THEORIE GEOMETRIQUE des
FORMES MODULAIRES
d'après le cours de
Magistère de Mathématiques
d' Alexeï PANCHISHKIN
1994-95

Université Joseph FOURIER et **Ecole Normale Supérieure**
Institut FOURIER
URA 188 du CNRS
Saint-Martin d'Hères

45, rue d'Ulm
PARIS

CONTENU de COURS

Chapitre 1. Espaces de formes modulaires

25 octobre 1994. Espaces de formes modulaires. Formes modulaires avec caractères de Dirichlet. Exemples et motivations d'étude des formes modulaires. Fonction de Ramanujan.

8 novembre 1994. Lien avec la théorie de représentation. Définition géométrique des formes modulaires commes fonctions de réseaux.

15 novembre 1994. Séries d'Eisenstein et leurs développement de Fourier. Fonction Δ comme un produit infinit.

22 novembre 1994. Structure des formes modulaires pour sur $\mathrm{SL}_2(\mathbf{Z})$. Applications. Congruence de Ramanujan et son interprétation galoisienne.

Chapitre 2. Surfaces de Riemann et formes modulaires

29 novembre 1994. Surfaces de Riemann. Domaine fondamental de $\mathrm{SL}_2(\mathbf{Z})$ comme surface de Riemann. Formes modulaires comme différentielles multiples et lien avec le théorème de Riemann–Roch.

6 décembre 1994. Théorème de Riemann–Roch pour les surfaces de Riemann compactes et pour les courbes projectives et lisses. Théorème de finitude des dimension. Théorème d'approximation. Groupe des classes de diviseurs. La classe canonique.

13 décembre 1994. Répartitions de Weil et le théorème de Riemann. Irregularité et ses propriétés.

20 décembre 1994. Résidus et dualité. Calcul d'irregularité. Corollaires du théorème de Riemann-Roch. Applications aux formes modulaires (dimensions des espaces de formes modulaires).

Chapitre 3. Courbes elliptiques et formes modulaires algébriques.

10 janvier 1995. Courbes elliptiques. Théorème d'Abel. Groupe de classes de diviseurs. Lois d'addition et la méthode de sécantes et tangentes.

17 janvier 1995. Déscription analytique des courbes elliptiques complexes et leurs homomorphismes. Théorème d'addition. Théorème de Jacobi (déscription du réseau correspondant à une différentielle non nulle). Classes d'isomorphisme des courbes elliptiques. L'invariant modulaire.

24 janvier 1995. La courbe de Tate. Points d'ordre fini: trois déscriptions. Isogénies et dualité. Formes modulaires algébriques et leur développement de Fourier algébrique.

31 janvier 1995. Opérateurs de Hecke. Déscription algébrique des opérateurs de Hecke à l'aide d'isogénies. Produit des opérateurs de Hecke. La transformation de Mellin comme un produit eulérien. Formes primitives.

Chapitre 1. Espaces de formes modulaires

25 octobre 1994.

25 octobre 1994. Espaces de formes modulaires. Formes modulaires avec caractères de Dirichlet. Exemples et motivations d'étude des formes modulaires. Fonction de Ramanujan.

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.
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 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*

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

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 $j(\gamma, z) = \dfrac{(\det\ \gamma)^{1/2}}{cz+d}$

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 $\mathcal{H}$;

(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 $\mathcal{H}$ dans $\mathbf{C}$.

(iii) Pour tout $\sigma \in \mathrm{SL}(2, \mathbf{Z})$, il existe un entier naturel $N(\sigma)$ tel que l'application f admette un développement "régulier" de la forme $(f|_k\ \sigma)(z) = \sum_{n \geq 0} a(n, \sigma) q^{n/N(\sigma)}$ 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 l'on se place dans le cas très particulier où Γ est le groupe SL(2,$\mathbf{Z}$), on obtient pour toute fonction ayant les propriétés (i) et (ii) une fonction holomorphe sur $\mathcal{H}$ qui est invariante par l'action usuelle de SL(2,$\mathbf{Z}$). En particulier le groupe SL(2,$\mathbf{Z}$) contient la matrice correspondant à la translation de vecteur 1, soit $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 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 SL(2,$\mathbf{Z}$), il existe un plus petit entier n, diviseur de l'indice de Γ dans SL(2,$\mathbf{Z}$), tel que T^n appartienne à Γ et pour tout $\sigma \in SL(2, \mathbf{Z})$, il existe un entier $N(\sigma)$ tel que $T^{N(\sigma)}$ appartienne à $\sigma\Gamma\sigma^{-1}$. On obtient ainsi la propriété périodique de période $N(\sigma)$.

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 structure 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 $\mathcal{M}(t,\Gamma)$.

1.1.6. Caractères de Dirichlet.

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.

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 ne se 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

1.1.7. 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 Frölich A., ch. VIII.

1.1.8. Formes modulaires avec caractère

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

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

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

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

$$\forall \gamma = \begin{pmatrix} a\,b \\ c\,d \end{pmatrix} \in \Gamma_0(N), \quad f|_k\ \gamma = \chi(d) f.$$

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

1.1.9. Proposition. Pour tout sous-groupe d'indice fini Γ de SL(2,$\mathbf{Z}$), 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

1.1.10. 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,$\mathbf{Z}$) 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.

1.2. Motivations: 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:

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

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

1.2.1 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,$\mathbf{Z}$).

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

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

Cette dernière formule fut conjecturée par Ramanujan puis démontrée par Mordell et 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 commode 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:

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

1.2.3. 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 $\mathrm{Re}(s)>13/2$.

1.2.4. 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:

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

1.2.5. 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 1.2.1, 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 $K=\pi\sqrt{2/3}$.

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

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

puis la relation de congruence plus générale:

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

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 quotient $G_\mathfrak{p}/I_\mathfrak{p}$ s'identifie au groupe de Galois $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ de la clôture algébrique du corps fini $\mathbf{F}_p$. Le groupe $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est isomorphe au groupe procyclique $\hat{\mathbf{Z}}$ engendgré par le morphisme de Frobenius Fr_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 $\rho_l(Fr_p) \equiv \begin{pmatrix} p^{11} & * \\ 0 & 1 \end{pmatrix} \mathrm{mod}\ 691$, d'où $\tau(p) \equiv 1 + p^{11} \mathrm{mod}\ 691$.

1.2.7. 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.

8 novembre 1994. Lien avec la théorie de représentation. Définition géométrique des formes modulaires commes fonctions de réseaux.

1.3. Lien entre formes modulaires et représentations

Formes modulaires (plus généralement, formes automorphes) sont certaines fonctions sur les groupes réductifs réels $G(\mathbf{R})$ (ou sur les espaces symétriques $G(\mathbf{R})/K \cdot Z$ associés, K étant un sous–groupe maximal compact, Z le centre de $G(\mathbf{R})$). Ces fonctions sont des objets d'analyse, mais il arrive qu'ils sont étroitement liées aux a) équations diophantiennes ("schémas arithmétiques"), et aux b) représentations galoisiennes. On peut établir un lien entre ces trois types d'objets à l'aide des fonctions L correspondantes.

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.

1.3.1. 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 $\theta \in \mathbf{R}$

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

1.3.2. 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 $\mathrm{GL}(2, \mathbf{R})$ 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 notion d'adèle. 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 d'adèles $\mathbf{A}$ 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 d'adèles 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 $g \mapsto \pi_f(h)(g) = f(gh)$).

Alors toute forme modulaire

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

peut être relevé à une fonction f^0 sur le groupe $\mathrm{GL}_2(\mathbf{R})$ qui satisfait la condition d'invariance suivante:

$$f^0(\gamma g) = f^0(g) \quad \text{for all} \quad \gamma \in \Gamma_N \subset \mathrm{GL}_2(\mathbf{R}).$$

Pour définir f^0 on pose

$$f^0(g) = \begin{cases} f(g(i))j(g,i)^{-k}, & \text{if } \det g > 0 \\ f(g(-i))j(g,-i)^{-k}, & \text{if } \det g < 0, \end{cases}$$

où $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{R})$, $j(g,i) = |\det g|^{-1/2}(cz+d)$ le facteur d'automorphie.

On a $f^0(xg) = \exp(-ik\theta)f^0(g)$ if $x = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est une rotation par l'angle θ.

Considerons le groupe $\mathrm{GL}_2(\mathbf{A})$ des matrices non–dégénérées à coefficients dans l'anneau d'adèles $\mathbf{A}$ et son sous–groupe

$$U(N) = \left\{ g = 1 \times \prod_p g_p \in \mathrm{GL}_2(\mathbf{A}) \mid g_p \in \mathrm{GL}_2(\mathbf{Z}_p), g_p \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N\mathbf{Z}_p \right\}.)$$

Selon le *théorème chinois* (*théorème d'approximation*) on a la décomposition suivante:

$$\Gamma_N \backslash \mathrm{GL}_2(\mathbf{R}) = \mathrm{GL}_2(\mathbf{Q}) \backslash \mathrm{GL}_2(\mathbf{A}) / U(N),$$

qui nous premet voir f^0 comme une fonction sur $\mathrm{GL}_2(\mathbf{A})$.

L'action de $\mathrm{GL}_2(\mathbf{A})$ sur f^0 par les décalage de l'argument définit une représentation $\pi = \pi_f$ du groupe $\mathrm{GL}_2(\mathbf{A})$ dans l'espace des fonctions lisses à valeurs complexes sur $\mathrm{GL}_2(\mathbf{A})$, pour laquelle

$$(\pi(h)f^0)(g) = f^0(gh) \quad (g, h \in \mathrm{GL}_2(\mathbf{A})).$$

L'observation-clè du développement modern de la théorie des formes modulaires fait par Langlands et Piatetski–Shapiro dit que la propiété de la multiplicativité de type 1.2.2 pour les coefficients de Fourier (normalisés) d'une forme modulaire est équivalaent à irréductibilité de la représentation correspondante π_f du groupe $\mathrm{GL}_2(\mathbf{A})$. Autrement dit, la condition que la représentation π_f e irreductible admèt une interprétation arithmétique remarquable: f est une forme propre des opérateurs de Hecke (pour presque p).

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 $\pi_{f,v}$.

Dans ce cas le produit tensoriel infinit

$$\pi = \otimes_v \pi_v,$$

où π_v sont représentations des groupes locals $\mathrm{GL}_2(\mathbf{Q}_{p_v})$ et $\mathrm{GL}_2(\mathbf{R})$ (avec p_v les nombres premiers où $v = \infty$).

Jacquet et Langlands ont choisi comme une point de base de construction de fonctions L associées aux formes automorphes les représentation irréductibles des groupes de type $\mathrm{GL}_2(\mathbf{Q}_v)$. Telles représentations peuvent être classifié explicitement. En particulier, on vérifie que les représentations π_v ci–dessus pour presque tout $v = v_p$ ont la forme d'une représentation induite $\pi_v = \mathrm{Ind}(\mu_1 \otimes \mu_2)$ d'une représentation de dimension un du sous–groupe es matrices diagonales: $(\mu_1 \otimes \mu_2)\left(\begin{smallmatrix} x & o \\ o & y \end{smallmatrix}\right) = \mu_2(x)\mu_1(y)$, où $\mu_i : \mathbf{Q}_p^\times \to \mathbf{C}^\times$ sont des quasicaratères non–ramifiés.

Cette classification permet de définir pour presque tout p l'élément

$$h_p = \begin{pmatrix} \mu_1(p) & 0 \\ 0 & \mu_2(p) \end{pmatrix} \in \mathrm{GL}_2(\mathbf{C})$$

et le produit d'Euler suivant:

$$L(\pi_f, s) = \prod_{p \notin S} L(\pi_p, s) = \prod_{p \notin S} \det\left(1_2 - p^{-s} h_p\right)^{-1}$$

étendu sur presque tout nombres premiers.

Il arrive que la fonction $L(\pi, s)$ coïncide essentialement avec la *transformation de Mellin* de la forme modulaire initiale f:

$$L(s, f) = L(\pi_f, s + (k-1)/2).$$

La notion d'une forme primitive f a le sens suivant: la fonction f^0 de l'espace de représentation a le stabilisateur maximal possible dans l'espace de représentation. La théorie d'Atkin – Lehner peut être reformuler en disant que la représentaion π_f entre avec la multiplicité un dans la représentation régulier du groupe $\mathrm{GL}_2(\mathbf{A})$ (l'espace de toutes les fonctions intégrables avec carrée).

1.4. 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

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

Soit $\mathcal{L}$ désigne l'ensemble de tous les réseaux dans $\mathbf{C}$.

1.4. 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: $H \in \mathcal{H}_{-k}$.

1.4.2. 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

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

1.4.3. 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 $\mathrm{Im}\,(\omega_1/\omega_2) > 0$ 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

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

1.4.4. 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)

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

15 novembre 1994. Séries d'Eisenstein et leurs développement de Fourier. Fonction Δ comme un produit infinit.

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

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

Cette série converge absolument pour $k > 2$.

1.5.1. 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 par le développement suivant

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

(Table numérique:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = B_5 = \cdots = 0,\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},$$
$$B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730}\ B_{14} = \frac{7}{6},\ B_{16} = -\frac{3617}{510}\ B_{18} = \frac{43867}{798}\ ,\ldots).$$

On a

$$\zeta(k) = -\frac{(2\pi i)^k}{2}\frac{B_k}{k!},\quad \zeta(2) = \frac{\pi^2}{6},\quad \zeta(4) = \frac{\pi^4}{90},\quad \zeta(6) = \frac{\pi^6}{945},\cdots$$

puis on a

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

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

$$G_4(z) = 2\zeta(4)E_4(z) = \frac{2\pi^4}{90}\left[1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right],$$

$$G_6(z) = 2\zeta(6)E_6(z) = \frac{2\pi^6}{945}\left[1 - 540\sum_{n=1}^{\infty}\sigma_5(n)q^n\right],$$

$$g_2 = 60G_4 = \frac{4\pi^4}{3}E_4 = \frac{(2\pi)^4}{12}E_4, \quad g_3 = 140G_6 = \frac{8\pi^6}{27} = \frac{(2\pi)^6}{216}E_6, .$$

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

$$\sin(\pi a) = \pi a\prod_{n=1}^{\infty}\left(1 - \frac{a^2}{n^2}\right). \tag{5.1}$$

La dérivée logarithmiue de (5.1) nous donne

$$\pi\mathrm{ctg}\pi a = \frac{1}{a} + \sum_{n=1}^{\infty}\left(\frac{1}{a+n} - \frac{1}{a-n}\right). \tag{5.2}$$

Remarquons

$$\pi i\frac{e^{\pi ia} + e^{-\pi ia}}{e^{\pi ia} - e^{-\pi ia}} = \pi i + \frac{2\pi i}{e^{2\pi ia} - 1} = \pi i - 2\pi i\sum_{n=1}^{\infty}e^{2\pi ina} \tag{5.3}$$

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

$$\zeta(k) = -\frac{(2\pi i)^k}{2}\frac{B_k}{k!}, \tag{5.4}$$

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 (5.3) par raport à a $(k-1)$ fois:

$$-(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} e^{2\pi ina} = (-1)^{k-1}(k-1)! \sum_{n\in\mathbf{Z}} (a+n)^{-k}, \quad (k \in 2\mathbf{Z}, k \geq 2). \tag{5.5}$$

Posons $a = mz$ alors

$$\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi inmz} = \sum_{n\in\mathbf{Z}} (mz+n)^{-k}. \tag{5.6}$$

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

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}\sum_{n=-\infty}^{\infty} (mz+n)^{-k} = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{m,d=1}^{\infty} d^{k-1} q^{md}\right]. \tag{5.7}$$

Remarquons que la série double dans (5.7) est absolument convergente pour $k > 2$ mais la séries (5.7) a un sens aussi pour $k = 2$ comme une série réitérative avec la convergence conditionnelle. On finie la démonsration en substituant (5.4) dans (5.7).

