Introduction aux formes modulaires

Bruno Winckler (cours de Loïc Merel)

3 mars 2010

Table des matières

1 Formes modulaires classiques

1.1 Réseaux de $\mathbb{C}$

Un réseau de $\mathbb{C}$ est un $\mathbb{Z}$-module libre, discret, de rang 2 de $\mathbb{C}$ (autrement dit, il existe une base $(\vec{e_1}, \vec{e_2})$ sur $\mathbb{Z}$ libre sur $\mathbb{R}$). Un tel réseau s'écrit $\mathbb{Z}\vec{e_1} + \mathbb{Z}\vec{e_2}$.

On peut considérer $\mathscr{R}$ l'espace des réseaux. Il est muni d'une action de $GL_2(\mathbb{R})$ par $u(\mathbb{Z}\vec{e_1}+\mathbb{Z}\vec{e_2}) = \mathbb{Z}u(\vec{e_1})+\mathbb{Z}u(\vec{e_2})$. Le stabilisateur de tout réseau est $GL_2(\mathbb{Z})$.

Remarque : Si Λ est un réseau de $\mathbb{C}$, on peut considérer $\mathbb{C}/\Lambda$, qui est une courbe elliptique sur $\mathbb{C}$ (et une surface de Riemann, un groupe algébrique, *etc.*). Ces objets ainsi obtenus grâce à Λ et Λ' sont isomorphes si, et seulement si il existe $\lambda \in \mathbb{C}^*$ tel que $\lambda\Lambda = \Lambda'$.

On a donc une action de $\mathbb{C}^*$ sur $\mathscr{R}$. Le réseau $\mathbb{Z}e_1+\mathbb{Z}e_2$ s'écrit $e_1\left(\mathbb{Z}+\frac{e_2}{e_1}\mathbb{Z}\right)$ et $e_2\left(\mathbb{Z}+\frac{e_1}{e_2}\mathbb{Z}\right)$. On choisit de telle sorte que $\mathbb{Z}e_1+\mathbb{Z}e_2 = e_i(\mathbb{Z}+\mathbb{Z}\tau)$ avec $\Im(\tau) > 0$.

Soient τ et τ' dans $\mathcal{H}$ le demi-plan des nombres complexes de partie imaginaire strictement positive. À quelle condition a-t-on $\mathbb{Z}+\mathbb{Z}\tau \equiv \mathbb{Z}+\mathbb{Z}\tau' \mod \mathbb{C}^*$? Si, et seulement si il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ tel que $\frac{a\tau+b}{c\tau+d} = \tau'$. Comme $\tau, \tau' \in \mathcal{H}$, on a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Une fonction F sur $\mathscr{R}$ définit une fonction f sur $\mathcal{H}$ par $f(\tau) = F(\mathbb{Z}+\mathbb{Z}\tau)$. Soit k un entier. On dit que $F : \mathscr{R} \to \mathbb{C}$ est homogène de poids k si on a $F(\lambda\Lambda) = \lambda^k F(\Lambda)$ pour tout $\lambda \in \mathbb{C}^*$ et tout Λ. Cela se traduit ainsi sur f : soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. On a

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-k} f(\tau).$$

On note aussi $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = \frac{a\tau+b}{c\tau+d}$. Pour $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{R})$, $\alpha\delta - \beta\gamma > 0$ et $f : \mathcal{H} \to \mathbb{C}$, on pose

$$f|_{k\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)}(\tau) = (\gamma\tau+\delta)^{-k} \det\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{k/2} f\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\tau\right).$$

Le fait que $F : \mathscr{R} \to \mathbb{C}$ soit une fonction homogène de poids k se traduit par $f|_{k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = f$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $f : \mathcal{H} \to \mathbb{C}$. On aimerait imposer deux restrictions supplémentaires : l'holomorphie selon τ, et le comportement asymptotique lorsque τ se rapproche du bord de $\mathcal{H}$.

1.2 Formes modulaires

Soit $k \in \mathbb{N}$. Une forme modulaire de poids k est une fonction $f : \mathcal{H} \to \mathbb{C}$ holomorphe qui vérifie $f|_{k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = f$ pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. En particulier, pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $f|_{k\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)}(\tau) = f(\tau+1)$, donc f s'écrit

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n, q = e^{2i\pi\tau}, a_n \in \mathbb{C}.$$

Alors, on impose de plus $f(\tau) = \sum_{n\geq 0} a_n q^n$ (c'est l'holomorphie à l'infini). On a $f(\tau) \to a_0$ quand $\tau \to \infty$.

Le bord de $\mathcal{H}$ est constitué de $\mathbb{P}^1(\mathbb{Q})$. On prolonge la topologie de $\mathcal{H}$ à $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ de la façon suivante : $GL_2(\mathbb{Q})$ agit sur $\mathbb{P}^1(\mathbb{Q})$ par homographies. Une base de voisinages de $x \in \mathbb{P}^1(\mathbb{Q})$, $x \neq \infty$ est formée par l'intérieur d'un horocycle. Si $x = \infty$, une base de voisinages est l'ensemble des demi-plans supérieurs horizontaux.

On note M_k le $\mathbb{C}$-espace vectoriel des formes modulaires de poids k. On note $M_k^0 = \{f = \sum_{n\geq 0} a_n q^n \in M_k | a_0 = 0\}$. C'est le sous-espace des formes modulaires paraboliques. On a $\mathrm{codim}(M_k^0) \leq 1$. On peut se limiter à k pair dans la suite du cours, car si f est une forme modulaire de poids k impair, on a $f(\tau) = (-1)^k f(\tau) = -f(\tau)$ (en prenant $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = -I_2$), donc $f(\tau) = 0$ pour tout τ.

Si f et f' sont modulaires de poids k et k' respectivement, ff' est modulaire de poids $k+k'$. On peut considérer $\oplus_{k\geq 0} M_k$ qui est l'algèbre graduée des formes modulaires.

1.3 Séries d'Eisenstein

Soit $k > 2$ pair, et Λ un réseau de $\mathbb{C}$. On pose $\tilde{G_k}(\Lambda) = \sum'_{\lambda \in L} \frac{1}{\lambda^k}$, homogène de poids $-k$ si elle est définie. Si $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, on pose

$$G_k(\tau) = \frac{(k-1)!}{2(2i\pi)^k} \tilde{G_k}(\Lambda) = \frac{(k-1)!}{2(2i\pi)^k} \sum_{(m,n)\in\mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m\tau + n)^k}.$$

Alors :

$$G_k(\tau) = \frac{1}{2}\zeta(1-k) + \sum_{k=1}^{\infty} \sigma_{k-1}(n) q^n,$$

où $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

(Note personnelle : à partir d'ici, et jusqu'au paragraphe « Compléments », j'ai perdu mes notes de cours ; par conséquent, les preuves ne sont probablement pas les mêmes que celles du cours de M. Merel, et il manque peut-être quelques propriétés)

Preuve : On part de la formule bien connue :

$$\pi \mathrm{cotan}(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right),$$

qui peut par exemple se déduire du développement en série de Fourier de la fonction $t \mapsto \cos(\alpha t)$ définie sur $[-\pi, \pi]$ puis prolongée par 2π-périodicité, dans laquelle on pose ensuite $t = \pi$ et $x = \alpha\pi$.

On a de plus $\pi \mathrm{cotan}(\pi z) = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = i\pi \frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi \sum_{n=0}^{\infty} q^n$. Alors, en comparant les deux égalités, et par dérivations successives, on obtient :

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

Or

$$G_k(\tau) = \frac{(k-1)!}{2(2i\pi)^k} \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^k} = \frac{(k-1)!}{2(2i\pi)^k}\left(2\zeta(k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(m\tau+n)^k}\right).$$

Alors, d'après ce qu'on vient d'établir :

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

À l'aide de ceci, on obtient le résultat après simplifications. □

Remarque : Si on pose $E_k = \frac{G_k}{2\zeta(k)}$, on a $E_k(\tau) = 1 + (-1)^{k/2}\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$, où $B_k = \frac{k!}{2^{k-1}\pi^k}\zeta(k)$ est le k-ième nombre de Bernoulli.

On a donc des formes modulaires pour tout $k > 2$ pair. Les séries d'Eisenstein de poids les plus bas sont E_4 et E_6. Il s'avère qu'ils engendrent l'algèbre des formes modulaires, comme on le verra plus tard. Notons

$$\Delta = 60^3 G_4^3 - 27\cdot 140^2 G_6^2.$$

On vérifie que $\Delta(\infty) = 0$. Autrement dit, Δ est une forme parabolique de poids 12.

1.4 Le groupe modulaire

Notons $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$. Soient $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ deux éléments de $PSL_2(\mathbb{Z})$. On a $Sz = -\frac{1}{z}$, $Tz = z+1$, $S^2 = 1$, $(ST)^3 = 1$. Soit, d'autre part, l'ensemble D des complexes z vérifiant $|z| \geq 1$ et $\Re(z) \leq \frac{1}{2}$. Alors :

Théorème 1 *1. Pour tout $z \in \mathcal{H}$, il existe $g \in PSL_2(\mathbb{Z})$ tel que $gz \in D$.*

2. Si deux points distincts z, z' de D sont congrus modulo $PSL_2(\mathbb{Z})$, alors soit $\Re(z) = \pm 1/2$ et $z = z' \pm 1$, soit $|z| = 1$ et $z' = -\frac{1}{z}$.

3. $\mathrm{Stab}_{PSL_2(\mathbb{Z})}(z) = \{1\}$, sauf si $z = i$ (auquel cas c'est $\{1, S\}$) ou $z = j$ (auquel cas c'est $\{1, ST, (ST)^2\}$), ou $z = -\bar{j}$ (auquel cas c'est $\{1, TS, (TS)^2\}$).

Corollaire 1 *L'application canonique $D \to \mathcal{H}/PSL_2(\mathbb{Z})$ est surjective. Sa restriction à l'intérieur de D est injective.*

Théorème 2 *$PSL_2(\mathbb{Z})$ est engendré par S et T.*

Preuve du théorème 1 :Soit G le sous-groupe de $PSL_2(\mathbb{Z})$ engendré par S et T, et soit $z \in \mathcal{H}$. Montrons qu'il existe $g \in G$ tel que $gz \in D$. Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on a

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

et comme c et d sont entiers, le nombre de couples (c,d) tels que $|cz+d|$ soit inférieur à un nombre donné est fini. On en conclut qu'il existe $g \in G$ tel que $\Im(gz)$ soit maximal. Il existe d'autre part un entier n tel que $T^n gz$ soit de partie réelle entre $-1/2$ et $1/2$. Alors, $T^n gz$ appartient à D, car si $|T^n gz| < 1$, alors $ST^n gz$ aurait une partie imaginaire strictement plus grande que $\Im(T^n gz)$, ce qui est impossible. Alors, $g' = T^n g$ répond à la question.

Pour les deuxième et troisième points : soient $z \in D$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ tels que $gz \in D$. Quitte à remplacer (z,g) par (gz, g^{-1}), on peut supposer que $\Im(gz) \geq \Im(z)$, c'est-à-dire que $|cz+d| \leq 1$. Ceci est impossible pour $|c| \geq 1$, donc on étudie les cas $c \in \{0, \pm 1\}$.

Si $c = 0$, on a $d = \pm 1$ et g est une translation par $\pm b$. Comme $\Re(z)$ et $\Re(gz)$ sont entre $-1/2$ et $1/2$, on a soit $b = 0$ et $g = 1$, soit $b = \pm 1$, auquel cas l'un des nombres $\Re(z)$ et $\Re(gz)$ doit être égal à $-1/2$ et l'autre à $1/2$.

Si $c = 1$, alors $d = 0$, sauf si $z = j$ (ou $-\bar{j}$), et dans ce cas on peut avoir $d = 0$ ou 1 (ou $d = 0$ ou -1). Le cas $d = 0$ donne $|z| \leq 1$, d'où $|z| = 1$. Comme $ad - bc = 1$, $b = -1$, donc $gz = a - 1/z$ et la première partie de la discussion montre que $a = 0$, sauf si $\Re(z) = \pm 1/2$, c'est-à-dire si $z = j$ ou $-\bar{j}$, auquel cas on peut prendre $a = 0, -1$ ou $a = 0, 1$. Le cas $z = j$, $d = 1$ donne $a - b = 1$ et $gj = a - 1/(1+j) = a + j$, d'où $a = 0$ ou 1. On traite de même le cas $z = -\bar{j}$ et $d = -1$.

Enfin, le cas $c = -1$ se ramène au cas $c = 1$ en changeant les signes des coefficients de g.

Preuve du théorème 2 : Soit g un élément de $PSL_2(\mathbb{Z})$. Soit $z_0 = 2i$ et $z = gz_0$. Il existe $g' \in G$ tel que $g'z \in D$. Alors, z_0 et $g'z = g'gz_0$ sont congrus modulo $PSL_2(\mathbb{Z})$, et l'un d'eux est intérieur à D. Alors, ces points sont confondus et $g'g = 1$. Donc $g \in G$. □

Ceci montre entre autres que pour vérifier qu'une fonction est modulaire, il suffit de le vérifier pour S et T. Revenons aux réseaux :

Proposition 1 *$\mathscr{R}\backslash\mathbb{C}^* \simeq \mathcal{H}/PSL_2(\mathbb{Z})$ via $\mathbb{Z} + \tau\mathbb{Z} \mapsto \tau$.*

On remarque que $PSL_2(\mathbb{Z})$ peut être remplacé par $SL_2(\mathbb{Z})$ dans cette proposition.

1.5 Dimension de M_k

Si f est une fonction méromorphe sur $\mathcal{H}$, non identiquement nulle, on note $v_p(f)$ l'ordre de f en p, qui est l'entier n tel que $f/(z-p)^n$ soit holomorphe et non nulle en p. De plus, si $f = \sum_n a_n q^n$, notons $v_p(\infty) = \min\{n | a_n \neq 0\}$.

Théorème 3 *Soit f une fonction modulaire de poids k, non identiquement nulle. On a*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_j(f) + \sum_{i,j \neq z \in \mathcal{H}} v_z(f) = \frac{k}{12}. \tag{1}$$

Preuve : Cela résulte de l'intégration de f'/f sur un contour convenable. Voir [Ser] par exemple. □

On va alors pouvoir calculer la dimension de M_k. Remarquons d'abord que comme $G_k(\infty) \neq 0$, on a $M_k = M_k^0 \oplus \mathbb{C}G_k$ (M_k^0 est le noyau de la forme linéaire $f \mapsto f(\infty)$).

Théorème 4 *On a $M_k = 0$ pour k négatif et $k = 2$.*

Preuve : En effet, si f est un élément non nul de M_k, tous les termes du membre de gauche de la formule

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_j(f) + \sum_{i,j \neq z \in \mathcal{H}} v_z(f) = \frac{k}{12}$$

sont positifs, donc k est positif. Il n'y a pas de forme de modulaire de poids 2, car $\frac{1}{6}$ ne peut pas s'écrire sous la forme $n_1 + \frac{n_2}{2} + \frac{n_3}{3}$ avec n_i des entiers positifs. □

Théorème 5 *La multiplication par Δ définit un isomorphisme de M_{k-12} sur M_k^0.*

Preuve : Si on applique la formule ci-dessus à $f = G_4$ et $k = 2$, comme $\frac{1}{3} = 0 + \frac{0}{2} + \frac{1}{3}$ est la seule décomposition possible, on en conclut que $v_j(G_4) = 1$ et que $v_p(G_4) = 0$ sinon (modulo $SL_2(\mathbb{Z})$) : G_4 a un seul zéro (simple), en j. De même, on montre que G_6 a un seul zéro (simple) en i. Ceci montre que Δ ne s'annule pas en i, donc n'est pas identiquement nul. Comme le poids de Δ est 12, et que $v_\infty(\Delta) \geq 1$, on en déduit (toujours par la même formule) que $v_p(\Delta) = 0$ pour $p \neq \infty$ et que $v_\infty(\Delta) = 1$: Δ a un zéro unique en ∞ (en particulier Δ ne s'annule pas sur $\mathcal{H}$).

Si f est un élément de M_k^0, f/Δ est un élément de M_{k-12}, grâce à la formule $v_p(f/\Delta) = v_p(f) - v_p(\Delta) \geq 0$ pour tout p (distinguer les cas $p = \infty$ et $p \neq \infty$). Ceci démontre le théorème. □

Théorème 6 *Pour $k = 0, 4, 6, 8, 10$, M_k est un espace de dimension 1 admettant pour base $1, G_4, G_6, G_8, G_{10}$. On a $M_k^0 = 0$.*

Preuve : Si $k \leq 10$, on a $k - 12 < 0$ et donc $M_k^0 = 0$ d'après les deux théorèmes précédents. Alors, $\dim(M_k) \leq 1$. Comme 1, G_4, G_6, G_8 et G_{10} sont des éléments non nuls de M_0, M_2, M_4, M_6, M_8, M_{10}, on a $\dim(M_k) = 1$ pour les k cités dans l'énoncé du théorème. □

Par récurrence, on peut donc en déduire la dimension de tous les M_k.

Remarque : L'algèbre $\oplus_{k \geq 0} M_k$ est engendrée sur $\mathbb{C}$ par G_4 et G_6. En effet, les monômes $G_4^\alpha G_6^\beta$ avec $4\alpha + 6\beta = k$ engendrent M_k comme espace vectoriel : pour $k \leq 6$, c'est clair par les théorèmes précédents ($G_8 = \lambda G_4^2$, car ils sont sur une même droite vectorielle). Pour $k \geq 8$, on raisonne par récurrence. Soit (γ, δ) un couple d'entiers positifs tels que $4\gamma + 6\delta = k$ (c'est possible dès que $k \geq 2$). Alors, la forme modulaire $g = G_4^\gamma G_6^\delta$ est non nulle à l'infini. Si $f \in M_k$, il existe $\mu \in \mathbb{C}$ tel que $f - \mu g$ soit parabolique, donc de la forme Δh avec $h \in M_{k-12}$. On applique alors l'hypothèse de récurrence à h.

