases} 0, & \textit{si } N \textit{ est divisible par 4,} \\ \prod_{p|N}\left(1 + \left(\frac{-1}{p}\right)\right), & \textit{sinon} \end{cases}$$

$$\nu_3 = \begin{cases} 0, & \textit{si } N \textit{ est divisible par 9,} \\ \prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right), & \textit{sinon,} \end{cases}$$

$$\nu_\infty = \sum_{d|N, d>0} \varphi\left(\left(d, \frac{N}{d}\right)\right),$$

où φ est la fonction d'Euler.

Démonstration. Considérons d'abord l'ensemble A_N des paires (c,d) données par

$$A_N = \{(c,d) \mid (c,d) = 1,\ d|N, 0 < c \leq N/d\}.$$

Pour une telle (c,d) choisissons a, b tel que $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. Alors on obtient un système exact des réprésentant de $\Gamma_0 \backslash \mathrm{SL}_2(\mathbf{Z})$. En effet ces éléments ne sont pas équivalents modulo $\Gamma_0(N)$ et leur nombre est exactement égale à μ si-dessus.

Le nombre ν_∞ est égale au nombre des classes d'équivalence doulbles

$$\Gamma_0(N) \backslash \Gamma(1) / \Gamma_s$$

pour un point parabolique arbitraire s. Prenons $s = 0$. Alors ν_∞ est égale au nombre de paires de A_N modulo la relation d'èquivalence suivante:

$$(c,d) \sim (c', d') \Leftrightarrow \begin{pmatrix} * & * \\ c' & d' \end{pmatrix} = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \quad \textit{pour un } m \in \mathbf{Z}$$

Ceci implique $d = d', c' = c + dm$, i.e. pour un d fixé il y a exactement $\varphi\left(\left(d, \frac{N}{d}\right)\right)$ paires non–équivalentes, d'où la formule pour ν_∞.

Pour déterminer ν_3 notons par S_1 (par S_2) le nombre d'éléments elliptiques de $\Gamma(1)$ congrus à $\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ (resp. à τ^2). Nous allons vérifier que ν_3 coincide avec le nombre d'idéaux J de l'anneau $A = \mathbf{Z}[j]$ qui satisfont aux propriétés i) ii) si-dessous:

i) $N(J) = N = |A/J|$;

ii) J n'est pas divisible par aucun nombre positive supérieur à 1.

Ceci entraînera immédiatement la formule chrchée par la considération de la décomposition de J en produit des idéaux premiers.

Posons

$$L = \mathbf{Z}^2, L_N = \left\{ \begin{pmatrix} x \\ Ny \end{pmatrix} \in L | x, y \in Z \right\}.$$

Alors

$$\Gamma_0(N) = \{\gamma \in \Gamma(1) \mid \gamma L_N = L_N\}.$$

Pour $\sigma \in S_1 \cup S_2$ considérons L comme un A–module. Le fait que A est un anneau principal implique qu'il existe un $\mathbf{Z}$–isomorphisme $f : A \to L$ tel que $f(jx) = \sigma f(x)$ pour tous $x \in A$
.

Soit T l'ensemble de tous les $\mathbf{Z}$–isomorphismes de A à L, alors T est la réunion disjoit de T_1 et T_2, où

$$T_i = \{f \in T \mid \exists \sigma \in S_i \forall x \in A \quad on \quad a \quad f(jx) = \sigma f(x)\}$$

Posons $J = f^{-1}(L_N)$. De la caractèrisation de $\Gamma_0(N)$ si-dessus on voit facilement que J est un idéal de $A \Leftrightarrow \sigma \in \Gamma_0(N)$ qui satisfait les proprétés i) et ii): le fait que f est un $\mathbf{Z}$–isomorphisme entraîne que J n'est pas divisible par aucun nombre positive supérieur à 1 A parce que le même est vrai pour $L_N \subset L$.

Exercise. Vérifier que l'association σ à J provient une bijection entre l'ensemble des classes de cojugaison des éléments elliptiques σ dans $\Gamma_0(N)$ et des idéaux J aves les propriétés i), ii) si–dessus.

De même façon on trouve ν_2 en utilisant l'anneau $\mathbf{Z}[i]$.

Exemple. Soit $N = p$ un nombre premier. Alors $\nu_\infty = 2$, les point paraboliques non–équivalent sont 0 et ∞, le revêtement

$$\overline{\Gamma_0(p)\backslash H} \to \overline{\Gamma(1)\backslash H}$$

est de degré $p+1$, les indices de ramification en 0 et ∞ sont égaux à p et 1 resp.

Corollaire. Toutes les courbe modulaires $X_0(N)$ de genre ≤ 2 sont données par le tableau:

genre de $X_0(N)$	N
0	$1 \leq N \leq 10, 12, 13, 16, 18, 25$
1	$11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$
2	$22, 23, 26, 28, 29, 31, 37, 50$

Posons $\alpha = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ alors $\Gamma_0(N) = \alpha^{-1}\Gamma(1)\alpha$. Ceci implique que le corps de fonction $\mathbf{C}(X_0(N))$ est engendré par $J(z), J(Nz)$: $\mathbf{C}(X_0(N)) = \mathbf{C}(J(z), J(Nz))$.

2.3.8. Premiers application aux formes modulaires. En utilisant l'information obtenue si-dessus on va déterminer maintenant les dimensions des espaces des formes modulaires pour les sous–groupes de congruence.

L'idée de cette calcul et démonstrée par le remarque suivant:

Proposition. *Pour un sous–groupe* $\Gamma \subset \Gamma$ *d'indice fini il y a l'isomorphisme naturel*

$$\mathcal{S}_2(\Gamma) \xrightarrow{\sim} \Omega^1[X_\Gamma], \quad f(z) \mapsto f(z)\,dz$$

En effet, pour $f \in \mathcal{M}_2(\Gamma)$ le differentiel $f(z)\,dz$ est invariant par rapport á Γ et $dz = \frac{1}{2\pi i}\frac{dq}{q}$. Ceci implique que le differentiel $f(z)\,dz$ est holomorphe aux points $s \in \mathbf{Q}\cup\{\infty\}$ $\Leftrightarrow$ f est parabolique.

Corollaire. $\dim S_2(\Gamma) = g(X_\Gamma)$.

D'un autre côté, pour $f \in \mathcal{M}_2(\Gamma)$ la somme des résidus du differentiel $f(z)\,dz$ doit être égale à 0 par un théorème classique sur les surfaces de Riemann compactes. Ce differentiel n'a que des pôles simples au points. Cela nous donne la formule

$$\dim \mathcal{M}_2(\Gamma) = g + \nu_\infty - 1.$$

Considérons le cas particulier $\Gamma = \Gamma_0(23)$.
On a $g(X_0(23)) = 2$, d'où $\dim \mathcal{S}_2(\Gamma) = 2$, $\dim \mathcal{M}_2(\Gamma) = 3$ car $\nu_\infty = 2$.
Considérons les séries théta $\theta_1, \theta_2 \in \mathcal{M}_1(23, \varepsilon_{-23})$

$$\theta_1(z) = \sum_{m,n} q^{m^2+mn+6n^2}, \quad \theta_1 = \sum_{m,n} q^{2m^2+mn+3n^2}.$$

Alors $\theta_1^2, \theta_1\theta_2, \theta_2^2 \in \mathcal{M}_2(23)$ forme une base de $\mathcal{M}_2(23)$ et $\dim \mathcal{M}_1(23, \varepsilon_{-23}) = 2$ (sinon on obtiendrait trop de fonction dans $\mathcal{M}_2(23)$). Donc $\mathcal{S}_1(23, \varepsilon_{-23}) = 1$ et maintenant onpeut montrer l'identité suivante

$$\begin{aligned} f_{23}(z) = & q \prod_{m=1}^{\infty} (1-q^m)(1-q^{23m}) = \\ & \frac{1}{2} \left\{ \sum_{m,n} q^{m^2+mn+6n^2} - \sum_{m,n} q^{2m^2+mn+3n^2} \right\} \in \mathcal{S}_1(23, \varepsilon_{-23}). \end{aligned}$$

Notamment,

$$q \prod_{m=1}^{\infty} (1-q^m)(1-q^{23m}) = \eta(z)\eta(23z)$$

où $\eta(z) = q^{\frac{1}{24}} \prod_{m=1}^{\infty}(1-q^m)$ est la fonction eta de Dedekind donc $\eta^{24}(z) = \Delta(z)$. De même façon que pour Δ on verifie tout d'abord que $\eta(z)\eta(23z) \in S_1(23, \varepsilon_{-23})$, donc proportionnelle à $\theta_1 - \theta_2$. En comparant les coefficient de q on a l'identité cherchée.

2.3.9. Lois de transformation de la fonction eta de Dedekind

Considérons la fonction eta de Dedekind

$$\eta(z) = q^{\frac{1}{24}} \prod_{m=1}^{\infty} (1-q^m)$$

Déjà Dedekind lui-même a demontré que

$$\log \eta \left(\frac{az+b}{cz+d} \right)) = \log \eta(z) = \frac{1}{2} \log(cz+d) + \pi i S(a,b,c,d),$$

où la branche principale du logarithme est considéré, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, et $S(a,b,c,d) = \frac{a+d}{12c} - \frac{1}{4}\frac{c}{|c|} - s(c,d)$. L'expression $s(c,d)$ est appellé la somme de Dedekind, et elle admete l'expression élémentaire suivante

$$s(c,d) = \sum_{\mu=0}^{|c|-1} \left(\left(\frac{d\mu}{|c|} \right) \right) \left(\left(\frac{\mu}{|c|} \right) \right)$$

où $((x)) = x - [x] - \frac{1}{2}$, $[x]$ est le plus grand entier $\leq x$. Dedekind aussi a demontré la lois de réciprocité pour les sommes $s(c, d)$

$$s(c,d) + s(d,c) = \frac{1}{4} + \frac{1}{12}\left(\frac{c}{d} + \frac{1}{cd} + \frac{d}{c}\right)$$

pur $(c, d) = 1$. Le fait remarquable est que la lois de réciprocité de Gauss est entraîné de la lois de Dedekind pour $s(c, d)$. En effet, on peut utiliser la formule

$$\left(\frac{d}{c}\right) = (-1)^{\left(\frac{c-1}{2} - 6c \cdot s(d,c)\right)}, c \equiv 1 (\mathrm{mod} 2).$$

Les démonstrations de ces fait se trouvent, par exemple, dans l'article de Don Zagier "Nombres de classes et fractions continues", Astérisque N° 24–25 (1975) 81–97, et dans le livre "introduction to modular forms" de S.Lang, Ch. IX.

2.4. Dimensions des espaces des formes modulaires

2.4.1. Diviseur d'une forme automorphe. Considérons la surface de Riemann $X_\Gamma = \overline{\Gamma \backslash H}$ pour un sous–groupe fuchsien Γ de $\mathrm{SL}_2(\mathbf{R})$ de premier espèce (par la définition cela signifie que $X_\Gamma = \overline{\Gamma \backslash H}$ est compact).

Définition. On appelle forme modulaire méromorphe f de poids k sur Γ une fraction de type f_1/f_2, où $f_1 \in \mathcal{M}_{k_1}(\Gamma)$, $f_2 \in \mathcal{M}_{k_2}(\Gamma)$ avec $k = k_1 - k - 2$. L'espace vectoriel complex de telles formes est noté par $\mathcal{A}_k(\Gamma)$.

Posons $K = \mathcal{A}_0(\Gamma)$ alors $\mathcal{A}_k(\Gamma)$ devient un espace vectoriel sur K de dimension ≤ 1. On peut vérifier que $K \neq \{0\}$ pour $k \in \mathbf{Z}$, k paire si $-1 \in \Gamma$.

Pour $F \in \mathcal{A}_2(\Gamma)$ l'expression $F(z)\,dz$ est invariant par rapport à Γ, et il est evident que l'association

$$F \mapsto F(z)\,dz$$

définit un isomorphism

$$\mathcal{A}_2(\Gamma) \xrightarrow{\sim} \Omega^1(X_\Gamma)$$

sur l'espace complexe $\Omega^1(X_\Gamma)$ des differentiels m'eromorphes sur X_Γ.

D'un autre côté, pour $k = 2n$ on a

$$\mathcal{A}_{2n}(\Gamma) \xrightarrow{\sim} \Omega^n(X_\Gamma),$$

où $\Omega^n(X_\Gamma)$ désigne l'espace complexe des differentiels méromorphes multiples sur X_Γ.

Pour tout $f \in \mathcal{A}_k(\Gamma)$ on va définir le diviseur $\mathrm{div}(f)$ à la manière suivante. Soit $P \in X_\Gamma$. Si P correspond à un point $z_0 \in H$ on sait que le paramètre locale en P est définit par $t = \lambda(z)^e$, où λ un isomorphisme holomorphe de H sur le disque ouvert D tel que $\lambda(z_0) = 0$, $e = |\overline{\Gamma}_{z_0}|$ l'ordre du point z_0. Posons $\nu_P(f) = \nu_{(z-z_0)}(f)/e$. Soit P un point parabolique, $\varphi(s) = P$, où $\varphi : \overline{H} \to X_\Gamma$ la projection naturelle, $s \in Par(\Gamma)$. Soit ρ un élément de $\mathrm{SL}_2(\mathbf{R})$ tel que $\rho(s) = \infty$. Alors si-dessus

$$\rho\Gamma\rho^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \;|m \in \mathbf{Z} \right\}$$

pour un nombre $h > 0$. On appelle P régilier si $\rho\Gamma\rho^{-1}$ est engendré par la matrice $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$, et on appelle P non-régilier si $-1 \notin \Gamma$ et le groupe $\rho\Gamma\rho^{-1}$ est engendré par la matrice $-\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. Si s est non–régulier et k est impair, la fonction $g(z) = f|_k\rho^{-1}$ satisfait la condition $g(z+h) = -g(z)$ alors $g(z+2h) = g(z)$. Par la définition des formes modulaires on a

$$f|_k\rho^{-1} = \begin{cases} \Psi(q_h^{1/2}), & \text{si } P \text{ est non–régulier, } k \text{ est impair} \\ \Phi(q_h), & \text{sinon} \end{cases}$$

où $q_h = \exp(2\pi iz/h)$, Ψ, Φ certaines fonctions méromorphes au voisinage de l'origine. Posons

$$\nu_P(f) = \begin{cases} \nu_t\Psi(t)/2 \quad (t = q_h^{1/2}), & \text{si } P \text{ est non–régulier, } k \text{ est impair} \\ \nu_{q_h}\Phi(q_h), & \text{sinon.} \end{cases}$$

Soir $\mathrm{Div}_{\mathbf{Q}}(X_\Gamma) = \mathrm{Div}(X_\Gamma) \otimes \mathbf{Q}$ le groupe des diviseurs à coefficients rationnels. Alors on associe à tout $f \in \mathcal{A}_k(\Gamma)$ un élément $\mathrm{div}(f) \in \mathrm{Div}_{\mathbf{Q}}(X_\Gamma)$ par la règle:

$$\mathrm{div}(f) = \sum_{P \in X_\Gamma} \nu_P(f) \cdot P.$$

Il est clair de la d'efinition qur

$$\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + \mathrm{div}(f_2) \quad (f_1 \in \mathcal{A}_{k_1}(\Gamma), f_2 \in \mathcal{A}_{k_2}(\Gamma).$$

2.4.2. Proposition (caractérisation des formes modulaires et des formes paraboliques par leur diviseur) *Dans la notation si-dessus on a*

$$\mathcal{M}_k(\Gamma) = \{f \in \mathcal{A}_k(\Gamma) \mid \mathrm{div}(f) \geq 0\}$$

et

$$\mathcal{S}_k(\Gamma) = \begin{cases} \left\{ f \in \mathcal{A}_k(\Gamma) \mid \mathrm{div}(f) \geq \sum_{i=1}^{u} Q_i + \frac{1}{2}\sum_{j=1}^{u'} Q'_j \right\} & \textit{si } k \textit{ est impair et } -1 \notin \Gamma \\ \left\{ f \in \mathcal{A}_k(\Gamma) \mid \mathrm{div}(f) \geq \sum_{i=1}^{u} Q_i + \sum_{j=1}^{u'} Q'_j \right\} & \textit{sinon} \end{cases}$$

où Q_i (resp. Q'_j) parcourt les poins régulier (resp. non-régulier) de X_Γ.