1.5.2. 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

1.5.3. Proposition.

$$z^{-2}E_2(-z^{-1}) = E_2(z) + \frac{12}{2\pi i z}. \tag{5.8}$$

Démonstration da la proposition. On utilise la série (5.7) avec $k = 2$ qui converge conditionnelement:

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

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

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

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

Pour la démontrer on introduit le terme correctif suivant

$$b_{m,n}(z) = \frac{1}{(mz+n-1)(mz+n)} = \frac{1}{(mz+n-1)} - \frac{1}{(mz+n)} \tag{5.9}$$

Alors on obtient la série modifiée

$$\tilde{E}_2(z) = 1+\frac{3}{\pi^2}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty}\left((mz+n)^{-2} - b_{m,n}(z)\right) \tag{5.10}$$

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 (5.10) 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 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 1.5.3 et théorème 1.5.2.

22 novembre 1994. Structure des formes modulaires pour sur $\mathrm{SL}_2(\mathbf{Z})$. Applications. Congruence de Ramanujan et son interprétation galoisienne.

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

1.6.1. Domaine fondamentale du groupe modulaire. Soient $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. On a

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

Soit d'autre part, D le sous–ensemble de $\mathcal{H}$ formé de 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 $TS = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

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

Démontration des théorèmes 1.6.1 et 1.6.2. 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 1.6.1. 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 $\gamma \in \Gamma(1)$ 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'un 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.

1.6.3. 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 $\overline{\mathbf{R}}$.

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

Théorème 1.6.1 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 $e_p = 1$.

1.6.4. 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 $\displaystyle\sum_{p\in\Gamma(1)\backslash\mathcal{H}}{}^{*\prime}$ 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).

1.6.5. 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* $\mathcal{S}_k(\Gamma(1))$.

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

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

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

(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 1.6.5.

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

1.6.7. 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 déveloper $E_6^2(z)$ 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

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

et le développement implique

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

d'où la congruence.

1.6.8. 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:

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

oú $\zeta_N = \exp(2\pi i/N)$.

Cette formule est facilement impliquée par le développment

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

que nous avons déjà unilisé plus haut. D'un autre côté, pour tout $\gamma=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ 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 χ mod N quelconque):

$$\begin{aligned}
G_k^{a,N}(\Lambda,P)&=\sum_{l\in\Lambda+aP}l^{-k},\\
G_k^{\chi,N}(\Lambda,P)&=\sum_{a\bmod N}\overline{\chi}(a)G_k^{a,N}(\Lambda,P)),\\
G_k^{a,N}(\Lambda,\langle P\rangle)&=\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^*}G_k^{a,N}(\Lambda,P)
\end{aligned}$$

Exercise. Trouver les développements de Fourier des séries

$$\begin{aligned}
G_k(a,N,z)&=N^kG_k^{a,N}(\Lambda_z,\frac{1}{N})\\
G_k(\chi,N,z)&=N^kG_k^{\chi,N}(\Lambda_z,\frac{1}{N}).
\end{aligned}$$

Pour définir les séries d'Eisenstein dans les cas $k=1,2$ on introduit un paramètre additionnel $s\in\mathbf{C}$ et on utilise la méthode de Hecke basée sur un prolongement analytique au point $s=0$ des séries

$$G_k(z;a_1,a_2,N)=y^s\sum_{\substack{m_1\equiv a_1 \bmod N\\ m_2\equiv a_2 \bmod N}}(m_1z+m_2)^{-k}|m_1z+m_2|^{-2s},$$

qui sont absolument convergentes pour $k+\mathrm{Re}\,(2s)>2$, et qui satisfont les conditions d'automorphie pour tous tels $s\in C$.

Chapitre 2. Surfaces de Riemann et formes modulaires

29 novembre 1994. Surfaces de Riemann. Domaine fondamental de $\mathrm{SL}_2(\mathbf{Z})$ comme surface de Riemann. Formes modulaires comme différentielles multiples et lien avec le théorème de Riemann–Roch.

2.1. Surfaces de Riemann: généralités et exemples. 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 considèrer le domaine fondamentale $\Gamma\backslash\mathcal{H}$. Cependant, la structure de $\Gamma\backslash\mathcal{H}$ en général est beaucoup plus complqué que celle de $\mathrm{SL}(2,\mathbf{Z})\backslash\mathcal{H}$. Pour la mieux comprendre il faut fournir $\Gamma\backslash\mathcal{H}$ avec une structure d'une surface de Riemann, c'est à dire, d'une *variété analytique complexe de dimension* 1.

2.1.1. Rapplels sur les surfaces de Riemann (voir [Farkas–Kra]). Plus précisement, une surface de Riemann X est un espace topologique de Hausdorf avec la structure suivante:
1)
$$X = \cup_\alpha U_\alpha, \quad (U_\alpha, p_\alpha),\ p_\alpha : U_\alpha \xrightarrow{\sim} p_\alpha(U_\alpha) \subset \mathbf{C},$$
$(p_\alpha(U_\alpha)$ un ouvert, U_α s'appele une carte, p_α un homéomorphisme (un paramètre locale);
2) Si $U_\alpha \cup U_\beta \neq \emptyset$, l'application $p_\beta \circ p_\alpha : p_\alpha(U_\alpha \cup U_\beta) \xrightarrow{\sim} p_\beta(U_\alpha \cup U_\beta)$ est biholomorphe;
[3) on peut choisir une telle structure de façon maximale en utilisant le lemme de Zorn, mais on va pas utiliser ce choix; autrement dit, on considère une surface de Riemenn avec une classe d'équivalence d'atlases, et pas avec un seul atlas; ceci permet d'utiliser des cartes les plus commodes dans les situations concrètes.]

En tout cas, pour tout point $z_0 \in X$ soit $p_{z_0} : U_\alpha \to \mathbf{C}$ un paramètre local en z_0, i.e. un paramétre locale de $U_\alpha \ni z_0$ avec $p_{z_0}(z_0) = 0$. De plus, X est naturellement orienté par l'orientation induit de $\mathbf{C}$.

Soit maintenant X une surface de Riemann compacte. Alors la structure topologique de X est complétement déterminée par un nombre naturel $g = g(X)$ qui s'appell *le genre* de X. Pour décrire cette structure on utilise un *polygone normal* de $4g$ côtés de X désigné par
$$(a_1 b_1 a_1^{-1} b_1^{-1} \dots a_g b_g a_g^{-1} b_g^{-1})$$
(ou une *forme normale*) qui peut–être définit à partir d'une triangulation de X. Dans une triangulation d'une variété réele on appelle les triangles 2-simplices, les côtés 1-simplces, et les sometes 0-simplices. De plus on utilise les points $\{P_1, P_2, \dots,\}$ pour marquer les côtés et les triangles orientés comme $\langle P_1, P_2\rangle$ et $\langle P_1, P_2, P_3\rangle$ respectivement, donc $\langle P_1, P_2\rangle = -\langle P_2, P_1\rangle$, $\langle P_1, P_2, P_3\rangle = -\langle P_1, P_3, P_2\rangle$. Dans le cas où X est compacte une triangulation de X ne contient qu'un nombre fini de triangles.

Nous donnons quelques examples et propriétés des surfaces de Riemann: Exemples les plus connus de surfaces de Riemann sont:

2.1.2. 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 $\mathbf{CP}^1 = \mathbf{C} \cup \infty$

2.1.3. Tore 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 développements de Laurent de $\wp(u)$ et de $\wp'(u)$ sont

$$\wp(u) = u^{-2} + \sum_{n=2}^{\infty} (2n-1) G_{2n}(\Lambda) u^{2n-2} = u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6)$$

$$\wp'(u) = -2u^{-3} + \sum_{n=2}^{\infty} (2n-1)(2n-2) G_{2n}(\Lambda) u^{2n-3}$$

$$= -2u^{-3} + 6G_4 u + 20 G_6 u^3 + \mathcal{O}(u^5)$$

D'où on obtient la relation suivante

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

où

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

(voir Chapitre 3).

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

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

Posons

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

2.1.5. Lemme. *La fonction* $j(z)$ *provient isomorphismes* $\Gamma \backslash \mathcal{H} \xrightarrow{\sim} \mathbf{C}$ *et* $\overline{\Gamma \backslash \mathcal{H}} \xrightarrow{\sim} \overline{\mathbf{C}} = S^1 = \mathbf{C} \cup \infty$.

Preuve est impliquée par le fait que $j(z)$ est une fonction modulaire sur $\Gamma = \Gamma(1) = \mathrm{SL}(2, \mathbf{Z})$, i.e. une forme modulaire méromorphe de poids 0. En effet, pour tout $a \in \mathbf{C}$

la fonction $f(z) = j(z) - a$ est aussi une fonction modulaire sur Γ, et on a vu l'égalité

$$\frac{1}{2}\mathrm{ord}_{z=i}(f) + \frac{1}{3}\mathrm{ord}_{z=\rho}(f) + \sum_{\substack{P\in\Gamma\backslash H \\ P\neq i,\rho}} \mathrm{ord}_{z=P}(f) - 1 = 0,$$

car $\mathrm{ord}_{z=\infty}(f) = -1$. Ceci implique que f a une seule racine, notamment, soit $z = i$ avec multiplicité 2 (pour $a = 0$), soit $z = \rho$ avec multiplicité 3 (pour $a = 1$), soit $z = P \in H$, $P \neq i, \rho$.

On va fournir $\overline{\Gamma\backslash\mathcal{H}}$ 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.

2.2. Théorème de Riemann–Roch et ces corollaires.

2.2.1. Soit $F = \mathbf{C}(X)$ le corps de toutes les fonctions méromorphes sur une surface de Riemann X (i.e. les applications $f : X \to \overline{\mathbf{C}}$, avec $\overline{\mathbf{C}}$ la sphère de Riemann), ou $F = k(X)$ le corps des fonctions algébriques méromorphes sur une courbe algébrique X projective et lisse sur un corps $k = \overline{k}$ algébriquement clos (et on va utiliser la notaton $k = \mathbf{C}$ pour les surfaces de Rieman compactes). On identifie les points P de X avec les valuations discrétes $v_P : F \to \mathbf{Z}$ telles que $v_P(t)$ pour une uniformisante locale $t = t_P \in F^\times$ en P. Posons $\mathcal{O}_P = \{f \in F \mid (v_P(f) \geq 0\}$.

Attention: pour une surface de Riemann X il n'est pas évident qu'il existe une telle t, même que $\mathbf{C}(X) \neq \mathbf{C}$. On construit des fonction méromorphes (globales) non nulles à l'aide de la théorie de différentielles harmoniques (voir [Farkas et Kra], II.4, II.5), où on a montré que pour tous $P \neq Q$ il existe $f \in \mathbf{C}(X)^\times$, telle que $f \in \mathcal{O}_P$ mais $f \notin \mathcal{O}_Q$ ($v_P(f) \geq 0$, $v_Q(f) < 0$). Ce fait sera utilisé sans démonstration parce que pour les courbes algébriques c'est la définition d'un point, et sa démonstration dans le cas de surfaces de Riemann utilise des moyens essentielement analytiques. Posons

$$Div_X = \{\sum_P n_P P \mid n_P \in \mathbf{Z} \text{ presque tous nuls}\},$$

le groupe de diviseurs de X (le groupe abelien libre engendré par les points de X). On a un homomorphisme de groupes abeliens (*le degré*):

$$d : Div_X \to \mathbf{Z}, \quad d(\sum_P n_P P) = \sum_P n_P,$$

pour $D = \sum_P n_P P$ on écrit $v_P(D) = n_P$, et on dit que $D_1 \leq D_2$ si $\forall P \in X \;\; v_P(D_1) \leq v_P(D_2)$. Le symbol $S(D) = \{P \in X \mid n_P\}$ désigne le support de D (c'est un ensemble fini de diviseurs premiers).

Soit S maintenant un ensemble fini de diviseurs premiers (i.e. des points de X), et $D \in Div_X$ un diviseur.

Définition. (a)

$$F_S = \cap_{P\in S}\mathcal{O}_P, \quad F_S(D) = \{f \in F \mid \forall P \in S \;\; v_P(f) \geq -v_P(D)\},$$

(b)
$$\mathcal{L}(D) = \{f \in F \mid \forall P \in X \ \ v_P(f) \geq -v_P(D)\}.$$

On voit que F_S, $F_S(D)$, $\mathcal{L}(D)$ sont des espaces vectoriels sur k.

2.2.2. Théorème de finitude des dimensions. (a)

$$\dim_k \mathcal{L}(D) = l(D) < \infty,$$

(b) $\mathcal{L}(D) = 0$ *pour* $D \leq 0$,
(c) *pour tous* A, B *avec* $B \leq A$ *on* $l(A) - d(A) \leq l(B) - d(B)$.

2.2.3. Le théorème de Riemann–Roch donne un moyen de calcul des dimensions $l(D)$ à l'aide de différentielles.

Diviseur d'une fonction. Pour $f : X \to \overline{C}$ une fonction méromorphe posons $(f) = div(f) = \sum_P v_P(f)P \in Div_X$. On ecrit $(f) = (f)_0 - (f)_\infty$ où $(f)_0, (f)_\infty \geq 0$ le diviseur de zéros (de pôles) de f.

Diviseur d'une différentielle. Soit $\omega \in \Omega_X$, $t = t_P : X \to \overline{\mathbf{C}}$ une uniformisante locale en P, alors $(\omega) = div(\omega) = \sum_P v_P(f_P)P \in Div_X$, où $\omega = f_P dt_P$. Pour un diviseur $D \in Div_X$ on pose $\Omega_X(D) = \{\omega \in \Omega_X \mid (\omega) \geq D\}$.

Proposition. (a) $d(div(f)) = d(f) = 0$;
(b) $[F : k(f)] = d(f)_0 = d(f)_\infty =$ *"le nombre d'images réciproques de 0 ou de ∞"; en particulier pour* $f \notin k$ $d(f)_0 = d(f)_\infty > 0$.

Groupe des classes de diviseurs est définit comme le groupe quotient $Cl_X = Div_X/P_X$, où $P_X = \{(f) \mid f \in F^\times\} \subset Div_X$ le sous–groupe des diviseurs principaux.

2.2.4. Proposition. (a) *Les nombres* $d(A)$ *et* $l(A)$ *ne dépendent que de la classe de* A *dans* Cl_X.
(b) *La classe* K *d'une différentielle non–nulle* (ω) *dans* Cl_X *est bien définit et s'appele la classe canonique de* X, $K = K_X$.
(c) $\dim_k \Omega_X(D) = l(K - D)$.

Démonstration est directement impliquée par les deux propositions précédentes.

2.2.5. Théorème de Riemann–Roch. (a) *Il existe un nombre entier* $g = g(X)$ *tels que pour tout diviseur* D *on a*

$$l(D) = d(A) + 1 - g + l(K - D);$$

(b) *le nombre* g *coïncide avec* $l(K) = \dim_k \Omega_X(0) = \dim_k \Omega[X]$ *où* $\dim_k \Omega_X(0) = \dim_k \Omega[X]$ *la dimension du* k*-espace vectoriel des différentielles algébriques holomorphes sur* X *(on pose* $D = 0$ *dans (a)).*

6 décembre 1994. Théorème de Riemann–Roch pour les surfaces de Riemann compactes et pour les courbes projectives et lisses. Théorème de finitude des dimension. Théorème d'approximation. Groupe des classes de diviseurs. La classe canonique.