En fait, les monômes $G_4^\alpha G_6^\beta$ forment même une base. Pour montrer qu'ils sont linéairement indépendants, on suppose qu'ils ne le sont pas ; alors, la fonction G_4^α/G_6^β vérifierait une équation algébrique non triviale à coefficients dans $\mathbb{C}$, donc serait constante, absurde puisque G_4 s'annule en j mais pas G_6.

Enfin, posons $j = E_4^3/\Delta$. Alors la fonction j est une fonction modulaire (*i.e.* elle n'est pas supposée holomorphe en l'infini) de poids 0, holomorphe dans $\mathcal{H}$ et avec un pôle simple à l'infini, et de plus :

Proposition 2 *j définit, par passage au quotient, une bijection de $\mathcal{H}/SL_2(\mathbb{Z})$ dans $\mathbb{C}$.*

Preuve : Pour $\lambda \in \mathbb{C}$, la forme modulaire $f_\lambda = E_4^3 - \lambda\Delta$ a un zéro et un seul modulo $SL_2(\mathbb{Z})$. Il suffit d'appliquer la formule 1 avec $f = f_\lambda$ et $k = 12$. Les seules décompositions de 1 sous la forme $n_1 + \frac{n_2}{2} + \frac{n_3}{3}$ correspondent à (n_1, n_2, n_3) égal à $(1,0,0)$, $(0,2,0)$ ou $(0,0,3)$. Alors, f_λ s'annule en un point et un sur $\mathcal{H}/SL_2(\mathbb{Z})$. □

On peut montrer que toute fonction modulaire de poids 0 s'écrit comme fonction rationnelle de j.

Le développement de Δ Rappelons que $\Delta = 60^3 G_4^3 - 27 \cdot 140^2 G_6 = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 - \cdots$. Alors :

Théorème 7 *On a $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$.*

Preuve : Comme M_{12}^0 est de dimension 1, il suffit de montrer que $F = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ est modulaire. Alors, F et Δ seront proportionnels, de coefficient de proportionnalité 1. En fait, tout revient à prouver que $F(-1/z) = z^{12}F(z)$, et ceci passe par le calcul de la dérivée logarithmique des deux membres. Voir [Ser] par exemple. □

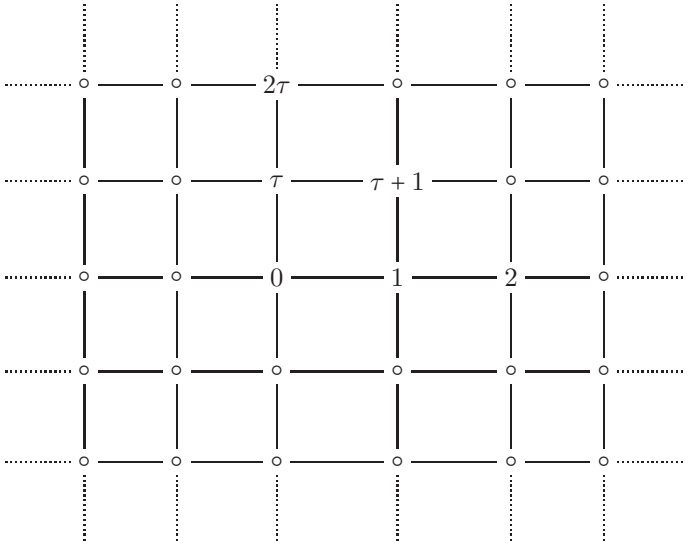
Compléments

1. Autre preuve que $M_2 = \{0\}$. Soit $f \in M_2$ non nulle. On a f non parabolique, donc on peut supposer que $f(\tau) = 1 + \sum_{n\geq 1} a_n q^n$. Donc $f^2 \in M_4$, et $f^3 \in M_6$. Donc $f^2 = E_4$ et $f^3 = E_6$. Or
$$E_4^3 - E_6^2 = (240 \times 3 + 504 \times 2)q + \cdots \neq 0,$$
absurde.
2. Pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Q})$, avec $ad - bc > 0$, et pour $f : \mathcal{H} \to \mathbb{C}$, on définit
$$f|_k\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = (c\tau + d)^{-k} \det\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{k/2} f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right)$$
3. Soit k un entier pair positif. On a $\dim M_k = \dim M_k^0 + 1$ sauf si $k = 2$, et $\dim M_k = \dim M_{k+12}^0$. D'où $\dim M_k = \begin{cases} E(k/12) \text{ si } k \equiv 2 \mod 12 \\ E(k/12) + 1 \text{ sinon.} \end{cases}$

1.6 Opérateurs de Hecke

Soit Λ un réseau de $\mathbb{C}$, $n \geq 1$. Quels sont les réseaux d'indice n de Λ ?

Exemple : Posons $n = 2$, et $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. Il existe alors trois réseaux d'indice 2 : $\mathbb{Z} + 2\tau\mathbb{Z}$, $2\mathbb{Z} + \tau\mathbb{Z}$ et $2\mathbb{Z} + (\tau + 1)\tau$.



Les réseaux d'indice n contiennent $n\Lambda$. On peut montrer que si n est un nombre premier, alors il y en a $n + 1$. Plus généralement, il y a $\sigma_1(n) = \sum_{d|n} d$ réseaux d'indice n.

Rappelons que $\mathscr{R}$ est l'espace des réseaux. Une correspondance sur un ensemble X est une application $X \to \mathbb{Z}[X]$. On définit la correspondance de Hecke T_n sur $\mathscr{R}$ par la formule

$$T_n(\Lambda) = \sum_{[\Lambda:\Lambda']=n} [\Lambda'],$$

et la correspondance de Hecke $T_{n,n}$ par $T_{n,n} = [n\Lambda]$ ($n\Lambda$ est d'indice n^2 dans Λ). Le degré de T_n est $\sum_{[\Lambda:\Lambda']=n} 1 = \sigma_1(n)$. Le degré de $T_{n,n}$ est 1. On peut voir une correspondance sur X comme un endomorphisme de $\mathbb{Z}[X]$, par $T\left(\sum \alpha_x [x]\right) = \sum \alpha_x T(x)$.

Proposition 3 *On a*

1. $T_n T_m = T_{nm}$ *pour* $n \wedge m = 1$.
2. $T_{n,n} T_{m,m} = T_{nm,nm}$ *pour* n *et* $m \geq 1$.
3. $T_n T_{m,m} = T_{m,m} T_n$ *pour* n *et* $m \geq 1$.
4. $T_{p^{r+1}} + p T_{p^r - 1} T_{p,p} = T_p T_{p^r}$ *pour* $p \in \mathbb{P}$ *et* $r \geq 1$.

Preuve : La deuxième formule est immédiate. La troisième découle de :

$$T_n T_{m,m}(\Lambda) = T_n(m\Lambda) = \sum_{[m\Lambda:\Lambda']=n} [\Lambda'] = \sum_{[\Lambda:\Lambda'']=n} [m\Lambda''] = T_{m,m} T_n(\Lambda).$$

La première formule découle du théorème de Bézout : il y a une bijection entre les sous-réseaux d'indice mn et les couples (Λ'', Λ''') où Λ'' (respectivement Λ''') est un sous-réseau d'indice n (respectivement m). Cette bijection est donnée par $\Lambda' \mapsto (\Lambda' + n\Lambda, \Lambda' + m\Lambda)$ et $(\Lambda'', \Lambda''') \mapsto \Lambda'' \cap \Lambda'''$. On en déduit :

$$T_{nm}(\Lambda) = \sum_{[\Lambda:\Lambda']=nm} [\Lambda'] = \sum_{[\Lambda:\Lambda'']=n, [\Lambda:\Lambda''']=m} [\Lambda'' \cap \Lambda'''] = \sum_{[\Lambda:\Lambda''']=m} \sum_{[\Lambda''':\Lambda^{(4)}]=n} [\Lambda^{(4)}],$$

d'où finalement $T_{nm}(\Lambda) = \sum_{[\Lambda:\Lambda''']=m} T_n[\Lambda'''] = T_m(T_n(\Lambda))$.

Pour la quatrième proposition, on veut montrer que pour $\Lambda \in \mathscr{R}$, $T_{p^r} T_p(\Lambda) = T_{p^{r+1}}(\Lambda) + pT_{p^{r-1}} T_{p,p}(\Lambda)$. Cette égalité exprime une relation entre sous-réseaux d'indice p^{r+1} de Λ.

Soit $\Lambda' \subseteq \Lambda$ d'indice p^{r+1}. Vérifions que Λ' apparait autant de fois de chaque coté.

Premier cas : Si $\Lambda' \subseteq \Lambda$, Λ' n'intervient pas dans $pT_{p,p}T_{p^{r-1}}(\Lambda)$, car $T_{p,p}(\Lambda) = [p\Lambda]$. Alors $\Lambda' + p\Lambda$ est d'indice p dans Λ. C'est le seul sous-réseau d'indice p contenant Λ'. Λ' intervient une seule fois dans $T_{p^{r+1}}(\Lambda)$. C'est un sous-réseau d'indice p^r de $\Lambda' + p\Lambda$ qui est un sous-réseau d'indice p de Λ. Donc Λ' intervient dans $T_{p^r} T_p(\Lambda)$. Il intervient une seule fois, car un seul sous-réseau d'indice p de Λ contient Λ'.

Second cas : Si $\Lambda' \subseteq p\Lambda$, on a Λ' contenu dans chacun des $p+1$ sous-réseaux d'indice p de Λ. Donc Λ' intervient $p+1$ fois dans $T_{p^r} T_p(\Lambda)$. Par ailleurs, Λ' intervient une fois dans $T_{p^{r+1}}(\Lambda)$. Comme $\Lambda' \subseteq p\Lambda$, $\frac{1}{p}\Lambda'$ est un sous-réseau d'indice p^{r-1} de Λ. Donc $\frac{1}{p}\Lambda'$ intervient une fois dans $T_{p^{r-1}}(\Lambda)$. Donc Λ' intervient une fois dans $T_{p,p}T_{p^{r-1}}(\Lambda)$ et donc p fois dans $T_{p,p}T_{p^{r-1}}(\Lambda)$. □

Remarque : Si on pense au lien entre courbe elliptique et réseau, donné par $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ (E étant une courbe elliptique), la correspondance de Hecke peut être vue comme $E \mapsto \sum_{[E(\mathbb{C}):C]=n} [E/C]$.

Formule explicite pour les T_n On a :

$$T_n(\mathbb{Z} + \tau\mathbb{Z}) = \sum_{\substack{ad=n \\ a \geq 1 \\ 0 \leq b < d}} (a\tau + b)\mathbb{Z} + (c\tau + d)\mathbb{Z} \quad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) \right).$$

On a bien là tous les réseaux d'indice n de $\mathbb{Z}+\tau\mathbb{Z}$. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. Alors $(a\tau+b)\mathbb{Z} + (c\tau+d)\mathbb{Z}$ est un sous-réseau d'indice n si, et seulement si $ad - bc = n$. Les réseaux obtenus à partir de M et $M' \in \mathcal{M}_2(\mathbb{Z})$ sont égaux si, et seulement si il existe $\gamma \in SL_2(\mathbb{Z})$ tel que $M' = \gamma M$.

Trouver explicitement les sous-réseaux d'indice n de Λ revient à trouver un système de représentants de $SL_2(\mathbb{Z})\backslash\underbrace{\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}) | ad-bc=n\right\}}_{=\mathcal{M}_2(\mathbb{Z})_n}$. Or $S_n = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad=n, a\geq 1, 0\leq b<d\right\}$ est un tel système de représentants.

Exercice : Le montrer en deux parties :

1. Montrer que si $\gamma\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ avec $\gamma \in SL_2(\mathbb{Z})$ et $ad = a'd' = n$, $a, a' \geq 1$, $0 \leq b < d$, $0 \leq b' < d'$, alors $\gamma = I_2$.
2. Montrer qu'on a $M_2(\mathbb{Z}) = SL_2(\mathbb{Z})S_n$. Indication : soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. On peut alors commencer par prendre $d = c \wedge d$.

Passons aux formes modulaires : soit $k \geq 0$ et $f \in M_k$. Soit $F : \mathscr{R} \to \mathbb{C}$ la fonction homogène de poids $-k$ associée. On pose

$$T_n(F)(\Lambda) = \sum_{[\Lambda:\Lambda']=n} F(\Lambda')n^{k-1}.$$

L'application $F \mapsto T_n(F)$ est $\mathbb{C}$-linéaire.

On pose

$$T_n(f)(\tau) = n^{k-1} \sum_{\substack{ad=n \\ a\geq 1 \\ 0\leq b<d}} f\left(\frac{a\tau+b}{d}\right)d^{-k} = n^{k/2-1} \sum_{\substack{ad=n \\ a\geq 1 \\ 0\leq b<d}} f|_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)}.$$

T_n est un endomorphisme de M_k : si F est homogène de poids $-k$, $T_n(F)$ l'est aussi. En effet,

$$T_n(F)(\lambda\Lambda) = n^{k-1} \sum_{[\lambda\Lambda:\Lambda']=n} F(\Lambda') = n^{k-1} \sum_{[\Lambda:\frac{1}{\lambda}\Lambda']=n} \lambda^{-k}F\left(\frac{1}{\lambda}\Lambda'\right) = \lambda^{-k}(T_n(F))(\Lambda).$$

On appelle T_n opérant sur M_k le n-ième opérateur de Hecke. De même, on a un opérateur $T_{n,n}$ sur M_k qui est trivial.

Proposition 4 (Action de T_n sur les q-développements) *Soit $f = \sum_{l=0}^{\infty} a_l q^l \in M_k$, $q = e^{2i\pi\tau}$. On a alors $T_n(f) = \sum_{m=0}^{\infty} b_m q^m$, avec $b_m = \sum_{r|n\wedge m} r^{k-1} a_{\frac{mn}{r^2}}$.*

Preuve : On a

$$T_n(f)(\tau) = n^{k-1} \sum_{\substack{ad=n \\ a\geq 1 \\ 0\leq b<d}} d^{-k} \sum_{l=0}^{\infty} a_l e^{2i\pi(\frac{a\tau+b}{d})l}$$

Or $\sum_{0\le b<d} e^{\frac{2i\pi kl}{d}} = \begin{cases} d \text{ si } d|l \\ 0 \text{ sinon.} \end{cases}$

On ne retient que les termes pour lesquels $d|l$ dans la somme. On pose $l = dj$ avec $j \in \mathbb{Z}$. On obtient

$$T_n(f)(\tau) = n^{k-1} \sum_{\substack{j\in\mathbb{Z} \\ ad=n}} d \cdot d^{k-1} a_{dj} q^{aj}.$$

Notons $m = cj$ et $a = r$. Alors, $dj = \frac{md}{r} = \frac{mn}{r^2}$. Finalement,

$$T_n(f)(\tau) = n^{k-1} \sum_{\substack{m\in\mathbb{Z} \\ r|m \\ r|n}} \left(\frac{n}{r}\right)^{r-k} a_{\frac{mn}{r^2}} q^m,$$

ce qui donne la formule cherchée après quelques aménagements. □

Corollaire 2 *On a $T_n(f)(\tau) = \sigma_{k-1}(n)a_0 + a_n q + \cdots$. Donc T_n laisse stable M_k^0.*

Notons a_n la forme linéaire $a_n : \begin{cases} M_k & \to & \mathbb{C} \\ f = \sum_{n\ge1} a_n q^n & \mapsto & a_n \end{cases}$. On a $a_n = a_1 \circ T_n$.

Soit $\mathbb{T}_k$ le sous-anneau de $\mathrm{End}(M_k)$ engendré par les T_n et $T_{n,n}$ pour $n \ge 1$. Il est commutatif, et appelé algèbre de Hecke.

Théorème 8 *L'accouplement*

$$\varphi : \begin{cases} \mathbb{T}_k \times M_k & \to & \mathbb{C} \\ (t, f) & \mapsto & a_1(tf) \end{cases}$$

est non dégénéré de chaque côté.

En particulier, considérer les injections induites et les dimensions de chaque espace implique l'isomorphisme de $\mathbb{C}$-espaces vectoriels $\mathrm{Hom}(\mathbb{T}_k, \mathbb{C}) \simeq M_k$ (on a un énoncé semblable pour M_k^0).