2.4.3. Proposition (sur le degré du diviseur d'une forme modulaire de niveau supérieur *Soit $P_1, ..., P_r$ les points elliptiques de X_Γ, $Q_1, ..., Q_u$ les points paraboliques* *réguliers,* $Q'_1, ..., Q'_{u'}$ *les points paraboliques non–réguliers de* Γ. *Soit* $f \in \mathcal{A}_k(\Gamma)$, $f \not\equiv 0$, *et, si* k *est pair* $\eta = f\,(dz)^{k/2}$. *Alors pour* k *pair on a*

$$\operatorname{div}(f) = \operatorname{div}(\eta) + \frac{k}{2} \cdot \left\{ \sum_{i=1}^{r} (1 - e_i^{-1}) P_i + \sum_{i=1}^{u} Q_i + \sum_{j=1}^{u'} Q'_j \right\}$$

et pour tout k *entier*

$$\deg \operatorname{div}(f) = \frac{k}{2} \left\{ (2g-2) + \sum_{i=1}^{r} (1 - e_i^{-1}) + u + u' \right\}.$$

Démonstration est entraînée des expressions pour dz/dt où t un paramètre local. Soit $P \in X_\Gamma$. Si P correspond à un point $z_0 \in H$ on sait que le paramètre locale en P est définit par $t = \lambda(z)^e$, où λ est si-dessus. Alors $dt/dz = d(\lambda(z)^e)/dz = e\lambda(z)^{e-1}(d\lambda/dz)$, ceci implique

$$\nu_t(dt/dz) = \nu_{\lambda(z)^e}(e\lambda(z)^{e-1} = \frac{e-1}{e} = 1 - e^{-1},$$

ou $\nu_t(dz/dt) = -(1 - e^{-1})$. Soit Q un point parabolique, $\varphi(s) = Q$, où $\varphi : \overline{H} \to X_\Gamma$ la projection naturelle, $s \in Par(\Gamma)$. Soit ρ si-dessus. Alors $t = q_h = \exp(2\pi i z/h)$ est le paramètre local si-dessus

$$\rho \Gamma \rho^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \; | m \in \mathbf{Z} \right\}.$$

On a $dt/dz = \frac{h}{2\pi i} t$ alors $\nu_Q(dz/dt) = -1$.

Il est commode d'écrire formellement

$$\operatorname{div}(dz) = \left\{ \sum_{i=1}^{r} (1 - e_i^{-1}) P_i + \sum_{i=1}^{u} Q_i + \sum_{j=1}^{u'} Q'_j \right\}.$$

Corollaire. *Pour* $\Gamma = \mathrm{SL}_2(\mathbf{Z})$, $f \in \mathcal{A}_k(\Gamma)$ *on a*

$$\deg \operatorname{div} f = \frac{k}{12}$$

Démonstration. En effet, $2g - 2 = -2$,

$$(2g-2) + \sum_{i=1}^{r} (1 - e_i^{-1}) + u + u' = -2 + 1 - \frac{1}{2} + 1 - \frac{1}{3} + 1 = \frac{1}{6},$$

et

$$\frac{k}{2} \left\{ (2g-2) + \sum_{i=1}^{r} (1 - e_i^{-1}) + u + u' \right\} = \frac{k}{12}.$$

Remarque. Le nombre

$$(2g-2)+\sum_{i=1}^{r}(1-e_i^{-1})+m$$

où $m=u+u'$ admet une interprétation géometrique important:

2.4.4. Théorème (le volume du domaine fondamentale) *La forme differentiel*

$$d\eta=\frac{dx\wedge dy}{y^2}=\frac{i}{y^2}dz\wedge\overline{dz},\quad \text{où}\quad \eta=y^{-1}dz,\ z=x+iy$$

est invariant par rapport à l'action de $\mathrm{SL}_2(\mathbf{R})$*, et elle definit une mesure* $\mathrm{SL}_2(\mathbf{R})$*-invariante* m *sur* H*. Pour la mesure du domaine fondamental de* $\Gamma\backslash H$ *on a la formule suivante:*

$$\frac{1}{2\pi}\int_{\Gamma\backslash H}y^{-2}dx\,dy=2g-2+m+\sum_{\nu=1}^{r}(1-e_\nu^{-1}).$$

(Pour la démonstration qui utilise la formule de Stokes voir G.Shimura, Ch.2, §2.5).

En particulière,

$$\int_{\mathrm{SL}_2(\mathbf{Z})\backslash H}y^{-2}dx\,dy=\frac{\pi}{3}.$$

Maintenant tout est prêt pour calculer les dimensions des espaces des formes modulaires. Soit $F_0\in\mathcal{A}_k(\Gamma)$, $F_0\not\equiv 0$. Posons $B=\mathrm{div}F_0$. Nous écrivons une forme modulaire méromorphe $F\in\mathcal{A}_k(\Gamma)$ sous la forme $F=fF_0$, où $f\in K=\mathcal{A}_0(\Gamma)$. On a déjà vu que

$$\mathcal{M}_k(\Gamma)=\{f\in\mathcal{A}_0(\Gamma)\mid \mathrm{div}(f)\geq -B\},$$

$$\mathcal{S}_k(\Gamma)=\left\{f\in\mathcal{A}_0(\Gamma)\mid \mathrm{div}(f)\geq -B+\sum_{i=1}^{u}Q_i+\sum_{j=1}^{u'}Q_j'\right\}.$$

Ici

$$-B,-B+\sum_{i=1}^{u}Q_i+\sum_{j=1}^{u'}Q_j'\in\mathrm{Div}_{\mathbf{Q}}(X_\Gamma).$$

Pour un $A=\sum_{P\in X_\Gamma}c_P\cdot P\in\mathrm{Div}_{\mathbf{Q}}(X_\Gamma)$ posons $[A]=\sum_{P\in X_\Gamma}[c_P]\cdot P$ (l'entier de A).

On vérifie facilement que $\mathrm{div}(f)\geq -A\Longleftrightarrow \mathrm{div}(f)\geq -[A]$. Soit $m=u+u'$ le nombre des points paraboliques. Pour $k=2n$ on voit que

$$\deg([B])=n(2q-2+m)+\sum_{i=1}^{r}[n(e_i-1)/e_i].$$

2.4.5. Théorème (Dimensions des espaces des formes modulaires de poids pair) *Soit* g *le genre de* X_Γ*,* m *le nombre des points paraboliques,* $e_1,\ldots,e_r$ *les ordres des points* *elliptiques (ou les éléments elliptiques de $\overline{\Gamma}$). Alors la dimension de l'espace vectoriel $\mathcal{M}_k$ pour un nombre pair k est donnée par la formule suivante*

$$\dim \mathcal{M}_k = \begin{cases} (k-1)(g-1) + \frac{k}{2}\cdot m + \sum_{i=1}^r [k(e_i-1)/2e_i]), & (k>2) \\ g+m-1, & (k=2, m>0) \\ g, & (k=2, m=0) \\ 1, & (k=0) \\ 0, & (k<0). \end{cases}$$

2.4.6. Théorème (Dimensions des espaces des formes paraboliques de poids pair) *La dimension de l'espace vectoriel $\mathcal{S}_k$ pour un nombre pair k est donnée par la formule suivante*

$$\dim \mathcal{S}_k = \begin{cases} (k-1)(g-1) + \left(\frac{k}{2}-1\right) m + \sum_{i=1}^r [k(e_i-1)/2e_i]), & (k>2) \\ g, & (k=2) \\ 1, & (k=0, m=0) \\ 0, & (k=0, m>0) \\ 0, & (k<0). \end{cases}$$

2.4.7. Théorème (Dimensions des espaces des formes modulaires de poids impair) *Soit $-1 \notin \Gamma$, u le nombre des points paraboliques réguliers, u' le nombre des points paraboliques non–réguliers, $e_1, ..., e_r$ les ordres des points elliptiques (ou les éléments elliptiques de $\overline{\Gamma}$ correspondants). Alors les dimensions de l'espaces vectoriels $\mathcal{M}_k$ et $\mathcal{S}_k(\Gamma)$ pour un nombre impair k sont donnée par les formules suivantes*

$$\dim \mathcal{M}_k = \begin{cases} (k-1)(g-1) + \frac{uk}{2} + \frac{u'(k-1)}{2} + \sum_{i=1}^r [k(e_i-1)/2e_i]), & (k \geq 3) \\ 0, & (k<3), \end{cases}$$

$$\dim \mathcal{S}_k = \begin{cases} (k-1)(g-1) + \frac{u(k-2)}{2} + \frac{u'(k-1)}{2} + \sum_{i=1}^r [k(e_i-1)/2e_i]), & (k \geq 3) \\ 0, & (k<3), \end{cases}$$

Démonstrations de tous ces théorèmes sont basées sur le théorème de Riemann–Roch. Par exemple, dans la situation du thérème 4.1 on identifie $\mathcal{M}_k(\Gamma)$ avec l'espace vectoriel

$$\mathcal{L}([B]) = \{f \in K |\ \mathrm{div}(f) \geq -B\},$$

On a

$$\deg([B]) - (2g-2) \geq (n-1)\left\{(2g-2) + \sum_{i=1}^r (1-e_i^{-1}) + m\right\}.$$

Si $n > 1$ ou $n = 1$ et $m > 0$ on a

$$l([B]) = \deg([B]) - g + 1$$

d'où le premier cas. Les autres cas sont considéré de la même façon ou plus facilement.

Remarque. Pour $k = 1$ cette méthode ne marche pas. On a $\deg([B]) = g - 1 + u/2$, ceci implique

$$\dim \mathcal{M}_1(\Gamma) \geq \frac{u}{2},$$

$$\dim \mathcal{M}_1(\Gamma) = \frac{u}{2} \textit{ pour } u > 2g - 2.$$

2.4.8. Exemple. Soit $N = 2, 3, 5, 11$ et $k = 24/(N+1)$. Alors $\mathcal{S}_k(\Gamma_0(N))$ a la dimension 1 et il est engendré par $(\Delta(z)\Delta(Nz))^{1/(N+1)}$.

En effet, la formule pour la dimension nous montre que $\dim(\mathcal{S}_k(\Gamma_0(N))) = 1$. D'autre part, la fonction $g(z) = \Delta(z)\Delta(Nz)$ est invariant par rapport a l'involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$, a des zéros d'ordre $N + 1$ en 0 et en ∞ et elle ne s'annule pas pour $z \in H$ (car elle donnée comme un produit convergent). Pour une forme parabolique $f \in \mathcal{S}_k(\Gamma_0(N))$ considérons la fraction $f^{1/(N+1)}/g$ qui est une constante car elle holomorphe sur $X_{\Gamma_0(N)}$ y compris les points 0 et ∞.

Chapitre 3. Théorie de Hecke

3.1. Opérateurs de Hecke

3.1.1. Motivations de la définition des opérateurs de Hecke. Opérateurs $U(m)$, $V(m)$ sur les développements de Fourier

Les exemples des séries d'Eisenstein et séries théta nous montrent un fait interessant: les coefficients de Fourier $a(n)$ de ces formes modulaires souvent soient les fonctions arithmétiques multiplicatives soit ils peuvent être représenter comme une combinaison linéaire de telle fonctions. Pour la fonction $\tau(n)$ de Ramanujan ces propriétés de multiplicativité ont la forme suivante:

$$\begin{aligned}
&\tau(mn) = \tau(n)\tau(m) \text{ for } (m,n) = 1,\\
&\tau(p^r) = \tau(p)\tau(p^{r-1}) - p^{11}\tau(p^{r-2}) \quad (p \text{ a prime number }, r \geq 2).
\end{aligned}$$

Soit m un entier positif, $f(z) = \sum_{n=0}^{\infty} a(n)e(nz)$ une fonction sur H. Alors la fonction suivante est définie

$$\begin{aligned}
f|U(m)(z) &= \sum_{n=0}^{\infty} a(mn)e(nz) = m^{k/2-1} \sum_{u \mod m} f|_k \begin{pmatrix} 1 & u \\ 0 & m \end{pmatrix},\\
f|V(m)(z) &= \sum_{n=0}^{\infty} a(n)e(mnz) = f(mz) = m^{-k/2} f|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Imaginons que l'opérateur

$$f \mapsto f|U(m)$$

agit sur l'espace des formes modulaires $\mathcal{M}_k(N,\psi)$. Alors on peut espérer à trouve une base de cet espace constitué par des fonctions propres de ces opérateurs. Si l'on suppose que f est une fonction propre on obtient la relation suivante

$$a(mn) = \lambda(m)a(n) \quad (n \in \mathbf{N})$$

où $\lambda(m)$ sont les valeurs propres correspondentes:

$$f|U(m) = \lambda(m)f.$$

Les propriétés de multiplicativité cherchées sont entraîner de cela. Cependent, si $f \in \mathcal{M}_k(N,\psi)$ alors dans le cas général on ne peut dire que

$$f|U(m)(z), f|V(m)(z) \in \mathcal{M}_k(mN,\psi),$$

et que

$$f|U(m)(z) \in \mathcal{M}_k(N,\psi)$$

n'a lieu quand m divise N. Pour évité cette difficulté dans le cas général remarquons que les matrices $\left(\begin{smallmatrix} 1 & u \\ 0 & m \end{smallmatrix}\right)$ dans la définition de $U(m)$ forment une partie d'un systéme exact des répresentantes des classes d'équivalance droits pour $\Gamma_0(N)\backslash\Delta_m(N)$, où $\Delta_m(N)$ note l'ensemble

$$\Delta_m(N) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}, c \equiv 0 \bmod N, \det\gamma = m\right\},$$

qui est invaiant par des multiplications droits par élements de $\Gamma_0(N)$. Comme une système complet des répresentantes des classes d'équivalance pour $\Gamma_0(N)\backslash\Delta_m(N)$ on peut prendre l'ensemble

$$\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d > 0, ad = m, b = 0, \ldots, d-1\right\}.$$

Ce fait nous permet de dfinir au lieu de $U(m)$ un autre opérateur qui agit sur l'espace des formes modulaires $\mathcal{M}_k(N, \psi)$. Cet autre opérateur s'appelle l'opérateur de Hecke $T(m)$:-

$$f \mapsto f|_k T(m) = m^{k/2-1} \sum_\sigma \psi(a_\sigma) f|_k \sigma,$$

où $\sigma = \left(\begin{smallmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{smallmatrix}\right) \in \Gamma_0(N)\backslash\Delta_m(N)$, $(m, N) = 1$.

3.1.2. L'action des opérateurs de Hecke sur les développements de Fourier. L'action de $T(m)$ sur les coefficients de Fourier est facile de déterminer en utilisant le système des representants si-dessus:

$$\begin{aligned} f|_k T(m) = &\sum_{m_1|m} \psi(m_1) m_1^{k-1} f|U(m/m_1)V(m_1) \\ =&a(0) \sum_{m_1|m} \psi(m_1) m_1^{k-1} \\ &+ \sum_{n=1}^{\infty} \sum_{m_1 \mid (m,n)} \psi(m_1) m_1^{k-1} a(mn/m_1^2) e(nz), \end{aligned}$$

où l'on utilise la convention que $a(x) = 0$ pour $x \notin \mathbf{Z}$.

Multiplication des systmes si-dessus nous montre que le règle de multiplication pour les opérateurs $T_k(m)$ a la forme donnée par la proposition suivante:

3.1.3. Proposition (la régle de la multiplication des opérateurs de Hecke). *Soit n, m premiers avec N. Alors*

$$T_k(m)T_k(n) = \sum_{m_1 \mid (m,n)} \psi(m_1) m_1^{k-1} T_k(mn/m_1^2). \qquad (*)$$

Démonstration. On va vérifier la regle (*) sur des développements de Fourier. On a

$$f|_k T(n) = \sum_{n_1|n} \psi(n_1) n_1^{k-1} f|U(n/n_1)V(n_1),$$

$$f|_k T(m) = \sum_{m_1|m} \psi(m_1) m_1^{k-1} f|U(m/m_1)V(m_1).$$

Alors

$$f|_k T(n)T(m) = \sum_{\substack{n_1,|n \\ m_1,|m}} \psi(n_1 m_1)(n_1 m_1)^{k-1} f|U(n/n_1)V(n_1)U(m/m_1)V(m_1).$$

Pour effectuer la commutation, on utilise

3.1.4. Lemme (la régle de commutation des opérateurs $U(m)$, $V(m)$). Soient $A, B \in \mathbf{N}$, δ =PGCD(A, B), alors pour $f = \sum_{n=0}^{\infty} a(n)e(nz)$ on a les identités suivantes:

$$f|V(A)U(B) = f|U(B/\delta)V(A/\delta).$$

En effet,

$$f|V(A)U(B) = \left(\sum_{n=0}^{\infty} a(n)e(nAz)\right)|U(B) = \sum_{\substack{n=0 \\ B|An}}^{\infty} a(n)e(nAz/B)$$

$$= \sum_{\substack{n=0 \\ (B/\delta)|(A/\delta)n}}^{\infty} a(n)e(nAz/B)) = \sum_{n=0}^{\infty} a((B/\delta)n)e(n(A/\delta)z) = f|U(B/\delta)V(A/\delta),$$

d'où le lemme.

Remarque. Lemme 3.1.4 montre que $f|V(A)U(A) = f$; par contre, $f|U(A)V(A) = \sum_{\substack{n=0 \\ A|n}}^{\infty} a(n)e(nz)$.

Si l'on utilise directement le lemme avec la notation δ = PGCD$(n_1, m/m_1)$, on voit que

$$f|_k T(n)T(m) = \sum_{\substack{n_1|n \\ m_1|m}} \psi(n_1 m_1)(n_1 m_1)^{k-1} f|U(n/n_1)U(m/m_1\delta)V(n_1/\delta)V(m_1)$$

$$= \sum_{\substack{n_1|n \\ m_1|m}} \psi(n_1 m_1)(n_1 m_1)^{k-1} f|U(nm/n_1 m_1 \delta)V(n_1 m_1/\delta).$$

Posons $n_2 = n_1/\delta$. Alors $n_2|(n/\delta)$, $m/m_1\delta \in \mathbf{Z}$, d'où $m_1|(m/\delta)$ et

$$f|_k T(n)T(m)$$
$$= \sum_{\delta|(n,m)} \psi(\delta)\delta^{k-1} \sum_{\substack{n_2|(n/\delta) \\ m_1|(m/\delta)}} \psi(n_2 m_1)(n_2 m_1)^{k-1} f|U((nm/\delta^2)/n_2 m_1)V(n_2 m_1),$$

d'où la proposition 3.1.3.