Tout d'abord on va démontrer le théorème de finitude des dimensions $l(A)$. Démonstration est basée sur le "Théorème chinois" sur X (plus précisement, le théorème sur l'indépendence des valuations)

2.2.6. Théorème d'approximation. (a) *Soient $v_1, \dots, v_n$ les valuations normalisées associées aux points $P_1, \dots, P_n$ correspondants. Alors $\forall a_i \in F$ et $\forall m_i \in \mathbf{Z}$ il existe un $a \in F$ tel que*

$$v_i(a - a_i) > m_i.$$

(b) *$\forall a_i \in F$ et $\forall m_i \in \mathbf{Z}$ il existe $u \in F$ tel que*

$$v_i(u - a_i) = m_i.$$

2.2.7. Théorme d'approximation implique le théorème de finitude. En effet, pour $B \leq A$ on a

$$\frac{\mathcal{L}(A)}{\mathcal{L}(B)} = \frac{\mathcal{L}(A)}{\mathcal{L}(A) \cap F_S(B)} = \frac{\mathcal{L}(A) + F_S(B)}{F_S(B)} \subset \frac{F_S(A)}{F_S(B)}.$$

2.2.8. Lemme. *Soit $B \leq A$, $S = Supp(A) \cup Supp(B)$. Alors*

$$\dim_k \frac{F_S(A)}{F_S(B)} = d(A) - d(B).$$

On a $A = B + P_1 + \ldots + P_n$ et il suffit de montrer que $\dim_k \dfrac{F_S(B+P)}{F_S(B)} = 1$. Par le théorème d'approximation il existe $u \in F^\times$ tel que $v_P(u) = v_P(B+P)$ et on v'erifie par d'efinition que l'applicaton $f \mapsto fu$ fourinie un isomorphisme $O_P/\mathfrak{m}_P \overset{\sim}{\to} \dfrac{F_S(B+P)}{F_S(B)}$ d'où le lemme.

Pour déduire le théorème de finituide on remarque que (b) est le résultat de l'égalité

$$k = \cap_P \mathcal{O}_P,$$

et $f \in \mathcal{L}(D) \subset \cap_P \mathcal{O}_P$ pour $D < 0$, et pour un P on a $f(P) = 0$, donc $f \equiv 0$.

Indiquons la démonstration du théorème de l'approximation, qui est est valable dans une situation très générale (pour un nombre fini des valuations indépendentes d'un corps). Remarquons que chaque v définit une norme de F par la formule $|x|_v = \rho^{v(x)}$ avec $0 < \rho < 1$. Alors on peut reformuler le théorème d'approximation de une façon très naturelle en disant que F est dense dans le produit $\hat{F}_1 \times \ldots \times \hat{F}_n$ des complétions correspondantes $\hat{F}_i$.

2.2.9. Lemme. *Soient $v_1, \dots, v_n$ les valuations de F tels que pour tous i, j, $i \neq j$ $\mathcal{O}_i \not\subset \mathcal{O}_j$. Alors il existe un $f \in F$ tel que $v_1(f) \geq 0$ et $v_2(f), \dots, v_n(f) < 0$.*

Raisonement par récurrence. Soit $g \in F$ tel que $v_1(g) \geq 0$ et $v_2(g), \dots, v_{n-1}(g) < 0$ alors on peut suposer que $v_n(g) \geq 0$ (sinon on pose $f = g$). D'autre part il existe $h \in F$

avec $v_1(h) \geq 0$ et $v_n(h) < 0$. Posons $f = g + h^m$, alors $v_1(f) \geq 0$, et l'inégalité $v_r(f)$ implique $r = 2, \ldots, n-1$. Ici on a deux cas: $v_r(h) \geq 0$ ou $v_r(h) < 0$. Si $v_r(h) \geq 0$, on a $v_r(g + h^m) < 0$. Sinon $v_r(h) < 0$ et l'hypothèse $v_r(g + h^{m_r}) \geq 0$ implique pour tout $m > m_r$

$$v_r(g + h^m) = \min\{v_r(g + h^{m_r}), v_r(h^m), v_r(h^{m_r})\} < 0,$$

donc f satisfait aux conditions du lemme pour m assez grand.

2.2.10. Lemme. *Sous les mêmes hypothèses il existe un $f_0 \in F$ tel que $v_1(f_0) > 0$ et $v_2(f_0), \ldots, v_n(f_0) < 0$.*

En effet pour un $h_0 \in F$ tel que $v(h_0) > 0$ et pour f comme dans Lemme 2.2.9 on a $f_0 = h_0 f^m$ pour m assez grand car $v_r(f_0) = v_r(h) + m v_r(f)$ et $v_r(f) < 0$ pour tout $r = 2, \ldots, n$.

2.2.11. Lemme. *Sous les mêmes hypothèses pour tout $l_i \in Z$ il existent n $f_i \in F$ tels que $v_1(f_1 - 1) > l_1$ et $v_2(f_2) > l_2, \ldots, v_n(f_n) < l_n$.*

Démonstration. Par lemme 2.2.9 il existent g_i tels que $v_i(g_i) > 0$ et $v_j(g_i) < 0$. Posons $f_i = \dfrac{1}{g_i^m + 1}$, alors

$$v_i(f_i - 1) = v_i\left(\frac{-g_i^m}{g_i^m + 1}\right) = v_i(g_i^m),$$

car $v_i(g_i^m + 1) = \min\{v_i(g_i^m), v_i(1)\} = 0$, et

$$v_j(f_i) = v_j\left(\frac{1}{g_i^m + 1}\right) = -v_j(g_i^m),$$

car $v_j(g_i^m + 1) = \min\{v_j(g_i^m), v_i(1)\} = v_j(g_i^m)$.

On finie la démonstration du théorème en posant

$$a = \sum_i a_i f_i, \quad \text{avec} \quad l_i = m_i - \min_{j=1}^{n} v_i(a_j)$$

car

$$v_i(a - a_i) = v_i \left(a_i(f_i - 1) + \sum_{j \neq i} a_j f_j \right) \geq \min\{v_i(a_i), v_i(f_i - 1), \ldots, v_i(a_j)\}.$$

Cela montre (a). Pour voir (b) on choisit un $b \in F$ tel que $v_i(b - a_i) > m_i$ et pour tout $i = 1, \ldots, n$, puis on choisit b_i tels que $v_i(b_i) = m_i$ et en utilisant encore Lemme 2.2.10, on trouve un c avec $v_i(c - b_i) > m_i$. On pose $u = b + c$, donc $u - a_i = b - a_i + c - b_i + b_i$ et $v_i(u - a_i) = \min\{v_i(b_i), v_i(a_i - b), v_i(c - b_i)\} = v_i(b_i) = m_i$.

2.2.12. Différentielles et calcul de $l(A)$. Soit R un anneau sur un autre anneau $\mathcal{O}$ (avec $i : \mathcal{O} \in R$ étant le morphisme de structure).

Définition. *Le module de différentielles $\Omega_{R/\mathcal{O}}$ est définit comme un R–module fourni avec une application de R-modules $d : R \to \Omega(R/\mathcal{O})$ qui satisfait la condition $d(rs) = rd(s) + sd(r)$, et qui est universel par rapport à cette condition. Une construction* *explicite: posons* $I = \mathrm{Ker}\,\delta$, $\delta : R\otimes_{\mathcal{O}} R \to R$ *morphisme de la multiplication, alors* $\Omega(R/\mathcal{O}) = I/I^2$, *et* $d(r) = r\otimes 1 - 1\otimes r$.

Proposition. *Soit* $R/\mathcal{O}$ *une extension des corps* $R = F$ *et* $k = \mathcal{O}$. *Alors* $\Omega(F/k)$ *est un espace vectoriel sur* F *et* $df_1, \ldots, f_n$ *est une base de* $\Omega(F/k)$ *sur* $F \iff F/k(f_1, \ldots, f_n)$ *est une extension séparable algébrique des corps.*

Démonstration voir [S.Lang, Algèbre]. En particulier, pour une courbe X sur k on pose $\Omega_X = \Omega(k(X)/k)$: alors $\dim_F \Omega_X = 1$ car le degré de transcendence de F/k est égale à 1.

Pour un $P\in X$ posons $\Omega_P = \Omega(\mathcal{O}_P/k)$, alors $\Omega_P = \mathcal{O}_P dt$, où dt une uniformisante locale en P, et dt est en même temps une base de Ω_X sur F.

Diviseur d'une fonction. Pour $f : X \to \overline{C}$ une fonction méromorphe posons $(f) = div(f) = \sum_P v_P(f)P \in Div_X$. On ecrit $(f) = (f)_0 - (f)_\infty$ où $(f)_0, (f)_\infty \geq 0$ le diviseur de zéros (de pôles) de f.

Diviseur d'une différentielle. Soit $\omega \in \Omega_X$, $t = t_P : X \to \overline{\mathbf{C}}$ une uniformisante locale en P, alors $(\omega) = div(\omega) = \sum_P v_P(f_P)P \in Div_X$, où $\omega = f_P dt_P$. Pour un diviseur $D \in Div_X$ on pose $\Omega_X(D) = \{\omega \in \Omega_X \mid (\omega) \geq D\}$.

Proposition. (a) $d(div(f)) = d(f) = 0$;
(b) $[F : k(f)] = d(f)_0 = d(f)_\infty =$ *"le nombre d'images réciproques de 0 ou de* ∞*"; en particulier pour* $f \notin k$ $d(f)_0 = d(f)_\infty > 0$.

Groupe des classes de diviseurs est définit comme le groupe quotient $Cl_X = Div_X/P_X$, où $P_X = \{(f) \mid f \in F^\times\} \subset Div_X$ le sous–groupe des diviseurs principaux.

Proposition. (a) *Les nombres* $d(A)$ *et* $l(A)$ *ne dépendent que de la classe de* A *dans* Cl_X.
(b) *La classe* K *d'une différentielle non–nulle* (ω) *dans* Cl_X *est bien définit et s'appele la classe canonique de* X, $K = K_X$.
(c) $\dim_k \Omega_X(D) = l(K-D)$.

Démonstration est directement impliquée par les deux propositions précedentes.

13 décembre 1994. Répartitions de Weil et le théorème de Riemann. Irregularité et ses propriétés.

Rappellons que le théorème de Riemann–Roch (théorme 2.2.5) affirme: (a) *Il existe un nombre entier* g *tels que pour tout diviseur* D *on a*

$$l(D) = d(A) + 1 - g + l(K-D);$$

(b) *le nombre* g *coïncide avec* $l(K) = \dim_k \Omega_X(0) = \dim_k \Omega[X]$ *où* $\dim_k \Omega_X(0) = \dim_k \Omega[X]$ *la dimension du* k*–espace vectoriel des différentielles algébriques holomorphes sur* X *(on pose* $D = 0$ *dans (a)).*

2.2.13. Corollaire. $d(K) = 2g - 2$ *(on pose* $D = K$ *dans (a))*

2.2.14. Corollaire. *$l(D) = d(D) + 1 - g$ pour tout D avec $d(D) > 2g - 2$ (on remarque que $l(D) = 0$ pour $d(D) < 0$; sinon $\exists h \in \mathcal{L}(D)$ donc $d((h)) \geq -d(D) > 0$; puis on utilise (a) où $l(K - D) = 0$).*

Démonstration du théorème utilise la notion de *répartition* (de Weil) $r = (r_P)_P$; elle est définie comme un vecteur infinit avec les composantes dans F avec $v_P(r_P) \geq 0$ pour presque tout P. Ces vecteurs forment un F–algèbre R (de dimension infinie), et pour tout $D \in Div_X$ on pose

$$R(D) = \{r = (r_P) \mid v_P(r_P) \geq -v_P(D)\}.$$

La démonstration se décompose en trois parties suivantes:

(1) "Théorème de Riemann") Il existe une constante, notée par $1-g$ telle que pour tout A $l(A) - d(A) \geq 1 - g$, et la borne est exacte, i.e. pour un D_0 on a $l(D_0) - l(D_0) = 1 - g$ (C'est la partie essentielle de la démonstration. Riemann a démontré ce théorème, mais n'est pas le théorème de Riemann–Roch sous la forme finale ci-dessus, qui a été démontré après quelque temps par Roch).

(2) Pour tout D

$$\dim_k \frac{R}{R(D) + F} = l(D) - d(D) + 1 - g.$$

Le nombre naturel $i(D) = l(D) - d(D) + 1 - g$ s'appel *irrégularité* de D, et cette affirmation est appélée parfois "la forme préliminaire du théorème de Riemann –Roch".

(3) Pour tout D

$$\dim_k \frac{R}{R(D) + F} = l(K - D).$$

(on peut considérer cette partie comme calcul de l'irrégularité $i(D)$).

2.2.15. Proposition ((1) implique (2)). (a) *Pour tous A, B avec $B \leq A$ on a*

$$\dim_k \frac{R(A) + F}{R(B) + F} = (l(B) - d(B)) - (l(A) - d(A)).$$

(b)*Pour le nombre $g = 1 - \min(l(A) - d(A))$ de (1) on a*

$$\dim_k \frac{R}{R(D) + F} = l(D) - d(D) - 1 + g.$$

Preuve. Par le théorème d'isomorphisme de Noether on a

$$\frac{R(A) + F}{R(B) + F} = \frac{R(A) + R(B) + F}{R(B) + F} = \frac{R(A)}{R(A) \cap (R(B) + F)}$$

mais la définition de $\mathcal{L}(A)$ signifie que $R(A) \cap (R(B) + F) = \mathcal{L}(A) + R(B)$, et donc

$$\frac{R(A) + F}{R(B) + F} = \frac{R(A)}{\mathcal{L}(A) + R(B)} = \frac{R(A)/R(B)}{(\mathcal{L}(A) + R(B))/R(B)}.$$

On voit également que

$$(\mathcal{L}(A)+R(B))/R(B)=\mathcal{L}(A)/(\mathcal{L}(A)\cap R(B))=\mathcal{L}(A)/\mathcal{L}(B),$$

donc

$$\frac{R(A)+F}{R(B)+F}=\frac{R(A)/R(B)}{\mathcal{L}(A)/\mathcal{L}(B)}.$$

L'affirmation (a) est maintenant impliqué par le lemme suivant

2.2.16. Lemme. *Pour tous A, B avec $B \leq A$ on a*

$$\dim_k \frac{R(A)}{R(B)} = d(A)-d(B).$$

Démonstration du lemme. Il suffit de construire un isomorphisme

$$\frac{F_S(A)}{F_S(B)} \xrightarrow{\sim} \frac{R(A)}{R(B)},$$

où $S = Supp(A)\cup Supp(B)$. Pour tout $f \in F_S(A)$ assignons la répartition suivante:

$$r=(r_P)_P=r(f), \quad \text{avec} \;\; r_Q=\begin{cases} f, & \text{pour} \quad P\in S, \\ r_P=0 & \text{sinon.}\end{cases}$$

Si $f \in F_S(B)$ on a $r \in R(B)$ alors $f \mapsto r(f)$ définit une application injective

$$\frac{F_S(A)}{F_S(B)} \to \frac{R(A)}{R(B)}.$$

D'autre part, cette application est surjective: par le théorème d'aproximation à partir d'une répartition $(r_P)_P$ on peut trouver une fonction $f \in F_S(A)$ telle que $v_P(f-r_P) \geq -v_P(r_P(B))$.

Pour vérifier l'affirmation (b) on prend le diviseur D_0 du theorème de Riemann donc $l(D_0)-l(D_0)=1-g$. Soit $D' = PPCM(D_0, A)$ où A est un diviseur donné. Alors $D_0 \leq D'$, $A \leq D'$ donc

$$1-g \leq l(D')-d(D') \leq l(D_0)-d(D_0)) = 1-g$$

et

$$\dim_k \frac{R}{R(A)+F} \geq \dim_k \frac{R(D')+F}{R(A)+F} = (l(A)-d(A))-(1-g),$$

et pour démontrer (b) il faut montrer l'inégalité réciproque:

$$\dim_k \frac{R}{R(A)+F} \leq (l(A)-d(A))-(1-g).$$

Soient $r_1,\dots,r_m \in R$ linéairement indépendants modulo $R(A)+F$. ll faut montrer que $m \leq l(A)-d(A)-1+g$. Pour cela on va construire un A' tel que $r_1,\dots,r_m \in R(A')$, alors

$$m \leq \dim_k \frac{R(A')}{R(A)+F} = (l(A)-d(A)) - (l(A')-d(A')) \leq (l(A)-d(A)) + (1-g).$$

Construction de A' est facile: on choisit un tel A' que pour tout $P \in X$

$$v_P(A') \geq \max(v_P(A), -v_P(r_1), \dots, -v_P(r_m))$$

(c'est possible car pour chaque $r_i \in R$ l'ensemble de $P \in X$ avec $-v_P(r_i)$ positive est fini), d'où le théorème.