Preuve : Soit $f \in M_k$ orthogonale à $\mathbb{T}_k$. On a alors $a_1(tf) = 0$ pour tout $t \in \mathbb{T}_k$. En particulier, $a_1(T_n f) = 0$ pour tout $n \ge 1$, donc $a_n(f) = 0$ pour tout $n \ge 1$, donc $f = 0$ (pour un poids non nul, les fonctions constantes non nulles ne sont pas des formes modulaires). Réciproquement, soit $t \in \mathbb{T}_k$ orthogonal à M_k. Alors $a_1(tf) = 0$ pour toute forme modulaire f de poids k, et donc $a_1(tT_n f) = 0$ pour tout $n \ge 1$ et tout $f \in M_k$, et donc $a_1(T_n tf) = 0$ puis $a_n(tf) = 0$. On en déduit $tf = 0$ pour tout $f \in M_k$, et $t = 0$. □

Remarque : On peut considérer $\mathrm{Hom}(\mathbb{T}_k, A)$ où A est un anneau tel que $\mathbb{Z}$, $\mathbb{Q}$, $\overline{\mathbb{F}_p}$, $\mathbb{Q}_p$, *etc.*

Soit $f \in M_k^0$. On dit que f est primitive si f est propre pour tous les T_n, et $a_1(f) = 1$. Posons $f = \sum_{n\ge1} a_n q^n$. On a alors

$$\underbrace{T_n(f)}_{=a_n q+\cdots} = \underbrace{\lambda_n f}_{=\lambda_n q+\cdots},$$

donc $T_n(f) = a_n f$ pour tout $n \geq 1$. Alors,

$$\varphi : \begin{cases} \mathbb{T}_k \times M_k & \to & \mathbb{C} \\ (t, f) & \mapsto & a_1(tf) \end{cases}$$

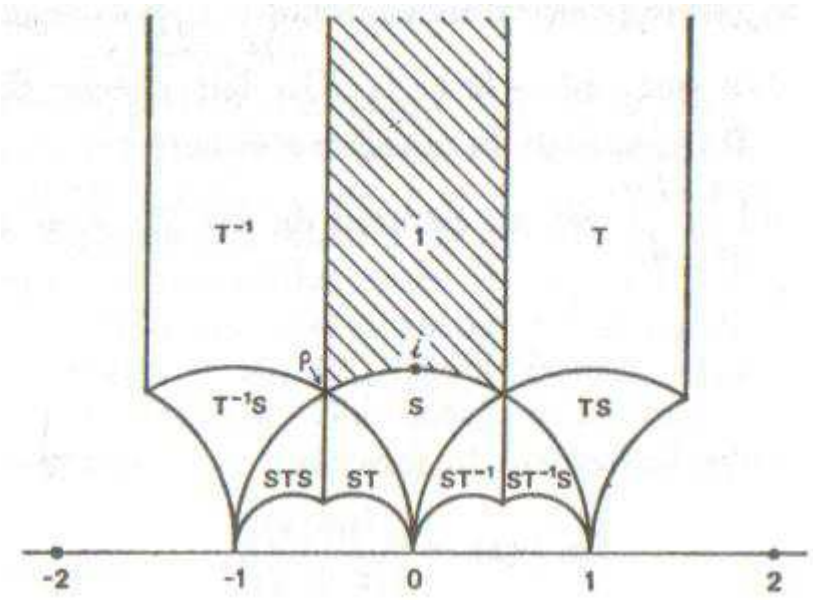
est un homomorphisme d'*anneaux* $*$.

Proposition 5 *On a* $T_n(G_k) = \sigma_{k-1}(n)G_k$, $n \geq 1$, $k \geq 4$.

Preuve : On se limite à $n = p$ premier, et on utilise la relation $\sigma_{k-1}(nm) = \sigma_{k-1}(n)\sigma_{k-1}(m)$, $n \wedge m = 1$, et la relation $\sigma_{k-1}(p^{r+1}) = \sigma_{k-1}(p)\sigma_{k-1}(p^r) + p \cdot p^{k-1}\sigma_{k-1}(p^{r-1})$, et ce qui en découle.

1.7 Le produit scalaire de Petersson

Soit $D \subseteq \mathcal{H}$. On dit que c'est un domaine fondamental pour l'action de $SL_2(\mathbb{Z})$ si c'est un ouvert formé de points dans des orbites distinctes sous $SL_2(\mathbb{Z})$, et si $\bar{D}$ contient un système de représentants de $SL_2(\mathbb{Z})\backslash\mathcal{H}$.



$D_0 = \{\tau \in \mathcal{H} || \tau| > 1, |\Re(\tau)| < \frac{1}{2}\}$ est un domaine fondamental. Soit $k > 0$, $f \in M_k$, $g \in M_k^0$, D un domaine fondamental de $\mathcal{H}$ pour $SL_2(\mathbb{Z})$. On pose

$$\langle f, g \rangle = \int_D f(\tau)\overline{g(\tau)}y^k \frac{\mathrm{d}x\mathrm{d}y}{y^2},$$

appelé produit scalaire de Petersson. Vérifions l'indépendance en D. On a

$$\frac{\mathrm{d}x\mathrm{d}y}{y^2} = \frac{i}{2}\frac{\mathrm{d}\tau \wedge \mathrm{d}\bar{\tau}}{(\Im(\tau))^2},$$

$*$. L'isomorphisme cité ci-dessus induit donc $\mathrm{Hom}_{ann}(\mathbb{T}_k, \mathbb{C}) \simeq \{\text{formes primitives}\}$.

avec $\tau = x + iy$, qui est invariante sous $SL_2(\mathbb{R})$ (et donc $SL_2(\mathbb{Z})$).

On a

$$\mathrm{d}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-2}(ad-bc)\mathrm{d}\tau,$$

et

$$\Im\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{(ad-bc)\Im(\tau)}{|c\tau+d|^2}$$

($\Im$ est « presque » modulaire). Alors, $\frac{\mathrm{d}x\mathrm{d}y}{y^2}$ est une forme différentielle $SL_2(\mathbb{Z})$-invariante.

Réinterprétons $f(\tau)\overline{g(\tau)}y^k$ en termes de réseaux : y est le volume de $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, donc le « volume » de $\mathbb{Z}+\tau\mathbb{Z}$ (*i.e.* le déterminant d'une base de ce $\mathbb{Z}$-module dans la base canonique), et $f(\tau)\overline{g(\tau)}y^k = f(\Lambda)\overline{g(\Lambda)}\mathrm{vol}(\Lambda)^k$. Comme $f(\lambda\Lambda) = \lambda^{-k}f(\Lambda)$, $\overline{g(\lambda\Lambda)} = \bar{\lambda}^{-k}\overline{g(\Lambda)}$ et $\mathrm{vol}(\lambda\Lambda) = |\lambda|^2\mathrm{vol}(\Lambda)$, on en déduit que $f(\tau)\overline{g(\tau)}y^k$ est homogène de poids 0 (donc ne dépend que de Λ dans $\mathbb{C}^*\backslash\mathscr{R}$). Or $\mathbb{C}^*\backslash\mathscr{R} \simeq SL_2(\mathbb{Z})\backslash\mathcal{H}$. Donc $\langle f, g\rangle$ ne dépend pas du choix de D. Vérifions la convergence, par exemple en prenant $D = D_0$ au voisinage de $i\infty$.

$\tau \mapsto f(\tau)$ est bornée sur D_0, car $f(iy) \to_{y\to\infty} f(i\infty)$ ($f \in M_k$). De plus, $g = \sum_{n\geq 1} a_n q^n$ donne $|g(\tau)| = O(e^{-2\pi y})$, d'où la convergence absolue.

$(f, g) \mapsto \langle f, g\rangle$ est une forme modulaire sesquilinéaire sur $M_k \times M_k^0$. Elle est non dégénérée sur M_k^0. Elle fait de M_k^0 un espace de Hilbert.

Proposition 6 *Soit $n \geq 1$. L'opérateur T_n est auto-adjoint pour $\langle , \rangle$.*

On le démontrera plus tard.

Corollaire 3 *Les opérateurs de Hecke sont simultanément diagonalisables, de valeurs propres réelles.*

L'aspect simultané provient du fait qu'ils commutent.

Corollaire 4 *Les formes primitives forment une base de M_k^0, et donc de M_k en ajoutant G_k, qui est orthogonale.*

1.8 Fonctions L

Soit $f = \sum_n a_n q^n$ une forme primitive de M_k^0.

Proposition 7 (Hardy) *On a $|a_n| \leq Cn^{k/2}$ où $C \geq 0$ est indépendante de n.*

Preuve : On a $a_n e^{-2\pi ny} = \int_0^1 f(x+iy)e^{-2i\pi nx}\mathrm{d}x$, et donc $|a_n|e^{-2\pi ny} \leq \int_0^1 |f(x+iy)|\mathrm{d}x$.

$|f(\tau)(\Im(\tau))^{k/2}|$ est invariant pour $SL_2(\mathbb{Z})$, donc est bornée par sa valeur sur D_0. Donc elle est bornée, car $|f(iy)| = O(e^{-2\pi y})$ quand $y \to \infty$. Donc il existe $c_1 > 0$ telle que $|f(\tau)(\Im(\tau))^{k/2}| \leq c_1$. On a donc

$$|a_n e^{-2\pi ny}| \leq \int_0^1 c_1 y^{-k/2}\mathrm{d}x = c_1 y^{-k/2},$$

d'où le résultat voulu en prenant $y = \frac{1}{n}$. □

Remarque : Deligne a montré (conjecture de Ramanujan-Petersson) que $|a_n| \leq n^{\frac{k-1}{2}}\sigma_0(n)$ avec $a_0 = 1$ (pour f primitive au moins). Considérons la série de Dirichlet $L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $s \in \mathbb{C}$. Comme $|a_n| = O(n^{k/2})$, cette série converge absolument pour $\Re(s - k/2) > 1$, donc pour $\Re(s) > \frac{k}{2} + 1$ (et même $\Re(s) > \frac{k+1}{2}$ d'après Deligne).

Proposition 8 (Produit eulérien) *On a*

$$L(f,s) = \prod_{p\in\mathbb{P}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}, \forall \Re(s) \geq \frac{k}{2} + 1.$$

Preuve : Comme f est primitive, on a $a_n a_m = a_{nm}$ pour n et m premiers entre eux, et $a_{p^{r+1}} = a_p a_{p^r} - p^{k-1} a_{p^{r-1}}$ pour p premier et $r \geq 1$. On a donc $L(f,s) = \prod_{p\in\mathbb{P}} \sum_{r\geq 0} \frac{a_{p^r}}{p^{rs}}$, et il reste à montrer que $(1 - a_p p^{-s} + p^{k-1-2s}) \sum_{r\geq 0} \frac{a_{p^r}}{p^{rs}} = 1$, ce qu'un calcul sommaire fournit. □

À présent, multiplions $L(f,s)$ par un facteur supplémentaire : soit $\Lambda(f,s) = \Gamma(s)(2\pi)^{-s} L(f,s)$, la fonction L complétée.

Théorème 9 *La fonction $s \mapsto \Lambda(f,s)$ admet un prolongement holomorphe à $\mathbb{C}$, et pour tout $s \in \mathbb{C}$, on a $\Lambda(f, k-s) = (-1)^{k/2}\Lambda(f,s)$.*

Remarque : Soit $(a_p)_{p\in Pre}$ une famille de nombres complexes tels que $|a_p| = O(n^{(k-1)/2})$. Alors, le produit $\prod_{p\in Pre} \frac{1}{1-a_p p^{-s}+p^{k-1-2s}}$ a aucune raison de se prolonger à $\mathbb{C}$.

Preuve : Considérons l'intégrale $\int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y^s}$. Comme $f(iy) = O(e^{-2\pi y})$ quand $y \to \infty$, et que $f\left(\frac{i}{y}\right) = (-1)^{k/2} y^k f(iy) = O(e^{-2\pi y})$ quand $y \to \infty$, l'intégrale converge. La fonction $s \mapsto \int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y}$ est analytique en s. On a :

$$\int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y} = \int_0^\infty \sum_{n\geq 1} a_n e^{-2\pi n y} y^s \frac{\mathrm{d}y}{y} = \sum_{n\geq 1} a_n \int_0^\infty e^{-2\pi n y} y^s \frac{\mathrm{d}y}{y},$$

et le changement de variable $u = 2\pi n y$ fournit

$$\int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y} = \sum_{n\geq 1} a_n \int_0^\infty e^{-u} (2\pi n)^{-s} u^s \frac{\mathrm{d}u}{u} = (2\pi)^{-s} \sum_{n\geq 1} \frac{a_n}{n^s} \int_0^\infty e^{-u} u^s \frac{\mathrm{d}u}{u} = \Lambda(f,s).$$

De plus,

$$\Lambda(f,s) = \int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y} = \int_0^\infty (-1)^{k/2} y^{-k} f\left(\frac{i}{y}\right) y^s \frac{\mathrm{d}y}{y} \overset{u=\frac{1}{y}}{=} \int_0^\infty (-1)^{k/2} u^{k-1} f(iu) \frac{\mathrm{d}u}{u} = (-1)^{k/2}\Lambda(f, k-s). \square$$

Une question naturelle en théorie des nombres est : où $s \mapsto \Lambda(f,s)$ s'annule-t-elle ? Forcément dans la bande critique ; la bande critique associée à $s \mapsto \Lambda(f,s)$ est la région du plan $\frac{k-1}{2} \leq \Re(s) \leq \frac{k+1}{2}$, la droite critique est $\Re(s) = \frac{k}{2}$, et les entiers critiques sont 1, 2, *etc.*, jusqu'à $k-1$. C'est le produit eulérien qui assure que $\Lambda(f,\cdot)$ ne s'annule pas pour $\Re(s) > \frac{k+1}{2}$.

Rappel : On a $G_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. On pose

$$L(G_k, s) = \sum_{n\geq 1} \frac{\sigma_{k-1}(n)}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-\sigma_{k-1}(p)p^{-s}+p^{k-1-2s}} = \prod_{p\in\mathbb{P}} \frac{1}{(1-p^{-s})(1-p^{k-1-s})} = \zeta(s)\zeta(s-k+1),$$

donc $L(G_k,\cdot)$ admet un prolongement méromorphe à $\mathbb{C}$. De plus, on a l'équation fonctionnelle $\Lambda(G_k,s) = (-1)^{k/2}\Lambda(G_k, k-s)$. On peut l'établir en utilisant $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ qui vérifie $Z(1-s) = Z(s)$ †

1.9 Le polynôme des périodes

En vue de calculer les formes modulaires (les valeurs des opérateurs de Hecke, *etc.*), et de comprendre $L(f,n)$ pour f primitive, n un entier critique, $1 \leq n \leq k-1$ (nature transcendante, signification arithmétique...), on introduit le polynôme des périodes comme suit :

Soit $k > 0$. Posons $w = k-2$. Soit $f \in M_k^0$. Le polynôme des périodes de f est défini par

$$r_f(X) = \int_0^{i\infty} f(\tau)(X-\tau)^w \mathrm{d}\tau = \sum_{j=0}^{w} i^{-j} \binom{w}{j} r_j(f) X^{w-j} \in \mathbb{C}[X]$$

avec $r_j(f) = \int_0^{\infty} f(it)t^j \mathrm{d}t = \Lambda(f, j+1) = j!(2\pi)^{-j-1}L(f,j+1)$. On pose $r(f) = r^+(f) + r^-(f)$ les parties paire et impaire.

Exemple : Si $f = \Delta$ ($k = 12, w = 10$), il existe $\Omega_+ \in \mathbb{R}$, $\Omega_- \in \mathbb{R}$ tels que :

j	0 ou 10	1 ou 9	2 ou 8	3 ou 7	4 ou 6	5
$r_j(\Delta)$	$\frac{192}{691}\Omega_+$	$\frac{384}{5}\Omega_-$	$\frac{16}{135}\Omega_+$	$40\Omega_-$	$\frac{8}{105}\Omega_+$	$32\Omega_-$

On a $\Omega_+ \simeq 0,021446\ldots$, et $\Omega_- = 0,000048\cdots i$.

Posons $\mathbb{C}[X]_w = \{P \in \mathbb{C}[X] | \deg(P) \leq w\}$. Pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $P \in \mathbb{C}[X]_w$, on pose $P|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}(X) = (cX+d)^w P\left(\frac{aX+b}{cX+d}\right) \in \mathbb{C}[X]$. On a

$$r(f)|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}(X) = \int_0^{i\infty} f(\tau)(aX+b-\tau(cX+d))^w \mathrm{d}\tau = \int_0^{i\infty} (-c\tau+a)^k f(\tau) \left(X - \frac{-b+d\tau}{-c\tau+a}\right)^w \frac{\mathrm{d}\tau}{(-c\tau+a)^2}$$

En prenant $\sigma = \gamma^{-1}\tau$, on a $r(f)|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}(X) = \int_{\gamma^{-1}0}^{\gamma^{-1}i\infty} f(\tau)(X-\tau)^w \mathrm{d}\tau$.

Posons $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $U = ST = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ et $U^3 = I_2$.

Proposition 9 *On a $r(f) + r(f)|_S = 0$, et $r(f) + r(f)|_U + r(f)|_{U^2} = 0$.*

Preuve : On a $r(f) + r(f)|_S = \int_0^{\infty} f(\tau)(X-\tau)^w \mathrm{d}\tau + \underbrace{\int_{S^{-1}0}^{S^{-1}\infty}}_{=\int_{\infty}^{0}} f(\tau)(X-\tau)^w \mathrm{d}\tau = 0$.

†. Note personnelle : l'égalité $L(G_k,s) = \zeta(s)\zeta(s-k+1)$ se déduit aisément de la formule $\sum_{n\geq 1}\frac{a_n}{n^s}\sum_{n\geq 1}\frac{b_n}{n^s} = \sum_{n\geq 1}\frac{(a*b)(n)}{n^s}$, où $(a*b)(n) = \sum_{d|n} a(d)b(n/d)$, appliqué à $\sigma_{k-1} = id^{k-1} * 1$.

Enfin, $r(f)+r(f)|_U+r(f)|_{U^2}=\int_0^\infty+\int_\infty^1+\int_1^0=0$. □

Bref, on a défini $r: M_k^0 \to \{P\in\mathbb{C}[X]_w | P+P|_S=0, P+P|_U+P|_{U^2}\}$. Étudions l'injectivité, la surjectivité de r, r^+ et r^-.