En particulier, les opérateurs $T_k(n)$ commutent. Si $f \in \mathcal{M}_k(N,\psi)$ est une fonction propre de tous les opérateurs $T_k(n)$ avec $(m,N)=1$, i.e. si l'on ait

$$f|T_k(m) = \lambda_h(m)f \quad ((m.n)=1),$$

alors l'evaluation de la règle de multiplication sur f implique

$$\lambda_f(m)\lambda_f(n) = \sum_{m_1 \ | \ (m,n)} \psi(m_1)m_1^{k-1}\lambda_f(mn/m_1^2).$$

3.1.5. Relations entre les coefficients de Fourier et les valeurs propres des opérateurs de Hecke. Produits euleriéns. La comparaison de coefficients de Fourier $a(n)$ provient l'identité suivante

$$a(0)\sum_{m_1|m} \psi(m_1)m_1^{k-1} = \lambda_f(m)a(0),$$

$$\sum_{m_1 \ | \ (m,n)} \psi(m_1)m_1^{k-1}a(mn/m_1^2) = \lambda_f(m)a(n).$$

En particulier, pour $n=1$ on a

$$a(m) = \lambda_f(m)a(1),$$

est pour $a(1) \neq 0$ la fonction $a(m)$ est alors proportionnelle à la fonction $\lambda(m)$ pour $(m,N)=1$.

Toutes ces propriétés peuvent être exprimer sous une forme commode en termes de séries de Dirichlet:

$$f(z) = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(N,\psi),$$

si-dessus posons formellement

$$L_N(s,f) = \sum_{\substack{n=1 \\ (N,n)=1}}^{\infty} \lambda_f(n)n^{-s}, \quad R_N(s,f) = \sum_{\substack{n=1 \\ (N,n)=1}}^{\infty} a(n)n^{-s}.$$

Alors ces séries de Dirichlet formelles satisfont les identités suivantes:

I) Le développement en produit d'Euler:

$$L_N(s,f) = \prod_{p \ : \ p \nmid N} [1 - \lambda_f(p)p^{-s} + \psi(p)p^{k-1-2s}]^{-1}.$$

II) $R_N(s,f) = a(1)L_N(s,f)$.

En effet, la règle de multiplicativité pour les nombres premiers distinct p_i, $p_i \not| N$ implique que

$$L_N(s,f) = \prod_{p\,:\,p \not| N} \left(\sum_{\delta=0}^{\infty} \lambda_f(p^\delta) p^{-\delta s} \right),$$

et la sommation de toute de ces séries par rapport à δ peut–être effectuer à l'aide de la relation

$$\lambda_f(p)\lambda_f(p^\delta) = \lambda_f(p^{\delta+1}) + \psi(p)\lambda_f(p^{\delta-1}) \ (\delta \geq 1).$$

L'equation II) est impliquée directement de $a(m) = \lambda_f(m)a(1)$.

Dans Chapitre 4 on considère aussi les facteurs manquants dans le produit eulérien $L_N(s,f)$ qui correspondent aux diviseurs premiers de N.

3.1.6. Algèbre de Hecke. Interprétation géométrique des opérateurs de Hecke (en termes de réseaux).

3.2. Produit scalaire de Petersson.

3.2.1. Définitions diverses du produit scalaire de Petersson. Une base formée par des fonctions propres des opérateurs de Hecke peut – être construit en utilisant le produit scalaire de Petersson. Pour une forme modulaire $h \in \mathcal{M}_k(N,\psi)$ le produit scalaire de Petersson de h avec $f \in \mathcal{S}_k(N,\psi)$ est définie par la formule

$$\langle f,h\rangle_N = \int_{\Gamma_0(N)\backslash H} \overline{f(z)} h(z) y^{k-2}\, dx\, dy,$$

où $z = x+iy$, $H/\Gamma_0(N)$ est un domain fondamental pour H modulo $\Gamma_0(N)$. Alors on a la décomposition suivante:

$$\mathcal{M}_k(N,\psi) = \mathcal{S}_k(N,\psi) \oplus \mathcal{E}_k(N,\psi),$$

où $\mathcal{E}_k(N,\psi)$ est appellé l'espace des séries d'Eisenstein, une base duquel peut–être explicitement décrite et elle est formée par les séries du type si-dessus (Lang S. (1983a), Hecke E. (1959), Shimura G. (1971)).

Parfois il est commode d'utiliser le produit de Petersson absolu: pour un sous–groupe $\Gamma \subset \Gamma(1) = \mathrm{SL}(2,\mathbf{Z})$ de l'indice fini, $h \in \mathcal{M}_k(\Gamma)$ le produit scalaire absolu de Petersson de h avec $f \in \mathcal{S}_k(\Gamma)$ est définie par la formule

$$\langle f,h\rangle = \frac{1}{(\overline{\Gamma(1)} : \overline{\Gamma})} \int_{\Gamma\backslash H} \overline{f(z)} h(z) y^{k-2}\, dx\, dy,$$

donc ce produit ne dépend pas de choix d'un groupe $\Gamma \subset \Gamma(1)$.

Il est commode d'écrire

$$\langle f,h\rangle = \int_{\Gamma\backslash H} \Omega(f,h),$$

où $\Omega(f,h)(= \Omega(f,h)(z)$ désigne la forme differentielle

$$\Omega(f,h) = \overline{f(z)} h(z) y^{k-2}\, dx\, dy,$$

donc pour tout $\gamma \in \Gamma$ on a

$$\Omega(f,h)(\gamma(z)) = \Omega(f,h)(z).$$

3.2.2. L'interprétation à l'aide de la mesure de Haar sur le groupe $\mathrm{SL}(2,\mathbf{R})$.

3.2.3. Proposition sur les propriétés fondamantales du produit scalaire de Petersson.
(i) Soit $f \in \mathcal{M}_k(\Gamma(N))$ $\alpha \in \mathrm{M}_2(\mathbf{Z})$, $\det\alpha = m$. *Alors* $f \in \mathcal{M}_k(\Gamma(Nm))$.
(ii) Soit $f \in \mathcal{M}_k(\Gamma(N))$, $h \in \mathcal{S}_k(\Gamma(N))$, $\alpha \in \mathrm{M}_2(\mathbf{Z})$, $\det\alpha = m$. *Alors pour le produit absolu de Petersson on a*

$$\langle f|\alpha, h|\alpha\rangle = \langle f, h|\alpha\rangle,$$

où $\alpha' = m\alpha^{-1}$
(iii)

$$\langle f|\alpha, h\rangle = \langle f, h|\alpha'\rangle,$$

où $\alpha' = m\alpha^{-1}$
(iv) Si f, g *sont* Γ*–invariant, alors le produit* $\langle f|\alpha, g\rangle$ *ne dépend que de la classe double* $\Gamma\alpha\Gamma$ *de* α.

Démonstration. En effet, pour tout $\gamma = 1 + Nmx \in \Gamma(Nm)$, $x \in \mathrm{M}_2(\mathbf{Z})$ on a $f|\alpha\gamma = f|\alpha\gamma\alpha^{-1}\alpha = f|(1 + Nm\alpha x\alpha^{-1})\alpha = f|\alpha$, car $m\alpha^{-1} \in \mathrm{M}_2(\mathbf{Z})$ et $1 + Nm\alpha x\alpha^{-1} \in \Gamma(N)$, d'où on obtient (i).

Pour montrer (ii), il suffit d'effectuer l'integration, en faisant le changement de variable $z \mapsto \alpha(z)$, et en remplacant le domaine fondamental $\mathcal{D}_\Gamma$ de Γ par le domaine fondamental $\alpha\mathcal{D}$ de $\alpha\Gamma\alpha^{-1}$. Si $\Gamma \supset \Gamma(N)$ alors $\alpha\Gamma\alpha^{-1} \supset \Gamma(Nm)$ et dans la définition du produit scalaire de Petersson on peut utiliser le domaine fondamental du groupe $\Gamma(Nm)$.

3.2.4. Normalité des opérateurs de Hecke. On vérifie que les opérateurs $T_k(m)$ sur $\mathcal{S}_k(N,\psi)$ sont normales par rapport au produit de Petersson pour $(m,N) = 1$. De plus, les operateurs sont ψ–Hermitiens:

Proposition. Pour tout $f, h \in \mathcal{S}_k(N,\psi)$ **et** $(m,N) = 1$ **on l'identité suivante:**

$$\psi(m)\langle f|T_k(m), h\rangle_N = \langle f, h|T_k(m)\rangle_N.$$

Démonstration utilise la définition matricielle des opérateurs de Hecke. Soit

$$\Gamma_0(N)\Delta_m(N)\Gamma_0(N) = \Delta_m(N),$$

alors

$$f|T(m) = m^{\frac{k}{2}-1} \sum_{\sigma\Gamma_0(N)\backslash\Delta_m(N)} \psi(a_\sigma) f|\sigma.$$

Par Lemme 3.2.3 (iii)

$$\langle f|T(m), h\rangle = m^{\frac{k}{2}-1} \sum_{\sigma\Gamma_0(N)\backslash\Delta_m(N)} \overline{\psi(a_\sigma)} \langle f, g|\sigma'\rangle.$$

Ecrivons $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\sigma' = \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \gamma_1 \sigma \gamma_2 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$, où

$$c_1 \equiv c_2 \equiv 0(\mathrm{mod} N), a \equiv a_1 d a_2 (\mathrm{mod} N),$$

$$\langle f, g|\sigma' \rangle = \langle f, g|\gamma_1 \sigma \gamma_2 \rangle = \langle f|\gamma_2^{-1}, g|\gamma_1 \sigma \rangle = \psi(a_1)\psi(a_2)\langle f, g|\sigma \rangle = \psi(a/d)\langle f, g|\sigma \rangle.$$

Alors

$$\langle f|T(m), h \rangle = m^{\frac{k}{2}-1} \sum_{\sigma \Gamma_0(N) \backslash \Delta_m(N)} \overline{\psi(a_\sigma)} \psi(a/d) \langle f, g|\sigma \rangle = \langle f, h|T(m) \rangle,$$

ceci entraîne la Proposition.

3.2.5. Lemme sur des familles commutatives des opérateurs normaux. *Soit* $\{A_i\}_{i \in I}$ *une famille des opérateurs normaux dans un espace* V *hérmitien complexe de dimension finie telle que* $A_i A_j = A_j A_i$ *pour tout* $i, j \in I$. *Alors il existe une base orthogonal de* V *formée par des fonctions propres de tout les opérateurs* A_i.

Démonstration est standarde: soit $V^{(\lambda)}$ le sous–espace non-nul des vecteurs propres de A_{i_0} de la valeur propre λ. On peut supposer que A_{i_0} n'est pas un opérateur scalaire, donc $\dim V^{(\lambda)} < \dim V$. Alors par réccurence on trouve dans $\dim V^{(\lambda)}$ un vecteur propre v de tout les opérateurs A_i, et on considère le complémentaire orthogonal $\langle v \rangle^\perp$ qui est stable pour tout A_i.

En utilisant de nouveau raisonement par réccurence on montre le lemme.

3.2.6. L'existence des bases de Hecke. Par un théorème général de l'algèbre linéaire sur les familles des opérateurs commutant normales on peut choisir une base orthogonale de $\mathcal{S}_k(N, \psi)$ formée par des fonctions propres de tous $T_k(m)$, $((m, N) = 1)$.

Une base avec cette propriété est appelée une base de Hecke. Dans le cas où le nombre m n'est pas divisible que par les diviseurs premiers du niveau N, on peut utiliser l'opérateur $U(m)$ au lieu de $T_k(m)$. Comme on a remarqué plus haut ces opérateurs opèrent sur $\mathcal{M}_k(N, \psi)$. Cependent, ils ne sont plus normal, est ne sont pas en général diagonalisables dans $\mathcal{S}_k(N, \psi)$.

3.3. La transformée de Mellin d'une forme modulaire et son prolongement analytique.

3.3.1. Définition de la transformée de Mellin. Convergence absolu dans un demi–plan droit Soit

$$f(z) = \sum_{n=0}^{\infty} a(n) e(nz) \in \mathcal{M}_k(N, \psi).$$

Alors la série de Dirichlet

$$R(s, f) = R_1(s, f) = \sum_{n=1}^{\infty} a(n) n^{-s}$$

converge absoluement pour Re $s \gg 0$.

Convergence de ces séries pour Re $(s) \gg 0$ est entraînée des éstimées suivantes pout des coefficients de Fourier:

a) Si $f \in \mathcal{M}_k(N,\psi)$ alors
$$|a(n)| = O(n^{k-1+\varepsilon}), \quad \varepsilon > 0$$
et la série de Dirichlet serie converge absoluement pour Re $s > k$.

b) Si $f \in \mathcal{S}_k(N,\psi)$ on a
$$|a(n)| = O(n^{\frac{k-1}{2}+\varepsilon}), \quad \varepsilon > 0$$
et les séries $L_N(s,f)$ et $R_N(s,f)$ converge absoluement pour Re $s > \frac{(k+1)}{2}$.

Les éstimées si–dessus utilise quelques propriétés fines des coefficients de Fourier $a(n)$. Cependent, l'utilisation seulement des propriétés analytiques de $f(z)$ (le fait que cette fonction est holomorhe et qu'elle satisfaite la condition d'automorphie) permet d'obtenir certains éstimées plus faibles:-

a)
$$|a(n)| = O(n^k), \text{ for } f \in \mathcal{M}_k(N,\psi);$$

b)
$$|a(n)| = O(n^{k/2}), \text{ for } f \in \mathcal{S}_k(N,\psi);$$
la dernière éstimée est entraîné par l'éstimation $|f(z)| = O(y^{-k/2})$ $(y \to 0,\ z = x + iy)$.

Un prolongement analytique de ces séries sur le plan complex entier peut–être construit en utilisant la transformée de Mellin de f:
$$(2\pi)^{-s}\Gamma(s)R(s,f) = \int_0^\infty [f(iy) - a(0)]y^{s-1}\,dy \quad (\mathrm{Re}\,(s) \gg 0).$$
Cela peut être établi par l'intégration terme-par-terme de la série
$$f(iy) - a(0) = \sum_{n=1}^{\infty} a(n)\exp(-2\pi ny)$$
et en utilisant la représentation de la fonction gamma:
$$\Gamma(s) = \int_0^\infty e^{-y}y^{s-1}\,dy \quad (\mathrm{Re}\,(s) > 0).$$
L'espace vectoriel de toutes les séries de type $R(s,f)$ pour $f \in \mathcal{M}_k(N,\psi)$ peut être caractériser par les propriétés analytiques de ces séries. D'après Andrianov A.N. (1974), on va donner cette caractérisation dans le cas $N = 1$.

3.3.2. Théorème A (Prolongement analytique de la transformée de Mellin). Soit $f \in \mathcal{M}_k = \mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$. Alors la série de Dirichlet $R(s,f)$ admet un prolongement méromorphe sur le plane complex entier, et si l'on pose
$$\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)R(s,f),$$

alors la fonction

$$\Lambda(s,f)+\frac{a(0)}{s}+\frac{(-1)^{k/2}a(0)}{k-s}$$

est une fonction entier. On a l'équation suivante

$$\Lambda(k-s,f)=(-1)^{k/2}\Lambda(s,f).$$

3.3.3. Théorème B (Caractérisation des formes modulaires par des propriétés analytiques des séries de Dirichlet correspondentes). Toute série de Dirichlet $R(s)=\sum_{n=1}^{\infty}a(n)n^{-s}$ avec les coefficients $a(n)$ de croissance au plus polynomiale de n, satisfante aux conditions analytiques si-dessus doit avoir la forme $R(s,f)$ pout une forme modulaire $f\in\mathcal{M}_k=\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$.

3.3.4. Démonstrations de théorèmes A et B. Pour démontrer Théorème A on utilise la transformée de Mellin et on écrit

$$\Lambda(s,f)=\int_0^{\infty}[f(iy)-a(0)]y^{s-1}\,dy\quad(\mathrm{Re}\,(s)>k+1).$$

En remarquant que $f(-1/z)=z^kf(z)$ on voit bien que

$$\begin{aligned}\Lambda(s,f)&=\int_1^{\infty}[f(iy)-a(0)]y^{s-1}\,dy-\frac{a(0)}{s}+\int_0^1 f(iy)y^{s-1}\,dy\\&=\int_1^{\infty}[f(iy)-a(0)]y^{s-1}\,dy-\frac{a(0)}{s}+\int_0^1 f(-1/iy)y^{-s-1}\,dy\\&=\int_1^{\infty}[f(iy)-a(0)](y^{s-1}+i^ky^{k-s-1})\,dy-\frac{a(0)}{s}-\frac{i^ka(0)}{k-s}.\end{aligned}$$

La fonction $f(iy)-a(0)$ tend vers zéro exponentiellement si $y\to\infty$, donc le dernier intégrale converge absoluement pour tout s et il représent une fonction holomorphe de la variable s. Ceci implique la première affirmation. La substitution $s\mapsto k-s$ dans l'intégrale entraîne l'équation fonctionnelle pour $\Lambda(s,f)$ qui est multiplie par i^k,

Pour démontrer théorème B il suffit d'utiliser la transformation réciproque de Mellin, et le fait que le groupe modulaire $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les matrices $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$. La transformation réciproque de Mellin est définie à l'aide de la formule

$$e^{-y}=\frac{1}{2\pi i}\int_{(\sigma_0)}\Gamma(s)y^{-s}ds,$$

où l'intégration est étendu sur la droite verticale $(\sigma_0)=\{\sigma_0+it\mid t\in\mathbf{R}\}$, $\sigma_0>0$, grâce à certain déformation standard du contour (σ_0), qui permet de réduire l'intégrale à la somme des résidus:

$$\mathrm{Res}_{s=-n}\Gamma(s)y^{-s}=\frac{(-1)^ny^n}{n!}\ (n\in\mathbf{Z},n\geq 0).$$

En appliquant cette formule, on ait

$$f(iy) - a(0) = \frac{1}{2\pi i}\int_{(\sigma_0)} \Lambda(s,f)\, y^{-s} ds, \quad \sigma_0 > 0,$$

et ceci permet de récupérer la forme $f(z)$ et ces propriétés d'automorphie des propriétés analytiques de $\Lambda(s,f)$ (prolongement analytique, équation fonctionnelle).