2.2.17. Démonstration du théorème de Riemann. Soit $f \in F^\times$ une fonction méromorphe non constante, $[F : k(f)] = N = d((f)_0) = d((f)_\infty)$. La démonstration se décompose en deux parties:

Proposition. (a) *Soit $D_0 = (f)_\infty > 0$. Alors il existe le minimum*

$$\min_m (l(mD_0) - d(mD_0)) = 1 - g;$$

(b) *pour tout D*

$$l(D) - d(D) \geq \min_m (l(mD_0) - d(mD_0)) = 1 - g.$$

Preuve de (a). Rappellons qu'un élément $h \in F$ s'appel *entier* sur $k[f]$ si

$$h^m + a_{m-1}h^{m-1} + \ldots + a_0 = 0 \;\text{ pour }\; a_i \in k[f],\; i = 1, \dots, m.$$

Cette propriété est équivalente au fait que l'anneau $k[f, h]$ est de génération fini comme $k[f]$–module. Il est claire que pour un $h_0 \in F$ quelconque satisfaisant une équation de type

$$b_m h_0^m + b_{m-1}h_0^{m-1} + \ldots + b_0 = 0 \;\text{ pour }\; b_i \in k[f],\; i = 1, \dots, m,$$

l'élément $h = b_m h_0$ est entier sur $k[f]$.

2.2.18. Lemme. *Si h est une fonction entière algébrique de f, pour tout $P \in X$ $f \in \mathcal{O}_P \Longleftrightarrow h \in \mathcal{O}_P$. Autrement dit, pour tout $P \in X$ $P \not| (f)_\infty$ implique $P \not| (h)_\infty$, est alors le diviseur $(h) + m(f)_\infty$ est positive pour m assez grands.*

Preuve du lemme: par l'hypothèse, l'élément h est un entier sur $\mathcal{O}_P$ donc la valeur $v_P(h)$ est positive (sinon les puissances h^m engendreraient un module de génération infinie sur $\mathcal{O}_P$).

Soit $g_1, \dots, g_N$ une base de l'extension $F/k[f]$. Par l'observation ci-desus on peut supposer que g_i sont des entiers de f, et si l'on cosidère $N(1+t)$ produits

$$f^i g_j, \quad (i = 0, \dots, t;\;\; j = 1, \dots, N)$$

on voit qu'ils sont linéairement indépendent sur k. Par le Lemme 2.218, il existe un nombre naturel s tel que

$$s(f)_\infty + (g_j) \geq 0 \Longrightarrow (s+t)(f)_\infty + (f^i g_j) \geq 0.$$

Ceci résulte

$$N(1+t) \leq l((s+t)(f)_\infty) \Longrightarrow l((s+t)(f)_\infty)(1+t) \geq d((f)_\infty),$$

et si l'on pose $m = s+t \geq s$ avec $t \gg 0$

$$l(m(f)_\infty) - d(m(f)_\infty) = (1-s)d((f)_\infty),$$

où dans la partie droite $(1-s)d((f)_\infty)$ est une constante, d'où on obtient (a).

Pour montrer (b) on utilise le fait que pour tout diviseurs D les nombres $l(D)$ et $d(D)$ ne dépendent que de la classe de D dans Cl_X. Posons $D_0 = (f)_\infty > 0$ ci-dessus, $D = D_1 - D_2$, $D_1, D_2 \geq 0$. Alors

$$l(mD_0 - D_1) - d(mD_0 - D_1) \geq l(mD_0) - d(mD_0) \geq 1-g,$$

et pour m asez grand on a

$$l(mD_0 - D_1) \geq md(D_0) - d(D_1) + 1 - g > o,$$

car $-d(D_1) + 1 - g$ est une constante, et $m \gg 0$. Autrement dit, pour $m \gg 0$ il existe une $h \in \mathcal{L}(mD_0 - D_1)$ non nulle, i.e.

$$(h) + mD_0 - D_1 \geq 0 \Longrightarrow -(h) + D_1 \leq mD_0 \Longrightarrow D_1 \leq mD_0 + (h),$$

donc

$$l(D_1) - d(D_1) = l(-(h) + D_1) - d(-(h) + D_1) \geq l(mD_0) - d(mD_0) \geq 1-g$$

pa la définition de $1-g$ dans (a).

D'autre part, $D = D_1 - D_2 \leq D_1$ alors

$$l(D) - d(D) \geq l(D_1) - d(D_1) \geq 1-g,$$

entraînant le théorème de Riemann.

20 décembre 1994. Résidus et dualité. Calcul d'irregularité. Corrolaires du théorème de Riemann-Roch. Applications aux formes modulaires (dimensions des espaces de formes modulaires).

2.2.19. Résidus et dualité. Pour montrer que

$$\dim_k \frac{R}{R(D)+F} = \dim_k \Omega_X(D) = l(K-D)$$

on construit un accouplement parfait entre $\Omega_X(D)$ et $\dfrac{R}{R(D)+F}$ à l'aide des *résidus*. Pour tout $P \in X$ et $\omega \in \Omega_X$ écrivons $\omega = f\,dt$ où $t = t_p$ une uniformisante locale en P, qui définit un isomorphisme

$$\hat{F}_P \xrightarrow{\sim} k((T)) \quad \text{pour} \quad \text{lequel} \quad t \mapsto T.$$

Soit $f \mapsto \sum_{n \gg -\infty} a_n T^n$ par cet isomorphisme, alors a_{-1} s'appel le *résidu* de ω en P, la notation traditionnelle est: $a_{-1} = \mathrm{Res}_P \omega$.

Proposition. (a) *La définition ne dépend pas du choix de l'uniformisante locale t en P;*
(b)$\forall \omega \in \Omega_X$ *on a* $\sum_{P \in X} \mathrm{Res}_P \omega = 0$.

Preuve est impliquée par l'observation $\mathrm{Res}_P \omega = \frac{1}{2\pi i} \oint_P w$ et par la formule de Stokes.

Construction de l'accouplement entre $\Omega_X(D)$ et $\dfrac{R}{R(D)+F}$. Pour $\forall \omega \in W_X$ et $r = (r_P) \in R$ on pose

$$\langle \omega, r \rangle = \sum_{P \in X} \mathrm{Res}_P (r_P \omega).$$

Alors on vérifie immédiatment les propriété naturelles suivantes:

(a) $\langle \omega, r \rangle = 0$ pour tout $r \in F$ (c'est l'affirmation (b) de la Proposition précédente);
(b) $\langle \omega, r \rangle = 0$ si $r \in R(D)$ et $\omega \in \Omega(D)$ (dans ce cas $r \in R(D)$ et $\omega \in \Omega(D)$ implique que $\omega r_P \in \Omega_P$);
(c) $\forall f \in F$ on a $\langle f\omega, r \rangle = \langle \omega, fr \rangle$ (F–linéarité).

Soit $\check{R}$ le dual de R (comme espace vectoriel sur k). On définit une application k–linéaire $\theta : \Omega_X \to \check{R}$ par la formule: $\langle \omega, \cdot \rangle$, $\theta(\omega)(r) = \langle \omega, r \rangle$ pour tout $\omega \in \Omega_X$ et $r \in R$.

Soit $J(D)$ désigne le k–espace dual de $\frac{R}{R(D)+F}$.

2.2.19. Théorème (déscripton du module de différentielles). *Pour tout D l'application θ définit un isomorphisme*

$$\theta : \Omega(D) \xrightarrow{\sim} J(D).$$

Preuve est basée sur deux lemmes suivants

2.2.20. Lemme. *Si $\theta(\omega) \in J(D)$ on a $\omega \in \Omega(D)$*

Sinon, $\exists P$ tel que $v_P(w) < v_P(D)$, et pour $n = v_P(\omega) + 1$ on a alors $n \le v_P(D)$. On définit $r = (r_Q)_{Q \in X}$ par

$$r_Q = \begin{cases} 0, & \text{si } Q \neq P \\ \dfrac{1}{t^n} & t \text{ étant une uniformisante locale en } P,\ Q = P. \end{cases}$$

On a

$$v_P(r_P \omega) = -1 \Longrightarrow \mathrm{Res}_P(r_P \omega) \neq 0, \text{ et } \langle \omega, r \rangle \neq 0$$

(contradiction)

Ce lemme implique directement l'injectivité de θ: si $\theta(\omega) = 0$, on a $\omega \in \Omega(D)$ pour tout $D \Longrightarrow \omega \equiv 0$

Pour montrer surjectivité on utilise le k–espace vectoriel

$$J = \varinjlim_{D} J(D) \subset \check{R}$$

formé par les formes linéaires sur R, qui s'annules sur un des sous espaces de type $R(D) + F$. Il y a une structure naturelle d'un F–espace vectoriel sur J définit par la formule $(fl)(r) = l(fr)$, avec $f \in F$, $r \in R$, $l : R \to k$, $l \in J$.

Alors le lemme précédant montre aussi que θ défini une application F–linéaire de Ω_X dans J. On sait que $\dim_F \Omega_X = 1$, et pour montrer la surjectivité on utlise

2.2.21. Lemme. $\dim_F J \leq 1$.

Sinon, il existent deux $\alpha, \alpha' \in J(D) \subset J$ linéairement indépendant sur F, donc l'application

$$(f, g) \mapsto f\alpha + g\alpha', \quad \mathcal{L}(\Delta_n) + \mathcal{L}(\Delta_n) \to J(D - \Delta_n)$$

doit être injective, où $\Delta_n = nP$. Par consequance,

$$\dim_k J(D - \Delta_n) \geq 2 \dim_k \mathcal{L}(\Delta_n)$$

Mais cette inégalité contradicte à la forme préliminaire du théorème de Riemann–Roch: d'une part,

$$\dim_k J(D - \Delta_n) = l(D - \Delta_n) - d(D - \Delta_n) + g - 1 = n + (g - 1 - d(D)) + l(D - \Delta_n),$$

donc pour $n \gg 0$ on a $d(D-\Delta_n) < 0$ et $l(D-\Delta_n) = 0$; d'autre part, $l(\Delta_n) \geq n+1-g = d(\Delta_n) + 1 - g$, et on obtient une contradiction pour $n \gg 0$.

2.2.22. Théorème de Riemann–Roch sur un corps arbitraire. Soit X un courbe algébrique projective et lisse sur un corps arbitraire k (pas necessairement algébriquement clos). Alors on peut généraliser le théorème de Riemann–Roch pour X, mais pour cela il faut modifier la notion du degré d'un diviseur $D = \sum_P n_P P$, où P parcourt les points de $k(X)$ (les valuations nomalisées de $k(X)$ triviales sur k). Un point P est dit k–rationnelle si $d_P = 1$, i.e. $P \in X(k)$ (il a donnée par ces coordonnées qui appartiennent à k). L'égalité $d_P = d$ signifie que les coordonnées de P appartiennent à une extension de degré d de k. On désigne par $d_P = \dim_k \mathcal{O}_P/\mathfrak{m}_P$ le degré du point P ($\mathcal{O}_P$ étant l'anneau de valuation, $\mathfrak{m}_P$ son idéale maximale). On pose $d(D) = d(\sum_P n_P P) = \sum_P n_P d_P$, $l(D) = \dim_k \mathcal{L}(D)$, $\mathcal{L}(D) = \{f \in k(X) \mid \forall P \;\; v_P(f) \geq -v_P(D)\}$.

Théorème de Riemann–Roch sur k. (a) *Il existe un nombre entier g tels que pour tout diviseur D on a*

$$l(D) = d(A) + 1 - g + l(K - D);$$

(b) *le nombre g coïncide avec $l(K) = \dim_k \Omega_X(0) = \dim_k \Omega[X]$ où $\dim_k \Omega_X(0) = \dim_k \Omega[X]$ la dimension du k-espace vectoriel des différentielles algébriques holomorphes sur X (on pose $D = 0$ dans (a)).*

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 la fémeture compacte 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 homéomorphisme $\varphi : U \to \Gamma_v\backslash U$.

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 homéomorphisme 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 homéomorphisme 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*

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

Démonstration est facilement impliquée par le fait $d(f^*(\omega)) = 2g' - 2$, $d((\omega)) = 2g - 2$, où ω une différentielle non nulle sur X.

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 $J(z) = \dfrac{1728E_4^3}{E_4^3 - E_6^2}$. On voit donc que $g(X_{\Gamma(1)}) = 0$.

En utilisant la description de la ramification ci–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 $e_1, \dots, e_t$ 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 $\mu = e_1 + \dots e_t$ ou $e_3 = 1$ ou 3. Le nombre d'indices k avec $e_k = 1$ est égale 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 conjugué 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 conjugué avec 1_2 modulo N. Le fait que $\Gamma(N)$ est distingué 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 ci-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 on désigne par S_1 (par S_2) le nombre d'éléments elliptiques de $\Gamma(1)$ congrus à $\tau=\begin{pmatrix} 0 & -1 \\ 1 & -1\end{pmatrix}$ (resp. à τ^2). Nous allons vérifier que ν_3 coïncide avec le nombre d'idéaux J de l'anneau $A=\mathbf{Z}[j]$ qui satisfont aux propriétés i) ii) ci–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 l'union disjointe 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 $\Gamma_0(N)$ ci-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 conjugaison des éléments elliptiques σ dans $\Gamma_0(N)$ et des idéaux J aves les propriétés i), ii) ci–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 points paraboliques non–équivaux 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 (respectivement).

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 ci-dessus on va déterminer maintenant les dimensions des espaces des formes modulaires pour les sous–groupes de congruence.

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

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

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

En effet, pour $f \in \mathcal{M}_2(\Gamma)$ la différentielle $f(z)\,dz$ est invariant par rapport á Γ et $dz = \frac{1}{2\pi i}\frac{dq}{q}$. Ceci implique que la différentielle $f(z)\,dz$ 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 de la différentielle $f(z)\,dz$ doit être égale à 0 par un théorème classique sur les surfaces de Riemann compactes. Cette différentielle n'a que des pôles simples au points. Cela nous donne la formule

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

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

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

sur l'espace complexe $\Omega^1(X_\Gamma)$ des différentielles méromorphes sur X_Γ.

D'un autre côté, pour $k = 2n$ on a

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

où $\Omega^n(X_\Gamma)$ désigne l'espace complexe des différentielles 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 ci-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 régulier si $\rho\Gamma\rho^{-1}$ est engendré par la matrice $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, et on appelle P non-régilier si $-1 \notin \Gamma$ et le groupe $\rho\Gamma\rho^{-1}$ est engendré par la matrice $-\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. 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 $q_h = \exp(2\pi i z/h)$, Ψ, Φ certaines fonctions méromorphes au voisinage de l'origine. Posons

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

Soit $\mathrm{Div}_{\mathbf{Q}}(X_\Gamma) = \mathrm{Div}(X_\Gamma) \otimes \mathbf{Q}$ 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 définition que

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

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

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

et

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

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 ci-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 ci-dessus. Alors $t = q_h = \exp(2\pi i z/h)$ est le paramètre local ci-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 $dt/dz = \dfrac{h}{2\pi i} t$ alors $\nu_Q(dz/dt) = -1$.

Il est commode a écrire formellement:

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

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

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

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 importante:

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

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

est invariant par rapport à l'action de $\mathrm{SL}_2(\mathbf{R})$, *et elle definit une mésure* $\mathrm{SL}_2(\mathbf{R})$*–invariante* m *sur* H. *Pour la mésure 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 $B = \mathrm{div} F_0$. On écrit 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

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

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

Ici

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

Pour un $A = \sum_{P \in X_\Gamma} c_P \cdot P \in \operatorname{Div}_{\mathbf{Q}}(X_\Gamma)$ posons $[A] = \sum_{P \in X_\Gamma} [c_P] \cdot P$ (la partie entière de A).