1.10 Cohomologie de $SL_2(\mathbb{Z})$

Soit G un groupe. Soit M un G-module à droite. On considère $H^0(G,M) = M^G = \{m\in M | \forall g\in G, m\cdot g = m\}$. Si on a une suite exacte courte de G-modules :

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0\ ,$$

on a :

$$0\longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \longrightarrow H^1(G,M')\longrightarrow H^1(G,M)\longrightarrow H^1(G,M'')\longrightarrow H^2(G,M')\to\cdots$$

pour mesurer le défaut de surjectivité.

Explicitement, on construit $H^1(G,M)$ ainsi : $H^1(G,M)=Z^1(G,M)/B^1(G,M)$, où $Z^1(G,M)=\{\varphi: G\to M | \forall g,h\in G, \varphi(gh)=\varphi(g)h+\varphi(h)\}$ est l'ensemble des 1-cocycles, et $B^1(G,M)=\{\varphi: G\to M | \exists m\in M; \forall g\in G, \varphi(g)=m\cdot g-m\}$ est l'ensemble des 1-cobords. Considérons le cas de $G=SL_2(\mathbb{Z})$. On a quelques exemples de $SL_2(\mathbb{Z})$-modules : $\mathbb{C}[X]_w$ avec l'action $(P,\gamma)\mapsto P|_\gamma$, ou encore $\mathbb{C}[\Gamma\backslash SL_2(\mathbb{Z})]$ pour $\Gamma\subseteq SL_2(\mathbb{Z})$.

Remarque : Si G est engendré par $g_1,\ldots,g_k$, un 1-cocycle est déterminé par ses valeurs en $g_1,\ldots,g_k$. On peut aussi remplacer $\mathbb{C}$ par n'importe quel anneau commutatif ci-dessus.

Théorème 10 *Soit M un $K[SL_2(\mathbb{Z})]$-module, où K est un corps de caractéristique différente de 2 et 3, tel que $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ opère trivialement sur M. On a un isomorphisme de K-espaces vectoriels*

$$H^1(SL_2(\mathbb{Z}),M)\simeq M/(M^S+M^U),$$

avec $M^S=\{m\in M | m\cdot S=m\}$ (de même pour définir M^U).

Preuve : Considérons $\Lambda : \begin{cases} Z^1(SL_2(\mathbb{Z}),M) & \to & \ker(1+S)\times\ker(1+U+U^2) \\ \varphi & \mapsto & (\varphi(S),\varphi(U)) \end{cases}$,

où $\ker(1+S)=\{m\in M | m\cdot(1+S)=0\}$, de même pour $\ker(1+U+U^2)$. On a $\varphi(I_2)=0$, et donc $\varphi(-I_2)=0$. On a de plus $0=\varphi(S^2)=\varphi(S)\varphi(1+S)$ et $0=\varphi(U^3)=\varphi(U)U^2+\varphi(U)U+\varphi(U)=\varphi(U)(U^2+U+1)$.

Comme $PSL_2(\mathbb{Z})$ est le produit libre des sous-groupes engendrés par S et U, cette application est surjective. Elle est injective car S et U engendrent $SL_2(\mathbb{Z})$. Comme S est une symétrie, on a $\ker(1+S)=\mathrm{im}(1-S)=M(1-S)\simeq M/M^S$ *via* $m+M^S\mapsto m(1-S)$ (on utilise ici la caractéristique différente de 2). De même, $\ker(1+U+U^2)=M(1-U)\simeq M/M^U$ *via* $m+M^U\mapsto m(1-U)$ (là encore, la caractéristique 3 est à éviter, sinon $\ker(1-U^3)=\ker((1-U)^3)\neq\ker(1+U+U^2)\oplus\ker(1-U)$).

Or $\Lambda(B^1(SL_2(\mathbb{Z},M)))$ est l'image diagonale (notée Δ) de M dans $M/M^S \times M/M^U$. En effet,

$$\Lambda(B^1(SL_2(\mathbb{Z},M))) = \{\varphi : SL_2(\mathbb{Z}) \to M | \exists m \in M; \varphi(S) = m\cdot S - m, \varphi(U) = m\cdot U - m\}$$

$$= \{\varphi : SL_2(\mathbb{Z}) \to M | \exists m \in M; \varphi(S) = m(1-S), \varphi(U) = m(1-U)\}.$$

Il reste à calculer $(M/M^S \times M/M^U)/\Delta$. Considérons l'application surjective

$$f : \begin{cases} M/M^S \times M/M^U & \to & M/(M^S + M^U) \\ (m_1 + M^S, m_2 + M^U) & \mapsto & m_1 - m_2 + M^S + M^U \end{cases}.$$

Montrons que son noyau égale Δ. Soient a, $b \in M^2$ tels que $a - b \in M^S + M^U$. Il existe alors a' et b' dans M^S et M^U respectivement, de sorte que $a-b = a'-b'$. On a donc $a - a' = b - b' = c$. On a $\begin{cases} a + M^S &=& c + M^S \\ b + M^U &=& c + M^U \end{cases}$, donc $(a + M^S, b + M^U) = (c + M^S, c + M^U) \in \Delta$. □

Application Posons $V_k = \mathbb{C}[X]_w$ comme $SL_2(\mathbb{Z})$-module. On a $H^1(SL_2(\mathbb{Z}), V_k) = \mathbb{C}[X]_w/(\mathbb{C}[X]_w^S + \mathbb{C}[X]_w^U)$.

Rappel : $< T >= \mathrm{Stab}_{PSL_2(\mathbb{Z})}(\infty)$. On pose

$$H^1_{\mathrm{par}}(SL_2(\mathbb{Z}), M) = \{\varphi \in Z^1(SL_2(\mathbb{Z}), M) | \varphi(T) = 0\}/B^1(SL_2(\mathbb{Z}), M) \subseteq H^1(SL_2(\mathbb{Z}), M)$$

la cohomologie parabolique.

Soit $f \in M_k^0$. Le 1-cocycle associé est $\begin{array}{ccc} SL_2(\mathbb{Z}) & \to & V_k \\ \gamma & \mapsto & \int_{\gamma^{-1}\infty}^{\infty} f(\tau)(X-\tau)^w \mathrm{d}\tau \end{array}$ (cocycle parabolique). Un 1-cocycle parabolique est déterminé par sa valeur en S, car sa valeur en T est nulle. Cette valeur en S est $r(f)$.

Remarque : La classe dans $H^1(SL_2(\mathbb{Z}), V_k)$ de $\gamma \mapsto \int_{\gamma^{-1}\tau_0}^{\tau_0} f(\tau)(X-\tau)^w \mathrm{d}\tau$ ne dépend pas de $\tau_0 \in \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Théorème 11 *On a*

$$\dim(H^1(SL_2(\mathbb{Z}), \mathbb{C}[X]_w)) = 2\dim(M_k^0)+1 = 2\dim(M_k)-1 = \dim(M_k)+\dim(M_k^0).$$

Preuve : On a $\dim(V_k) = w + 1 = k - 1$, et

$$\dim(H^1(SL_2(\mathbb{Z}), V_k)) = \dim(V_k/(V_k^S+V_k^U)) = w+1-\dim(V_k^S)-\dim(V_k^U)+\dim(V_k^S \cap V_k^U).$$

Or $V_k^S \cap V_k^U = V_k^{SL_2(\mathbb{Z})}$ est l'ensemble des polynômes constants de V_k (invariants sous l'action), c'est-à-dire $\mathbb{C}$ si $w = 0$ ($k = 2$), ou $\{0\}$ dans les autres cas.

Déterminons V_k^S. Soit $P = \sum_i a_i X^i \in V_k$. On a $P|_S = X^w \sum_i a_i \left(\frac{-1}{X}\right)^i = \sum_i (-1)^i a_i X^{w-i}$, donc $P|_S = P$ si, et seulement si $a_i = (-1)^i a_{w-i}$ pour tout i entre 0 et w. Alors :

$$\dim(V_k^S) = \begin{cases} \frac{w}{2} + 1 & \text{si } \frac{w}{2} \text{ impair } (k \equiv 2 \mod 4) \\ \frac{w}{2} & \text{si } \frac{w}{2} \text{ pair } (4|k) \end{cases}$$

Déterminons V_k^U. Soit $\rho \neq 1$ une racine cubique de l'unité dans $\mathbb{C}$. Pour $0 \leq a \leq w$, posons $Q_a = (X-\rho)^a (X-\bar{\rho})^{w-a}$. On a

$$Q_a|_U = (X+1)^w \left(\frac{-1}{X+1} - \rho\right)^a \left(\frac{-1}{X+1} - \bar{\rho}\right)^{w-a} = (-1-\rho X-\rho)^a (-1-\bar{\rho}X-\bar{\rho})^{w-a}$$

$$= \rho^a (-1)^a \left(X + \frac{1+\rho}{\rho}\right)^a \bar{\rho}^{w-a} (-1)^{w-a} \left(X + \frac{1+\bar{\rho}}{\bar{\rho}}\right)^{w-a} = \rho^a \bar{\rho}^{w-a} (X-\rho)^a (X-\bar{\rho})^{w-a} = \rho^a \bar{\rho}^{w-a} Q_a.$$

On a une base de vecteurs propres pour U. Comptons la multiplicité de 1 : M^U a pour base $\{Q_a | \rho^a \bar{\rho}^{w-a} = 1\} = \{Q_a | \rho^a \rho^{a-w} = 1\} = \{Q_a | 2a \equiv w \mod 3\}$: il y a $E\left(\frac{w}{3}\right)$ tels éléments entiers a entre 0 et w si $w \equiv 1 \mod 3$ $(3|k)$, et $E\left(\frac{w}{3}\right)+1$ si $w \not\equiv 1 \mod 3$ (*i.e.* $3 \not| \, k$).

On vérifie ensuite que $\dim(M_k) + \dim(M_k^0) = \dim(H^1(SL_2(\mathbb{Z}), V_k))$.

Proposition 10 *On a* $\dim(M_k) + \dim(M_k^0) = \dim(\ker(1+S) \cap \ker(1+U+U^2))$.

Preuve : On a

$$\dim(\ker(1+S) \cap \ker(1+U+U^2)) = \dim(\ker(1+S)) + \dim(\ker(1+U+U^2)) - \dim(\ker(1+S) + \ker(1+U+U^2)).$$

Or $\ker(1+S) = \mathrm{im}(1-S)$ et $\ker(1+U+U^2) = \mathrm{im}(1-U)$, et

$$\begin{cases} \dim(\mathrm{im}(1-S)) &= \dim(V_k) - \dim(\ker(1-S)) = w+1-\dim(V_k^S). \\ \dim(\mathrm{im}(1-U)) &= w+1-\dim(V_k^U). \end{cases}$$

Il reste à montrer que

$$\dim(\ker(1+S) \cap \ker(1+U+U^2)) = w+1,$$

i.e. $\ker(1+S) + \ker(1+U+U^2) = V_k$, ou encore $V_k = \mathrm{im}(S-1) + \mathrm{im}(U-1)$.

On a $\mathrm{im}(S-1) + \mathrm{im}(U-1) = \mathrm{im}(S-1) + \mathrm{im}(S(T-1)+S-1)$
$= \mathrm{im}(S-1) + \mathrm{im}(S(T-1)) = \mathrm{im}(S-1) + \mathrm{im}(T-1) \supseteq \mathrm{im}(T-1)$.

Pour $P \in V_k$, on a $P|_{T-1} = P(X+1) - P(X)$ de degré strictement inférieur à w. Donc $\begin{matrix} V_k & \to & V_k \\ P & \mapsto & P|_T - P \end{matrix}$ est d'image dans les polynômes de degré strictement inférieur à w, et de noyau les polynômes constants. C'est donc $\{P \in V_k | \deg(P) < w\}$. Comme $X^w - 1 = X^w(1-S) \in \mathrm{im}(S-1)$ et $X^w - 1 \notin \ker(T-1)$, on a bien $\mathrm{im}(T-1) + \mathrm{im}(S-1) \not\subseteq \ker(T-1)$, et donc $V_k = \mathrm{im}(T-1) + \mathrm{im}(S-1)$. □

Résumé : On a

$$\begin{array}{ccc} M_k \supseteq M_k^0 & \xrightarrow{\quad r \quad} & \ker(1+S) \cap \ker(1+U+U^2) \\ \downarrow & \nearrow_{\text{restriction à } S \text{ d'un cocycle}} & \\ H^1(SL_2(\mathbb{Z}), V_k) \supseteq H^1_{\mathrm{par}}(SL_2(\mathbb{Z}), V_k) & & \end{array}$$

Variante : on peut considérer $M_k^0 + \overline{M_k^0} \xrightarrow{r} \ker(1+S) \cap \ker(1+U+U^2)$, où $\overline{M_k^0}$ est l'ensemble des formes modulaires *anti*-holomorphes sur $\mathcal{H}$, de poids k, paraboliques. On peut montrer que r est injective, d'image un hyperplan ne contenant pas $X^w - 1$ (on peut vérifier que $X^w - 1 \in \ker(1+S) \cap \ker(1+U+U^2)$).

Problème : Déterminer l'image de r.

1.11 Polynômes des périodes et produit scalaire

Soient f et $g \in M_k^0$. On a

$$\langle f,g\rangle = \int_{SL_2(\mathbb{Z})\backslash\mathcal{H}} f(\tau)\overline{g(\tau)}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2} = \frac{1}{(2i)^{k-1}}\int_{SL_2(\mathbb{Z})\backslash\mathcal{H}} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\wedge\mathrm{d}\bar\tau$$

Théorème 12 *On a* $\langle f,g\rangle = -\frac{1}{6(2i)^{k-1}}\sum_{j,l}(i^{l-j}-i^{j-l})r_j(f)\overline{r_l(g)}$.

Corollaire 5 *$f\mapsto r(f)$, $f\mapsto r^+(f)$ et $f\mapsto r^-(f)$ sont injectives.*

Preuve : En effet, la forme bilinéaire sur V_k définie par la formule du théorème vérifie que V_k^+ est orthogonal à V_k^+, et que V_k^- est orthogonal à V_k^-. Alors, si $r^+(f)=0$, on a $\langle f,f\rangle = 0$ et donc $f=0$. □

Preuve du théorème : Posons $F(\tau)=\int_\infty^\tau f(u)(u-\bar\tau)^w\mathrm{d}u$. Ainsi, $\frac{\partial F}{\partial\tau} = f(\tau)(\tau-\bar\tau)^w$, et $\mathrm{d}(F\bar g\mathrm{d}\bar\tau) = \mathrm{d}F\bar g\mathrm{d}\bar\tau = f(\tau)(\tau-\bar\tau)^w\overline{g(\tau)}\mathrm{d}\tau\mathrm{d}\bar\tau$.

On utilise le théorème de Stokes : $\int_{D_0} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\mathrm{d}\bar\tau = \int_{M-TM+N-SN} F(\tau)\overline{g(\tau)}\mathrm{d}\bar\tau$, où M désigne le côté « gauche » de D_0 et N le demi-arc de cercle du côté $\Re(s)\le 0$ (S et T désignent toujours les mêmes matrices) ; un dessin est nécessaire. Bref, $\int_{M-TM+N-SN} = \int_{M-TM} + \int_{N-SN}$.