Théorèmes A et B peuvent–être étendus sur les formes modulaires de poids enties par rapport aux sous-groupes de congruence de $\mathrm{SL}_2(\mathbf{Z})$ (avec des complications techniques naturelles)

Dans cette situation le théorème généralisant Théorème A est appelé le théorème direct, et celui généralisant Théorème B est appelé le théorème inverse. Ce théorème inverse a été etabli par A.Weil (1967) en termes de séries de Dirichlet tordus

$$\Lambda^*(s,f,\chi) = (2\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty} \chi(n)a(n)n^{-s},$$

où χ est un caractère de Dirichlet. Supposons que la série

$$R(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$$

converge absoluement pour $s = k - \delta$, $\delta > 0$, et que pout tout $\chi \mod r$, $(r,N) = 1$ la fonction $\Lambda^*(s,f,\chi)$ est entier, bornée dans toute bande verticale et satisfait une certaine équation fonctionnelle liant $\Lambda^*(s,f,\chi)$ avec $\Lambda^*(k-s,f^\rho,\overline{\chi})$, où $f^\rho(z) = \sum_{n=0}^{\infty} \overline{a(n)}e(nz)$. Alors on peut deduire que la série de Fourier

$$f(z) = \sum_{n=0}^{\infty} a(n)e(nz)$$

représent une forme modulaire de $\mathcal{S}_k(N,\psi)$. Autrement dit, les propriétés nécessaires d'automorphie de cette série de Fourier peuvent–être deduit des équations fonctionnelles des séries de Dirichlet correspondentes; la forme precise de ces équations fonctionnelles est donnée par Weil A. (1967), voir ainsi Chapitre 4, §4.5.

Chapitre 4. Théorie des formes primitives

4.1. Formes vieilles et formes nouvelles

4.1.1. Motivation de la théorie des formes primitives. Un supplémentaire important à la théorie de Hecke a été suggeré par Atkin et Lehner.

Ceci est lié à une construction d'une bonne théorie des opérateurs de Hecke $T(p)$ dans les espaces des forme modulaires sur $\Gamma_0(N)$ pour p premier à N aussi bien pour les diviseurs de N.

Considérons un exemple simple. Soit $\mathcal{S}_{12}(\Gamma_0(2))$ l'espace vectoriel de dimension 2 contenant $f_2 = \Delta(z)$ et $f_1 = \Delta(2z)$. Ces formes ont le mêmes valeurs propres pour $T(p)$, $p \neq 2$, mais ils sont linéarement independent. On peut alors poser la question suivante: quelle restrictions faut-il imposer sur $f = \sum_{n=1}^{\infty} a_n e(nz) \in \mathcal{S}_k(N, \psi)$ afin que les coefficients a_n avec $(n, N) = 1$ déterminent f completement? Si $T(p)|f = 0$ pour tout $p, (p, N) = 1$, peut-on dire que $f \equiv 0$?

Pour trouver ces conditions on construit d'abord l'espace des formes vieilles

$$\mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N)) \subset \mathcal{S}_k(\Gamma_1(N))$$

comme la somme des images des opérateurs

$$V(d) : \mathcal{S}_k(\Gamma_1(N/d)) \to \mathcal{S}_k(\Gamma_1(N))$$

pour tous diviseurs d de niveau N. Posons

$$\mathcal{S}_k^{\mathrm{old}}(N, \psi) = \mathcal{S}_k(N, \psi) \cap \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N)).$$

Alors l'espace des formes nouvelles de niveau exact N est défini comme le complémentaire orthogonal de l'espace des formes vieilles, et on a la décomposition suivante:

$$\mathcal{S}_k(N, \psi) = \mathcal{S}_k^{\mathrm{new}}(N, \psi) \oplus \mathcal{S}_k^{\mathrm{old}}(N, \psi).$$

Le resultat principal de la théorie d'Atkin – Lehner dit que si une fonction

$$f \in \mathcal{S}_k^{\mathrm{new}}(N, \psi)$$

est une fonction propre des opérateurs de Hecke $T_k(m)$ avec $(N, m) = 1$, alors f est uniquement déterminée (à une constante multiplicative près) par ces valeurs absolues et on peut normaliser f par la condition $a(1) = 1$. Une forme primitive du conducteur N est alors définie comme une forme nouvelle normalisée $f \in \mathcal{S}_k^{\mathrm{new}}(N, \psi)$.

Pour telles formes f la condition $f|U(q) = a(q)f$ pour $q|N$ est automatiquement satisfaite.

On a le développement en produit d'Euler suivant:

$$\begin{aligned} L(s, f) &= \sum_{n=1}^{\infty} a(n) n^{-s} \\ &= \prod_{q|N} (1 - a(q)q^{-s})^{-1} \prod_{p \nmid N} (1 - a(p)p^{-s} + \psi(p)p^{k-1-2s})^{-1}, \end{aligned}$$

où $|a(q)| = q^{(k-1)/2}$ si le caractère ψ ne peut pas être défini modulo le niveau inférieur N/q, et si ψ est défini modulo N/q on a $a(q)^2 = \psi(q)q^{k-1}$ dans le cas où $q^2 \nmid N$, et $a(q) = 0$ sinon (i.e. pour $q^2|N$), voir Li W. (1975).

Soit $f(z) = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{S}_k(N, \psi)$ une forme primitive de conducteur C_f, $C_f|N$. Si on pose

$$W(C_f) = \begin{pmatrix} 0 & -1 \\ C_f & 0 \end{pmatrix}, \quad f^\rho(z) = \overline{f(-\overline{z})} = \sum_{n=0}^{\infty} \overline{a(n)}e(nz) \in \mathcal{S}_k(N, \overline{\psi}),$$

alors pour un nombre complex $\lambda(f)$ with $|\lambda(f)| = 1$ on a

$$f|_k W(C_f) = \lambda(f) f^\rho.$$

Formes primitives d'un conducteur donné sont caractérisées par cette identité, qui est équivalent à une certaine jolie équation fonctionnelle pour les séries de Dirichlet correspondentes (Li W. (1975), Theorem 9)

$$\begin{aligned} L(s, f) &= \prod_p (1 - a(p)p^{-s} + \psi(p)p^{k-1-2s})^{-1} \\ &= \prod_p [(1 - \alpha(p)p^{-s})(1 - \alpha'(p)p^{-s})]^{-1}, \end{aligned}$$

où

$$\alpha(p)\alpha'(p) = \psi(p)p^{k-1}, \quad \alpha(p) + \alpha'(p) = a(p).$$

Si l'on pose

$$\Lambda(s, f) = (2\pi/\sqrt{C_f})^{-s}\Gamma(s)L(s, f),$$

cette équation fonctionnelle prend la forme

$$\Lambda(k - s, f) = i^k \lambda(f)\Lambda(s, f^\rho).$$

Pour un caractère de Dirichlet primitif χ du conducteur C_χ premier à C_f, la forme modulaire tordue

$$f_\chi(z) = \sum_{n=0}^{\infty} \chi(n)a(n)e(nz) \in \mathcal{S}_k(C_f C_\chi^2, \psi)$$

est une forme primitive du conducteur $C_f C_\chi^2$.

On commence par définition des opérateurs de relevement suivants (voir S.Lang (1976), Ch. VIII):

$$\pi_1(d), \pi_2(d) : \mathcal{M}_k(\Gamma_1(N/d)) \to \mathcal{M}_k(\Gamma_1(N)),$$

$$(\pi_1(d)f)(z) = f(z) \ \ \text{l'inclusion naturelle}, \quad (\pi_2(d)f)(z) = g^k f(dz) = d^k f(dz).$$

4.1.2. **Lemme (sur les relevements des formes de niveaux inférieur).** *Pour d_1, d_2, $d_1 d_2|N$ on a*

$$\pi_i(d_1)\pi_i(d_2) = \pi_i(d_1 d_2), \quad i = 1, 2.$$

Les opérateurs commutent entre eux.

Démonstration est évidente.

Définition. (a) L'espace des formes vielles est défini comme la somme des images des opérateurs $\pi_i(d)$ por $d|N$:

$$\mathcal{M}_k^{\mathrm{old}}(\Gamma_1(N)) = \sum_{\substack{i=1,2\\ d|N}} \mathrm{Im}\,\pi_i(d), \quad \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N)) = \mathcal{M}_k^{\mathrm{old}}(\Gamma_1(N)) \cap \mathcal{S}_k(\Gamma_1(N))$$

(b) L'espace des formes nouvelles est définit comme le complémentaire orthogonal de l'espace des formes vieilles:

$$\mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N)) = \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))^{\perp}, \quad \mathcal{S}_k(\Gamma_1(N))) = \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N)) \oplus \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))).$$

On pose

$$\mathcal{S}_k^{\mathrm{new}}(N, \psi) = \mathcal{S}_k(N, \psi) \cap \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N)).$$

4.1.3. Stabilité des formes nouvelles par l'action de l'algèbre de Hecke. Nous utilisons la notation $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ pour l'algèbre de Hecke engendré par les opérateurs de Hecke $T(n)$, $(n, ND) = 1$ sur $\mathcal{M}_k(\Gamma_1(N))$. Il est clair que $T(n)$ commutent avec $\pi_i(d)$ (en vue de l'action des opérateurs $T(n)$ sur les développements de Fourier de formes modulaires de $\mathcal{M}_k(N, \psi)$ pour tout $\psi \bmod N$). Ceci implique que $\mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))$ est stable par $T(n)$, donc le même est vrai pour son complémentaire orthogonal $\mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N))$ car $T(n)$ sont normaux pour la métrique de Petersson.

Soit $W_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Dans ce qui suit on a besoin de l'identité

$$f|\pi_1(d)W_N = f|W_{N/d}\pi_2(d),$$

qui est équivalente à l'identité matricielle

$$\begin{pmatrix} 0 & -1 \\ N/d & 0 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

4.1.4. Lemme (sur l'existence d'une base des formes paraboliques formée par des formes relevées de formes nouvelles de niveau inférieur). *Il existe une base* $\{f_1, ..., f_r\}$ *de* $\mathcal{S}_k(\Gamma_1(N))$ *formée par des formes de type* $f_i = g_i|\pi_1(d_i)\pi_2(d_i')$, $g_i \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N/d_i d_i'))$, *et* g_i *sont des fonctions propres de l'algèbre de Hecke* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$.

Démonstration est évidemment entraînée par réccurence.

4.2. Structure des espaces des formes paraboliques comme modules sur l'algèbre de Hecke.

4.2.1. Théorème principal. *Soit* $f = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$. *Supposons qu'il existe* $D \geq 1$ *tel que* $a(n) = 0$ *pour tout* n *avec* $(n, ND) = 1$. *Alors il existe* $g_p \in \mathcal{M}_k(\Gamma_1(N/p))$ *pour* $p|N$ *tels que*

$$f = \sum_{p|N} g_p|V(p).$$

La condition du théorème peut-être exprimé sous la forme: il existe des séries formelles de $e(nz)$ $g_p = \sum_{n=0}^{\infty} b(n, g_p)e(nz)$ pour $p|N$ telles que

$$f = \sum_{p|N} g_p|V(p),$$

et l'affirmation dit que g_p peuvent-être choisis parmi $g_p \in \mathcal{M}_k(\Gamma_1(N/p))$.

4.2.2. Théorème (sur la non–annulation du premier coefficient de Fourier d'une forme nouvelle). *Soit* $f = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{S}_k(\Gamma_1(N))$, *et supposons que* f *est une fonction propre de* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$. *Si* $a(1) = 0$ *alors* $f \in \mathcal{S}_k^{\text{old}}(\Gamma_1(N))$ *(autrement dit, pour une fonction propre de* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ $f \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N))$, $f \neq 0$ *on a* $a(1) \neq 0$.
Démonstration. Soit $p \not| ND$, alors l'action des opérateurs de Hecke sur les développements de Fourier (voir 3.1.2) montre que $f|T(p) = \lambda_p f$ implique

$$\lambda_p a(n) = a(np) + \psi(p)p^{k-1}a(n/p)$$

(où $a(x) = 0$ pour $x \notin \mathbf{Z}$). Cela signifie que $a(1) \neq 0$ impliquerait $a(n) = 0$ pour tout n tels que $(n, ND) = 1$. Cela veut dire, en vue du théorème principal, $f \in \mathcal{S}_k^{\text{old}}(\Gamma_1(N))$ (une contradiction).

4.2.3. Normalisation des formes primitives. Soit $f \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N)), f \neq 0$ une fonction propre de $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$, $f \neq 0$. Alors le théorème 4.2.2. nous dit qu'on peut normaliser f par la condition $a(1) = 1$.

Définition. On appelle forme primitive une fonction $f \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N))$ qui est une fonction propre de $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ normalisé par la condition $a(1) = 1$.

4.2.4. Théorème (propriétés de la multiplicité un). *(i) Soient* f, g *deux formes paraboliques de* $\mathcal{S}_k(\Gamma_1(N))$ *qui sont fonctions propres de l'algèbre* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ *de mêmes valeurs propres. Alors si* $0 \neq f \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N))$ *implique* $d = cf$ *pour une constante* c.
(ii) $\mathcal{S}_k^{\text{new}}(\Gamma_1(N))$ *coïncide avec la somme directe des espaces propres pour l'action de l'algèbre* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ *qui ont la multiplicité égale à un. En même temps l'espace vectoriel* $\mathcal{S}_k^{\text{old}}(\Gamma_1(N))$ *s'identifie avec la somme directe des sous-espaces propres de* $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ *de la multiplicité strictement plus grande que un.*

Démonstration. Cas 1. Supposons que $g \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N))$. Alors $a(1; g) \neq 0$ pour $g = \sum_{n=1}^{\infty} a(n; g)e(nz)$, et pour une constante c $a(1, f - cg) = 0$. Par 4.2.2 $f - cg \in \mathcal{S}_k^{\text{old}}(\Gamma_1(N))$, d'où $f - cg \equiv 0$ car $f - cg \in \mathcal{S}_k^{\text{new}}(\Gamma_1(N))$.

Cas 2. Supposons que $g \in \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))$. Alors $g = \sum_i c_i f_i$, où $f_i = \pi_1(d_i)\pi_2(d_i')g_i$, où $d_i d_i' > 1$ et g_i sont des fonctions propres de l'algèbre de Hecke $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$. Remarquons que les valeurs propres de f_i sont egaux et coïncident avec celles de $g \neq 0$ car f_i forment une parti d'une base (elles sont linéairement independent, et d'existence d'une valeur propre differente on obtient facilement une relation linéaire parmi elles). Posons $h = \pi_1(d_i d_i')g_i \neq 0$. On a $a(1; f - ch)$ pour une constante c car $a(1;h) \neq 0$ par 4.2.3 ($g_i \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N/d_i d_i'))$). Alors $f - ch \in \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))$, $h \in \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))$, d'où $f \in \mathcal{S}_k^{\mathrm{old}}(\Gamma_1(N))$ (une contradiction).

4.3. Démonstration du théorème principal. Rapelons qu'on veut démontrer le théorème suivante:

Soit $f = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$. Supposons qu'il existe $D \geq 1$ tel que $a(n) = 0$ pour tout n avec $(n, ND) = 1$. Alors il existe $g_p \in \mathcal{M}_k(\Gamma_1(N/p))$ pour $p|N$ tels que

$$f = \sum_{p|N} g_p | V(p).$$

4.3.1. La méthode de "péluchage". Considérons les opérateurs $U(p)$, $V(p)$ de 3.1.1. Alors pour $f = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$

$$f|U(p)V(p) = \sum_{\substack{n=0 \\ p|n}}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(Np^2)),$$

$$f|(I - U(p)V(p)) = \sum_{\substack{n=0 \\ p\nmid n}}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(Np^2)).$$

Ceci implique que la condition du théorème peut-être exprimer à la façon suivante:

$$f| \prod_{p|ND} (I - U(p)V(p)) = 0.$$

On va utiliser cette égalité pour trouver explicitement g_p.

4.3.2. Préparation: formes modulaires pour $\Gamma_1(M, N)$ est traces.
(a) Notation:

$$\Gamma_1(M, N) = \left\{ \begin{pmatrix} a\, b \\ c\, d \end{pmatrix} \mid b \equiv 0(\mathrm{mod} N), c \equiv 0(\mathrm{mod} M), a \equiv d \equiv (\mathrm{mod} MN) \right\},$$

$$\Gamma_0(M, N) = \left\{ \begin{pmatrix} a\, b \\ c\, d \end{pmatrix} \mid b \equiv 1(\mathrm{mod} N), c \equiv 1(\mathrm{mod} M) \right\}.$$

De même façon on définit les espaces

$$\mathcal{M}_k(\Gamma_1(M, N)), \mathcal{S}_k(\Gamma_1(M, N)), \mathcal{M}_k(M, N, \psi), \mathcal{M}_k(M, N, \psi)$$

pour un caractère ψ mod MN.