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

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

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, $e_1, ..., e_r$ 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*

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

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*

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

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*

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

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

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

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

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 considérés 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

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

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

2.4.8. Exemple. Soit $N = 2, 3, 5, 11$ et $k = 24/(N+1)$. Alors $\mathcal{S}_k(\Gamma_0)$ 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 est 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 est holomorphe sur $X_{\Gamma_0(N)}$ (y compris les points 0 et ∞).

10 janvier 1995.

Courbes elliptiques. Théorème d'Abel. Groupe de classes de diviseurs. Lois d'addition et la méthode de sécantes et tangentes.

Chapitre 3. Courbes elliptiques et formes modulaires algébriques.

3.1.0. Généralités. On va commencer par des généralités sur les courbes elliptiques sur un corps arbitraire k (pas necessairement algébriquement clos).

Définition. Une courbe projective et lisse X est dit *elliptique* s'il existe un point k–rationel $o \in X(k)$ et si $g = g(X) = 1$.

Pour étudier telles courbes on utilise le théorème de Riemann–Roch sur k qui implique que pour une courbe de genre 1 on a

$$\forall D \quad d(D) > 0 = 2g - 2 \Longrightarrow l(D) = d(D).$$

Soit Cl_X^0 le groupe de classes de diviseurs k–rationels de degré zéro.

3.1.1. Théorème d'Abel. *Soit C_P désigne la classe de $(P) - (o)$ dans Cl_X^0. Alors l'application $X(k) \xrightarrow{\sim} Cl_X^0$ définie par $P \mapsto C_P$ est une bijection.*

Démonstration. Injectivité: on ecrit $D_1 \sim D_2$ s'il existe $f \in k(X)$ telle que $(f) = D_1 - D_2$. Supposons que $(P) - (o) \sim (Q) - (o) \Longleftrightarrow (P) \sim (Q)$; il faut montrer que $P = Q$. Sinon, il existe $f \in k(X)$ telle que $(f) = (P) - (Q)$, $(f)_0 = P$, $(f)_\infty = Q$, $[k(X) : k(f)] = 1 = d((f)_0)$, et $X \xrightarrow{\sim} \mathbf{P}_k^1$ ce que contradit au fait $g(\mathbf{P}_k^1) = 0$.
Surjectivité. On remarque tout d'abord que pour tout P, $Q \in X(k)$ il existe un seul $R \in X(k)$ tel que $(P)+(Q) \sim (R)+(o)$ (i.e. $C_P + C_Q = C_R$ dans le groupe Cl_X^0. En effet $l((P) + (Q) - (o)) = 1$, donc il existe $f \in k(X)$ avec $(f) = n_P(P) + n_Q(Q) + n_o(o) + \ldots$, où $n_P \geq -1$, $n_Q \geq -1$, $n_o \geq 1$, et tous les autres coefficients non–negatifs. Le fait $d((f)) = 0$ implique que soit $(f) = -(P) - (Q) + 2(o)$, soit il existe un $R \neq o$ tel que $(f) = -(P) - (Q) + (o) + (R)$ (on exclut la possibilité $(f) = -(P) + (o)$ par le même argument ci–dessus).

Soit $D \geq 0$, alors le raisonement par recurrence évident montre qu'il existe un seul $R \in X(k)$ tel que $D \sim m(o) + R$ (on commence par $D = (P) + (Q)$, et on écrit généralement $D = D' + (P)$, $D' \sim (m-1)(o) + R'$, $(P) + (R') \sim (o) + (R)$.

Maintement pour tout D de degré zéro on a $D = D_1 - D_2$, D_1, $D_2 > 0$, $D_1 \sim m(o) + (P_1)$, $D_2 \sim m(o) + (P_2)$, donc $D \sim (P_1) - (P_2) \sim (R) - (o)$, i.e. la classe de D coïncide avec C_R, d'où la surjectivité.

3.1.2. Cubique planaire projective. Rappelons qu'une courbe projective planaire $\mathcal{C}$ est définit par une équation de type $F(X : Y : Z) = 0$, où $F(X : Y : Z)$ est une forme homogène des variables projectives X, Y, Z. On dit que $\mathcal{C}$ est lisse si le système

$$F = F'_X = F'_Y = F'_Z = 0$$

n'a pas de solutions non–triviales dans sur $\overline{k}$.

On sait qu'une courbe elliptique $\mathcal{C}$ possède une seule différentielle ω à une constante multiplicative près car $l(K) = 1$, où K désigne la classe canonique. Le théorème précédent permet de montrer que i) $\mathcal{C}$ est une groupe algébrique; ii) $\mathcal{C}$ est isomorphe à une cubique planaire.

Théorème. (a) *Toute courbe $\mathcal{C}$ de genre 1 avec $o \in \mathcal{C}(k)$ est isomorphe à une cubique planaire*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où par l'équation homogène correspondante

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_5Z^3,\ o = (0:1:0),$$

(b) *Si $Car(k) \neq 2,3$, on peut définir $\mathcal{C}$ par une équation affine de type*

$$y^2 = x^3 + ax + b,$$

où par l'équation homogène correspondante

$$Y^2Z = X^3 + aXZ^2 + bZ^3,\ o = (0:1:0).$$

.

Preuve (voir [Appendix de J.Tate dans S. Lang, "Elliptic functions"]). Il existe $x \in \mathcal{L}(2o)$ non-constante. Alors x a un pôle d'ordre 2 en o, car les élément de $\mathcal{L}(o) \subset \mathcal{L}(2o)$ sont les constantes. Puis, $l(3o) = 3$, donc il existe une fonction $y \in \mathcal{L}(3o)$ avec un pôle d'ordre 3 en o. Soit t une uniformisante locale en o. On choisie ω, x et y de telle façon que

$$\omega = dt + \ldots = dt(1 + \mathcal{O}(t)),\quad x = t^{-2} + \ldots = t^{-2}(1 + \mathcal{O}(t)),\quad y = -t^{-3}(1 + \mathcal{O}(t)).$$

Alors

$$\mathcal{L}(o) = \langle 1 \rangle,\quad \mathcal{L}(2o) = \langle 1, x \rangle,\quad \mathcal{L}(3o) = \langle 1, x, y \rangle,\quad \mathcal{L}(5o) = \langle 1, x, y, xy, x^2 \rangle,$$

et $x^3 - y^2 \in \mathcal{L}(5o)$, d'où on obtient l'équation affine ci–dessus. Sa completion projective est une modèle projective lisse de $\mathcal{C}$. La lissité est facile à montrer par l'absurd: sinon la projection de centre en un point singulier nous donne une fonction $\mathcal{C} \to \mathbf{P}^1_k$ de degré 1, mais ls courbe $\mathcal{C}$ n'est pas rationelle.

Si $Car(k) \neq 2$, on utilise la substitution

$$y \mapsto y + \frac{a_1}{2} \quad x + \frac{a_3}{2}$$

pour éliminer les coefficients a_1, a_3. Si de plus $Car(k) \neq 3$, on utilise la substitution $x \mapsto x + \frac{a_2}{3}$ pour éliminer le coefficients a_2. Ceci résulte que dans le cas $Car(k) \neq 2, 3$ on peut amener l'equation de la courbe à la forme

$$y^2 = x^3 + ax + b \quad (a, b \in k).$$

On vérifie que cette courbe est lisse ssi le polynôme cubique à droite n'a pas de racines multiplies (directement par la définiton des points singuliers comme des solutions de l'équation $F = F_X = F_Y = F_Z$ où dans le cas générale $F(X,Y,Z) = Y^2 + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$).

La différentielle holomorphe est donnée par

$$\omega = \frac{dx}{2y + a_1 + a_3} = \frac{dx}{\Phi'_y} = -\frac{dy}{\Phi'_x} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

où $\Phi(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$ l'èquation affine de la courbe $\mathcal{C}$. En effet, grâce à l'équaton $\Phi(x, y) = 0$ on a sur $\mathcal{C}$

$$\Phi'_x \, dx + \Phi'_y \, dy = 0,$$

et Φ, Φ'_x, Φ'_y ne s'annulent pas en même temps. La forme de Weierstrass de $\mathcal{C}$ est

$$y^2 = 4x^3 - g_2x - g_3.$$

Le *discriminant*

$$\Delta = g_2^3 - 27g_3^2$$

ne s'annule pas (on a $\Delta = 2^{-4}(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$, où $4x^3 - g_2x - g_3 = 4(x - x_1)(x - x_2)(x - x_3)$.

3.1.3. Lois de groupe sur $\mathcal{C}$ est induite par la bijection du théorème d'Abel $X(k) \tilde{\to} Cl^0_X$. Si on amène $\mathcal{C}$ à la forme d'une cubique planaire, on peut décrire la lois d'addition par la "méthode de sécantes et tangentes" de Poincaré: pour trois points différentes $P_i = (x_i, y_i)$ $(i = 1, 2, 3)$

$$\begin{aligned} &P_1 + P_2 + P_3 = o \Longleftrightarrow ((P_1) - (o)) + ((P_2) - (o)) + ((P_3) - (o)) \sim 0 \\ &\Longleftrightarrow (P_1) + (P_2) + (P_3) - 3(o) \sim 0, \end{aligned}$$

et P_3 est uniquement définit par P_1, P_2.

Soit $h(x, y) = 0$ l'équation de la droite passante par P_1 et P_2, alors il y a un seule troisième point P_3 d'intersection de la droite avec $\mathcal{C}$. On a $(h) = (P_1)+(P_2)+(P_3)-3(o)$, d'où la méthode.

Il est facile á décrire cette méthode par les formules explicites.

Remarques. Si $\mathcal{C}$ est une courbe projective qui est définit par des équation polynomials à coefficients dans k, admettante une structure (algébrique) de groupe et un point rationel $o \in \mathcal{C}(k)$ sur k comme l'élément neutre, alors on peut montrer par les moyens de la géométrie algébrique que: (i) la lois de groupe est unique et commutative; (ii) $\mathcal{C}$ est lisse; (iii) il existe une différentielle holomorphe non–nuls ω sur $\mathcal{C}$ construite à partir du point o à l'aide des décalage de groupe, donc la classe canonique $K_{\mathcal{C}}$ est nulle; ceci implique que $g(\mathcal{C}) = 1$ car $d(K_{\mathcal{C}}) = 2g - 2 = 0$.

17 janvier 1995. Déscription analytique des courbes elliptiques complexes et leurs homomorphismes. Théorème d'addition. Théorème de Jacobi (déscription du réseau correspondant à une différentielle non nulle. Classes d'isomorphisme des courbes elliptiques. l'invariant modulaire.

3.1.4. Equation de Weierstrass et théorème d'addition. La forme de Weierstrass paraît dans la théorie de l'uniformisation complexe des courbes elliptiques. Considérons un tore complexe de type $\mathbf{C}/\Lambda$, où $\Lambda = \langle\omega_1, \omega_2\rangle$ 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 à voir que les développements de Laurent de $\wp(u)$ et de $\wp'(u)$ sont

$$\wp(u) = u^{-2} + \sum_{n=2}^{\infty} (2n-1) G_{2n}(\Lambda) u^{2n-2} = u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6)$$
$$\wp'(u) = -2u^{-3} + \sum_{n=2}^{\infty} (2n-1)(2n-2) G_{2n}(\Lambda) u^{2n-3}$$
$$= -2u^{-3} + 6G_4 u + 20 G_6 u^3 + \mathcal{O}(u^5)$$

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 Laurent en 0 contient ne que des puissances positives de u:

$$\begin{aligned}
\wp(u) &= u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6), \\
\wp^3(u) &= u^{-6} + 9G_4 u^{-2} + 15G_6 + \mathcal{O}(u^2) \\
\wp'(u) &= -2u^{-3} + 6G_4 u + 20G_6 u^3 + \mathcal{O}(u^5), \\
\wp'^2(u) &= 4u^6 - 24G_4 u^{-2} - 80G_6 + \mathcal{O}(u^2)
\end{aligned}$$

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).

Maintenant on désigne par $E_\Lambda \subset \mathbf{P}^2_{\mathbf{C}}$ la courbe définie par l'equation de Weierstrass avec g_2 et g_3 ci-dessus, et on définit une application

$$\mathbf{C}/\Lambda \overset{\sim}{\to} E_\Lambda(\mathbf{C})$$

par $u \mapsto (\wp(u) : \wp'(u) : 1)$, si u n'est pas dans Λ, et 0 s'applique sur (0:1:0).

L'application définie un isomorphisme complexe analytique . Pour décrire explicitement l'application inverse on peut aussi utiliser la différentielle

$$dx/y = dx/\sqrt{4x^2 - g_2x - g_3}$$

sur $E = E_\Lambda(\mathbf{C})$ et l'intégrer autour un contour qui joint un point initial fixe (disons, o) avec un point varié. L'intégral depends du choix de contour mais l'image dans $\mathbf{C}/\Lambda$ est invariant. Le réseau

$$\Lambda = \left\{ \int_\gamma \omega \;\mid\; \gamma \in H_1(E(\mathbf{C}), \mathbf{Z}) \right\}$$

est définit par le choix de la différentielle; si l'on remplace ω par $u\omega$, $u \in \mathbf{C}$, le réseau Λ ce remplace par le réseau $\Lambda' = u\Lambda$.

L'isomorphisme $\mathbf{C}/\Lambda \tilde{\to} E_\Lambda(\mathbf{C})$ est compatible avec les structures naturelles de groupe. En termes de fonctions elliptiques, ce fait s'exprime comme le *théorème d'addition* des fonction elliptiques:

Théorème. Soit u_1, $u_2 \notin \Lambda$, et $u_1 \pm u_2 \notin \Lambda$, alors

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right)^2.$$

En termes des coordonnées (x, y) on a

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$

où

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = P_1 + P_2 = (x_3, y_3).$$

sl Démonstration du théorème d'addition et basée sur la

Proposition. (a) *Pour une fonction* $0 \neq f \in F_\Lambda$ *avec* $(f) = \sum_{u\in\mathbf{C}/\Lambda} n_u(u)$ *on a* $\sum_{u\in\mathbf{C}/\Lambda} n_u = 0$*;*

(b) *Pour* $0 \neq f \in F_\Lambda$ *avec* $(f) = \sum_{u\in\mathbf{C}/\Lambda} n_u(u)$ *on a* $\sum_{u\in\mathbf{C}/\Lambda} n_u u \equiv 0 (\mathrm{mod}\Lambda)$.

Preuve. La première affirmation exprime le fait $d^\circ(f) = 0$. La deuxième est impliqué par un calcule facile de l'intégrale

$$\int_{\partial\Pi} u\frac{f'(u)}{f(u)}du = 2\pi i \sum_u n_u u,$$

où Π désigne le parallelogramme fondamental de Λ, et $\partial\Pi$ son borne. D'autre part, l'intégrale peut être calculer à l'aide de calcule les intégrales lelong les côtés opposites. Par exemple, un des deux couples de ces intégrales est égale à

$$\int_\alpha^{\alpha+\omega_1} u\frac{f'(u)}{f(u)}du - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} u\frac{f'(u)}{f(u)}du$$
$$- \omega_2 \int_\alpha^{\alpha+\omega_1} u\frac{f'(u)}{f(u)}du = 2\pi i k\omega_2,$$

d'où la Proposition.

Maintenant, pour $u_1, u_2 \in \mathbf{C}/\Lambda$, $u_1 \not\equiv \mathrm{mod}\Lambda$ soit

$$\wp'(u_1) = a\wp(u_1) + b, \quad \wp'(u_2) = a\wp(u_2) + b,$$

i.e. $y = ax + b$ la droite passante à traverse de (x_i, y_i), où $x_i = \wp(u_i)$, $y_i = \wp'(u_i)$, $(i = 1, 2)$. La fonction $\wp(u) - (a\wp(u) + b)$ a exactement trois zéros, comptées avec multiplicités, $u = u_1, u_2, u_3$. On a alors par Proposition $u_1 + u_2 + u_3 \equiv 0(\mathrm{mod}\Lambda)$. On a soit $u_1 = u_3$, $2u_1 + u_2 \equiv 0(\mathrm{mod}\Lambda)$, soit $u_3 \equiv -(u_1 + u_2)(\mathrm{mod}\Lambda)$. Ceci implique que le polynôme $4x^3 - g_2 - g_3 - (ax + b)^2$ a trois racines $x_i = \wp(u_i)$, $(i = 1, 2, 3)$, i.e. $4x^3 - g_2 - g_3 - (ax + b)^2 = 4(x - \wp(u_1))(x - \wp(u_2))(x - \wp(u_3))$. Car $a(\wp(u_1) - \wp(u_2)) = \wp'(u_1) - \wp'(u_2)$, on a

$$\wp(u_1) + \wp(u_2) + \wp(u_3) = \frac{a^2}{4}$$

(coefficient de x^2), d'où

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right)^2,$$

et si $u_1 = u_2 = u$, on a

$$\wp(2u) = -2\wp(u) + \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2.$$

(passage à la limite).