Lemme 1 *Pour $\gamma\in SL_2(\mathbb{Z})$, on a $F(\gamma\tau) = (c\bar\tau+d)^{-w}F(\tau) + \int_\infty^{\gamma\infty} f(u)(u-\gamma\bar\tau)^w\mathrm{d}u$.*

Preuve du lemme : On a $F(\gamma\tau) = \int_\infty^{\gamma\tau} f(u)(u-\gamma\bar\tau)^w\mathrm{d}u = \int_{\gamma\infty}^{\gamma\tau} + \int_\infty^{\gamma\infty} \overset{\gamma v=u}{=} \int_\infty^\tau f(\gamma v)(\gamma v-\gamma\bar\tau)\mathrm{d}\gamma v + \int_\infty^{\gamma\infty} = (c\bar\tau+d)^{-w}\int_\infty^\tau f(v)(v-\bar\tau)^w\mathrm{d}v + \int_\infty^{\gamma\infty}$
$= (c\bar\tau+d)F(\tau) + \int_\infty^{\gamma\infty} f(u)(u-\gamma\bar\tau)\mathrm{d}u$. □

Lemme 2 *On a, pour $\mathscr{C}$ un chemin de $\mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$ et $\gamma\in SL_2(\mathbb{Z})$, $\int_{\mathscr{C}-\gamma(\mathscr{C})} F(\tau)\overline{g(\tau)}\mathrm{d}\bar\tau = \int_{\mathscr{C}}\int_\infty^{\gamma^{-1}\infty} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\wedge\mathrm{d}\bar\tau$.*

Preuve du lemme : On a $\int_{\gamma(\mathscr{C})} F(\tau)\overline{g(\tau)}\mathrm{d}\bar\tau = \int_{\mathscr{C}} F(\gamma\tau)\overline{g(\gamma\tau)}\overline{\mathrm{d}\gamma\tau} = \int_{\mathscr{C}} F(\tau)(c\bar\tau+d)^{-w}\overline{g(\gamma\tau)}\overline{\mathrm{d}\gamma\tau} + \int_{\mathscr{C}}\int_\infty^{\gamma\infty} f(\tau)\overline{g(\tau)}(\tau-\overline{\gamma\tau})(c\bar\tau+d)^w\mathrm{d}\tau\mathrm{d}\bar\tau = \int_{\mathscr{C}} F(\tau)\overline{g(\tau)}\mathrm{d}\bar\tau + \int_{\mathscr{C}}\int_\infty^{\gamma\infty} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\mathrm{d}\bar\tau$ ‡. □

Revenons à $\langle f,g\rangle$. On a

$$\langle f,g\rangle = \int_M\int_\infty^{T\infty} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\mathrm{d}\bar\tau + \int_N\int_\infty^{S\infty} f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\mathrm{d}\bar\tau$$

$$= \int_i^\rho\int_\infty^0 f(\tau)\overline{g(\tau)}(\tau-\bar\tau)^w\mathrm{d}\tau\mathrm{d}\bar\tau = J - I,$$

où

$$I = \int_i^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau, \text{ et}$$

‡. Vérifiez les signes, il y a peut-être une erreur.

$$J = \int_\rho^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau.$$

On utilise la formule $\int_a^b f(\tau)P(\tau)\mathrm{d}\tau = \int_{\gamma^{-1}a}^{\gamma^{-1}b} f(\tau)P|_\gamma(\tau)\mathrm{d}\tau$. D'où :

$$2I = 2\int_i^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau = \int_i^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau + \int_{Si}^{S\infty} f(\tau)\underbrace{\overline{r(g)|_S}}_{=-\overline{r(g)}}(\tau)\mathrm{d}\tau = \int_0^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau.$$

De même, des calculs lourds mais sans mystère, utilisant la formule $r(g)+r(g)|_U+r(g)|_U^2 = 0$, montrent que

$$3J = \int_0^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau - \int_0^\infty f(\tau)\overline{r(g)|_U}(\tau)\mathrm{d}\tau.$$

D'où :

$$I-J = \frac{1}{6}\int_0^\infty f(\tau)\overline{r(g)}(\tau)\mathrm{d}\tau + \frac{1}{3}\int_0^\infty f(\tau)\overline{r(g)|_U}(\tau)\mathrm{d}\tau = -\frac{1}{6}\left(\int_0^\infty f(\tau)(\overline{r(g)|_{U^2}} - \overline{r(g)|_U})(\tau)\mathrm{d}\tau\right).$$

Remarque : On a $\int_0^\infty f(\tau)\overline{r(g)|_\gamma}(\tau)\mathrm{d}\tau = \int_0^\infty r(f)|_{\gamma^{-1}}(\tau)\overline{g(\tau)}\mathrm{d}\tau$. D'où :

$$I - J = -\frac{1}{6}\int_0^\infty r(f)|_U\overline{g(\tau)}\mathrm{d}\bar\tau + \frac{1}{6}\int_0^\infty f(\tau)\overline{r(g)}|_U\mathrm{d}\tau.$$

Comme $U = ST$ et $S0 = \infty$, on a

$$I - J = -\frac{1}{6}\int_{S0}^{S\infty} r(f)|_T(\bar\tau)\overline{g(\tau)}\mathrm{d}\bar\tau + \frac{1}{6}\int_{S0}^{S\infty} f(\tau)\overline{r(g)|_T}(\tau)\mathrm{d}\bar\tau.$$

Or $r(f)|_T(\bar\tau) = r(f)(\bar\tau+1) = \sum_{j=0}^w i^{-j}\binom{w}{j} r_j(f)\sum_{l=0}^{w-j}\binom{w-j}{l}\bar\tau^l$. D'où

$$\int_0^\infty r(f)|_T(\bar\tau)\overline{g(\tau)}\mathrm{d}\bar\tau = \sum_{j=0}^w\sum_{l=0}^{w-j} i^{-j}\binom{w}{j} r_j(f)\sum_{l=0}^{w-j}\binom{w-j}{l}\overline{r_l(g)}i^l.$$

On trouve semblablement une expression pour la seconde intégrale, ce qui fournit le résultat de l'énoncé du théorème. □

Conclusion : Pour étudier les formes modulaires, on peut se ramener à V_k, ou plutôt $\ker(1+S)\cap\ker(1+U+U^2)$ dans V_k.

1.12 Application aux opérateurs de Hecke

Soit $k \geq 2$. Pour $n \geq 1$, l'opérateur T_n opère sur M_k et M_k^0. Notons $\mathbb{T}_k$ le sous-anneau de $\mathrm{End}(M_k)$ engendré par les T_n $(n \geq 1)$, et $\mathbb{T}_k^0$ le sous-anneau de $\mathrm{End}(M_k^0)$ engendré par les T_n $(n \geq 1)$.

Théorème 13 *Les valeurs propres de T_n sur M_k^0 sont des entiers algébriques de degré inférieur ou égal à $\dim(M_k^0)$. De même pour tout $T \in \mathbb{T}_k$.*

Corollaire 6 *Les anneaux $\mathbb{T}_k$ et $\mathbb{T}_k^0$ sont isomorphes à un sous-anneau du produit d'anneaux d'entiers de corps de nombres.*

Preuve : En effet, sous réserve de démonstration, soit $\mathscr{P} = \{\text{formes primitives de } M_k\}$. Pour chaque $f \in \mathscr{P}$, considérons $\psi_f : \begin{cases} \mathbb{T}_k & \to & \mathbb{C} \\ t & \mapsto & a_1(tf) \end{cases}$. C'est un homomorphisme d'anneaux à valeurs dans $\bar{\mathbb{Z}}$ (ensemble des entiers algébriques de $\mathbb{C}$). Donc $\psi_f(\mathbb{T}_k)$ est un sous-anneau $\mathscr{O}_f$ de $\mathbb{C}$, contenu dans $\bar{\mathbb{Z}}$.

Posons $K_f = \mathrm{Frac}(\mathscr{O}_f)$, dont tous les éléments sont de degré inférieur ou égal à $\dim(M_k^0)$. Donc $[K_f : \mathbb{Q}] \le \dim(M_k^0)$. $\psi : \begin{cases} \mathbb{T}_k & \to & \prod_{f\in\mathscr{P}} K_f \\ t & \mapsto & (\psi_f(t))_{f\in\mathscr{P}} \end{cases}$ permet l'identification voulue. □

Corollaire 7 *Soit f une forme primitive, et soit $\sigma \in \mathrm{Aut}(\mathbb{C})$. La série $\sum_{n\ge1} \sigma(a_n)q^n$ est le q-développement d'une forme primitive (conjuguée de f).*

Preuve : En effet, l'homomorphisme $\mathbb{C}$-linéaire $\mathrm{Hom}_{\text{groupes}}(\mathbb{T}_k, \mathbb{C}) \simeq M_k$ fait correspondre aux formes primitives les homomorphismes d'anneaux. Donc si $\psi \in \mathrm{Hom}_{\text{ann}}(\mathbb{T}_k, \mathbb{C})$, alors $\sigma \circ \psi \in \mathrm{Hom}_{\text{ann}}(\mathbb{T}_k, \mathbb{C})$. □

Si $f \in \sum_{n\ge1} a_n q^n$ est une forme primitive avec $K_f = \mathbb{Q}(a_1, a_2, \dots, a_n, \dots)$, elle possède $[K_f : \mathbb{Q}]$ conjuguées.

Fait expérimental : Dans tous les cas connus, il y a une seule classe de conjugaison de M_k^0. Est-ce toujours le cas ? (Spécifique à $SL_2(\mathbb{Z})$)

Cela résulterait du fait que les valeurs propres de T_n sont des entiers algébriques de degré $\dim(M_k^0)$.

Preuve du théorème : Montrons qu'il existe un sous-$\mathbb{Z}$-module $\mathscr{M}_k^0$ de M_k^0 tel que $M_k^0 = \mathscr{M}_k^0 \otimes_{\mathbb{Z}} \mathbb{C}$ et $\mathscr{M}_k^0$ stable par T_n. Considérons $\{f \in M_k^0 | r(f)^- \in \mathbb{Z}[X]\}$.

Proposition 11 *Soit $f \in M_k^0$ telle que $r(f) \in \mathbb{Z}[X]$. Alors $r(T_n(f)) \in \mathbb{Z}[X]$.*

Lemme 3 *On a $\int_{\gamma u}^{\gamma v} f(\tau)\tau^i \mathrm{d}\tau = \int_u^v f(\tau)(a\tau+b)^i(c\tau+d)^{w-i}\mathrm{d}\tau$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $u, v \in \mathbb{P}^1(\mathbb{Q})$, $0 \le i \le w = k-2$.*

On en déduit $\int_{\gamma_0}^{\gamma\infty} f(\tau)\tau^i \mathrm{d}\tau \in \sum_{j=0}^w \mathbb{Z} r_j(f)$.

Lemme 4 *On a $\int_u^v f(\tau)\tau^i \mathrm{d}\tau \in \sum_{j=0}^w \mathbb{Z} r_j(f)$.*

Preuve : On peut supposer $u = 0$ et $v \neq \infty$ (sinon, on a déjà un $r_j(f)$). Posons $v = \frac{p}{q}$ avec $p \wedge q = 1$ et $q > 0$. Raisonnons par récurrence sur $\max(|p|, q)$. Quitte à appliquer S, on peut supposer $|p| \ge q$ (en vertu du lemme précédent). Si $p \ge q$, on applique $\gamma = T$ et on a $T\frac{p}{q} = \frac{p+q}{q}$. On a

$$\int_0^{p/q} f(\tau)\tau^i \mathrm{d}\tau = \underbrace{\int_0^1 f(\tau)\tau^i \mathrm{d}\tau}_{=-\int_{V0}^{V\infty} f(\tau)\tau^i \mathrm{d}\tau} + \underbrace{\int_1^{p/q} f(\tau)\tau^i \mathrm{d}\tau}_{=\int_{T0}^{T\left(\frac{p}{q}-1\right)}} \in \sum_{j=0}^w \mathbb{Z} r_j(f)$$

par le lemme précédent et par récurrence (on a noté $V = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$). □

Démontrons enfin la proposition : on a

$$T_n(f)(\tau) = \sum_{d|n, b \bmod d} \frac{n^{k-1}}{d^k} f\left(\frac{n\tau}{d^2} + \frac{b}{a}\right)$$

et $r_i(T_n(f)) = \sum_{b,d} \int_0^\infty \frac{n^{k-1}}{d^k} f\left(\frac{n\tau}{d^2} + \frac{b}{a}\right) \tau^i \mathrm{d}\tau = \sum_{b,d} \frac{n^w}{d^w} \int_{\frac{b}{a}}^\infty f(\tau') \left(\frac{d^2\tau' - bd}{n}\right)^i \mathrm{d}\tau'$, combinaison linéaire entière des $r_j(f)$.

De plus, T_n respecte les parties paire et impaire des polynômes de périodes, *i.e.* $P(X) \mapsto P(-X)$ commute à T_n. Donc $\mathscr{M}_k^0 = \{f \in M_k^0 | r(f)^- \in \mathbb{Z}[X]\}$ est stable par T_n, et $\mathscr{M}_k^0 \otimes_{\mathbb{Z}} \mathbb{C} \simeq M_k^0$, d'où le théorème §. □

Corollaire 8 *Soit f une forme primitive de M_k^0. Il existe Ω_f^+ et Ω_f^- dans $\mathbb{C}$ tels que $\Lambda(f,i) \in \mathscr{O}_{K_f}\Omega_f^+$ pour i pair entre 1 et $k-1$, et $\Lambda(f,i) \in \mathscr{O}_{K_f}\Omega_f^-$ (pour i impair entre 1 et $k-1$).*

K_f dénote ici l'extension de $\mathbb{Q}$ engendrée par les coefficients du q-développement de f, et $\mathscr{O}_{K_f}$ son anneau des entiers. On pourrait remplacer $\mathscr{O}_{K_f}$ par $\mathscr{O}_f$, car $\mathscr{O}_f$ est d'indice fini dans $\mathscr{O}_{K_f}$. À noter que $\Lambda(f,i)$, pour $i \leq 0$ ou $i \geq k$, est de nature différente.

Preuve : En effet, il existe $g \in M_k^0$ telle que g est propre pour $\mathbb{T}_k^0$ avec les mêmes valeurs propres que f, et $r(g)^- \in K_f[X]$, et même $r(g)^- \in O_{K_f}[X]$. Il existe $\Omega_f^- \in \mathbb{C}$ tel que $f = \Omega_f^- g$. On a alors $r(f)^- = \Omega_f^- r(g)^-$. D'où le théorème pour i impair. De même pour i pair. □

Autre approche pour l'intégralité des valeurs propres de Hecke :

Proposition 12 *On a $\oplus_{k\geq 0} M_k = \mathbb{C}[E_4, E_6]$.*

On en déduit que $\mathbb{Z}[E_4, E_6]$ est une $\mathbb{Z}$-structure sur M_k, dont on peut vérifier qu'elle est stable par Hecke.

Pour exprimer $r(T_n(f))$ en fonction de n et de $r(f)$, on a la formule :

$$r(T_n(f)) = \sum_{\substack{a>b\geq 0 \\ d>c\geq 0 \\ ad+bc=n}} r_f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}(X) = \sum r_f\left(\frac{aX+b}{cX+d}\right)(cX+d)^w.$$

En particulier, pour $n = 2$: $r(T_2(f)) = r_f(2X) + r_f(2X+1) + r_f\left(\frac{X}{X+2}\right)(X+2)^w + r_f\left(\frac{X}{2}\right)2^w$.

§. Note personnelle : on a montré l'existence d'une $\mathbb{Z}$-structure sur M_k^0. En d'autres termes, on a trouvé une structure de $\mathbb{Z}$-module à M_k^0 de sorte que la base de ce $\mathbb{Z}$-module engendre M_k^0 sur $\mathbb{C}$. Alors, $\mathbb{T}_k \hookrightarrow \mathrm{End}(\mathscr{M}_k^0) \simeq \mathbb{Z}^r$. Les valeurs propres des T_n sont alors des entiers algébriques, car ce sont les racines des polynômes caractéristiques, lesquels sont à coefficients entiers (les coefficients matriciels des T_n sont entiers).

Compléments : On va démontrer que les T_n sont auto-adjoints pour $\langle , \rangle$. En effet, $SL_2(\mathbb{Z})\backslash\mathcal{H} \simeq \mathbb{C}^*\backslash\mathscr{R}$, *via* $\tau \mapsto \mathbb{Z}+\mathbb{Z}\tau$. La mesure de Haar de $\mathcal{H}$ s'envoie donc dans $\mathbb{C}^*\backslash\mathscr{R}$ pour donner $\mathrm{d}\mu$. Considérons

$$\mathscr{R}_n = \{(\Lambda, \Lambda') | \Lambda, \Lambda' \text{ réseaux avec } \Lambda' \subseteq \Lambda \text{ d'indice } n\}$$

(stable par l'action de $\mathbb{C}^*$). On a une involution sur $\mathbb{C}^*\backslash\mathscr{R}_n$, $W_n : (\Lambda, \Lambda') \mapsto (\Lambda', n\Lambda)$.

Notons $f : \begin{cases} \mathcal{H} & \to & \mathbb{C}^*\backslash\mathscr{R}_n \\ \tau & \mapsto & (\mathbb{Z}+\mathbb{Z}\tau, -n\tau\mathbb{Z}+\mathbb{Z}) \end{cases}$ et $g : \begin{cases} \mathcal{H} & \to & \mathcal{H} \\ \tau & \mapsto & -\frac{1}{n\tau} \end{cases}$. Alors, comme $(\mathbb{Z}+\mathbb{Z}\left(\frac{-1}{n\tau}\right), -n\left(\frac{-1}{n\tau}\right)\mathbb{Z}+\mathbb{Z}) \overset{W_n}{\mapsto} (\mathbb{Z}+\mathbb{Z}\tau, n\tau\mathbb{Z}+\mathbb{Z})$, le diagramme suivant commute :

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{g} & \mathcal{H} \\ \downarrow{\scriptstyle f} & & \downarrow \\ \mathbb{C}^*\backslash\mathscr{R}_n & \xrightarrow{W_n} & \mathbb{C}^*\backslash\mathscr{R}_n \\ \downarrow{\scriptstyle pr_1} & & \\ \mathbb{C}^*\backslash\mathscr{R} & & \end{array}$$

Comme $\frac{\mathrm{d}x\mathrm{d}y}{y^2}$ est $GL_2(\mathbb{R})$-invariante, elle induit une mesure $\mathrm{d}\mu_n$ W_n-invariante sur $\mathscr{R}_n$. Soient $f \in M_k^0$, $g \in M_k$. Alors, en notant F et G les fonctions de réseaux associées :

$$\langle f, g\rangle = \int_{\mathbb{C}^*\backslash\mathscr{R}} F(\Lambda)\overline{G(\Lambda)}\mathrm{vol}(\Lambda)^k \mathrm{d}\mu,$$

et donc

$$\langle T_n(f), g\rangle = n^{k-1} \int_{\mathbb{C}^*\backslash\mathscr{R}} \sum_{[\Lambda:\Lambda']=n} F(\Lambda')\overline{G(\Lambda)}\mathrm{vol}(\Lambda)^k \mathrm{d}\mu = n^{k-1} \int_{\mathbb{C}^*\backslash\mathscr{R}_n} F(\Lambda')\overline{G(\Lambda)}\mathrm{vol}(\Lambda)^k \mathrm{d}\mu$$

$$= n^{k-1} \int_{\mathbb{C}^*\backslash\mathscr{R}_n} F(n\Lambda)\overline{G(\Lambda')}\mathrm{vol}(\Lambda')^k \mathrm{d}\mu = n^{k-1} \int_{\mathbb{C}^*\backslash\mathscr{R}_n} n^{-k} F(\Lambda)\overline{G(\Lambda')} n^k \mathrm{vol}(\Lambda)^k \mathrm{d}\mu = \langle f, T_n(g)\rangle.$$

Remarque : On a $\mathbb{C}^*\backslash\mathscr{R} \simeq SL_2(\mathbb{Z})\backslash\mathcal{H}$ et $\mathbb{C}^*\backslash\mathscr{R}_n \simeq \Gamma_0(n)\backslash\mathcal{H}$ (si n est premier), où $\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}); n|c \right\}$.