(b) **Lemme.** *Soit* $B_d = \left(\begin{smallmatrix} d & o \\ o & 1 \end{smallmatrix}\right)$. *Alors* B_N *défini un isomorphisme*

$$\mathcal{M}_k(M, N, \psi) \overset{B_N}{\tilde{\to}} \mathcal{M}_k(MN, \psi).$$

Démonstration est facilement impliquée par l'égalité

$$\begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & bN^{-1} \\ cN & d \end{pmatrix}.$$

(c) *Traces.* Pour un sous-groupe $\Gamma' \subset \Gamma$ d'indice fini, et pour $f \in \mathcal{M}_k(\Gamma')$ on défini

$$f|\mathrm{Tr}_{\Gamma}^{\Gamma'} = \sum_{\sigma \in \Gamma' \backslash \Gamma} f|\sigma.$$

Comme un exemple considérons

(d) **Lemme.** *On a*

$$(\Gamma_1(N) : \Gamma_1(N, p)) = \begin{cases} p, & \textit{pour } p|N \\ p+1, & \textit{pour } p \not| N, \end{cases}$$

de plus,

$$\Gamma_1(N, p) \backslash \Gamma_1(N) = \begin{cases} T^j, j \bmod p & \textit{pour } p|N \\ T^j, j \bmod p, Q = \left(\begin{smallmatrix} px & 1 \\ Ny & 1 \end{smallmatrix}\right) \in \Gamma_1(N) & \textit{pour } p \not| N. \end{cases}$$

On laisse démonstration du lemme au lécteur comme un exercice simple.

4.3.3. Involutions d'Atkin–Lehner. Soit $p^\alpha || N$ ($\mathrm{ord}_p N = \alpha$). Posons

$$W_{N,p} = \begin{pmatrix} p^\alpha x & 1 \\ Ny & p^\alpha \end{pmatrix} \in \mathrm{M}_2(\mathbf{Z}), \quad \det W_{N,p} = p^\alpha.$$

Propriétés de $W_{N,p}$*:*
(i) $W_{N,p} \Gamma_0(N) W_{N,p}^{-1} = \Gamma_0(N)$;
(ii)

$$W_{N,p}^2 = \begin{pmatrix} p^\alpha & 0 \\ 0 & p^\alpha \end{pmatrix} \gamma, \quad]ga \in \Gamma_0(N), \quad \gamma \equiv \begin{pmatrix} * & * \\ 0 & p^\alpha \end{pmatrix} \bmod (N/p^\alpha);$$

(iii) Si $p \not| N$ *on a* $W_{Np,p} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) Q = \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right) B_p^{-1} Q$, *où* Q *est comme dans Lemme 4.3.3.d.*
(iv) Pour tout $q|N$ *et* $p \not| N$ *on ait* $T(p) W_{N,q} = W_{N,q} T(p)$.

Démonstration se réduit à une vérification simple (voir aussi Li W. (1975), p.288). Un corollaire intéressant dit que $W_{N,p}$ induisent des involution holomorphe de la surface de

Riemann $X_0(N)$. Nous allons donner plus bas une interprétation géométrique des involutions d'Atkin–Lehner en utilisant la discription de $X_0(N)$ comme l'ensemble des classes d'isogénies cycliques d'ordre N des courbes elliptiques. Toute telle isogénie admet une décomposition en produit des p–composantes, et l'involution $W_{N,p}$ corresponde à lópération du remplacement de la p–composante d'isogénie par l'isogénie duale.

Formellement,

$$W_{N,p} = \begin{pmatrix} p^\alpha x & 1 \\ Ny & p^\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^\alpha \end{pmatrix} \cdot \gamma_1 \; = \; \gamma_2 \cdot \begin{pmatrix} p^\alpha & 0 \\ 0 & 1 \end{pmatrix}$$

où

$$\gamma_1 = \begin{pmatrix} p^\alpha x & 1 \\ (N/p^\alpha)y & 1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} x & 1 \\ (N/p^\alpha)y & p^\alpha \end{pmatrix} \in \Gamma_0(N/p^\alpha).$$

Donc pour un $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ on a

$$W_{N,p}\sigma W_{N,p}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & p^\alpha \end{pmatrix} \gamma_1\sigma\gamma_1^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p^\alpha \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & p^{-\alpha}b_1 \\ p^\alpha c_1 & d_1 \end{pmatrix},$$

où $\gamma_1\sigma\gamma_1^{-1} = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right) \in \Gamma_0(N/p^\alpha)$, et

$$\begin{aligned} W_{N,p}\sigma W_{N,p}^{-1} &= \gamma_2 \begin{pmatrix} p^\alpha & 0 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} p^\alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \gamma_2^{-1} \\ &= \gamma_2 \begin{pmatrix} a & p^\alpha b \\ p^{-\alpha}c & d \end{pmatrix} \gamma_2^{-1} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \Gamma_0(N/p^\alpha). \end{aligned}$$

Ceci implique

$$c_2 = p^\alpha c_1 \equiv 0 \bmod N, b_2 = p^{-\alpha}b_1 \in \mathbf{Z}, d_2 = d_1 \equiv d (\mathrm{mod} N/p^\alpha),$$

car $\gamma_1 \in \Gamma_1(N/p^\alpha)$.

D'autre part,

$$W_{N,p}^2 = \begin{pmatrix} p^\alpha x & 1 \\ Ny & p^\alpha \end{pmatrix} \begin{pmatrix} p^\alpha x & 1 \\ Ny & p^\alpha \end{pmatrix} = \begin{pmatrix} p^\alpha & 0 \\ 0 & p^\alpha \end{pmatrix} \begin{pmatrix} * & * \\ Nxy + Ny & (N/p^\alpha)y + p^\alpha \end{pmatrix}$$

où

$$\begin{pmatrix} * & * \\ Nxy + Ny & (N/p^\alpha)y + p^\alpha \end{pmatrix} \in \Gamma_0(N),$$

alors $f|W_{N,p}^2 = \psi(p^\alpha)f$ (ici ψ est considéré comme un caractère $\mathrm{mod} N/p^\alpha$).

La propriété $T(p)W_{Nq} = W_{N,q}T(p)$ ce déduit facilement du fait

$$W_{N,p}\Delta_m(N)W_{N,p}^{-1} = \Delta_m(N).$$

4.3.4. Théorème de Hecke (sur l'annulation de l'image de $V(p)$ pour p premier au niveau N). *Soit $f = g|V(p) \in \mathcal{M}_k(\Gamma_1(N))$, où $g = \sum_{n=0}^{\infty} b(n)e(nz)$ est une série de Fourier en $e(nz)$. Alors $f \equiv 0$.*

Démonstration. On a $g = p^{\frac{k}{2}} f|B_p^{-1} \in \mathcal{M}_k(\Gamma_1(N,p))$, car Lemme 4.3.2b est applicable à $f \in \mathcal{M}_k(\Gamma_1(N)) \subset \mathcal{M}_k(\Gamma_1(Np))$ avec $M = N$, $N = p$. D'autre part $g|T = g$ et il resulte que $g \in \Gamma_1(N)$ car $\Gamma_1(N)$ es engendré par $\Gamma_1(N,p)$ et T. Par réccurrence on va voir que $f|V(p^m) \in \mathcal{M}_k(\Gamma_1(N))$. Ceci est entraîner de l'identité

$$\begin{aligned} &f|V(p^m)T(p) = f|V(p^m)|(U(p) + \psi(p)p^{k-1}V(p)) = \\ &f|V(p^{m-1}) + \psi(p)p^{k-1}f|V(p^{m+1}) = g|V(p^m) + \psi(p)p^{k-1}g|V(p^{m+2}). \end{aligned}$$

Maintenant il reste de remarquer que: (i) le séries de Fourier $f|V(p^m) \in \Gamma_1(N)$ sont linéairement independent et que (ii) $\dim \mathcal{M}_k(\Gamma_1(N)) < \infty$.

4.3.5. Réduction du théorème pour des nombres premiers non divisants le niveau. Tout d'abord on va pélucher tout les diviseurs premiers $p|D$, $p \nmid N$.

Théorème. *Sous les hypothse du théorème principal on peut supposer sans réstriction de généralité que $D = 1$, c'est à dire, $a(n) = 0$ pour tout $(n, N) = 1$.*

Démonstration. Soit $p_1, ..., p_r | ND$, $p = p_r \nmid N$. Posons

$$g = f| \prod_{i=1}^{r-1} (I - U(p_i)V(p_i)) \in \mathcal{M}_k(\Gamma_1(Np_1^2 \cdot ... \cdot p_{r-1}^2)).$$

Par l'hypothèse

$$g|(I - U(p)V(p)) = 0 \Rightarrow g = g|U(p)V(p).$$

Alors $g = h|V(p)$ pour $h = g|U(p)$, dóù $g \equiv 0$, et on procéde par réccurence.

4.3.6. Longueur d'une forme modulaire. Pour procéder encore plus loin il est commode d'utiliser la notion de la longueur d'une forme modulaire $f = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$.

Définition. On dit que f est de longueur $\le s$ (par rapport aux nombres premiers $p_1, ..., p_s$ si

$$a(n) \Rightarrow \exists i = 1, ..., s \quad p_i | n.$$

(c'est à dire, il existe des séries formelles de $e(nz)$ $g_{p_i} = \sum_{n=0}^{\infty} b(n, g_{p_i})e(nz)$ telles que

$$f = \sum_{i=1}^{s} g_{p_i}|V(p_i),$$

Alors Théorème principal peut-être réduit à l'affirmation suivante:

Théorème (sur la longuer). *Soit $f = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$ est de longeur $\le s$ par rapport aux nombres premiers $p_1, ..., p_s$, $p = p_s$. Alors il existe*

$$h \in \mathcal{M}_k(\Gamma_1(N/p))$$

telle que $f - h_p|V(p)$ est de longuer $\leq s-1$.

Dans ce qui suit on va supposer $f = f_\psi$, øù $f = \sum_{\psi \bmod N} f_\psi$ la décomposition qui corresponde à la décomposition en somme directe

$$\mathcal{M}_k(\Gamma_1(N)) = \oplus_{\psi \bmod N} \mathcal{M}_k(N.\psi).$$

4.3.7. Réduction au cas de formes avec un caractère de Dirichlet défini modulo N/p (p un diviseur premier de niveau).

Lemme. *Soit $p|N$, $f \in \mathcal{M}_k(N.\psi)$ et ψ n'est pas défini* $\mathrm{mod} N/p$. *Si $f = g|V(p) \in \mathcal{M}_k(\Gamma_1(N))$, où $g = \sum_{n=0}^\infty b(n)e(nz)$ est une série de Fourier en $e(nz)$. Alors $f \equiv 0$.*

Démonstration. Le fait que $g|T = g$ implique $f|\begin{pmatrix} 1 & 1/p \\ 0 & 1 \end{pmatrix} = f$. Puis, $f|\begin{pmatrix} 1 & 1 \\ N & N+1 \end{pmatrix} = f$. Alors, pour tout $u, v, \in \mathbf{Z}$ f est invariant par l'action de la matrice

$$\gamma = \begin{pmatrix} 1 & u/p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ N & N+1 \end{pmatrix} \begin{pmatrix} 1 & v/p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 + \frac{Nu}{p} & 1 + \frac{v}{p} + \frac{Nuv}{p^2} \\ N & 1 + N + \frac{Nv}{p} \end{pmatrix}$$

Considérons deux cas:

I) $p^2|N$. On choisit u, $v \bmod p$ de telle façon que $u \equiv -v (\mathrm{mod} p)$ alors $\gamma \in \Gamma_0(N)$ et pour un choix convenable $\psi(1 + \frac{Nv}{p}) \neq 1$ car la réstriction de ψ sur le sous–groupe $(1 + (N/p)\mathbf{Z}/N\mathbf{Z})^\times \subset (\mathbf{Z}/N\mathbf{Z})^\times$ est non–trivial.

II) $p^2 \not| N$. Posons $N = pN'$. On choisit u, $v \bmod p$ de telle façon que $u + v + N'uv \equiv 0 \bmod p$. De nouvaux, pour un choix convenable $\psi(1 + N'v) \neq 1$ car la réstriction de ψ sur le sous–groupe $(1 + (N/p)\mathbf{Z}/N\mathbf{Z})^\times \subset (\mathbf{Z}/N\mathbf{Z})^\times$ est non–trivial.

Dans ce qui suit on va supposer sans réstriction de généralité que ψ est défini mod $N/p_1p_2 \cdot \ldots \cdot_s$. En effet, le fonction $f|\prod_{i=1}^{s-1}(I - U(p_i)V(p_i))$ est annulée par l'opérateur $(I - U(p)V(p))$. Ceci imlique $f = g|V(p)$ aves $g = f|U(p)$, d'où $f \equiv 0$, ou ψ est défini $\mathrm{mod} N/p$.

4.3.8. Lemme (sur certaines propriétés des opérateurs $U(p)$ et B_p^{-1}). *Soit $p|N$, $f \in \mathcal{M}_k(N, \psi)$, ψ est défini* $\mathrm{mod} N/p$. *Alors*

(a) $f|B_p^{-1} \in \mathcal{M}_k(\Gamma_1(N/p, p))$.

(b)

$$f|U(p) = \begin{cases} \mathcal{M}_k(\Gamma_1(N)), & \text{pour } p|N \\ \mathcal{M}(\Gamma_1(N/p)), & \text{pour } p^2|N \end{cases}.$$

(c)Soit $g = \sum_{n=0}^\infty b(n)e(nz)$ une forme modulaire de niveau quelconque. Supposons que $g|V(p) \in \mathcal{M}_k(N.\psi)$, et que ψ est défini $\mathrm{mod} N/p$. *Alors $g \in \mathcal{M}_k(N/p.\psi)$.*

Démonstration de (a) est directement impliquée par Lemme 4.3.2.b. Pour (b) on remarque que $f|B_p^{-1} \in \Gamma_1(N, p)$ (pour $p|N$), et que $f|B_p^{-1} \in \Gamma_1(N/p, p)$ (pour $p^2|N$) (par (a)).

Considérons le diagram suivant des sous-groupes

$$\begin{array}{ccc} \Gamma_1(N/p, p) & \supset & \Gamma_1(N, p) \\ \cap & & \cap \\ \Gamma_1(N/p) & \supset & \Gamma_1(N). \end{array}$$

Par Lemme 4.3.2.d
$$f|U(p) = p^{\frac{k}{2}-1}(f|B_p^{-1})\mathrm{Tr}$$
où $\mathrm{Tr} = \mathrm{Tr}_{\Gamma_1(N)}^{\Gamma_1(N,p)}$ (pour $p|N$), et $\mathrm{Tr} = \mathrm{Tr}_{\Gamma_1(N/p)}^{\Gamma_1(N/p,p)}$ (pour $p^2|N$) d' où (b).

Pour montrer (c) posons $f = g|V(p)$, alors $g = p^{-\frac{k}{2}} f|B_p^{-1}$ est invariant par $\Gamma_1(N/p,p)$ et par T, donc aussi par $\Gamma_1(N\mathfrak{p})$, d'où on a (c).

4.3.9. Le cas des nombres premiers qui divisent le niveau avec ses carrés. Supposons $p^2|N$, alors le théorème sur la onguer est vrai pour $p_s = p$. En effet, on peut poser $h = f|U(p) \in \mathcal{M}_k(\Gamma_1(N/p))$. Alors $f - h|V(p) = f(I - U(p)V(p))$ a la longuer $\leq s-1$.

4.3.10. Le cas des nombres premiers qui divisent le niveau sans carrés. Considérons le cas le plus dificile, où $p|N$, $p^2 \not| N$, et $f = f_\psi$, ψ est défini modulo $N\mathfrak{p}$.

Soit $p_1, ...p_r$ tout les diviseurs premiers de N, $p_1^2, ..., p_t^2 \not| N$, $p_{t+1}^2, ..., p_r^2|N$. En vue de 4.3.9 on peut supposer que $s \leq t$ dans le théorème sur la longueur.

Posons $f^{(2)} = f|(I - U(p_1)V(p_1))$, $g_{p_1} = f|U(p_1)$. C'est une fonction de longuer $\leq s-1$ par rapport aux $p_2, ..., p_s$. Par réccurence, posons

$$f^{(i+1)} = f|\prod_{j=1}^{i}(I - U(p_i)V(p_i)), \quad g_{p_i} = f^{(i)}|U(p_i).$$

Alors il est facile de voir que
$$f = \sum_{i=1}^{s} g_{p_i}|V(p_i),$$

et g_{p_i} sont des séries de Fourier de $e(nz)$. En effet, $f^{(2)} = f - g_{p_1}|V(p_1)$ est de longuer $\leq s-1$ est par l'hypothse de réccurence

$$f^{(2)} = \sum_{i=2}^{s} g_{p_i}|V(p_i).$$

On voit des définitions que

$$g_{p_i} \in \mathcal{M}_k(\Gamma_1(Np_1\cdots p_i)) \subset \mathcal{M}_k(\Gamma_1(N^2/p))$$

car $\Gamma_1(N^2/p) \subset \Gamma_1(Np_1\cdots p_i)$. Puis,

$$g_p \in \mathcal{M}_k(\Gamma_1(N^2/p^2))$$

car

$$g_p = f - \sum_{i=2}^{s} g_{p_i}|V(p_i) \in \mathcal{M}_k(\Gamma_1(N^2/p))$$

et on applique de nouveau Lemme 4.3.8c.