3.1.5. Homomorphismes et classification des courbes elliptiques

Soit $E \xrightarrow{\sim} \mathbf{C}/\Lambda$, $E' \xrightarrow{\sim} \mathbf{C}/\Lambda'$, alors un homomorphisme complexe analytique $\mathbf{C}/\Lambda \xrightarrow{\lambda} \mathbf{C}/\Lambda'$ a la forme $u \mapsto \alpha u$ pour un $\alpha \in \mathbf{C}$. En effet, dans un voisinage de 0 on a $\lambda(u) = a_0 + a_1 u + a_2 u^2 + \ldots$, et $\lambda(u_1 + u_2) = \lambda(u_1) + \lambda(u_2)$, d'où $\lambda(u) = a_1 u$, et $\alpha = a_1$. Pour tout $u \in \mathbf{C}$ il existe un $N \in \mathbf{N}$ tel que u/N est dans le voisinage ci-dessus, et $\lambda(u/N) = \alpha u/N$, donc on a de nouveau $\lambda(u) = \alpha u$.

Ceci implique que

$$\mathrm{Hom}(E, E') = \mathrm{Hom}(\mathbf{C}/\Lambda, \mathbf{C}/\Lambda') = \{\mu \in \mathbf{C} \mid \mu\Lambda \subset \Lambda'\},$$

$$\mathrm{End}(E) = \mathrm{Hom}(\mathbf{C}/\Lambda, \mathbf{C}/\Lambda) = \{\mu \in \mathbf{C} \mid \mu\Lambda \subset \Lambda\},$$

et on pose

$$\mathrm{End}_{\mathbf{Q}}(E) = \mathrm{End}(E) \otimes \mathbf{Q} = \{\mu \in \mathbf{C} \mid \mu(\mathbf{Q}\Lambda) \subset \mathbf{Q}\Lambda\}.$$

On voit de cette description que les coefficients g_2 et g_3 sont définis aux replacements $g_2 \mapsto \mu^4 g_2, g_3 \mapsto \mu^6 g_3 (\mu \in k)$ près. *L'invariant modulaire* J_E de la courbe E est définit par $J_E = 1728 j_E = (12)^3 j_E$, où

$$j = \frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{g_2^3}{\Delta}.$$

Deux courbes ont le même invariant ssi ils devient isomorphes sur une clôture algébrique de k (en effet, elles sont isomorphes sur une extension de degré 6 de k). Ce reśultat reste valable sur n'importe quel corps k de $Car(k) \neq 2, 3$; plus precisement,

3.1.6. Théorème. (a) *Soient* $E : y^2 = 4x^3 - g_2x - g_3$, $E' : y^2 = 4x^3 - g_2'x - g_3'$ *deux courbes elliptiques sous la forme de Weierstrass, qui sont isomorphes sur* k, *et* $\lambda : E \to E'$ *un tel isomorphisme. Alors il existe* $\mu \in k$ *tel que* $g_2' = \mu^4 g_2, g_3' = \mu^6 g_3$, $\lambda(x, y) = (\mu^2 x, \mu^3 y)$.
(b) $\forall j \in k$ *il existe* E *telle que* $j_E = j$.

Preuve de (a) utilise le théorème de Riemann–Roch. Pour les différentielles ω, ω' de E et de E', et pour coordonnées (x, y) de E' considérons le composées $x \circ \lambda = \lambda^* x$, $y \circ \lambda = \lambda^* y$, $\omega' \circ \lambda = \lambda^* \omega'$. Alors il existe un $\mu \in k$ tel que $\lambda^* \omega' = \mu w$, et

$$\lambda^* x = \mu^2 x + r, \quad \lambda^* y = \mu^3 y + s\mu^2 x + t, \quad r, s, t \in k.$$

On a les relation $y^2 = 4x^3 - g_2'x - g_3'$,

$$(\mu^3 y + s\mu^2 x + t)^2 = 4(\mu^2 x + r)^3 - g_2(\mu^2 x + r) - g_3,$$

qui impliquent $r = s = t = 0$ et (a).

Pour montrer (b) on remarque tout d'abord qu'on obtient $j_E = 0$ si l'on prend $g_2 = 0$, i.e. $E : y^2 = 4x^3 - 1$, et on obtient $j_E = 0$ si l'on prend $g_2 = 1$, $E : y^2 = 4x^3 - x$. Dans le cas général on cherche E sous la forme $E : y^2 = 4x^3 - gx - g$ avec $j = g/(g - 27)$.

3.1.7. Théorème. *Pour tous nombres complexes* r, s *avec* $r^3 - 27s^2 \neq 0$ *il existe un réseau* Λ *tel que* $g_2(\Lambda) = r$, $g_3(\Lambda) = s$.

Preuve est basée sur

3.1.8. Lemme. *La fonction*

$$j(z) = j(\Lambda_z) = \frac{g_2^3(z)}{g_2^3(z) - 27g_3^2(z)}$$

prends toutes les valeurs complexes strictement une fois.

Démonstration du lemme (voir aussi 2.1.5) est impliquée par le fait que $j(z)$ est une fonction modulaire sur $\Gamma = \Gamma(1) = \mathrm{SL}(2, \mathbf{Z})$, i.e. une forme modulaire méromorphe de poids 0, qui provient isomorphismes $j : \Gamma\backslash H \xrightarrow{\sim} \mathbf{C}$, $j : \overline{\Gamma\backslash H} \xrightarrow{\sim} \overline{\mathbf{C}}$. En effet, pour tout $a \in \mathbf{C}$ la fonction $f(z) = j(z) - a$ est aussi une fonction modulaire sur Γ, et on a vu l'egalité

$$\frac{1}{2}\mathrm{ord}_{z=i}(f) + \frac{1}{3}\mathrm{ord}_{z=\rho}(f) + \sum_{\substack{P \in \Gamma\backslash H \\ P \neq i, \rho}} \mathrm{ord}_{z=P}(f) - 1 = 0,$$

car $\mathrm{ord}_{z=\infty}(f) = -1$. Ceci implique que f a une seule racine, notamment, soit $z = i$ avec multiplicité 2 (pour $a = 0$), soit $z = \rho$ avec multiplicité 3 (pour $a = 1$), soit $z = P \in H$, $P \neq i, \rho$.

Maintenant considérons la courbe elliptique $\mathcal{C} : y^2 = 4x^3 - rx - s$ avec l'invariant $j = r^3/(r^3 - 27s^2)$ et le lemme implique qu'il existe un réseau Λ' tel que $j(\Lambda') = j$. Si $\mathcal{C}' : y^2 = 4x^3 - g_2(\Lambda') - g_3(\Lambda')$ la courbe de Weierstrass correspondante à Λ', $j(\mathcal{C}') =$

$j(\Lambda') = j$, et $\mathcal{C} \xrightarrow{\sim} \mathcal{C}'$. Le théorème precédent nous dit qu'il existe u $\mu \in \mathbf{C}^\times$ tel que $r = \mu^4 g_2(\Lambda')$, $s = \mu^6 g_3(\Lambda')$, et $\Lambda = \mu\Lambda'$ est le réseau cherché.

Définition. *Un $\lambda \in \mathrm{Hom}(E, E')$ s'appel isogénie si une des conditions équivalentes est satisfaite:*
(i) $\lambda \neq 0$*; (ii)* $\mathrm{Ker}\,\lambda$ *est fini; (ii)* λ *est surjective.*

3.1.9. Théorème. *Soit $E \xrightarrow{\sim} \mathbf{C}/\Lambda$, $E' \xrightarrow{\sim} \mathbf{C}/\Lambda'$. On choisie des bases $\{\omega_1, \omega_2\}$ de Λ et $\{\omega_1', \omega_2'\}$ de Λ' de telle façon que $z = \omega_1/\omega_2 \in H$, $z' = \omega_1'/\omega_2' \in H$. Alors E et E' sont isomorphes (resp. isogènes) ssi $\exists g \in \mathrm{SL}_2(\mathbf{Z})$ (resp. $\exists g \in \mathrm{GL}_2^+(\mathbf{Q})$ tel que $z = g(z')$).*

Preuve. Si E et E' sont isomorphes (resp. isogènes), on a $\mu\Lambda \subset \Lambda'$, et $\mu\Lambda = \Lambda'$ (resp. $\mu(\mathbf{Q}\Lambda) = \mathbf{Q}\Lambda'$) pour un $\mu \in \mathbf{C}^\times$. Posons $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où

$$\mu\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix},$$

d'où $z = g(z')$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\det g > 0$ et $g \in \mathrm{SL}_2(\mathbf{Z})$ (resp. $\exists g \in \mathrm{GL}_2^+(\mathbf{Q})$, $z = g(z')$).

Réciproquement, si $g(z') = z$, $g \in \mathrm{SL}_2(\mathbf{Z})$ (resp. $\exists g \in \mathrm{GL}_2^+(\mathbf{Q})$, $z = g(z')$), posons $\alpha = cz' + d$, alors

$$\alpha\begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z' \\ 1 \end{pmatrix},$$

ou

$$(\alpha\omega_1'/\omega_2)\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

3.1.10. Endomorphismes et automorphismes.

Définition. Une courbe elliptique E est dit à multiplication complexe si $\mathrm{End}(E) \neq \mathbf{Z}$.

Le théorème précedent nous montre que E_z est à multiplication complexe ssi $\gamma(z) = z$ pour une $\gamma \in \mathrm{GL}^+(\mathbf{Q})$ non–scalaire $\iff$ $\mathbf{Q}(z)$ est une extension quadratique imaginaire de $\mathbf{Q}$.

Exemples. (a) Soit $j = 0$, $\Lambda = \langle i \rangle 1$,, alors E_Λ est à multiplication complexe par $\mathbf{Q}(i)$; (b) Soit $j = 1$, $\Lambda = \langle \rho \rangle 1$,, alors E_Λ est à multiplication complexe par $\mathbf{Q}(\rho)$.

3.1.11. Liaison avec formes modulaires. Deux courbes E_z, $E_{z'}$ sont isomorphes ssi $z' = \frac{az+b}{cz+d}$ pour une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$. En effet, on a vu qu'un isomorphisme complex analytique $\mathbf{C}/\Lambda \xrightarrow{\sim} \mathbf{C}/\Lambda'$ est necessairement induit par la multiplication par un $\alpha \in \mathbf{C}^\times$. Dans ce cas $\Lambda_z = \alpha\Lambda_{z'}$, et $(\alpha, \alpha z')$ est une base de Λ_z, puis $\alpha = cz + d, \alpha z' = az + b$, avec une transformation unimodulaire: $(1, z'), (\alpha, \alpha z')$, et $(1, z)$ definis la même orientation de $\mathbf{C}$. On a alors

$$g_2(z') = \alpha^4 g_2(z), \quad g_3(z') = \alpha^6 g_3(z).$$

A savoir, les classes d'isomorphisme des courbes elliptiques sur $\mathbf{C}$ correspondent bijectivement aux points de l'espace quotient $\Gamma\backslash H$, où H le demi–plan superieur

$$H = \{z \in \mathbf{C} | \mathrm{Im}\,(z) > 0\},$$

et $\Gamma = SL(2,\mathbf{Z})$ opère sur H comme ci–dessus. Selon le théorème classique de Jacobi, le discriminant $\Delta = \Delta(z)$ de E_z peut s'exprime comme

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

pour tout $z \in \mathbf{C}$ with $Im(\tau) > 0, q = \exp(2\pi i \tau)$. La fonction $\tau(n)$ est *la fonction de Ramanujan*. L'invariant absolu de E_z est par définition

$$J(z) = 1728 g_2(z)^3/\Delta(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n) q^n,$$

où $c(1) = 196884$, $c(2) = 21493760, \ldots, c(n) \in \mathbf{Z}$. On a vue que J prends toutes les valeurs complexes, donc toute courbe elliptique sur $\mathbf{C}$ est isomorphe à E_z pour un $z \in \mathbf{C}$.

Topologiquement, $\mathbf{C}/\Lambda$ est une surface de Riemann de rang 1. S'il on remplace z par $\gamma(z)$ avec $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ alors le réseau $\Lambda_z = \mathbf{Z} + z\mathbf{Z}$ se remplace par le réseau

$$\Lambda_{\gamma(z)} = \mathbf{Z} + \gamma(z)\mathbf{Z} = (cz+d)^{-1}(\mathbf{Z} + z\mathbf{Z}) = (cz+d)^{-1}\Lambda_z,$$

et la courbe correspondante se remplace par la courbe de Weierstrass

$$g_2(\gamma(z)) = (cz+d)^4 g_2(z), \quad g_3(\gamma(z)) = (cz+d)^6 g_3(z).$$

Le discriminant du polynôme cubique de la partie droite dans l'équation de Weierstrass est une forme parabolique de poids 12 par rapport à $\Gamma = \mathrm{SL}_2(\mathbf{Z})$:

$$2^{-4}(g_2^3 - 27g_3^2) = 2^{-4}(2\pi)^{12} e(z) \prod_{m=1}^{\infty} (1-e(mz))^{24} = 2^{-4}(2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e(nz).$$

La fonction

$$J(z) = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n$$

est invariante par $\Gamma = \mathrm{SL}_2(\mathbf{Z})$, i.e. c'est une fonction modulaire (forme modulaire meromorphe de poids 0). On a $\mathrm{ord}_{q=0} J = -1$.

3.1.12. Points d'ordre fini et isogénies de courbes elliptiques complexes. L'uniformisation complexe d'une courbe elliptique E sur $\mathbf{C}$, $\mathbf{C}/\Lambda \xrightarrow{\sim} E(\mathbf{C})$ montre que le groupe E_N des points annulés par N sur $E(\mathbf{C})$ est isomorphe à

$$(\mathbf{Z}/N\mathbf{Z}) \times (\mathbf{Z}/N\mathbf{Z}) = \left\{ \left(\frac{a\omega_1 + b\omega_2}{N}, \frac{c\omega_1 + d\omega_2}{N}\right) \mid a,b,c,d \in \mathbf{Z}/N\mathbf{Z} \right\}.$$

On va écrire E sous la forme de Weierstrass: $E : y^2 = 4x^3 - g_2 x - g_3$

Exemple. Soit $N = 2$, alors

$$\wp'(\omega_1/2) = \wp'((\omega_1+\omega_2)/2) = \wp'(\omega_2/2) = 0,$$

et les points d'ordre 2 sur E sont $(x,y) = (\wp(\omega_1/2), 0)$, $(\wp((\omega_1+\omega_2)/2), 0)$, $(\wp(\omega_2/2), 0)$.

Par définition,

$$P \in E(\mathbf{C}) \Longleftrightarrow \exists f \in \mathbf{C}(E) \text{ avec } (f) = N((P) - (o)).$$

On a $E_N = \mathrm{Ker}\,(E(\mathbf{C}) \stackrel{N\delta}{\to} E(\mathbf{C}))$, où $N\delta$ le morphisme de multiplication par N sur E, δ le morphisme identique. Formules pour la lois d'adition nous montrent que dans les coordonnées homogènes

$$N\delta((X:Y:Z)) = (X_N(X:Y:Z) : Y_N(X:Y:Z) : Z_N(X:Y:Z))$$

avec des polynômes $X_N(X:Y:Z)$, $Y_N(X:Y:Z)$, $Z_N(X:Y:Z)$ à coefficients dans $k = \mathbf{Q}(g_2, g_3)$. Ceci implique que

$$P = (X:Y:Z) \in E(\mathbf{C}) \Longleftrightarrow X_N(X:Y:Z) = 0, \quad Z_N(X:Y:Z) = 0,$$

et pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/k)$ on a $P^\sigma = P$. Pour trouver les coordonnées des points d'ordre fini, on va construire un polynôme F_N dont les racines coïncident avec les x–coordonnées des points d'ordre N.