Pourquoi les formes modulaires ? Exemple : Considérons $P = X^3 - X - 1$ de discriminant -23, et soit K son corps de décomposition sur $\mathbb{Q}$ (non ramifié en dehors de 23). On a $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_3$. On a $\mathfrak{S}_3 \subseteq GL_2(\mathbb{F}_{23})$ (engendré par $\begin{pmatrix} 12 & 15 \\ -15 & 12 \end{pmatrix}$ d'ordre 3 et $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ d'ordre 2), ce qui induit une représentation $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL_2(\mathbb{F}_{23})$. Soit l un nombre premier, alors $X^3 - X - 1$ est scindé dans $\mathbb{F}_l$ si, et seulement $\tau(l) \equiv 2 \mod 23$ (τ est ici la fonction de Ramanujan ; on a $\Delta = \sum \tau(n) q^n \equiv \sum_{m,n\in\mathbb{Z}} q^{m^2+mn+n^2} - \sum_{m,n\in\mathbb{Z}} q^{2m^2+mn+3n^2} \mod 23$) ; il est

irréductible dans $\mathbb{F}_l$ si, et seulement si $\tau(l) \equiv 1 \mod 23$, et a une seule racine dans $\mathbb{F}_l$ si, et seulement si $\tau(l) \equiv 0 \mod 23$.

Si $l \in \mathbb{P} \setminus \{23\}$, on a une substitution de Frobenius bien définie $\mathrm{Frob}_l \in \mathrm{Gal}(K/Q)$, à conjugaison près. Le polynôme caractéristique de $\rho(\mathrm{Frob}_l)$ est bien défini dans $\mathbb{F}_{23}[X]$, et est (théorème) $X^2 - \tau(l)X + l^{11} \mod 23$ ($l^{11} = \det(\mathrm{Frob_l})$ peut se déduire de la réciprocité quadratique).

Plus généralement, soit $K/\mathbb{Q}$ une extension galoisienne finie non ramifiée en dehors de $l_1, \ldots, l_n$, et soit $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL_2(\mathbb{F}_q)$ (q de caractéristique p). Pour $l \neq l_1, \ldots, l_n$, $\rho(\mathrm{Frob}_l)$ a pour polynôme caractéristique $X^2 - a_l X + b_l$. D'après Khare-Wintenberger, il existe une forme modulaire (pour $\Gamma_1(n)$, avec $n = \prod_{i=1}^n l_i^{\alpha_i}$) $f = \sum_n c_n q^n$ telle que $c_l \equiv a_l \mod p$ pour l premier différent des l_i.

2 Le langage adélique

Soit p un nombre premier. On suppose connues l'existence et les propriétés de l'anneau $\mathbb{Z}_p$ des entiers p-adiques, et de son corps de fractions $\mathbb{Q}_p$: en particulier, $\mathbb{Z}_p$ est un espace métrique (pour la distance $d(x,y) = p^{-v_p(x-y)}$) dans lequel $\mathbb{Z}$ est dense, et $\mathbb{Q}_p$ est localement compact, $\mathbb{Z}_p$ en est un sous-anneau ouvert. Le corps $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$. On a $v_p(x) \geq 0$ si, et seulement si $x \in \mathbb{Z}_p$.

Pour s'habituer à la topologie de $\mathbb{Z}_p$ et $\mathbb{Q}_p$, démontrons tout de même quelques résultats :

Proposition 13 *Pour tout $x \in \mathbb{Z}_p$ et $\alpha \geq 0$, la boule ouverte centrée en x et de rayon $p^{-\alpha}$ (notée $B(x, p^{-\alpha})$) égale la boule fermée centrée en x et de rayon $p^{-\alpha-1}$ (notée $B_f(x, p^{-\alpha-1})$). Plus précisément, si $x = a_0 + a_1 p + \cdots + a_n p^n + \cdots$, alors $B(x, p^{-\alpha}) = a_0 + a_1 p + \cdots + a_{\alpha+1} p^{\alpha+1} + p^{\alpha+2}\mathbb{Z}_p$.*

Alors, toute boule ouverte est aussi fermée. Cette proposition montre également que si $x \in B(x_0, p^n)$, alors $B(x, p^n) = B(x_0, p^n)$, et que l'intersection de deux boules est soit vide, soit l'une des deux boules.

Preuve : En effet,

$$B(x, p^{-\alpha}) = \{y \in \mathbb{Q}_p \| x - y| < p^{-\alpha}\} = \{y \in \mathbb{Q}_p | \underbrace{v_p(x-y) > \alpha}_{\Leftrightarrow v_p(x-y) \geq \alpha+1}\} = B_f(x, p^{-\alpha-1}).$$

De plus, $v_p(x-y) > \alpha$ si, et seulement si $x \equiv y \mod p^{\alpha+1}$. Alors, $y \in a_0 + a_1 p + \cdots + a_\alpha p^\alpha + p^{\alpha+1}\mathbb{Z}_p$. □

Proposition 14 *$\mathbb{Z}_p$ est compact.*

Preuve : On a

$$\mathbb{Z}_p = \bigsqcup_{a \in [\![0, p-1]\!]} a + p\mathbb{Z}_p.$$

Supposons que $\mathbb{Z}_p$ soit recouvert par des ouverts Ω_j. Montrons qu'on peut en extraire un sous-recouvrement fini. Supposons qu'il n'existe pas de sous-recouvrement fini de $\mathbb{Z}_p$; il existe alors $a_0 \in [\![0, p-1]\!]$ tel que $a_0 + p\mathbb{Z}_p$ ne soit

pas recouvert par un sous-recouvrement fini. En recommençant l'opération, il existe $a_1 \in [\![0, p-1]\!]$ tel que $a_0 + a_1 p + p^2\mathbb{Z}_p$ ne soit pas recouvert par un sous-recouvrement fini, et ainsi de suite. Considérons $x = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$ obtenu à la limite. Il existe j tel que $x \in \Omega_j$. Il existe alors une boule ouverte centrée en x, de rayon p^{-r}, contenue dans Ω_j. $B(x, p^{-r}) = a_0 + a_1 p + \cdots + a_r p^r + p^{r+1}\mathbb{Z}_p$ ne peut être recouvert par un sous-recouvrement fini, or cette boule est recouverte par Ω_j, contradiction ! □

On en déduit que $\mathbb{Q}_p$ est localement compact, car 0 a pour voisinage $\mathbb{Z}_p = B_f(0, 1)$.

2.1 Adèles

Posons $\mathscr{S}$ l'ensemble des places[¶] de $\mathbb{Q}$. On peut considérer le plongement diagonal $\mathbb{Q} \hookrightarrow \mathbb{R} \times \prod_p \mathbb{Q}_p$, mais cet anneau est beaucoup trop gros. En pratique, comme un rationnel x est dans $\mathbb{Z}_p$ pour tout p sauf un nombre fini, on préfère considérer l'anneau des adèles défini ainsi :

$$\mathbb{A} = \{(x_v)_{v \in \mathscr{S}} \in \mathbb{R} \times \prod_p \mathbb{Q}_p | x_p \in \mathbb{Z}_p \text{ pour presque tout } p\}.$$

C'est un anneau qui contient $\mathbb{Q}$ diagonalement et $\mathbb{R} \times \prod_p \mathbb{Z}_p$. C'est le sous-anneau de $\mathbb{R} \times \prod_p \mathbb{Q}_p$ [‖] engendré par $\mathbb{Q}$ et $\mathbb{R} \times \prod_p \mathbb{Z}_p$. Dorénavant, je note $\tilde{\forall}$ pour « pour presque tout ».

Pour N, M tels que $M|N$, on a $\pi_{N,M} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$ qui forme un système projectif. Alors,

$$\hat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z} \hookrightarrow \prod_N \mathbb{Z}/N\mathbb{Z}$$

est appelé le complété profini de $\mathbb{Z}$. On a un isomorphisme d'anneaux $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, *via* $(u_N)_{N \geq 1} \mapsto ((u_{p^n})_{n \geq 1})_p$ (lemme chinois).

2.2 La topologie des adèles

Soit $(X_i)_{i \in I}$ et $(Y_i)_{i \in I}$ des espaces topologiques, avec Y_i ouvert dans X_i. Considérons le produit restreint $\mathbb{X} = \{(x_i)_{i \in I} \in \prod_i X_i | x_i \in Y_i \quad \tilde{\forall} i\}$. On définit la topologie de produit restreint sur $\mathbb{X}$ ainsi : une base de voisinages de $(x_i)_{i \in I}$ est formée par $\prod_i V_i$, où V_i est un voisinage de x_i dans X_i et $V_i = Y_i$ $\tilde{\forall} i$.

Concrètement : si $x^{(n)} = (x_i^{(n)})_{i \in I}$ est une suite de X_i, elle converge vers $y = (y_i)_{i \in I}$ si, et seulement si :

1. Il existe $J \subseteq I$ fini, tel que pour tout $i \notin J$ et $n \geq 0$, $x_i^{(n)} \in Y_i$.
2. $x_i^{(n)} \to y_i$ quand $n \to \infty$.

¶. Une place est une classe d'équivalence de valeurs absolues, pour la relation d'équivalence $|\cdot|_v \sim |\cdot|_w \Leftrightarrow |\cdot|_v = |\cdot|^a$ avec $a > 0$. Il y a une place pour chaque nombre premier, et une place pour la valeur absolue.

‖. Parfois, on note $\mathbb{R} = \mathbb{Q}_\infty$, et cet anneau s'écrit plus sobrement $\prod_{v \in \mathscr{S}} \mathbb{Q}_v$.

Application : On pose $I = \mathscr{S}$, $X_p = \mathbb{Q}_p$, $X_\infty = \mathbb{R}$, $Y_p = \mathbb{Z}_p$, $Y_\infty = \mathbb{R}$. Soit S un sous-ensemble fini de $\mathscr{S}$. On pose

$$\mathbb{A}_S = \mathbb{R} \times \prod_{p \notin S} \mathbb{Z}_p \times \prod_{p \in S} \mathbb{Q}_p$$

l'anneau des S-adèles. On a $\mathbb{A} = \cup_S A_S$. Une base de voisinages de 0 dans $\mathbb{A}$ est formée par les $V_\infty \times \prod_p p^{n_p}\mathbb{Z}_p$ où V_∞ est un ouvert de $\mathbb{R}$ contenant 0, et $p^{n_p}\mathbb{Z}_p$ est, comme on l'a vu, une boule ouverte de $\mathbb{Q}_p$ contenant 0, avec $n_p \in \mathbb{Z}$, $n_p = 0, \tilde{\forall} p$.

Proposition 15 *$\mathbb{A}$ est localement compact, $\mathbb{Q}$ est un sous-groupe discret de $\mathbb{A}$ et $\mathbb{A}/\mathbb{Q}$ est compact.*

Preuve : Pour montrer que $\mathbb{A}$ est localement compact, il suffit de voir que 0 admet un voisinage compact : $V = \left[-\frac{1}{2}, \frac{1}{2}\right] \times \prod_p \mathbb{Z}_p$ (compact car produit de compacts). De plus, 0 est isolé, car V est un voisinage de 0 qui contient 0 comme seul nombre rationnel. En effet, soit $x = \frac{a}{b} \in \mathbb{Q} \cap V$ avec a et $b \in \mathbb{Z} \setminus \{0\}$. Pour que $x \in \mathbb{Z}_p$, il faut $p \nmid b$. Alors, $x \in \mathbb{Z} \setminus \{0\}$, ce qui contredit $x \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Alors, 0 est isolé, donc $\mathbb{Q}$ est discret.

Enfin, montrons le dernier point : si l'image de V dans $\mathbb{A}/\mathbb{Q}$ est $\mathbb{A}/\mathbb{Q}$, c'est gagné. Et c'est bien le cas, comme on va le voir. Il est clair que ceci équivaut à $\mathbb{A} = V + \mathbb{Q}$. Soit $x = (x_v)_{v \in \mathscr{S}} \in \mathbb{A}$, montrons qu'il existe $r \in \mathbb{Q}$ tel que $x - r \in V$. Il existe $S \subseteq \mathscr{S}$ fini tel que $x_p \in \mathbb{Z}_p$ pour tout $p \notin S$. Pour $p \in S$, il existe $n_p \geq 0$ tel que $x_p \in \frac{1}{p^{n_p}}\mathbb{Z}_p$. Notons $N = \prod_{p \notin S} p^{n_p}$, et soit $y \in \mathbb{Z}$ tel que $y = Nx_p \mod p^{n_p}$ pour tout $p \in S$ (un tel y existe, par le lemme chinois). Posons $r = \frac{y}{N}$, $r \in \mathbb{Z}_p$ pour $p \notin S$. On a $x_p - r \in \mathbb{Z}_p$ pour $p \notin S$ (trivialement), et $x_p - r = \frac{Nx_p - y}{B} \in \mathbb{Z}_p$ pour $p \in S$. Alors, $x - r \in \mathbb{R} \times \prod_p \mathbb{Z}_p$. Il existe $n \in \mathbb{Z}$ tel que $x_\infty - r - n \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. On a donc $x - r - n \in V$, et donc $x \in \mathbb{Q} + V$. □

Remarques :

– Il est important de remarquer l'analogie topologique suivante :

$$\mathbb{Z} \subseteq \mathbb{R}$$

$$\mathbb{Q} \subseteq \mathbb{A}.$$

$\mathbb{R}$ est localement compact, $\mathbb{Z}$ est discret dans $\mathbb{R}$, $\mathbb{R}/\mathbb{Z}$ est compact. Ces propriétés sont à la base de l'analyse de Fourier (ce qui est exploité dans la thèse de Tate).

– Si K est un corps de nombres, on peut poser $\mathbb{A}_K = \mathbb{A} \otimes_{\mathbb{Q}} K$.

Soit $N \geq 1$, $N = \prod_p p^{n_p}$ avec $n_p \geq 0$. Posons $\mathbb{A}_N = \mathbb{R} \times \prod_p p^{n_p}\mathbb{Z}_p$, sous-groupe de $\mathbb{A}$. On a $\mathbb{A}_1 = \mathbb{R} \times \prod_p \mathbb{Z}_p \simeq \mathbb{R} \times \hat{\mathbb{Z}}$, et $\mathbb{A} = \mathbb{A}_1 + \mathbb{Q}$, d'après ci-dessus. Mieux, on a $\mathbb{A} = \mathbb{A}_N + \mathbb{Q}$, car $\mathbb{A}_N = N\mathbb{A}_1$, $\mathbb{A} = N\mathbb{A}$ et $\mathbb{Q} = N\mathbb{Q}$.

Proposition 16 *On a $\mathbb{A}/\mathbb{A}_N \simeq \mathbb{Q}/N\mathbb{Z}$ et $\mathbb{A}/\mathbb{Q} = \varprojlim_N \mathbb{R}/N\mathbb{Z}$.*

Preuve : Considérons $f_N : \begin{cases} \mathbb{A}/(\mathbb{Q} + N\hat{Z}) & \to & \mathbb{R}/N\mathbb{Z} \\ (x_v)_{v \in \mathscr{S}} & \mapsto & x_\infty + N\mathbb{Z} \end{cases}$. L'application est bien définie, car si $x \in \mathbb{A}$, il existe $r \in \mathbb{Q}$ tel que $x - r \in \mathbb{A}_N$, et donc $x - r \in N\hat{\mathbb{Z}}$ en

dehors de la composante ∞. Donc $x_\infty + \underbrace{(\mathbb{Q} \cap N\hat{Z})}_{=N\mathbb{Z}}$ est bien défini. En passant à la limite sur N, on trouve

$$\mathbb{A}/\mathbb{Q} = \varprojlim_N \mathbb{A}/(\mathbb{Q} + N\hat{Z}) \simeq \varprojlim_N \mathbb{R}/N\mathbb{Z}.$$

De plus, $\mathbb{A}/\mathbb{A}_N = (\mathbb{Q} + \mathbb{A}_N)/\mathbb{A}_N \simeq \mathbb{Q}/(\mathbb{Q} \cap \mathbb{A}_N) \simeq \mathbb{Q}/N\mathbb{Z}$.

2.3 Théorèmes d'approximation

Un voisinage de 0 dans $\mathbb{A}$ contient un ensemble de la forme $V_\infty \times \prod_p p^{n_p}\mathbb{Z}_p$ avec $n_p \in \mathbb{Z}$, $n_p = 0, \tilde{\forall} p$. Une suite $(x_n)_{n\geq 0} = ((x_v^{(n)})_{v\in\mathscr{S}})_{n\geq 0}$ tend vers 0 dans $\mathbb{A}$ si

1. Il existe $S \subseteq \mathscr{S}$ fini, tel que pour tout $p \notin S$ et $n \geq 0$, $x_p^{(n)} \in \mathbb{Z}_p$.
2. $x_v^{(n)} \to 0$ quand $n \to \infty$, dans $\mathbb{Q}_v$.

Soit $S \subseteq \mathscr{S}$. Considérons $\mathbb{A}^{(S)} = \{(x_v)_{v\in\mathscr{S}} \in \prod_v \mathbb{Q}_v | x_p \notin \mathbb{Z}_p \forall p \in S\}$. C'est un sous-anneau de $\mathbb{A}$ et un anneau quotient ; on a $\mathbb{A} = \mathbb{A}^{(S)} \times \mathbb{A}^{(\mathscr{S}\setminus S)}$.