Pour finir la démonstration posons

$$h = (1+p^{-1})^{-1}(f|U(p) + p^{\frac{k}{2}-1} f|W_{N,p})$$

où la matrice

$$W_{N,p} = \begin{pmatrix} px & 1 \\ Ny & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \cdot Q,$$

est choisite de telle façon que $y \equiv 0 \bmod \frac{N}{p}$, donc $Q \in \Gamma_0(N^2/p^2)$.

Proposition. *(a)* $h \in \mathcal{M}_k(N/p, \psi)$,
(b) $f - h|V(p)$ *est de longueur* $\leq s-1$.

Démonstration. (a)

$$f|U(p) + p^{\frac{k}{2}-1} f|W_{N,p} =$$
$$p^{\frac{k}{2}-1}\Big(\sum_{j \bmod p} f|b_p^{-1}T^j + f|B_p^{-1}Q\Big) = p^{\frac{k}{2}-1}(f|B_p^{-1})|\mathrm{Tr}^{\Gamma_1(N/p,p)}_{\Gamma_1(N/p)} \in \mathcal{M}_k(N/p, \psi),$$

car $f|B_p^{-1} \in \mathcal{M}_k(N/p, p, \psi)$ par Lemme 4.3.2a.
(b) Ecrivons

$$h|V(p) = (1+p^{-1})^{-1}(f|U(p)|V(p) + p^{\frac{k}{2}-1} f|W_{N,p}|V(p)),$$

et substituons

$$f = \sum_{i=1}^{s} g_{p_i}|V(p_i) = g_p|V(p) + \sum_{i=1}^{s-1} g_{p_i}|V(p_i).$$

Comme resultat on obtient

$$h|V(p) =$$
$$(1+p^{-1})^{-1}\Big(g_p|V(p)U(p)V(p) + \sum_{i=1}^{s-1} g_{p_i}|V(p_i)U(p)V(p)) +$$
$$p^{\frac{k}{2}-1} g_p|V(p)|W_{N,p}|V(p) + p^{\frac{k}{2}-1}\sum_{i=1}^{s-1} g_{p_i}|V(p_i)|W_{N,p}|V(p)\Big) =$$
$$(1+p^{-1})^{-1}\left(g_p + p^{\frac{k}{2}-1}p^{-\frac{k}{2}} g_p|B_p B_p^{-1} Q V(p) + \sum_{i=1}^{s-1} h_{p_i}\right),$$

où

$$h_{p_i} = (1+p^{-1})^{-1}\left(g_{p_i}|V(p_i)U(p)V(p) + p^{\frac{k}{2}-1} g_{p_i}|V(p_i)|W_{N,p}|V(p)\right).$$

On voit que $g_p|B_p B_p^{-1} Q V(p) = g_p|V(p)$ car $Q \in \Gamma_0(\frac{N^2}{p^2})$ C'est à dire,

$$h|V(p) = g_p|V(p) + \sum_{i=1}^{s-1} h_{p_i},$$

et il reste à montrer que la longueur de $\sum_{i=1}^{s-1} h_{p_i}$ est $\le s-1$.

Ceci est entraîner par deux identités suivantes:

(i)

$$g_{p_i}|V(p_i)U(p)V(p) = g_{p_i}|V(p)U(p)V(p_i),$$

(ii) pour une série de Fourier de $e(nz)$ on a

$$g_{p_i}|V(p_i)|W_{N,p} = \varphi_{p_i}|V(p_i).$$

(iii)

$$g_{p_i}|V(p_i)|W_{N,p}V(p) = \varphi_{p_i}|V(p_i)V(p) = \varphi_{p_i}|V(p)V(p_i).$$

Pour montrer (i), il suffit d'utiliser la commutativité de $V(p_i)$ avec $U(p), V(p)$. Pour (ii) on remarque

$$\varphi_{p_i} = g_{p_i}|B_{p_i}|W_{N,p}|B_{p_i}^{-1} = g_{p_i}|X.$$

Notre choix special la matrice $W_{N,p}$ garantie que cette matrice normalise le groupe $\Gamma_0(N^2/p)$, donc la matrice

$$X = B_{p_i}W_{N,p}B_{p_i}^{-1}$$

normalise le groupe $\Gamma_0(N^2/pp_i)$. Alors

$$\varphi_{p_i}|T = g_{p_i}|XTX^{-1}X = g_{p_i}|X,$$

car $XTX^{-1} \in \Gamma_1(N^2/pp_i)$ (la dérnière inclusion peut–être aussi facilement vérifiée directement).

Bien entendu, (iii) est impliqué de (i) est (ii). La démonstration du théorème principal est finie.

4.4. Caractérisation des formes nouvelles à l'aide de la trace.

Pour un sous-groupe $\Gamma' \subset \Gamma$ d'indice fini, et pour $f \in \mathcal{M}_k(\Gamma')$ on défini

$$f|\mathrm{Tr}_{\Gamma}^{\Gamma'} = \sum_{\sigma \in \Gamma' \backslash \Gamma} f|\sigma.$$

Soient $f = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{M}_k(\Gamma_1(N))$ une forme modulaire, $\Omega_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ l'involution principal du groupe $\Gamma_0(N)$. Alors

$$W_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} W_N^{-1} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1/N \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c/N \\ -Nb & a \end{pmatrix},$$

donc $f|W_N \in \mathcal{M}_k(\Gamma_1(N))$ car W_N normalise aussi $\Gamma_1(N)$. De plus,

$$f \in \mathcal{M}_k(N, \psi) \Rightarrow f|W_N \in \mathcal{M}_k(N, \psi),$$

par l'identité matricielle si-dessus.

On va caractériser les formes nouvelles $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N))$ par des propriétes d'an-nulation des traces $f|Tr^{\Gamma_1(N)}_{\Gamma_1(N/d)}$ et $(f|W_N)|Tr^{\Gamma_1(N)}_{\Gamma_1(N/d)}$.

4.4.1. Lemme (Régles de commutation de l'involution avec des opérateurs de relevement). *Pour tout* $f =\in \mathcal{M}_k(\Gamma_1(N))$, $g \in \mathcal{M}_k(\Gamma_1(N/d))$ *on a*

(a)

$$f|\pi_1(d)W_N = f|W_{N/d}\pi_2(d).$$

(b)

$$g|\pi_2(d)|W_N = g|W_{N/d}\pi_1(d).$$

Démonstration est facilement impliqué par les égalités

$$\begin{pmatrix} 0 & -1 \\ N/d & 0 \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix},$$

$$\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ N/d & 0 \end{pmatrix}.$$

Soit maintenant $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N))$.

4.4.2. Théorème. L'action de l'involution sur les formes nouvelles.

(a)

$$f|W_N \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N)), \quad \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N)) \overset{W_N}{\tilde{\to}} \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N));$$

(b)

$$f \in \mathcal{S}_k^{\mathrm{new}}(N,\psi) \Rightarrow f|W_N \in \mathcal{S}_k^{\mathrm{new}}(N,\overline{\psi}),\ \mathcal{S}_k^{\mathrm{new}}((N,\psi) \overset{W_N}{\tilde{\to}} \mathcal{S}_k^{\mathrm{new}}(N,\overline{\psi}).$$

Démonstration. Il faut vérifier que pour tout $d|N$, $d > 1$, $g \in \mathcal{M}_k(\Gamma_1(N/d))$

$$\langle f|W_N, g\rangle = 0 = \langle f|W_N, g|\pi_2(d)\rangle.$$

Mais par 4.4.1.a

$$\langle f|W_N, g\rangle = \langle f, g\Omega_N\rangle = \langle f, g|W_{N/d}\pi_2(d)\rangle = 0$$

car $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N))$, $g|W_{N/d}\pi_2(d)\rangle) \in \mathcal{M}_k^{\mathrm{old}}(\Gamma_1(N))$. De même, par 4.4.1.b

$$\langle f|W_N, g|\pi_2(d)\rangle = \langle f, g|\pi_2(d)|W_N\rangle = \langle f, g|W_{N/d}\pi_1(d)\rangle = 0.$$

4.4.3. Proposition (La trace d'une forme modulaire et le produit de Petersson). *Soit* $f =\in \mathcal{S}_k(\Gamma_1(N))$, $g \in \mathcal{M}_k(\Gamma_1(N/d))$. *Alors*

$$\langle f, g\rangle = (\Gamma_1(N) : \Gamma_1(N/d))^{-1}\langle f|Tr^{\Gamma_1(N)}_{\Gamma_1(N/d)}, g\rangle,$$

ou dans la notation relative

$$\langle f, g\rangle_{\Gamma_(N)} = \langle f|Tr^{\Gamma_1(N)}_{\Gamma_1(N/d)}, g\rangle_{\Gamma_(N/d)}.$$

Démonstration.

$$\langle f|Tr^{\Gamma_1(N)}_{\Gamma_1(N/d)}, g\rangle = \langle \sum_{\sigma\in\Gamma_1(N)\backslash\Gamma_1(N/d)} f|\sigma, g\rangle =$$

$$\sum_{\sigma\Gamma_1(N)\backslash\Gamma_1(N/d)} \langle f, g|\sigma^{-1}\rangle = \sum_{\sigma\Gamma_1(N)\backslash\Gamma_1(N/d)} \langle f, g\rangle = (\Gamma_1(N) : \Gamma_1(N/d))\langle f, g\rangle.$$

4.4.4. Théorème (Caractérisation des formes nouvelles).
(i).

$$f \in \operatorname{Im}\pi_1(d)^\perp \Leftrightarrow \operatorname{Tr}^{\Gamma_1(N)}_{\Gamma_1(N/d)} f = 0;$$

(ii).

$$f \in \operatorname{Im}\pi_2(d)^\perp \Leftrightarrow \operatorname{Tr}^{\Gamma_1(N)}_{\Gamma_1(N/d)} (f|W_{N/d} = 0.$$

Démonstration.
(i)

$$f \in \operatorname{Im}\pi_1(d)^\perp \Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g\rangle = 0$$
$$\Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle \operatorname{Tr}^{\Gamma_1(N)}_{\Gamma_1(N/d)} f, g\rangle = 0 \Leftrightarrow \operatorname{Tr}^{\Gamma_1(N)}_{\Gamma_1(N/d)} f = 0.$$

(ii) De même,

$$f \in \operatorname{Im}\pi_2(d)^\perp \Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g|\pi_2(d)\rangle = 0$$
$$\Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g|W_{N/d}\pi_2(d)\rangle = 0,$$

car $W_{N/d} : \mathcal{M}_k(\Gamma_1(N/d)) \tilde{\to} \mathcal{M}_k(\Gamma_1(N/d))$ est un isomorphisme. Alors,

$$\forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g|\pi_2(d)\rangle = 0 \Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g|W_{N/d}\pi_2(d)\rangle = 0$$
$$\Leftrightarrow \forall g \in \mathcal{M}_k(\Gamma_1(N/d)) \quad \langle f, g|W_N\rangle = 0 = \langle f|W_N, g\rangle \Leftrightarrow \operatorname{Tr}^{\Gamma_1(N)}_{\Gamma_1(N/d)}(f|W_N) = 0.$$

4.5. Fonctions L des formes primitives.
L'importance des fonctions L des formes primitives a été déjà illustrée par le théorme de Deligne–Serre, et par Conjecture de Taniyama–Weil qui essentialement affirment que les fonctions L proviennent identifications suivantes:

$$\left\{\begin{matrix}\text{formes primitives}\\ \text{de } \mathcal{S}_1(N,\psi)\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{représentations complexes irréductibles}\\ \text{impaires de dim} = 2 \text{ de } \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \text{ modulo } \cong,\end{matrix}\right\}$$

$$\left\{\begin{matrix}\text{formes primitives } f = \sum_{n=1}^\infty \in \mathcal{S}_2(N,1),\\ \text{avec } a(n) \in \mathbf{Q}\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{courbes elliptiques}\\ \text{sur } \mathbf{Q} \text{ modulo } \sim,\end{matrix}\right\}$$

où $E \sim E' \iff L(E, s) = L(E', s)$. Il est important aussi que les facteurs "mauvais" des fonctions L (qui correspondent aux diviseurs premiers de niveau d'une forme primitive) s'identifient par ces corespondences. Le théorème suivant donne une déscription très explicite des fonctions L des dormes primitives.

4.5.1. Théoreme *(voir Li W. (1975), theorem 3). Soit $f = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{S}_k^{\mathrm{new}}(N, \psi)$ une forme primitive. Alors on a le développement en produit eulérien suivant:*

$$\begin{aligned} L(s, f) &= \sum_{n=1}^{\infty} a(n)n^{-s} \\ &= \prod_{q|N} (1 - a(q)q^{-s})^{-1} \prod_{p\not| N} (1 - a(p)p^{-s} + \psi(p)p^{k-1-2s})^{-1}, \end{aligned}$$

où $|a(q)| = q^{(k-1)/2}$ si le caractère ψ ne peut pas être défini modulo le niveau inférieur N/q, et on a $a(q)^2 = \psi(q)q^{k-2}$ si ψ est défini modulo N/q dans le cas où $q^2 \not| N$, et $a(q) = 0$ sinon.

Démonstration. Soit $g = \sum_{n=1}^{\infty} a(n; g)e(nz) \in \mathcal{M}_k(N, \psi)$ une forme modulaire. On utiise les propriétés suivantes des opérateurs

$$g|W_N(z) = g| \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} (z) = N^{k/2}z^k g(-1/Nz),$$

$$g^{\rho}(z) = g|K(z) = \overline{g(-\overline{z})} = \sum_{n=0}^{\infty} \overline{a(n; g)}e(nz) :$$

1) $g|W_N(z), g^{\rho}(z) \in \mathcal{M}_k(N, \overline{\psi})$,

2) $W_N^2 = (-1)^k$, $K^2 = 1$, $W_N K = (-1)^k K W_N$, $T_p K = K T_p$ $(p \not| N)$, $W_N T_p = \overline{\psi}(p) T_p W_N$;

3)

$$\mathcal{S}_k^{\mathrm{old}}(N, \psi) \overset{W_N}{\tilde{\to}} \mathcal{S}_k^{\mathrm{old}}(N, \overline{\psi}), \quad \mathcal{S}_k^{\mathrm{old}}(N, \psi) \overset{K}{\tilde{\to}} \mathcal{S}_k^{\mathrm{old}}(N, \overline{\psi}),$$

$$\mathcal{S}_k^{\mathrm{new}}(N, \psi) \overset{W_N}{\tilde{\to}} \mathcal{S}_k^{\mathrm{new}}(N, \overline{\psi}), \quad \mathcal{S}_k^{\mathrm{new}}(N, \psi) \overset{K}{\tilde{\to}} \mathcal{S}_k^{\mathrm{new}}(N, \overline{\psi}).$$

4)

$$f \in \mathcal{S}_k^{\mathrm{new}}(N, \psi) \Rightarrow f|W_N = \lambda f|K,$$

pour une constante λ, $|\lambda| = 1$.

4.5.2. Valeurs propres des opérateurs $U(p)$ pour les diviseurs p du niveau d'une forme modulare.

Lemme. *Soit $f = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{S}_k(N, \psi)$, où ψ n'est pas défini modulo N/p, $f|U(p) = c_p f$. Alors*

$$f|(W_N U(p))^2 = |c_p|^2 f = p^{k-1} f,$$

d'où $|c_p| = p^(k-1)/2$.

Démonstration. Considérons les formes modulaires

$$f|W_N \in \mathcal{S}_k(N, \overline{\psi}), \quad f|W_N = \lambda f|K,$$

où $|\lambda| = 1$. On a $f|KU(p) = \overline{c_p} f$, car $\overline{a(pn)} = \overline{c_p}\overline{a(n)}$. Ceci implique

$$(f|W_N U(p))|W_N U(p) = \lambda c_p (f|K|W_N U(p)) = |\lambda|^2 |c_p|^2 f = |c_p|^2 f,$$

entraînant la première égalité.