Cas I. Soit N impaire. Alors $x \neq \wp(\omega_1)$, $\wp(\omega_2)$, $\wp((\omega_1 + \omega_2)/2)$. Soit

$$f_N(z) = N \prod (\wp(z) - \wp(u)),$$

où u parcourt tous les $u \in \mathbf{C}/\Lambda$ non nuls tels que $Nu \in \Lambda$, et on choisit un seul élément dans chaque couple u, $-u$. Alors $f_N(z) = F_N(\wp(z))$, où $F_N(x) \in \mathbf{C}[x]$ un polynôme de degré $(N^2-1)/2$. La fanction f_N est paire, elle a $N^2 - 1$ zéros simples, et un seul pôle en $z = 0$ d'ordre $N^2 - 1$, avec le terme principal N/z^{N^2-1} en $z = 0$.

Cas II. Soit N paire. Considŕons le produit $\tilde{f}_N(z) = N \prod (\wp(z) - \wp(u))$ étendu sur tous les $u \in \mathbf{C}/\Lambda$ non nuls tels que $Nu \in \Lambda$ mais $2u \not\subset \Lambda$, i.e. $u \neq \omega_1$, ω_2, $(\omega_1 + \omega_2)/2$. Alors $\tilde{f}_N = F_N(\wp(z))$, où $F_N(x) \in \mathbf{C}[x]$ un polynôme de degré $(N^2 - 4)/2$. La fanction $\tilde{f}_N$ est paire, elle a $N^2 - 4$ zéros simples, et un seul pôle en $z = 0$ d'ordre $N^2 - 4$, avec le terme principal N/z^{N^2-4} en $z = 0$. Il est claire que les racines du polynôme F_N sont permutées par tout $\sigma \in \mathrm{Aut}(\mathbf{C}/k)$, alors ces coefficients sont dans k.

3.1.13. Représentations galoisiennes associées à E. Si P, $Q \in E(\mathbf{C})$, $\sigma \in G_k = \mathrm{Gal}(\overline{k}/k)$, on a P^σ, $Q^\sigma \in E(\overline{k})$, et $(P+Q)^\sigma = P^\sigma + Q^\sigma$, d'où on obtient une représentation galoisienne

$$\rho_{(N),E} : G_k \to \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z}),$$

car tout $\sigma \in G_k$ définie un automorphisme de $E_N(\overline{k}) = E_N(\mathbf{C}) \stackrel{\sim}{\to} (\mathbf{Z}/N\mathbf{Z})^2$. Les coefficients matriciels de $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \rho_{N,E}(\sigma)$ sont donnée par l'égalité $P^\sigma = (x^\sigma, y^\sigma) = P_{(a\omega_1 + b\omega_2)/N, (c\omega_1 + d\omega_2)/N}$.

Représentations l–adiques. Soit $N = l^n$, où l un nombre premier, alors passage à limite provient une représentation l–adique de G_k

$$\rho_{l,E} : G_k \to \mathrm{GL}(2, \mathbf{Z}_l) = \mathrm{GL}(T_l),$$

où $T_l(E) = \varprojlim_n E(\overline{k})_{l^n}$, la limite est prise par les morhismes

$$E(\overline{k})_{l^n} \overset{l\delta}{\leftarrow} E(\overline{k})_{l^{n+1}}$$

de multiplication par l.

3.1.14. Classes d'équivalence d'isogénies. Soient E et E' isogènes. On choisie des bases $\{\omega_1, \omega_2\}$ de Λ et $\{\omega_1', \omega_2'\}$ de Λ' de telle façon que $z = \omega_1/\omega_2 \in H$, $z' = \omega_1'/\omega_2' \in H$, alors $\exists \mu\ \mu\Lambda \subset \Lambda'$, et $\mu\mathbf{Q}\Lambda = \mathbf{Q}\Lambda'$ pour un $\mu \in \mathbf{C}^\times$, et $\exists g \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbf{Z})$

$$\mu\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

Deux isogénies $E \overset{\mu_1}{\to} E'$ et $E \overset{\mu_2}{\to} E'$ s'appelent équivalentes si $\operatorname{Ker} \mu_1 = \operatorname{Ker} \mu_2$.

Pour décrire les classes d'équivalence d'isogénies, on remarque que $\mu_1 \sim \mu_2 \iff \mu_1(\Lambda) = \mu_2(\Lambda)$, les classes d'équivalence correspondent aux sous–réseaux $\mu(\Lambda) \subset \Lambda'$. Changement de base de sous réseax $\mu(\Lambda)$ correspond au remplacement

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \gamma\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \quad \gamma \in \mathrm{SL}_2(\mathbf{Z}),$$

ceci implique que g se remplace par γg, car

$$\gamma\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

La structure du noyau $\operatorname{Ker} \mu \overset{\sim}{\to} \Lambda'/\mu\Lambda$ est facile à décrire à l'aide de changement de base de tous les deux réseaux Λ et Λ', ce qui correspond à des remplacements de type:

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \gamma\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \quad \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \mapsto \gamma'\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}, \quad \gamma, \gamma' \in \mathrm{SL}_2(\mathbf{Z}).$$

Alors g se remplace par $\gamma g \gamma'^{-1}$, car

$$\gamma\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma'^{-1}\gamma'\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix},$$

et $\exists \gamma, \gamma'$ tels que

$$\gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma'^{-1} = \begin{pmatrix} a' & 0 \\ 0 & d' \end{pmatrix}$$

i.e. on peut choisir les bases de Λ et de Λ' de telle façon que

$$\mu\omega_1 = a'\omega_1', \quad \mu\omega_2 = d'\omega_2',$$

et

$$\operatorname{Ker} \mu \overset{\sim}{\to} \Lambda'/\mu\Lambda \overset{\sim}{\to} (\mathbf{Z}/a'\mathbf{Z}) \oplus (\mathbf{Z}/d'\mathbf{Z}), \quad (a'|d')$$

Un isogénie λ s'appelle *cyclique* si $\operatorname{Ker} \lambda$ est un groupe cuclique, i.e. si $a' = 1 \iff g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est primitive $\det g = |\operatorname{Ker} \lambda|$.

3.1.15. Isogénie duale. Soit $E \stackrel{\mu}{\to} E'$ une isogénies des coures elliptiques définies sur $\mathbf{C}$ Alors $E(\mathbf{C}) \stackrel{\sim}{\to} Cl_E^0$, $E'(\mathbf{C}) \stackrel{\sim}{\to} Cl_{E'}^0$, μ est surjective, donc l'application $P \mapsto \mu^{-1}(P)$ induit un homomorphisme $\check{\mu} : Cl_{E'} \to Cl_E$, qui définit l'isogénie duale $\check{\mu}$: $\check{\mu} : Cl_{E'}^0 \to Cl_E^0$, pour laquelle

$$\check{\mu}((P') - (o')) = (P_1) + \ldots + (P_m) - (Q_1) - \ldots - (Q_m),$$

avec

$$\mu^{-1}(P') = \{P_1, \ldots, P_m\}, \quad \mu^{-1}(o') = \{Q_1, \ldots, Q_m\},$$

(et on peut suposer que $Q_1 = o$, $P_1 = P$, et que $P_j = P_1 + Q_j$).

Proposition. *On a* $\check{\mu} \circ \mu = m\delta_E$, $\mu \circ \check{\mu} = m\delta_{E'}$ *où* $m = \deg \mu$.

Preuve. Soit $\mu(P) = P'$. Il faut montrer que

$$\begin{aligned}&(P_1) + \ldots + (P_m) - (Q_1) - \ldots - (Q_m) = \\ &(P_1 + Q_1) + \ldots + (P_1 + Q_m) - (Q_1) - \ldots - (Q_m) \sim m((P) - (o))\end{aligned}$$

sur E, et que

$$\mu(P_1) + \ldots + \mu(P_m) - \mu(Q_1) - \ldots - \mu(Q_m) \sim m((P') - (o')).$$

La deuxième équivalence est triviale, et la première est impliquée par définition de la lois d'addition:

$$\sum a_i P_i = 0 \text{ dans } E(\mathbf{C}) \Longleftrightarrow \sum a_i (P_i) \sim 0 \ \& \ \sum a_i = 0.$$

Déscription analytique de l'isogénie duale. Soient $E = \mathbf{C}/\Lambda$, $E' = \mathbf{C}/\Lambda'$ isogènes, et $\Lambda = \langle \omega_1, \omega_2 \rangle$ et $\Lambda' = \langle \omega_1', \omega_2' \rangle$ ci-dessus, $z = \omega_1/\omega_2 \in H$, $z' = \omega_1'/\omega_2' \in H$, alors $\exists \mu$ $\mu\Lambda \subset \Lambda'$, et $\exists g \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbf{Z})$

$$\mu \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix},$$

$$\check{\mu} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Alors

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$$

et $\check{\mu}$ est donnée dans les bases chosis par $g^\iota = m^{-1} g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

24 janvier 1995. La courbe de Tate. Points d'ordre fini: trois déscriptions. Isogénies et dualité. Formes modulaires algébriques et leur développement de Fourier algébrique.

3.1.16. La courbe de Tate. Considérons l'équation de Weierstrass pour $\mathbf{C}/\Lambda$, où $\Lambda = \langle 2\pi i, 2\pi i z \rangle = 2\pi i \mathbf{Z} + 2\pi i z \mathbf{Z}$, $\omega = 2\pi i \, dz$:

$$Y^2 = 4X^3 - \frac{E_4}{12} X + \frac{E_6}{216} \quad (X = \wp(2\pi i z, \Lambda), \ Y = \wp'(2\pi i z, \Lambda)),$$

avec

$$12(2\pi i)^{-4}g_2(z) = E_4 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \quad (q = \exp(2\pi i z),$$

$$-216(2\pi i)^{-6}g_3(z) = E_4 = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Si l'on pose

$$X = x + \frac{1}{12}, Y = x + 2y,$$

on obtient une nouvelle équation dont les coeffisient sont dans $\mathbf{Z}[[q]]$:

$$Tate(q) : y^2 + xy = x^3 + B(q)x + C(q),$$

où

$$B(q) = -5\left(\frac{E_4 - 1}{240}\right) = -5\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$C(q) = \frac{-5\left(\frac{E_4-1}{240}\right) - 7\left(\frac{E_6-1}{-504}\right)}{12} = \sum_{n=1}^{\infty}\frac{-5\sigma_3(n) - 7\sigma_5(n)}{12}q^n.$$

Cette équation définie une courbe eliptique sur l'anneau $\mathbf{Z}((q))$ dont la différentielle canonique ω_{can} est

$$\frac{dx}{2y+x} = \frac{dX}{Y}.$$

(Rappel:

$$G_k(z) = \frac{2(2\pi i)^k}{(k-1)!}\cdot\left(-\frac{B_k}{2k}\right)\left[1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)\exp(2\pi i n z)\right] = -\frac{(2\pi i)^k B_k}{k!}E_k,$$

où

$$\begin{cases} g_2 = 60G_4 = (2\pi i)^4\dfrac{E_4}{12} \\ g_3 = 140G_6 = -(2\pi i)^6\dfrac{E_6}{216}.) \end{cases}$$

Soit $N \geq 1$ un nombre naturel. On pose

$$Tate(q^N) : y^2 + xy = x^3 + B(q^N)x + C(q^N).$$

Posons $t = \exp(2\pi i u)$, alors les points d'ordre N sur $Tate(q^N)$ correspondent aux $t = \zeta_N^i q^j$, $(0 \leq i, j \leq N-1)$, $\zeta_N = \exp(2\pi i/N)$, et leurs coordonnées sont données par

$$\begin{cases} x(t) = \displaystyle\sum_{k\in\mathbf{Z}}\frac{q^{Nk}t}{(1-q^{Nk}t)^2} - 2\sum_{k=1}^{\infty}\frac{q^{Nk}}{(1-q^{Nk}t)^2} \\ y(t) = \displaystyle\sum_{k\in\mathbf{Z}}\frac{(q^{Nk}t)^2}{(1-q^{Nk}t)^3} + \sum_{k=1}^{\infty}\frac{q^{Nk}}{(1-q^{Nk}t)^2}. \end{cases}$$

Pour des applications arithmétiques de la courbe de Tate il est très important que ces coordonnées sont dans l'anneau $\mathbf{Z}[\zeta_N, N^{-1}][[q]]$.

Preuve utilise l'identité

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

Pour le réseau $\Lambda = 2\pi i(\mathbf{Z}+z\mathbf{Z})$ on a

$$X = \wp(2\pi i u) = (2\pi i)^{-2}\left(u^{-2}+\sum_{m,n}{}'\left((u+mz+n)^{-2}-(mz+n)^{-2}\right)\right) =$$

$$(2\pi i)^{-2}\left(\sum_{m\in\mathbf{Z}}\sum_{n\in\mathbf{Z}}(u+mz+n)^{-2} - 2\sum_{m=1}^{\infty}\sum_{n\in\mathbf{Z}}(mz+n)^{-2} - 2\zeta(2)\right) =$$

$$\sum_{m\in\mathbf{Z}}\sum_{n=1}^{\infty} ne^{2\pi i(u+mz)n} - 2\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} ne^{2\pi i mnz} + \frac{1}{12},$$

d'où on obtient les identités ci-dessus.

3.1.17. Familles analytiques des courbes elliptiques. Pour un entier N considérons les sous–groupes de congruence suivants:

$$\Gamma_0(N) = \{\gamma\in \mathrm{SL}_2(\mathbf{Z}) \mid c_\gamma \equiv 0 \bmod N\},$$
$$\Gamma_1(N) = \{\gamma\in \Gamma_0(N) \mid a_\gamma \equiv d_\gamma \equiv 1 \bmod N\},$$
$$\Gamma(N) = \{\gamma\in \mathrm{SL}_2(\mathbf{Z}) \mid \gamma \equiv 1 \bmod N\}.$$

Les domains fondamentaux de H modulo l'action de ces groupes, à savoir: (a) $\Gamma_0(N)\backslash H$, (b) $\Gamma_1(N)\backslash H$, (c) $\Gamma(N)\backslash H$, peuvent être identifier respectivement avec les ensembles des claases d'isomorphisme sur $\mathbf{C}$ des multiplets suivantes:

(a) $(E, \langle P\rangle)$, une courbe elliptique sur $\mathbf{C}$ et un sous–groupe cyclique d'ordre N, $\langle P\rangle \subset E(\mathbf{C}), \mathrm{Card}\langle P\rangle = N$;

(b) (E, P), une courbe elliptique sur $\mathbf{C}$ et un point d'ordre N, $P\in E(\mathbf{C}), \mathrm{Card}\langle P\rangle = N$;

(c) (E, P, Q), une courbe elliptique sur $\mathbf{C}$ et une base de points d'ordre N:

$$P, Q \in E(\mathbf{C})_N = \langle P\rangle \oplus \langle Q\rangle \cong \mathbf{Z}/N\mathbf{Z}\oplus \mathbf{Z}/N\mathbf{Z}.$$

Pour décrire cette identification on associe à un point $z\in H$ les multiplets suivants:

(a) $(\mathbf{C}/\Lambda_z, \langle 1/N\rangle \bmod \Lambda_z)$);

(b) $(\mathbf{C}/\Lambda_z, 1/N \bmod \Lambda_z)$;

(c) $(\mathbf{C}/\Lambda_z, 1/N \bmod \Lambda_z, z/N \bmod \Lambda_z)$.