Théorème 14 (Approximation forte) *Supposons que $S \neq \mathscr{S}$. L'image du plongement diagonal $\mathbb{Q} \hookrightarrow \mathbb{A}^{(S)}$ est dense.*

Preuve : On peut supposer que $S = \mathscr{S} \setminus \{|\cdot|_v\}$. Soit $x = (x_v)_{v\in S} \in \mathbb{A}^{(S)}$. Approximons cet élément par un nombre rationnel x_0.

Le premier cas est celui de $|\cdot|_v = |\cdot|_\infty$. Considérons un voisinage de 0 dans $\mathbb{A}^{(S)}$ de la forme $\prod_p p^{n_p}\mathbb{Z}_p$ (avec $\tilde{\forall} p, n_p = 0$, selon S). Soit $S_x = \{p \in \mathscr{S} | x_p \notin \mathbb{Z}_p\}$ (fini). Considérons $m \in \mathbb{Z}$ tel que $mx_p \in \mathbb{Z}_p$ pour tout $p \in S_x$. Soit $y \in \mathbb{Z}$ tel que $y \equiv mx_p \mod p^{n_p + v_p(m)}\mathbb{Z}_p$ pour tout $p \in S_x$ (toujours par le lemme chinois). Posons $x_0 = \frac{y}{m} \in \mathbb{Q}$. On a bien $x_p - x_0 = x_p - \frac{y}{m} = \frac{mx_p - y}{m} \in p^{n_p}\mathbb{Z}_p$, donc $x - x_0 \in \prod_p p^{n_p}\mathbb{Z}_p$. On a trouvé x dans $x_0 + \prod_p p^{n_p}\mathbb{Z}_p$.

Le deuxième cas est celui de $|\cdot|_v = |\cdot|_{p_0}$ pour p_0 premier. Un voisinage de 0 dans $\mathbb{A}^{(S)}$ contient un ensemble de la forme $V =]-\varepsilon, \varepsilon[\times \prod_{p\neq p_0} p^{n_p}\mathbb{Z}_p$ (avec $\tilde{\forall} p$, $n_p = 0$, selon S). Cherchons $x_0 \in \mathbb{Q} \cap (x + V)$. Comme ci-dessus, on doit trouver $x_1 \in \mathbb{Q} \cap (x + \mathbb{R} \times \prod_{p\neq p_0} p^{n_p}\mathbb{Z}_p)$. Il reste à montrer que $|x_0 - x_1| > \varepsilon$. Si $y \in \mathbb{Z}\left[\frac{1}{p_0}\right]$, on a $y \in \mathbb{Z}_p$ pour $p \neq p_0$. Posons $N = \prod_p p^{n_p}$. Si $y \in \mathbb{Z}\left[\frac{1}{p_0}\right]$, on a $Ny \in N\mathbb{Z}_p = p^{n_p}\mathbb{Z}_p$ pour $p \neq p_0$. On a alors $x_1 + y \in \mathbb{Q} \cap (x + \prod_{p\neq p_0} p^{n_p}\mathbb{Z}_p)$. Comme $\mathbb{Z}\left[\frac{1}{p_0}\right]$ est dense dans $\mathbb{R}$, on peut trouver y tel que $|x_\infty - x_1 - y|_\infty < \varepsilon$. On choisit $x_0 = x_1 + y$, et c'est bon ! □

Théorème 15 (Approximation faible) *Soit K un corps. Soient $|\cdot|_1$, $|\cdot|_2$, …, $|\cdot|_n$ des valeurs absolues de K, deux à deux non équivalentes. L'image de K par le plongement diagonal $K \to \prod_i K_i$, où K_i est le complété de K pour $|\cdot|_i$, est dense.*

Corollaire 9 *Deux valeurs absolues non équivalentes définissent des topologies différentes.*

2.4 Analyse de Fourier locale

Soit G un groupe topologique abélien. Soit $\mathbb{U} = \{z \in \mathbb{C} || z| = 1\} (\simeq \mathbb{R}/\mathbb{Z}) \subseteq \mathbb{C}$. Un caractère de G est un morphisme continu de groupes $G \to \mathbb{U}$, et $\hat{G}$ constitue l'ensemble de ces morphismes ; on l'appelle le dual de Pontryagin de G. Ce groupe est muni d'une topologie : une base de voisinages de 1 est formée par les $W(K,V) = \{\chi \in \hat{G} | \chi(K) \subseteq V\}$ où K est compact, et V un voisinage de 1 dans $\mathbb{U}$. On l'appelle topologie compacte-ouverte.

Si $G = (\mathbb{R}, +)$, alors on a $\mathbb{R} \simeq \hat{\mathbb{R}}$ *via* $x \mapsto (y \mapsto \exp(2i\pi xy))$. Alors, $\mathbb{R} \simeq \hat{\hat{\mathbb{R}}}$, et il s'agit en fait d'un phénomène général : si G est localement compact, alors $G \simeq \hat{\hat{G}}$, et même canoniquement : *via* $g \mapsto (\chi \mapsto \chi(g))$.

Si $G = (\mathbb{R}/\mathbb{Z}, +)$, on a $\hat{G} \simeq \mathbb{Z}$, et si $G = (\mathbb{Z}, +)$, alors $\hat{G} \simeq \mathbb{R}/\mathbb{Z}$. On remarque que $\mathbb{R}/\mathbb{Z}$ est compact et $\mathbb{Z}$ est discret.

Étudions le cas où $G = \mathbb{Q}_p$. Soit $\psi \in \hat{\mathbb{Q}_p}$.

Lemme 5 *$\psi(\mathbb{Q}_p)$ est inclus dans l'ensemble des racines d'ordre une puissance de p.*

Preuve : Soit $a \in \mathbb{Q}_p$. Considérons $ap^n \to 0$ quand $n \to \infty$. On a $\psi(ap^n) = \psi(a)^{p^n} \to \psi(0) = 1$ quand $n \to \infty$. Il faut donc que $\psi(a)$ soit une racine d'ordre une puissance de p. □

Lemme 6 *$\psi(p^r\mathbb{Z}_p)$ est fini pour $r \in \mathbb{Z}$. C'est $\{1\}$, ou ce n'est pas contenu dans $V_0 = \{\exp(2i\pi x) | x \in]-1/2, 1/2[\}$.*

La deuxième assertion se vérifie aisément sur un dessin.
Preuve : Comme $p^r\mathbb{Z}_p$ est compact, $\psi(p^r\mathbb{Z}_p)$ est un sous-groupe compact de $\mathbb{U}$. Or un sous-groupe de $\mathbb{U}$ est dense ou fini. Comme $\psi(p^r\mathbb{Z}_p) \neq \mathbb{U}$, $\psi(p^r\mathbb{Z}_p)$ est fini. □

Lemme 7 *Une base de voisinages de 1 dans $\hat{\mathbb{Q}}_p$ est formée par les*

$$A_r = \{\psi \in \hat{\mathbb{Q}_p} | \psi(p^r\mathbb{Z}_p) = 1\}.$$

Preuve : Soit K un compact de $\mathbb{Q}_p$. Soit V un voisinage de 1 dans $\mathbb{U}$. Il existe $r \in \mathbb{Z}$ tel que $K \subseteq p^r\mathbb{Z}_p$. On a

$$W(K,V) = \{\psi \in \hat{\mathbb{Q}_p} | \psi(K) \subseteq V\} \supseteq \{\psi \in \hat{\mathbb{Q}_p} | \psi(p^r\mathbb{Z}_p) \subseteq V\} \supseteq \underbrace{\{\psi \in \hat{\mathbb{Q}} | \psi(p^r\mathbb{Z}_p) = 1\}}_{=W(p^r\mathbb{Z}_p, V_0)} = A_r. \square$$

Conclusion : Les $W(K,V)$ et les A_r définissent la même topologie.

Considérons $\mathbb{Q}_p/\mathbb{Z}_p$. Tout élément de $\mathbb{Q}_p$ s'écrit sous la forme $\frac{a}{p^n}$ avec $a \in \mathbb{Z}_p$. Sa classe dans $\mathbb{Q}_p/\mathbb{Z}_p$ s'écrit $\frac{a}{p^n} + \mathbb{Z}_p$, avec $a \in \mathbb{Z}_p$. Elle ne dépend que de a mod p^n. Elle coïncide avec $\frac{a_0}{p^n} + \mathbb{Z}_p$, $a_0 \in \mathbb{Z}$, si $a_0 \equiv a \mod p^n\mathbb{Z}_p$. L'entier a_0 est déterminé modulo $p^n\mathbb{Z}$, donc $\frac{a_0}{p^n}$ est bien défini dans $\mathbb{Q}/\mathbb{Z}$. On a ainsi défini un morphisme de groupes injectif

$$i : \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \to & \mathbb{Q}/\mathbb{Z} \\ \frac{a_0}{p^n} + \mathbb{Z}_p & \mapsto & \frac{a_0}{p^n} + \mathbb{Z} \end{cases}$$

avec $a_0 \in \mathbb{Z}$ et $n \geq 0$. On a donc des homomorphismes de groupes :

$$\mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z} \simeq \mathbb{U},$$

où le dernier isomorphisme est donné par $x \mapsto \exp(2i\pi x)$. On appelle i_p cette composée d'applications. On a $\exp(2i\pi i_p(x)) = 1$ si, et seulement si $x \in \mathbb{Z}_p$. De plus, l'image de i_p est contenue dans les éléments d'ordre une puissance de p, et $\exp(2i\pi i_p(x))$ est racine d'ordre une puissance de p lorsque $x \in \mathbb{Q}_p$.

Considérons $\varphi : \begin{cases} \mathbb{Q}_p & \to & \hat{\mathbb{Q}}_p \\ x & \mapsto & y \mapsto \exp(2i\pi i_p(xy)) \end{cases}$.

Théorème 16 *φ est un isomorphisme de groupes topologiques.*

Preuve : φ est injective : soit $x \in \mathbb{Q}_p$ tel que $\varphi(x) = 1$, c'est-à-dire tel que pour tout $y \in \mathbb{Q}_p$, $\exp(2i\pi i_p(xy)) = 1$. Alors, $xy \in \mathbb{Z}_p$ pour tout $y \in \mathbb{Q}_p$, d'où $x = 0$ à cause de la valuation de xy.

φ est de plus continue, car

$$\varphi^{-1}(A_r) = \{x \in \mathbb{Q}_p | \forall y \in p^r\mathbb{Z}_p, \exp(2i\pi i_p(xy)) = 1\} = p^{-r}\mathbb{Z}_p,$$

qui est voisinage de 0 dans $\mathbb{Z}_p$. On a de plus que φ est d'image dense. En effet, soit $\psi \in \hat{\mathbb{Q}}_p$ et $r \in \mathbb{Z}$. Montrons qu'il existe $x \in \mathbb{Q}_p$ tel que $\varphi(x) \in \psi \cdot A_r$ (c'est-à-dire : $\varphi(x)$ et ψ coïncident sur $p^r\mathbb{Z}_p$). Soit $x \in \mathbb{Q}_p$ tel que $\psi(p^r) = \exp(2i\pi i_p(p^r x))$. Alors $\frac{\psi}{\varphi(x)}(p^r) = 1$, et donc $\frac{\psi}{\varphi(x)}(p^r\mathbb{Z}_p) = 1$ car $p^r\mathbb{Z}_p$ est l'adhérence du groupe engendré par p^r dans $\mathbb{Q}_p$.

Enfin, $\varphi(\mathbb{Q}_p)$ est fermé dans $\hat{\mathbb{Q}}_p$. En effet, $\varphi(\mathbb{Q}_p)$ est complet : soit $(\varphi(x_n))_{n\geq 1}$ une suite de Cauchy dans $\varphi(\mathbb{Q}_p)$, c'est-à-dire que pour tout $r \in \mathbb{Z}$, on a

$$\frac{\varphi(x_n)}{\varphi(x_m)} = \varphi(x_n - x_m) \in A_r$$

pour n et m assez grands. Autrement dit,

$$\exp(2i\pi i_p((x_n - x_m)p^r\mathbb{Z}_p)) = 1$$

pour n et m assez grands, c'est-à-dire $p^r(x_n - x_m)\mathbb{Z}_p \subseteq \mathbb{Z}_p$, donc $x_n - x_m \in p^{-r}\mathbb{Z}_p$ pour n et m assez grands. Donc la suite $(x_n)_{n\geq 1}$ est de Cauchy dans $\mathbb{Q}_p$ qui est complet, donc $x_n \to x$ quand $n \to \infty$. Comme φ est continue, $\varphi(x_n) \to \varphi(x)$ quand $n \to \infty$.

Bref, l'image est donc complète puis fermée. Or une partie fermée et dense est l'espace tout entier, d'où $\varphi(\mathbb{Q}_p) = \hat{\mathbb{Q}}_p$. On a donc le résultat, car φ^{-1} est clairement continue : on a $\varphi(p^r\mathbb{Z}_p) = A_{-r}$. L'image d'un voisinage de 0 dans $\mathbb{Q}_p$ est un voisinage de 1 dans $\hat{\mathbb{Q}}_p$. □

Corollaire 10 *On a $\mathbb{Z}_p^\perp = \{\psi \in \hat{\mathbb{Q}}_p | \psi(\mathbb{Z}_p) = 1\} \simeq \{x \in \mathbb{Q}_p | \varphi(x)(\mathbb{Z}_p) = 1\}$.*

De plus on a $\hat{\mathbb{Z}}_p \simeq \hat{Q}_p/\mathbb{Z}_p^\perp \simeq \mathbb{Q}_p/\mathbb{Z}_p$ (ce qui est isomorphe encore aux racines de l'unité dans $\mathbb{U}$ d'ordre une puissance de p).

2.5 Analyse de Fourier sur les adèles

Considérons $i_\infty : \begin{cases} \mathbb{R} & \to & \mathbb{R}/\mathbb{Z} \\ x & \mapsto & -x+\mathbb{Z} \end{cases}$, et $f : \begin{cases} \mathbb{A} & \to & \mathbb{U} \\ (x_v)_{v\in\mathscr{S}} & \mapsto & \prod_{v\in\mathscr{S}} \exp(2i\pi i_v(x_v)) \end{cases}$
(le produit est fini, car $x_p \in \mathbb{Z}_p$ pour presque tout p, donc $\exp(2i\pi i_v(x_v)) = 1$ pour presque tout p). On en déduit l'application bi-additive et équivariante

$$\phi : \begin{cases} \mathbb{A}\times\mathbb{A} & \to & \mathbb{U} \\ ((x_v)_{v\in\mathscr{S}},(y_v)_{v\in\mathscr{S}}) & \mapsto & \prod_{v\in\mathscr{S}} \exp(2i\pi i_v(xy)) \end{cases}.$$

Elle prolonge les accouplement $\mathbb{R}\times\mathbb{R}\to\mathbb{U}$ et $\mathbb{Q}_p\times\mathbb{Q}_p\to\mathbb{U}$ précédemment définis.

Théorème 17 *Cela définit un isomorphisme de groupes topologiques $\mathbb{A}\simeq\hat{\mathbb{A}}$.*

Preuve : Le théorème découle de

Proposition 17 *Soit G un produit restreint de groupes topologiques $(G_i)_{i\in I}$ vis-à-vis de sous-groupes compacts ouverts $(H_i)_{i\in I}$. Alors $\hat{G}$ s'identifie au produit restreint des $(\hat{G}_i)_{i\in I}$ vis-à-vis des $(H_i)^\perp_{i\in I}$,* via $\chi\mapsto\prod_{i\in I}\chi_{|G_i}$. □

Théorème 18 *On a $\mathbb{Q}^\perp\simeq\mathbb{Q}$ (isomorphisme de groupes induit par l'isomorphisme précédent).*

Preuve : On a, tout d'abord, $\mathbb{Q}\hookrightarrow\mathbb{Q}^\perp$: pour $x,y\in\mathbb{Q}$, $\prod_{v\in\mathscr{S}}\exp(2i\pi i_v(xy)) = 1$ car pour tout $z\in\mathbb{Q}$:

$$\prod_{v\in\mathscr{S}}\exp(2i\pi i_v(xy)) = 1 \Leftrightarrow \sum_{v\in\mathscr{S}} i_v(z) = 0 \in \mathbb{Q}/\mathbb{Z},$$

ce qui est vrai car si on écrit $z = \sum_p \frac{a_p}{p^{n_p}}$ avec $a_{p_0}\in\mathbb{Z}$ (c'est toujours possible), alors $\sum_v i_v(z) = i_\infty(z) + \sum_p i_p(z) = -z + \sum_p \frac{a_p}{p^{n_p}} \in -z+z+\mathbb{Z} = \mathbb{Z}$.