On va calculer explicitement $f|(W_N U(p))^2$ et on va montrer que $f|(W_N U(p))^2 = p^{k-1} f$.

$$(f|W_N U(p))|W_N U(p) = (p^{\frac{k}{2}-1})^2 \sum_{u,v \bmod p} f| \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & p \end{pmatrix}$$

$$p^{\frac{k}{2}-1})^2 \sum_{u,v \bmod p} f| \begin{pmatrix} 0 & -p \\ N & Nu \end{pmatrix} \begin{pmatrix} 0 & -p \\ N & Nv \end{pmatrix} = p^{k-2} \sum_{u,v \bmod p} f| \begin{pmatrix} -pN & -pNv \\ N^2 u & -N + N^2 uv \end{pmatrix} =$$

$$p^{k-2} \sum_{u,v \bmod p} f|\sigma_{u,v},$$

où $\sigma_{u,v} = \left(\begin{smallmatrix} 1 & v \\ -(N/p)u & 1-(N/p)uv \end{smallmatrix}\right)$. On voit bien que la somme des termes avec $u \equiv 0 \bmod p$ est egale à $p^{k-1} f$, et il reste à montrer que la somme de tous les autres termes s'annule. Pour cela on remarque

$$\sigma_{u,v} = \sigma_{u,v} \sigma_{1,t}^{-1} \sigma_{1,t}$$

et on eśsaye d'obtenir une matrice $\sigma_{u,v}\sigma_{1,t}^{-1} \in \Gamma_0(N)$ en supposant que $u \not\equiv 0 \bmod p$. Ecrivons

$$\sigma_{u,v}\sigma_{1,t}^{-1} = \begin{pmatrix} 1 & v \\ -(N/p)u & 1-(N/p)uv \end{pmatrix} \begin{pmatrix} 1 & t \\ -N/p & 1-(N/p)t \end{pmatrix}^{-1} =$$

$$\begin{pmatrix} 1 & v \\ -(N/p)u & 1-(N/p)uv \end{pmatrix} \begin{pmatrix} 1-(N/p)t & -t \\ N/p & 1 \end{pmatrix} =$$

$$\begin{pmatrix} * & * \\ (N/p)(-u+1+(N/p)u(t-v)) & 1+(N/p)u(t-v) \end{pmatrix}.$$

Considérons deux possibilities

I) $p \not| (N/p) \Rightarrow t = t_v$ est uniquement déterminé par la condition $-u+1+(N/p)u(t-v) \equiv 0 \bmod p$, et pour tout v fixé la sommation par rapport à u donne

$$\sum_u f|\sigma_{u,v}\sigma_{1,t_v}^{-1} = \sum_{l \in (1+(N/p)\mathbf{Z}/N\mathbf{Z})^\times} \psi(l) f = 0,$$

car le nombre $l = 1+(N/p)(ut-uv)$ est uniquement déteminé modulo N par ses propriétés $l \equiv u \bmod p$, $l \equiv 1 \bmod (N/p)$, et la restriction de ψ sur le sous–groupe $(1+(N/p)\mathbf{Z}/N\mathbf{Z})^\times$ n'est pas triviale.

II) $p^2|N$. On voit que

$$\sigma_{u,v} = \begin{pmatrix} 1 & v \\ -(N/p)u & 1-(N/p)uv \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (N/p)u & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -(N/p)u & 1 \end{pmatrix}$$
$$= \begin{pmatrix} * & * \\ N(N/p^2)u^2v & 1-(N/p)uv \end{pmatrix}$$

et pour tout $u \not\equiv 0 \bmod p$ on effectue la sommation

$$\sum_{v \bmod p} \psi(1-(N/p)uv) = 0$$

par la même raison si–déssus.

Démonstration du théorème 4.5.1 est basée sur les relations de 3.5.1 entre les coefficients de Fourier $a(n)$ et les valeurs propres des opérateurs de Hecke $\lambda_f(n)$:

$$a(m) = \lambda_f(m)a(1),$$

est pour $a(1) \neq 0$ la fonction $a(m)$ est alors proportionnelle à la fonction $\lambda(m)$ pour $(m, N) = 1$.

D'autre part, pour une forme primitive f et $q|N$ on a $f|U(q) = \lambda_(q)f$ car $T(p)$ et $U(q)$ commutent entre eux, et et l'espace propre de $\mathcal{H}_k^{(N)}(N,\psi)$ correspondant aux valeurs propres $\lambda_f(p)$ ($T(p)$, $p \not| N$) et de dimension 1 par 4.2.4.

Ceci implique $\lambda_f(q)a(n) = a(qn)$ pour tout n, et si $a(1) = 1$, on ait $a(q) = \lambda_f(q)$.

Ces propriétés s'expriment sous une forme commode en termes de séries de Dirichlet:

$$f(z) = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{S}_k(N,\psi),$$

si-dessus posons formellement

$$L(s,f) = \sum_{n=1}^{\infty} \lambda_f(n)n^{-s}, \quad R(s,f) = \sum_{n=1}^{\infty} a(n)n^{-s}.$$

Alors ces séries de Dirichlet formelles satisfont les identités suivantes:

I) Le développement en produit d'Euler:

$$L(s,f) = \prod_{q\,:\,q|N} (1-\lambda_f(q)q^{-s})^{-1} \prod_{p\,:\,p\not|N} [1-\lambda_f(p)p^{-s} + \psi(p)p^{k-1-2s}]^{-1}.$$

II) $R(s,f) = a(1)L(s,f)$.

En effet, la règle de multiplicativité pour les nombres premiers distinct p_i, $p_i \not| N$ implique que

$$L(s,f) = \prod_{q\,:\,q|N} \left(\sum_{\delta=0}^{\infty} \lambda_f(q^\delta) q^{-\delta s} \right) \prod_{p\,:\,p\not| N} \left(\sum_{\delta=0}^{\infty} \lambda_f(p^\delta) p^{-\delta s} \right),$$

et la sommation de toute de ces séries par rapport à δ peut–être effectuer à l'aide des relations:

$$\lambda_f(q^\delta) = \lambda_f(q)^\delta \quad (q|N),$$
$$\lambda_f(p)\lambda_f(p^\delta) = \lambda_f(p^{\delta+1}) + \psi(p)\lambda_f(p^{\delta-1}) \quad (\delta \geq 1,\ p \not| N)$$

(voir 3.1.3).

L'equation II) est impliquée directement de $a(m) = \lambda_f(m)a(1)$ donc on ait $a(q) = \lambda_f(q)$ si f est normalisée par $a(1) = 1$.

Cas I) $|a(q)| = q^{(k-1)/2}$ si le caractère ψ ne peut pas être défini modulo le niveau inférieur N/q, $q^2 \not| N$.

Ce cas est implique directement du lemme 4.5.2.

Cas II) et on a $a(q)^2 = \psi(q)q^{k-2}$ si ψ est défini modulo N/q dans le cas où $q^2 \not| N$

Pour cela on considére la fonction

$$f|U(q) + q^{\frac{k}{2}-1} f|W_{N,q} \in \mathcal{S}_k(N/q, \psi)$$

comme dans 4.3.10.

Le fait que f est une forme nouvelle de niveau N résult $f|U(q) + q^{\frac{k}{2}-1} f|W_{N,q} = 0$ car $f|U(q) = a(q)f$, $f \sim f|W_{N,q}$ donc $f|U(q) + q^{\frac{k}{2}-1} f|W_{N,q} \sim f$, où $f \sim g$ signifie que pour un $D \geq 1$ f, g sont les fonctions propres de $\mathcal{H}_k^{(ND)}(\Gamma_1(N))$ avec les mêmes valeurs propres. Ici on utilise la propriété suivante des involutions d'Atkin–Lehner $|W_{N,q}$: pour $p \not| N$ $f|T(p)W_{N,q} = f|W_{N,q}T(p)$ (voir 4.3.3).

Alors $f|U(q) + q^{\frac{k}{2}-1} f|W_{N,q}$

Cas III) $a(q) = 0$ si $q^2|N$

Par Lemme 4.3.8 on sait que $f|U(q) = a(q)f \in \mathcal{S}_k(\Gamma_1(N/q))$, d'où $a(q)f = 0 \Rightarrow a(q) = 0$ car f est une forme nouvelle de niveau N.

4.5.3. Transformation de Mellin d'une forme primitive. On sait de 3.3 que la transformation de Mellin d'une forme modulaire

$$f(z) = \sum_{n=0}^{\infty} a(n)e(nz) \in \mathcal{M}_k(N, \psi).$$

est la série de Dirichlet suivante

$$R(s,f) = \sum_{n=1}^{\infty} a(n)n^{-s}$$

qui converge absoluement pour Re $s \gg 0$.

Convergence de ces séries pour Re $(s) \gg 0$ est entraînée des éstimées suivantes pout des coefficients de Fourier:

a) Si $f \in \mathcal{M}_k(N, \psi)$ alors

$$|a(n)| = O(n^{k-1+\varepsilon}), \quad \varepsilon > 0$$

et la série de Dirichlet serie converge absoluement pour Re $s > k$.

b) Si $f \in \mathcal{S}_k(N, \psi)$ on a

$$|a(n)| = O(n^{\frac{k-1}{2}+\varepsilon}), \quad \varepsilon > 0$$

et les séries $L(s, f)$ et $R(s, f)$ convergent absoluement pour Re $s > \frac{(k+1)}{2}$.

Les éstimées si–dessus utilise quelques propriétés fines des coefficients de Fourier $a(n)$. Cependent, l'utilisation seulement des propriétés analytiques de $f(z)$ (le fait que cette fonction est holomorhe et qu'elle satisfaite la condition d'automorphie) permet d'obtenir certains éstimées plus faibles:-

a)

$$|a(n)| = O(n^k), \text{ for } f \in \mathcal{M}_k(N, \psi);$$

b)

$$|a(n)| = O(n^{k/2}), \text{ for } f \in \mathcal{S}_k(N, \psi);$$

la dernière éstimée est entraîné par l'éstimation $|f(z)| = O(y^{-k/2})$ $(y \to 0,\ z = x + iy)$. En effet, la fonction $y^{\frac{k}{2}}|f(z)|$ est invariante par $\Gamma_0(N)$ et elle est bornée sur H, car elle est bonée sur un domaine fondamental $\Gamma_0(N)\backslash H$, d'où $|f(z)| = \mathcal{O}(y^{-k/2})$ $(y \to 0)$. D'autre part, $f(x+iy) = \sum_{n=1}^{\infty} a(n)e^{-2\pi ny}e(nx)$, et

$$a(n)e^{-2\pi ny} = \int_0^1 f(x+iy)e(-nx)dx,$$

donc l'évaluation en $y = \frac{1}{n}$ donne l'éstimation cherchée.

Un prolongement analytique de ces séries sur le plan complex entier on construit en utilisant la transformée de Mellin de f:

$$(2\pi)^{-s}\Gamma(s)R(s, f) = \int_0^{\infty} [f(iy) - a(0)]y^{s-1}\,dy \quad (\text{Re}\,(s) \gg 0).$$

Cela peut être établi par l'intégration terme-par-terme de la série

$$f(iy) - a(0) = \sum_{n=1}^{\infty} a(n)\exp(-2\pi ny)$$

et en utilisant la représentation de la fonction gamma:

$$\Gamma(s) = \int_0^{\infty} e^{-y}y^{s-1}\,dy \quad (\text{Re}\,(s) > 0).$$

Lemme (Hecke). *Soit* $f(z) = \sum_{n=0} a(n)e(nz)$, $g(z) = \sum_{n=0} a(n)e(nz)$ *deux séries de Fourier avec* $|a(n)|, |b(n)| = \mathcal{O}(n^\sigma)$, $\varphi(s) = \sum_{n=1} a(n)n^{-s}$, $\psi(s) = \sum_{n=1} b(n)n^{-s}$ *les séries de Dirichlet correspondantes,* $\Phi(s) = (2\pi)^{-s}\Gamma(s)\varphi(s)$, $\Psi(s) = (2\pi)^{-s}\Gamma(s)\psi(s)$.

Supposons que poour un $A > 0$ *les fonctions*

$$A^{-\frac{s}{2}}\Phi(s) + \frac{a(0)}{s} + \frac{i^k b(0)}{k-s}, \quad A^{-\frac{s}{2}}\Psi(s) + \frac{b(0)}{s} + \frac{i^k a(0)}{k-s}$$

sont holomorphe et bornée dans toute bande verticale $\sigma_1 < \mathrm{Re}\,(s) < \sigma_2$. *Alors les conditions suivantes (A) ey (B) sont équivalentes:*
(A) $\Phi(s) = Ci^k A^{\frac{k}{2}-s}\Psi(k-s)$,
(B) $f(z) = CA^{-\frac{k}{2}}z^{-k}g(-1/Az) = Cg|_k W_A$.

Démonstration est basée sur la transformation réciproque de Mellin:

$$f(iy) - a(0) = \frac{1}{2\pi i}\int_{(\sigma_0)} \Phi(s)\, y^{-s} ds, \quad \sigma_0 > 0,$$

$$g(iy) - b(0) = \frac{1}{2\pi i}\int_{(\sigma_0)} \Psi(s)\, y^{-s} ds, \quad \sigma_0 > 0.$$

4.5.4. Equation fonctionnelle d'une forme primitive.

Soit $f \in \mathcal{S}_k(N,\psi)$ une forme primitive. Alors $f|W_N = \lambda f^\rho$, et le lemme de Hecke montre que la série de Dirichlet $R(s,f)$ admet un prolongement holomorphe sur le plan complex entier. Alors la fonction

$$\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)R(s,f),$$

est holomorphe pour tout $s \in \mathbf{C}$, On a l'équation fonctionnelle suivante

$$\Lambda(k-s,f) = i^k\lambda N^{\frac{k}{2}-s}\Lambda(s,f^\rho).$$

4.5.5. Caractérisation des formes primitives par des équations fonctionnelles.

Soit $f(z) = \sum_{n=1}^\infty a(n)e(nz) \in \mathcal{S}_k(N,\psi)$ une forme primitive de conducteur N,

$$\begin{aligned} L(s,f) &= \prod_p (1 - a(p)p^{-s} + \psi(p)p^{k-1-2s})^{-1} \\ &= \prod_p [(1-\alpha(p)p^{-s})(1-\alpha'(p)p^{-s})]^{-1}, \end{aligned}$$

où

$$\alpha(p)\alpha'(p) = \psi(p)p^{k-1}, \quad \alpha(p) + \alpha'(p) = a(p).$$

Si l'on pose

$$f|K(z) = f^\rho(z) = \overline{f(-\overline{z})} = \sum_{n=0}^\infty \overline{a(n)}e(nz) \in \mathcal{S}_k(N,\overline{\psi}),$$

alors on sait que pour un nombre complex $\lambda(f)$ with $|\lambda(f)| = 1$ on a

$$f|_k W_N = \lambda(f) f^\rho,$$

et on a l'équation fonctionnelle prend la forme

$$\Lambda(k-s, f) = i^k \lambda(f) \Lambda(s, f^\rho).$$

Réciproquement,

Théorème (Li W. (1975), Theorem 9). *Soit* $f(z) = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{S}_k(N, \psi)$ *une forme parabolique telle que*

$$\begin{aligned} L(s,f) &= \prod_p (1 - a(p)p^{-s} + \psi(p)p^{k-1-2s})^{-1} \\ &= \prod_p [(1-\alpha(p)p^{-s})(1-\alpha'(p)p^{-s})]^{-1}, \end{aligned}$$

et

$$f|W_N = cf|K,$$

pour une constante c. *Alors* f *est une forme primitive du conducteur* N. *Autrement dit, les formes primitives d'un conducteur donné sont caractérisées par l'existence du développement en produit eulérien et par l'équation fonctionnelle si–dessus.*

Plan de démonstration (voir Li (1975), p. 308-312). L'action d'opérateurs de Hecke sur les coefficients de Fourier montre que $f|T(p) = a(p)$ pour tout p avec $(p, N) = 1$, et $f|U(q) = a(q)f$ pour tout $q|N$. Il existe une forme primitive $g \in \mathcal{S}_k(N/d, \psi)$ de niveau N/d qui est équivalente à f, telle que $f = \sum_{\delta|(N/d)} c_\delta g|B_\delta$ pour certaines constantes complexes c_d. Il faut démontrer que $d = 1$. Le fait que g est primitive implique

$$g|W_{N/d} = c' g|K$$

pour une autre constante c'. On sait que $|c| = |c'| = 1$. On a

$$f|W_N = \sum_{\delta|(N/d)} c_\delta g|B_\delta W_N = \sum_{\delta|(N/d)} c_\delta g|W_{N/\delta} B_\delta =$$
$$\sum_{\delta|(N/d)} c_\delta g|W_{N/d} B_{d/\delta} = \sum_{\delta|(N/d)} c_\delta c' g|K B_{d/\delta},$$

d'autre part,

$$f|W_N = cf|K = \sum_{\delta|(N/d)} c\overline{c_\delta} g|K|B_\delta.$$

Ceci implique que pour tout $\delta|d$ on a

$$c_{d/\delta} c' = c\overline{c_\delta}$$

car les fonctions $g|K|B_\delta$ sont linérairement indépendentes. Evidemment, $c_1 = 1$ car g est normalisée, et $a(1) = 1$. Ceci implique $|c_d| = 1$. Soit $g = \sum_{n=1}^{\infty} b(n)e(nz) \in \mathcal{S}_k(N/d, \psi)$. Le caractère ψ est automatiquement défini modulo N/d. Remarqueons que la condition du théorème implique $f|U(q) = a(q)$ pour tout $q|N$.

Considérons tous les diviseurs possibles de d. Pour aller plus loin, il faut considérer les cas suivants:

I) $q^2 \nmid N$, $q \nmid (N/d)$ $(q^2|d)$. Dans ce cas on a $b(q)g = g|T(q) = g|U(q) - \psi(q)q^{k-1}g|V(q)$,

Lemme. *Dans la notation si–dessus pour* $q|d$, $q \nmid N/d$, $q^2 \nmid N$ *on ait* $|a(q)|^2 = q^{k-1}$ *et pour tout* $\delta|d$, $q \nmid d$ *on ait* $c_{q\delta} = -\psi(q)\overline{a(q)}q^{-k/2}c_\delta$.