3.2. Formes modulaires algébriques

3.2.1. Courbes elliptiques sur un anneau R. Pour tout idéal premier $\mathfrak{p} \subset R$ soit $R/\mathfrak{p}$ l'anneau (intègre) residuel de $\mathfrak{p}$, $k(\mathfrak{p})$ son corps de fractions. De point de vue un peu naïf on va considérer une courbe elliptique E sur R comme définie par un système d'équations homogènes dans un éspace projectif

$$\mathbf{P}_R^n = \{(a_0 : a_1 : \ldots : a_n) \,|\forall i \quad a_i \in R,\ (a_0, a_1, \ldots, a_n) = R\}$$

de telle façon que (i) pour tout $\mathfrak{p}$ $E \bmod \mathfrak{p}$ (où $E \otimes k(\mathfrak{p})$) est une courbe elliptique sur $k(\mathfrak{p})$, (ii) il existe un point $o \in E(R)$ (une solutions dans $\mathbf{P}_R^n$ du système).

On va désigner par ω_E le R–module de R–différentielles de E (si R est intègre avec l'anneau de fraction K, $\omega_R \subset \Omega_{E/K}$, $\forall \mathfrak{p}\ \ \omega_R \otimes_R k(\mathfrak{p}) = \Omega_{k(\mathfrak{p})}[E_{k(\mathfrak{p})}]$.

(Pour donner des définitions plus presises on est obligé d'utilise le language de schéma [Deligne–Serre, p.510], [Katz, p.77–81]: une courbe elliptique sur un schéma S est un morphisme propre et lisse $E \to S$ muni d'une section $e : S \to E$, de fibres géométriques des courbes elliptiques. Lorsque S est le spectre d'un anneau commutatif A on dit aussi que E est une courbe elliptique sur A.On pose $\omega_E = e^*\Omega^1_{E/S}$: pour $S = \mathrm{Spec}(A)$, ω_E s'identifie à un A-module inversible.)

3.2.2. Formes modulaires sur R. Soit R un anneau sur lequel N est inversible. Une forme modulaire de poids k sur $\Gamma_1(N)$, méromorphe à l'infinie, définie sur R, est une loi qui, à tout courbe elliptique E sur une R–algèbre A, munie d'un point P (ou d'un plongement $\alpha : \mu_N \hookrightarrow E$), associe un élément $f(E, \alpha)$ de $\omega_E^{\otimes k}$. On exige que cette loi soit compatible aux isomorphismes, et à l'extensions des scalaires.

De façon équivalente, on peut définir une forme modulaire de poids k sur $\Gamma_1(N)$, méromorphe à l'infinie, définie sur R, est une loi qui, à tout courbe elliptique E sur une R–algèbre A, munie d'une base ω du R–module ω_E et d'un point P, associe un élément $f(E, \alpha, \omega)$ de A tel que

(i) $f(E, \alpha, \omega)$ ne dépend que de la classe de A–isomorphisme du triple (E, α, ω);

(ii) f est homogène de degré $-k$ par rapport à la deuxième variable: pour tout $\lambda \in A^\times$

$$f(E/A, \alpha, \lambda\omega) = \lambda^{-k} f(E/A, \alpha, \omega).$$

(iii) Cette loi est compatible avec extension de scalaires: $g : A \to B$

$$f(E \otimes_A B, \alpha, \omega \otimes_A B) = g(f(E/A, \alpha, \omega)).$$

Soit f comme ci–desus. Si $d \in (\mathbf{Z}/N\mathbf{Z})^\times$, on définit la forme modulaire $f|R_d$ par

$$(f|R_d)(E, \alpha, w) = f(E, d\alpha, \omega).$$

Si ψ un homomorphisme de $(\mathbf{Z}/N\mathbf{Z})^\times$ dans $\mathbf{R}^\times$, on dit que f est de type (k, ψ) sur $\Gamma_0(N)$ si $f|R_d = \psi(d)f$ pour tout $d \in (\mathbf{Z}/N\mathbf{Z})^\times$.

Faisons $R = \mathbf{C}$. La donnée de $\alpha : \mu_N \to E$ équivaut alors à celle du point

$$\alpha(\exp(2\pi i/N)$$

qui est d'ordre N. A une forme modulaire algébrique f ci dessus, on associe une fonction (encore notée par f) sur le demi–plan H par la régle

$$f(z) = f(E_z, 1/N, 2\pi i du),$$

où E_z désigne la courbe elliptique $\mathbf{C}/z\mathbf{Z}+\mathbf{Z}$, $u \in \mathbf{C}/z\mathbf{Z}+\mathbf{Z}$ la variable complexe sur E_z. Posons $f(z) = f_\infty(e^{2\pi iz})$, alors

$$f_\infty(q) = f(\mathbf{C}^\times/q^{\mathbf{Z}}, Id, dt/t) \quad (0 < |q| < 1, \quad t = \exp(2\pi iu)),$$

où Id est déduite de l'inclusion de μ_N dans $\mathbf{C}^\times$.

3.2.3. Développement de Fourier d'une forme modulaire algébrique est définit à l'aide de la courbe de Tate $\mathbf{G}_m/q^{\mathbf{Z}}$ sur l'anneau $\mathbf{Z}((q)) = \mathbf{Z}[[q]](q^{-1})$, qui est définit ci–dessus par l'équation

$$Tate(q) : y^2 + xy = x^3 + B(q)x + C(q),$$

où

$$B(q) = -5\left(\frac{E_4-1}{240}\right) = -5\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$C(q) = \frac{-5\left(\frac{E_4-1}{240}\right) - 7\left(\frac{E_6-1}{-504}\right)}{12} = \sum_{n=1}^{\infty}\frac{-5\sigma_3(n)-7\sigma_5(n)}{12}q^n,$$

$$E_4 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \quad (q = \exp(2\pi iz),$$

$$E_4 = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Cette équation définie une courbe elliptique sur l'anneau $\mathbf{Z}((q))$ qui est munie d'une différentielle canonique

$$\omega_{can} = dt/t = \frac{dx}{2y+x},$$

et d'un plongement naturel $Id : \mu_N \to \mathbf{G}_m/q^{\mathbf{Z}}$ (remarquons que le groupe μ_N est défini sur $\mathbf{Z}$ par l'équation $x^N - 1 = 0$, dont on a un plongement naturel $Id : \mu_N \to \mathbf{G}_m$, $\mathbf{G}_m$ étant le groupe multiplicatif (un groupe algébrique sur $\mathbf{Q}$). Si f est une forme de poids k sur Γ_1, méromorphe à l'infinie, et définie sur un anneau R, on pose

$$f_\infty(q) = f(\mathbf{G}_m/q^{\mathbf{Z}}, Id, dt/t) \in \mathbf{Z}((q)) \otimes R \subset R((q)).$$

(Ici $\mathbf{G}_m/q^{\mathbf{Z}}$ désigne la courbe sur $\mathbf{Z}((q)) \otimes R$ déduite de la courbe de Tate par extension des scalaires.)

Posons

$$f_\infty(q) = \sum a_n q^n \quad \text{et} \quad (f|R_d)_\infty(q) = \sum a_n(d)q^n, \quad d \in (\mathbf{Z}/N\mathbf{Z})^\times.$$

31 janvier 1995. Opérateurs de Hecke. Déscription algébrique des opérateurs de Hecke à l'aide d'isogénies. Produit des opérateurs de Hecke. La transformation de Mellin comme un produit eulérien. Formes primitives.

3.3. Opérateurs de Hecke

3.3.1. 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:

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

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

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

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 invariant par des multiplications droits par élements de $\Gamma_0(N)$. Pour 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 définir 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 $\sigma = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \in \Gamma_0(N)\backslash\Delta_m(N)$, $(m, N) = 1$.

3.3.2. 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 ci-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 ci-dessus nous montre que le règle de multiplication pour les opérateurs $T_k(m)$ a la forme donnée par la proposition suivante:

3.3.3. 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

3.3.4. 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 3.3.4 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 $\delta = \mathrm{PGCD}(n_1, m/m_1)$, 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 3.3.3.

En particulier, les opérateurs $T_k(n)$ commutent entre eux. 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

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

3.3.5. 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

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

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

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:

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

ci-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 distincts p_i, $p_i \nmid N$ implique que

$$L_N(s, f) = \prod_{p \ : \ p \nmid N} \left(\sum_{\delta=0}^{\infty} \lambda_f(p^\delta)p^{-\delta s} \right),$$

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.

3.3.6. Algèbre de Hecke. Interprétation géométrique des opérateurs de Hecke. Soit $f = \sum a_n q^n$ une forme modulaire (au sens habituelle) de type (k, ψ) sur $\Gamma_0(N)$, et soit p un nombre premier. On pose

$$f|T_p = \sum a_{pn} q^n + \psi(p) p^{k-1} \sum a_n q^{pn}, \quad \text{si} \quad p \not| N,$$

$$f|U_p = \sum a_{pn} q^n \quad \text{si} \quad p|N.$$

On obtient ainsi une autre forme modulaire de type (k, ψ) sur $\Gamma_0(N)$, qui est paraboliqie, si f est.

Déscription géométrique des opérateurs de Hecke. Si f une forme de type (k, ψ) sur $\Gamma_0(N)$ définie sur un corps algébriquement clos R de caractéristique $\neq p$ (à valeurs dans les différentielles multiples), on a

$$(f|T_p)(E, \alpha) = \frac{1}{p} \sum_{\varphi} \varphi^*(f(\varphi E, \varphi \circ \alpha)),$$

où φ parcourt les clases d'isogénies $\varphi : E \to E'$ de degré p de source E (deux isogénies étant dans la même classe si leurs noyaux sont égaux). La notation $\varphi^* : \omega_{\varphi E}^{\otimes k} \to \omega_E^{\otimes k}$ signifie le changement de variable $t \mapsto \varphi(t)$ dans les différentielles multiples. Les T_p commutent entre eux, et commutent aux R_d.

La définition ci–dessus est équivalente à la définition commode utilisé par Katz [Katz, 1.11]: si f une forme de type (k, ψ) sur $\Gamma_0(N)$ définie sur un corps algébriquement clos R de caractéristique $\neq p$, à valeurs scalaires, on pose

$$(f|T_p)(E, \alpha, \omega) = p^{k-1} \sum_{\varphi} \varphi^*(f(\varphi E, \varphi \circ \alpha, \check{\varphi}^*)),$$

où $\check{\varphi} : \varphi(E) \to E$ l'isogénie duale à φ,

$$\check{\varphi}^* : \omega_E^{\otimes k} \to \omega_{\varphi E}^{\otimes k}.$$

En effet, pour une base ω de ω_E, et une base ω' de $\omega_{\varphi E} = \omega_{E'}$ on a par définition

$$f(E, \alpha) = f(E, \alpha, \omega)\omega^{\otimes k}, \quad f(\varphi E, \varphi \circ \alpha) = f(\varphi E, \varphi \circ \alpha, \omega')(\omega')^{\otimes k},$$

d'où

$$\varphi^*(f(\varphi E, \varphi \circ \alpha)) = \varphi^*(f(\varphi E, \varphi \circ \alpha, \omega')(\omega')^{\otimes k}) = f(\varphi E, \varphi \circ \alpha, \omega')\varphi^*(\omega')^{\otimes k},$$

avec

$$f(E, \alpha, \omega), \quad f(\varphi E, \varphi \circ \alpha) \in R.$$

Posons $\omega' = \check{\varphi}^* \omega$, alors

$$f(\varphi E, \varphi \circ \alpha, \check{\varphi}^* \omega)(\varphi^* \circ \check{\varphi}^* \omega)^{\otimes k} = p^k f(\varphi E, \varphi \circ \alpha, \check{\varphi}^* \omega)\omega^{\otimes k}$$

car $\check{\varphi} \circ \varphi = p\delta$, $(\varphi^* \circ \check{\varphi}^* \omega)^{\otimes k} = p^k \omega^{\otimes k}$.

L'action de T_p sur les développement de Fourier: on vérifie que si p est un nombre premier ne divisant pas N, on a

$$f|T_p = \sum_n a_{pn} q^n + \psi(p) p^{k-1} \sum_n a_n q^{pn}.$$

3.4. Produit scalaire de Petersson.

3.4.1. 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 ci-dessus ([La2], [He], [Sh]).

Parfois il est plus commode à 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

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

3.4.2. L'interprétation à l'aide de la mesure de Haar sur le groupe $\mathrm{SL}(2, \mathbf{R})$ **[voir De].**

3.4.3. 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 $\Gamma(Nm)$.

3.4.4. 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 a 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 3.4.3 (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 $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

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

où

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

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

Alors

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

ceci entraîne la Proposition.

3.4.5. 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 $A_iA_j = A_jA_i$ 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.

3.4.6. 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 $\mathcal{S}_k(N, \psi)$.

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

3.5.1. 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 $\mathrm{Re}\ s \gg 0$.

Convergence de ces séries pour $\mathrm{Re}\,(s) \gg 0$ 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 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 ci–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 $N = 1$.

3.5.2. 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 plan 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

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

3.5.3. 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 ci-dessus doit avoir la forme $R(s,f)$ pour une forme modulaire $f \in \mathcal{M}_k = \mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$.*

3.5.4. 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 $f(-1/z) = z^k f(z)$ on voit bien que

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

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 à 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 étendue 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:

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

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.

3.5.5. Formes primitives. (voir [Miy]). 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

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

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

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

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:

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

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

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

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

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

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

Bibliographie

[An] *Andrianov, A.N.*: Euler products attached to Siegel modularforms of degree 2, 29 (1974) 44–109 (en russe)

[Ca–Fr] *Cassels, J.W.S., Frölich, A. ,eds.*: Algebraic Number Theory. Proc. Int. Congr. Lond. Math. Soc., Washington DC: Thompson, 1967.

[Cha] *Chandrasekharan*: K. Arithmetical functions

[De] *Deligne P.*: Formes modulaires et représentaton de GL(2), Modular Functions of One Variable , Lect. Notes in Math 349 (1973), 55–106

[De–Se] *Deligne P., Serre J.–P.*: Formes modulaires de poids 1,Ann. Sci. ENS, 7(1974), 506–530

[De-Ra] *Deligne P., Rapoport M.*: Les schémas de courbes elliptiques, Lecture Notes in Math. 349 (1973),Springer–Verlag, p.143–316

[Deu] *Deuring M.*: Lectures on algébraic curves, Lecture Notes in Math. 315 (1972)

[Fa-Kra] *Farkas–Kra*: Riemann surfaces

[Ge] *Gelbart, S.*: Automorphic forms on adèle groups. Ann. Math. Stud., 83 (1975)

[He] *Hecke*: Mathematische Werke, Vandenhoek und Ruprecht, Göttingen, 1970

[Hi] *Hida H.,*: Elementary theory of L–functions and Eisenstein series. London Math. Soc. Student Texts 26, Cambridge, 1993

[Ja–La] *Jacquet, H. Langlands, R.P.*: Automorphic forms on $GL(2)$. Lecture Notes in Math., 114 (1970)

[Ka] *Katz N.M.*: p–adic properties of modular schemes and modular forms, Lecture Notes in Math. 350 (1973),Springer–Verlag, p.69–190

[Ka–Ma] *Katz N.M. and Mazur B.*: Arithmetic moduli of elliptic curves, Ann. of Math. Studies, 108, Princeton University Press, 1985

[Ko] *Koblitz N*: Introduction to elliptic curves and modular forms. New York: Springer Verlag, 1984

[La1] *Lang S.*: Introduction to modular forms. Springer–Verlag, 1983

[La2] *Lang S.*: Elliptic functions, Reading, Mass.: Addison – Wesley, 1973.

[Miy] *Miyake T.*: Modular forms, Springer Verlag, 1989

[Se1] *Serre J.–P.*: Cours d'arithmétique, Paris 1970

[Se2] *Serre J.–P.*: Groupes algébriques et corps de classes, Paris

[Sh] *Shimura Gôro*: Introduction to arithmetic theory of automorphic functions, Princeton University Press, 1971

[We] *Weil, A.*: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann., 168 (1967), 149-156.