Démonstration du lemme est basée sur l'égalité

$$a(q)f = f|U(q) = \sum_{\delta|(N/d)} c_\delta \delta^{k/2} g|V(\delta)U(q) == \sum_{\delta|(N/d)} c_\delta \delta^{k/2} g|U(q)V(\delta).$$

Ce lemme implique $|c_{\delta q}| = q^{-1/2}|c_\delta|$ pour tout $\delta|d$, $q \nmid d$.

II) $q^2|N$, $q|d$, alors $a(q) = 0$, et on obtient

$$\begin{aligned} f|U(q) = 0 = &\sum_{\delta|(N/d)} c_\delta g|B_\delta U(q) = \\ = &\sum_{q\nmid\delta|(N/d)} c_\delta \delta^{k/2} g|V(\delta)U(q) + \sum_{q|\delta|(N/d)} c_\delta \delta^{k/2} g|V(\delta)U(q) \\ = &\sum_{q\nmid\delta|(N/d)} c_\delta \delta^{k/2} g|U(q)V(\delta) + \sum_{q|\delta|(N/d)} c_\delta \delta^{k/2} g|V(\delta/q) \\ &\sum_{q\nmid\delta|(N/d)} c_\delta \delta^{k/2} g|b(q)V(\delta) - \sum_{q\nmid\delta|(N/d)} c_\delta \delta^{k/2}\psi(q)q^{(k-1)/2} g|V(\delta q) \\ &+ \sum_{q|\delta|(N/d)} c_\delta \delta^{k/2} g|V(\delta/q), \end{aligned}$$

d'où

$$\begin{cases} b(q)c_\delta + q^{k/2}c_{\delta q} = 0, & \text{pour } q \nmid \delta|d, \\ -\psi(q)q^{(k-1)/2}c_\delta + q^k c_{\delta q^2} = 0 & \text{pour } q \nmid \delta|d, \\ c_\delta = 0 & \text{pour } q^3|\delta|d, \end{cases}$$

III) $q|d$, $q|(N/d)$, alors de nouveau $a(q) = 0$, et on obtient

$$\begin{cases} b(q)c_\delta + q^{k/2}c_{\delta q} = 0, & \text{pour } q \nmid \delta|d, \\ c_\delta = 0 & \text{pour } q^2|\delta|d. \end{cases}$$

Maintenant on peut écrire: $d = K_1K_2K_3$, où

$$q|K_1 \Longleftrightarrow q|d, q \nmid N/d, q^2 \nmid N, \quad K_1 = q_1 \cdots q_t,$$

$$q|K_2 \Longleftrightarrow q|d, q \nmid N/d, q^2|N, \quad K_2 = (q_1' \cdots q_r')^2,$$

$$q|K_3 \Longleftrightarrow q|d, q|N/d, \quad K_3 = q_1'' \cdots q_s'',$$

Si l'on applique tous ces égalités, on obtient

$$|c_d| = K_1^{-1/2}K_2^{-1/2}K_3^{-1/2}|c_1| == K_1^{-1/2}K_2^{-1/2}K_3^{-1/2} = 1,$$

car $|c_1| = 1$, d'où $K_1 = K_2 = K_3 = 1$, $d = 1$, entraînant le théorème.

Remarque. Ce théorème montre que les formes primitives $f = \sum_{n=1}^{\infty} a(n)e(nz) \in \mathcal{S}_k(N,\psi)$ peuvent être caractérisées comme les fonctions propres des opérateurs $T(p)$, $U(q)$, et KW_N normalisées par $a(1) = 1$.

4.5.6. Critère de Weil et courbes elliptiques de Weil. Le critère, été etabli par A.Weil (1967), donne des conditions nécessaires et suffisantes pour qu'une séries de Fourier $f(z) = \sum_{n=0}^{\infty} a(n)e(nz)$ représent une forme modulaire de $M_k(N,\psi)$ en termes de séries de Dirichlet tordus

$$\Lambda(s,f,\chi) = (2\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty}\chi(n)a(n)n^{-s},$$

où χ est un caractère de Dirichlet.

Si $f \in M_k(N,\psi)$, et χ est primitive mod$m$ on introduit le twist

$$f_\chi(z) = \sum_{n=0}^{\infty}\chi(n)a(n)e(nz) = \chi(-1)f|\frac{G(\chi)}{m}\sum_{a \bmod m}\overline{\chi}(a)\begin{pmatrix} m & a \\ 0 & m\end{pmatrix},$$

où $G(\chi) = \sum_{a \bmod m}\chi(a)e(a/m)$ la somme de Gauss.

Il n'est pas dificile à montrer que

$$f_\chi(z) \in \mathcal{S}_k(Nm^2, \psi\chi^2),$$

et si $f|W_N = C_1 f^\rho$, on ait

$$f_\chi|W_{Nm^2} = C_\chi f_{\overline{\chi}}^\rho = C_\chi(f_\chi)|K, \tag{A}$$

où

$$C_\chi = C_1\frac{G(\chi)}{G(\overline{\chi})}\chi(-N)\psi(m).$$

Pour montrer cela on utilise les propriétés connues de sommes de Gauss.

Lemme. *Posons* $G_b(\chi) = \sum_{a \bmod m}\chi(a)e(ab/m)$, *et soit* χ *primitif modulo* m. *Alors:*
(i) $G_b(\chi) = \overline{\chi(b)}G(\chi)$,
(ii) $G(\overline{\chi})G(\chi) = \chi(-1)m$.

On voit que (A) est équivalent à l'identité

$$f|\frac{G(\chi)}{m}\sum_{a \bmod m}\overline{\chi(a)}\begin{pmatrix} m & a \\ 0 & m\end{pmatrix} = C_\chi f|\frac{G(\chi)}{m}\sum_{a \bmod m}\overline{\chi(a)}\begin{pmatrix} m & a \\ 0 & m\end{pmatrix}|KW_{Nm^2},$$

puis on effectue la commutation dans la partie droite:

$$
\begin{aligned}
&C_\chi f| \frac{G(\chi)}{m} \sum_{a \bmod m} \overline{\chi(a)} \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} |KW_{Nm^2} = \\
&C_\chi \frac{\overline{G(\chi)}}{m} \sum_{a \bmod m} \chi(a) f|K \begin{pmatrix} m & -a \\ 0 & m \end{pmatrix} |W_{Nm^2} = \\
&C_\chi \frac{G(\overline{\chi})}{m} \sum_{a \bmod m} \chi(a) f|K \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} |W_{Nm^2},
\end{aligned}
$$

car $f| \left(\begin{smallmatrix} m & a \\ 0 & m \end{smallmatrix}\right) |KW_{Nm^2} = f|K \left(\begin{smallmatrix} m & -a \\ 0 & m \end{smallmatrix}\right) W_{Nm^2}$, et on remplace a par $-a$.

Remarquons que

$$
f|K \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} W_{Nm^2} = f|KW_N \gamma(a,b) \begin{pmatrix} m & b \\ o & m \end{pmatrix} \quad \gamma(a,b) = \begin{pmatrix} m & -b \\ -Na & n \end{pmatrix} \in \Gamma_0(N),
$$

car

$$
W_N \gamma(a,b) \begin{pmatrix} m & b \\ o & m \end{pmatrix} \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} = \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} W_{Nm^2}, \quad -Nab \equiv 1 (\mathrm{mod} m).
$$

Alors on récrit (A) sous la forme (B):

$$
G(\chi) \sum_{a \bmod m} \overline{\chi(a)} f| \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} = C_\chi G(\overline{\chi}) \overline{\chi(-N)} \sum_{a \bmod m} \overline{\chi(b)} f|KW_N \gamma(a,b) \begin{pmatrix} m & b \\ 0 & m \end{pmatrix}. \quad (B)
$$

Maintenant on voit

$$
f|KW_N = (-1)^k f|W_N K = (-1)^k (C_1 f|K)K = (-1)^k \overline{C_1} f,
$$

$$
f|KW_N \gamma(a,b) = (-1)^k \overline{C_1 \psi n} f = (-1)^k C_1^{-1} \psi(m) f
$$

et (B) implique que C_χ est donné par la formule si–dessus.

Il est important pour la suite que (B) s'écrit sous la forme équivalente (C):

$$
\sum_{a \bmod m} \overline{\chi(a)} f| \begin{pmatrix} m & a \\ 0 & m \end{pmatrix} = \psi(m) \sum_{a \bmod m} \overline{\chi(b)} f| \gamma(a,b) \begin{pmatrix} m & b \\ 0 & m \end{pmatrix}
$$

car $-Nab \equiv 1 (\mathrm{mod} N)$.

La transformation de Mellin nous provient donc l'équation fonctionnelle suivante:

$$
\Lambda^*(s, f, \chi) = C_\chi i^k (Nm^2)^{\frac{k}{2} - s} \Lambda^*(k - s, f^\rho, \overline{\chi}).
$$

Le résultat réciproque est plus profond

Théorème. (A.Weil, 1967) *Supposons que la série*

$$
R(s) = \sum_{n=1}^{\infty} a(n) n^{-s}
$$

converge absoluement pour $s = k - \delta$, $\delta > 0$, *et que pour tout* $\chi \mod m$, $(m, N) = 1$ *la fonction* $\Lambda^*(s, f, \chi)$ *est entier, bornée dans toute bande verticale et satisfait l'équation fonctionnelle suivante*

$$\Lambda^*(s, f, \chi) = C_\chi i^k (Nm^2)^{\frac{k}{2}-s} \Lambda^*(k - s, f^\rho, \overline{\chi}),$$

où $f^\rho(z) = \sum_{n=1}^\infty \overline{a(n)} e(nz)$, $C_\chi = C_1 \frac{G(\chi)}{G(\overline{\chi})} \chi(-N)\psi(m)$. *Alors*

$$f(z) = \sum_{n=1}^\infty a(n)e(nz)$$

représent une forme modulaire de $\mathcal{S}_k(N, \psi)$.

Autrement dit, les propriétés nécessaires d'automorphie de cette série de Fourier peuvent–être deduit des équations fonctionnelles des séries de Dirichlet correspondentes.

Plan de démonstration. Soit $\mathbf{C}[[\mathrm{GL}^+(2, \mathbf{R})]]$ l'algèbre du groupe $\mathrm{GL}^+(2, \mathbf{R})$,

$$\Omega_f \subset \mathbf{C}[[\mathrm{GL}^+(2, \mathbf{R})]]$$

l'idéal droit formé par $w \in \mathbf{C}[[\mathrm{GL}^+(2, \mathbf{R})]]$ tels que $f|w = 0$.

Il faut montrer que pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ $w = (\psi(d) - \gamma) = \psi(d)(1 - \psi(a)\gamma) \in \Omega_f$.

Tout d'abord on va considérer les éléments $\gamma = \gamma(a, b) = \left(\begin{smallmatrix} m & -b \\ -Nb & n \end{smallmatrix}\right) \in \Gamma_0(N)$ si–dessus et on va montrer que

$$(1 - \psi(m)\gamma(a, b)) \in \Omega_f.$$

pour tout $\gamma(a, b) = \left(\begin{smallmatrix} m & -b \\ -Nb & n \end{smallmatrix}\right)$ avec $m, n \in S$, où S et l'ensemble des nombres naturels m tel que l'equation fonctionnelle est satisfaite pour tout $\chi \bmod m$.

Lemme. *L'égalité (C) est equivalente à (D): pour tout* $b, b' \bmod m$, $(b, m) = (b', m) = 1$ *on ait*

$$(1 - \psi(m)\gamma(a, b)) \begin{pmatrix} m & b \\ 0 & m \end{pmatrix} \equiv (1 - \psi(m)\gamma(a', b')) \begin{pmatrix} m & b' \\ 0 & m \end{pmatrix} (\mathrm{mod}\Omega_f). \qquad (D)$$

Démonstration du lemme est simple: pour tout $b', b'' \bmod m$, $(b', m) = (b'', m) = 1$ il faut multiplier les deux parties de (C) par $\chi(b'') - \chi(b')$ et effectuer la sommation par rapport à χ.

Posons

$$\gamma = \gamma(a, b) = \begin{pmatrix} m & -b \\ -Na & n \end{pmatrix}, \quad \gamma^{-1} = \begin{pmatrix} n & b \\ Na & m \end{pmatrix} \gamma' = \begin{pmatrix} m & b \\ Na & n \end{pmatrix}, \quad \gamma'^{-1} = \begin{pmatrix} n & -b \\ -Na & m \end{pmatrix},$$

et remarquons que (D) implique

$$(1 - \psi(m)\gamma) \begin{pmatrix} m & b \\ 0 & m \end{pmatrix} \equiv (1 - \psi(m)\gamma') \begin{pmatrix} m & -b \\ 0 & m \end{pmatrix} \bmod \Omega_f,$$

d'où

$$1-\psi(m)\gamma' \equiv (1-\psi(m)\gamma)\begin{pmatrix} m & 2b \\ 0 & m \end{pmatrix} \bmod \Omega_f \qquad (D.a)$$

D'autre part, on peut utiliser les mêmes arguments pour n au lieu de m:

$$(1-\psi(n)\gamma'^{-1})\begin{pmatrix} n & b \\ 0 & n \end{pmatrix} \equiv (1-\psi(n)\gamma^{-1})\begin{pmatrix} n & -b \\ 0 & n \end{pmatrix}(\mathrm{mod}\Omega_f),$$

d'où

$$\psi(n)(1-\psi(m)\gamma')\gamma'^{-1} \equiv (1-\psi(n)\gamma^{-1})\begin{pmatrix} n & -2b \\ 0 & n \end{pmatrix}(\mathrm{mod}\Omega_f),$$

puis

$$1-\psi(m)\gamma' \equiv (1-\psi(m)\gamma)\gamma^{-1}\begin{pmatrix} n & -2b \\ 0 & n \end{pmatrix}\gamma'(\mathrm{mod}\Omega_f) \qquad (D.b)$$

Si l'on sustrait (D.b) de (D.a), on obtient l'identité suivant:

$$(1-\psi(m)\gamma)(1-\mu)\begin{pmatrix} m & -2b \\ 0 & m \end{pmatrix}(\mathrm{mod}\Omega_f),$$

où

$$\begin{aligned}\mu = \gamma^{-1}\begin{pmatrix} 1 & -\frac{2b}{n} \\ 0 & 1 \end{pmatrix}\gamma'\begin{pmatrix} 1 & -\frac{2b}{m} \\ 0 & 1 \end{pmatrix} = \\ \begin{pmatrix} n & -b \\ Na & \frac{2}{n}-m \end{pmatrix}\begin{pmatrix} m & -b \\ Na & \frac{2}{m}-n \end{pmatrix} = \\ \begin{pmatrix} 1 & -\frac{2b}{m} \\ \frac{2Na}{n} & \frac{4}{nm}-3 \end{pmatrix}\end{aligned}$$

est un élément elliptique de $\mathrm{SL}(2,\mathbf{R})$ d'ordre infini. Maintenant on a $(1-\psi(m)\gamma)(1-\mu) \equiv 0(\mathrm{mod}\Omega_f)$ donc la fonction $g = f|(1-\psi(m)\gamma)$ a la propriété $g\mu^j = g$ pour tout $j \in \mathbf{Z}$. Pour un point $z \in H$ non fixé l'orbit $\mu^j(z)$ est dense dans un cercle qui passe autour de z_0, le seul point fixé $\mu(z_0)$, $z_0 \in H$. Ceci implique que g est constante, puis $g = C$ est identiquement nul: si l'on désigne $\mu = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on ait $g|\mu = (cz+d)^{-k}C = C = 0$ car $c \neq 0$.

Pour finir la démonstration il reste à montrer que $1-\psi(a)\gamma \in \Omega_f$ pour tous les autres éléments $\gamma = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Tout d'abord, soit $c=0$, $\gamma = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, alors $f = f|ga$ car f est périodique de période 1. Puis, soit $b = 0$, $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ Nc & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$. Alors

$$\begin{pmatrix} 1 & 0 \\ Nc & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}^{-1}$$

donc

$$f|\begin{pmatrix} 1 & 0 \\ Nc & 1 \end{pmatrix} = f|W_N \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} W_N^{-1} = (-1)^k f|W_N \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} W_N =$$
$$(-1)^k f|K^2 W_N \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} W_N = f|KW_N K \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} W_N =$$
$$C_1 f| \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} KW_N = C_1 \overline{C}_1 f = f,$$

en vue des propriétés connues de K et W_N: $KW_N = (-1)^k W_N K$, $W_N^2 = (-1)^2$, et du fait $f|KW_N = C_1 f$ qui est équivalent à l'équation fonctionnelle avec $\chi = 1$, $m = 1$. Finalement, si $\gamma = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \Gamma_0(N)$, $b \neq 0$, on choisi $s, t \in Z$ de telle façon que $m = a + Nbs, n = d + Nbt \in S$. Alors

$$\gamma = \begin{pmatrix} 1 & 0 \\ -Nt & 1 \end{pmatrix} \begin{pmatrix} m & b \\ Nb' & n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -Ns & 1 \end{pmatrix};$$

ceci implique

$$f|\gamma = \psi(n) f = \psi(d) f.$$

On a démontré les propriété d'automorphie; il reste à vérifier que f s'annule aux points de $\Gamma_0(N)$. Pour cela on utilise la convergeance absolue de la série

$$R(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$$

pour $s = k - \delta$, $\delta > 0$. Il n'est pas dificile à déduire de cela que $f(x + iy) = \mathcal{O}(y^{-k+\delta})$ pour $y \to 0$. Cela signifie que f est une forme parabolique de $S_k(N, \psi)$.