Le groupe $\mathbb{A}/\mathbb{Q}$ est compact, et $\widehat{\mathbb{A}/\mathbb{Q}}\simeq\mathbb{Q}^\perp$, donc $\mathbb{Q}^\perp$ est discret **. De plus, $\mathbb{Q}^\perp$ est un $\mathbb{Q}$-espace vectoriel. Considérons l'espace quotient $\mathbb{Q}^\perp/\mathbb{Q}$ contenu dans $\mathbb{A}/\mathbb{Q}$. Si $\mathbb{Q}^\perp/\mathbb{Q}$ est discret, ce qui est évident, alors il est fini car $\mathbb{A}/\mathbb{Q}$ est compact. Alors, $\dim_{\mathbb{Q}}(\mathbb{Q}^\perp/\mathbb{Q}) = 1$, et $\mathbb{Q}^\perp = \mathbb{Q}$. □

Corollaire 11 *On a $\widehat{\mathbb{A}/\mathbb{Q}}\simeq\mathbb{Q}$ et $\hat{\mathbb{Q}}\simeq\mathbb{A}/\mathbb{Q}$.*

2.6 Idèles

Quelle est la structure de $\mathbb{Q}_p^*$, pour p premier ? $v_p : \mathbb{Q}_p^*\to\mathbb{Z}$ est surjective, de noyau $\mathbb{Z}_p^*$. On a $\mathbb{Q}_p^*\simeq\mathbb{Z}_p^*\times\mathbb{Z}\simeq\mathbb{Z}_p^*\times p^{\mathbb{Z}}$, et

$$\mathbb{Z}_p^* \supseteq 1+p\mathbb{Z}_p \supseteq 1+p^2\mathbb{Z}_p \supseteq \cdots \supseteq 1+p^n\mathbb{Z}_p \supseteq \cdots$$

**. Si G est compact, alors $\hat{G}$ est discret (et vice-versa). En effet, il suffit de montrer que $\{1\}$ est ouvert dans $\hat{G}$, et c'est le cas : un caractère d'un groupe compact est surjectif ou d'image finie, car un sous-groupe de $\mathbb{U}\simeq\mathbb{R}/\mathbb{Z}$ est soit fini, soit dense, et l'image d'un caractère est un sous-groupe compact. Bref, considérons $W(G,V_0) = \{\chi\in\hat{G}|\chi(G)\subseteq V_0\} = \{\chi\in\hat{G}|\chi(G) = 1\} = \{1\}$ pour V_0 assez petit (ne contenant pas de sous-groupe propre).

On peut noter $U_p^{(n)} = 1 + p^n\mathbb{Z}_p = B(1, p^{-n-1})$ si $n \geq 1$, $U_p^{(0)} = \mathbb{Z}_p^*$ sinon. $\mathbb{Q}_p^*$ est un groupe topologique, pour la topologie héritée de $\mathbb{Q}_p$. On a $\mathbb{Z}_p^*/U_p^{(n)} \simeq (\mathbb{Z}/p^n\mathbb{Z})^*$, et en fait

$$\mathbb{Z}_p^* = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$$

si $p \neq 2$ (sinon, $\mathbb{Z}_2^* \simeq \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$).

Le groupe des idèles est $\mathbb{A}^*$. Il contient $\mathbb{R}^*$, $\mathbb{Q}_p^*$ et $\mathbb{Q}^*$ (diagonalement). La topologie de $\mathbb{A}^*$ n'est pas celle induite par $\mathbb{A}$, mais celle du produit restreint sur $\mathbb{R}^* \times \prod_p \mathbb{Q}_p^*$ vis-à-vis des sous-groupes $\mathbb{Z}_p^* \subseteq \mathbb{Q}_p^*$ (pour p premier).

Soit $S \subseteq \mathscr{S}$ fini. On pose $\Lambda_S = \mathbb{R}^* \times \prod_{p\in S} \mathbb{Q}_p^* \times \prod_{p\notin S} \mathbb{Z}_p^*$. C'est le groupe des S-idèles. $\mathbb{A}^* = \cup_S \Lambda_S$.

Considérons $\|\cdot\| : \begin{cases} \mathbb{A}^* & \to & \mathbb{R}_+^* \\ x = (x_v)_{v\in\mathscr{S}} & \mapsto & \prod_{v\in\mathscr{S}} |x|_v = \|x\| \end{cases}$. C'est un homomorphisme de groupes continu et surjectif. On pose $\mathbb{A}^{*0} = \ker(\|\cdot\|)$.

Proposition 18 (Formule du produit) $\mathbb{Q}^* \subseteq \mathbb{A}^{*0}$.

C'est évident, en écrivant ce que vaut $\|x\|$.

Proposition 19 *$\mathbb{A}^*$ est localement compact, $\mathbb{Q}^*$ est discret dans $\mathbb{A}^*$ et $\mathbb{A}^{*0}/\mathbb{Q}^*$ est compact.*

Preuve : $\left[\frac{1}{2}, 2\right] \times \prod_p \mathbb{Z}_p^*$ est un voisinage compact de 1 qui ne contient que 1 comme nombre rationnel. Donc on a les deux premières assertions. Montrons la troisième.

Remarquons que $\mathbb{A}^* = \mathbb{Q}^*(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*)$. En effet, si $(x_v)_{v\in\mathscr{S}} \in \mathbb{A}^*$, soit $S = \{p \in \mathscr{S} | x_p \notin \mathbb{Z}_p^*\}$. Écrivons $x_p = p^{n_p} y_p$ avec $y_p \in \mathbb{Z}_p^*$ et $n_p \in \mathbb{Z}$, et posons $x = \prod_p p^{n_p} \in \mathbb{Q}^*$, puis $y_\infty = x_\infty$. Alors, $(x_v)_{v\in\mathscr{S}} = \underbrace{x}_{\in\mathbb{Q}^*} \underbrace{(y_v)_{v\in\mathscr{S}}}_{\in\mathbb{R}^*\times\prod_p \mathbb{Z}_p^*}$.

Bref, ceci implique

$$\mathbb{A}^{*0}/\mathbb{Q}^* = ((\mathbb{Q}^*(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*)) \cap \mathbb{A}^{*0})/\mathbb{Q}^* = (\mathbb{Q}^*(\{\pm 1\} \times \prod_p \mathbb{Z}_p^*))/\mathbb{Q}^*$$

$$\simeq (\{\pm 1\} \times \prod_p \mathbb{Z}_p^*)/(\mathbb{Q}^* \cap (\{\pm\} \times \prod_p \mathbb{Z}_p^*) \simeq \prod_p \mathbb{Z}_p *,$$

qui est bien un compact, car $\mathbb{Z}_p^* = \cup_{a=1}^{p-1} \underbrace{(a + p\mathbb{Z}_p)}_{=B_f(a,p^{-1})}$ est compact. □

Remarque : Si on remplace $\mathbb{Q}$ par un corps de nombres K, l'assertion $\mathbb{A}_K^{*0}$ est compact si, et seulement si on a la finitude du nombre de classes d'idéaux et le théorème des unités de Dirichlet.

2.7 Caractères et quasi-caractères du groupe des idèles

Soit G un groupe topologique. Un quasi-caractère de G est un homomorphisme de groupes $G \to \mathbb{C}^*$. Si $G = \mathbb{R}^*$, un quasi-caractère de $\mathbb{R}^*$ est de la forme

$x \mapsto |x|_\infty^s$ sur $\mathbb{R}_+^*$ avec $s \in \mathbb{C}$, et donc de la forme $x \mapsto |x|_\infty^s$ ou $x \mapsto |x|_\infty^s \text{signe}(x)$ sur $\mathbb{R}^*$. Soit χ un quasi-caractère de $\mathbb{Q}_p^*$. $\chi(\mathbb{Z}_p^*)$ est un sous-groupe compact de $\mathbb{C}^*$, et donc $\chi(\mathbb{Z}_p^*) \subseteq \mathbb{U}$. Comme $\mathbb{Q}_p^* \simeq \mathbb{Z}_p^* \times p^{\mathbb{Z}}$, χ est un caractère si, et seulement si $\chi(p) \in \mathbb{U}$.

Proposition 20 *Il existe un caractère χ_0 de $\mathbb{Q}_p^*$ et $s \in \mathbb{C}$ tels que $\chi = \chi_0 |\cdot|_p^s$.*

Preuve : On pose $\chi_0(x) = \frac{\chi(x)}{|x|_p^s}$, où s est défini par $\chi(p)p^s \in \mathbb{U}$. □

Comme χ est continu et $\mathbb{Z}_p^*$ compact, $\chi(\mathbb{Z}_p^*)$ est un sous-groupe fini de $\mathbb{U}$. Donc $\{x \in \mathbb{Z}_p^* | \chi(x) = 1\}$ contient un ensemble de la forme $U_p^{(n)}$ avec $n \geq 0$. Le plus petit n tel que $\chi(U_p^{(n)}) = 1$ s'appelle le conducteur de χ (on peut aussi le noter p^n, ou mieux $p^n\mathbb{Z}_p$, vu comme idéal de $\mathbb{Z}_p$). On dit que χ est non ramifié si $n = 0$ (*i.e.* $\chi(\mathbb{Z}_p^*) = 1$), alors $\chi(x)$ ne dépend que de $|x|_p$, $x \in \mathbb{Q}_p^*$.

Un quasi-caractère χ de $\mathbb{A}^*$ définit une collection de quasi-caractères $(\chi_v)_{v \in \mathscr{S}}$ de $\mathbb{Q}_v^*$. Comme il est continu, on a $\chi(x^{(n)}) \to_{n\to\infty} 1$ lorsque $x^{(n)} \to_{n\to\infty} 1$. Posons $x^{(n)} = (x_v^{(n)})_{v \in \mathscr{S}}$.

1. Il existe $S \subseteq \mathscr{S}$ fini, tel que pour tout $p \notin S$ et $n \geq 0$, $x_p^{(n)} \in \mathbb{Z}_p^*$.
2. $x_v^{(n)} \to 1$ quand $n \to \infty$ $(v \in \mathscr{S})$.

Remarque : Il manque encore une information en la place $|\cdot|_\infty$.

On dit que χ est un caractère de Hecke (ou grand caractère, ou *Großencharakter*) si $\chi(\mathbb{Q}^*) = 1$.

Proposition 21 *Dans telle situation, il existe $\chi_0 \in \text{Hom}_{continu}(\mathbb{A}^*/\mathbb{Q}^*, \mathbb{U})$ et $s \in \mathbb{C}$ tels que0 $\chi = \chi_0 \cdot \|\cdot\|^s$.*

Preuve : Comme $\mathbb{A}^{*0}/\mathbb{Q}^*$ est compact, on a $\chi(\mathbb{A}^{*0}) \subseteq \mathbb{U}$. Or, il existe s tel qu'on ait le diagramme suivant :

$$\begin{array}{ccc} \mathbb{A}^*/\mathbb{A}^{*0} & \xrightarrow{\|\cdot\|} & \mathbb{R}_+^* , \\ \downarrow \chi & \swarrow_{r \mapsto r^s} & \\ \mathbb{C}^*/\mathbb{U} \simeq \mathbb{R}_+^* & & \end{array}$$

d'où le résultat. □

χ_0 est alors déterminé par $\chi_{|\mathbb{A}^{*0}/\mathbb{Q}^*}$. Soit $N = \prod_p p^{n_p}$ le conducteur de χ, c'est-à-dire le conducteur de χ_0. Posons $U^{(N)} = U_\infty^{(0)} \times \prod_p U_p^{(n_p)} \subseteq \mathbb{A}^*$, où $U_\infty^{(0)} = \mathbb{R}^*$, et $U^{N_\infty} = U_\infty^{(1)} \times \prod_p U_p^{(n_p)}$ où $U_\infty^{(1)} = \mathbb{R}_+^*$. Ce sont les groupes d'idèles de rayon N et N_∞ respectivement. On a $\chi_0(U^{(N_\infty)}) = 1$ et même $\chi_0(U^{(N)}) = 1$ si $\chi_0(-1) = 1$.

χ est un caractère de $\mathbb{A}^*/(\mathbb{Q}^* U^{(N_\infty)})$. Déterminons $\mathbb{A}^{*0}/(\mathbb{Q}^* U^{(N_\infty)})$ et $\mathbb{A}^*/(\mathbb{Q}U^{(N)})$.

Proposition 22 *On a $\mathbb{A}^{*0}/(\mathbb{Q}^* U^{(N)}) \simeq (\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$, et $\mathbb{A}^{*0}/(\mathbb{Q}^* U^{(N_\infty)}) \simeq (\mathbb{Z}/N\mathbb{Z})^*$.*

Preuve : On a $\mathbb{A}^* = \mathbb{Q}^*(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*) \simeq \mathbb{Q}^* \times (\mathbb{R}^* \times \prod_p \mathbb{Z}_p^*)/\{\pm 1\}$, et donc $\mathbb{A}^{*0}/\mathbb{Q}^* = \{\pm 1\} \times \prod_p \mathbb{Z}_p^*/\{\pm 1\}$.

Posons $N' = N$ ou N_∞. Alors $\mathbb{A}^{*0}/(\mathbb{Q}^* U^{(N')}) = (\underbrace{\mathbb{R}^*/U_\infty^{(n_\infty)}}_{=1 \text{ ou } \{\pm 1\}} \times \prod_p \underbrace{\mathbb{Z}_p^*/U_p^{(n_p)}}_{=(\mathbb{Z}/p^{n_p}\mathbb{Z})^*})$.

Bref, c'est $(\mathbb{Z}/N\mathbb{Z})^*$ ou $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. □

Petite disgression : $(\mathbb{Z}/N\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $\zeta_N = \exp\left(\frac{2i\pi}{N}\right)$.

Théorème 19 (Kronecker-Weber) *Toute extension abélienne $K/\mathbb{Q}$ est contenue dans l'extension cyclotomique $\mathbb{Q}(\zeta_N)$, avec ζ_N approprié.*

Donc tout caractère de $\mathrm{Gal}(K/\mathbb{Q})$ provient d'un caractère de $(\mathbb{Z}/N\mathbb{Z})^* \simeq \mathbb{A}^{*0}/(\mathbb{Q}^* U^{N_\infty})$.

Reformulation : On a

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) & \xrightarrow{\sim} & \mathbb{A}^{*0}/\mathbb{Q}^* \\ \uparrow & & \uparrow \\ \mathrm{Gal}(\overline{\mathbb{Q}}_v, \mathbb{Q}_v) & \xrightarrow{\sim} & \mathbb{Q}_v^* \end{array}$$

où l'isomorphisme du haut est un isomorphisme de groupes bicontinu. Ceci est encore valable si on remplace $\mathbb{Q}$ par K, et on a affaire à la théorie du corps de classe.

Soit $\chi = \prod_v \chi_v$ un quasi-caractère de $\mathbb{A}^*/\mathbb{Q}^*$. On peut considérer

$$L(\chi, s) = \prod_{\substack{p \in \mathscr{S} \\ p \neq \infty ; \chi(p) \text{ non ramifié}}} \frac{1}{1 - \chi(p) p^{-s}}.$$

Remarque : On peut incorporer la variable s dans χ, en remplaçant χ par $\chi \|\cdot\|^s$, ou on peut supposer que χ est un caractère. On a, si ψ est le caractère de Dirichlet associé à χ :

$$L(\chi, s) = \prod_{\substack{p \in \mathscr{S} \\ p \neq \infty ; p \nmid N}} \frac{1}{1 - \psi(p) p^{-s}} = \sum_{n \wedge N = 1} \frac{\psi(n)}{n^s}$$

une fonction L de Dirichlet. On pose $L_\infty(\chi_\infty, s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right)$ si $\chi_\infty(-1) = 1$, *i.e.* si $n_\infty = 0$, et $L_p(\chi_p, s) = p^{n_p s/2} = |p|_p^{-n_p s/2}$ si χ_p est ramifié, et

$$\Lambda(\chi, s) = L_\infty(\chi_\infty, s) \prod_{p, \chi(p) \text{ ramifié}} L_p(\chi_p, s) L(\chi, s).$$

Théorème 20 *$s \mapsto \Lambda(\chi, s)$ admet un prolongement analytique à $\mathbb{C}$ (holomorphe si $\chi \neq 1$, méromorphe avec des pôles en 0 et 1 qui sont simples sinon), et on a $\Lambda(\chi, s) = w_\chi \Lambda(\bar{\chi}, 1 - s)$ où $w_\chi \in \mathbb{U}$.*

Tout ceci peut se démontrer via les travaux de Tate dans sa thèse, mais nous n'avons pas eu le temps d'aller jusqu'au bout. On revient donc aux formes modulaires.

2.8 Le demi-plan vu comme espace symétrique

On sait que $GL_2(\mathbb{R})^+$ agit sur $\mathcal{H}$ par homographies. On a $GL_2(\mathbb{R})^+ i = \mathcal{H}$, et $\mathrm{Stab}_{GL_2(\mathbb{R})^+}(i)$ est l'ensemble des similitudes $(\mathbb{R}^* \cdot SO_2(\mathbb{R}))$. Donc $\mathcal{H} \simeq GL_2(\mathbb{R})^+ / Z(\mathbb{R}) SO_2(\mathbb{R})$, et même $SL_2(\mathbb{R})/SO_2(\mathbb{R}) \simeq \mathcal{H}$. Une forme modulaire est

- une fonction sur $\mathcal{H}$
- une fonction sur $GL_2(\mathbb{R})^+$
- une fonction sur $\mathscr{R}$.

Un réseau de $\mathbb{C} \simeq \mathbb{R}^2$ est un sous-groupe discret cocompact de $\mathbb{R}^2$. Rappelons l'analogie $\mathbb{Q} \subseteq \mathbb{A}$ et $\mathbb{Z} \subseteq \mathbb{R}$. Peut-on voir les formes modulaires comme des fonctions sur les réseaux de $\mathbb{A}^2$?

2.9 Les réseaux de $\mathbb{A}^2$

Un réseau de $\mathbb{A}^2$ est un sous-$\mathbb{Q}$-espace vectoriel discret et cocompact. Si Λ est un sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{A}^2$, cela revient à dire que $\Lambda \otimes_{\mathbb{Q}} \mathbb{A}^2 \simeq \mathbb{A}^2$, ou encore qu'il existe $\vec{e_1}$, $\vec{e_2} \in \mathbb{A}^2$ $\mathbb{A}$-linéairement indépendants tels que $\Lambda = \mathbb{Q}\vec{e_1} + \mathbb{Q}\vec{e_2}$. Si $(\vec{e_1}, \vec{e_2})$ est la base canonique de $\mathbb{A}^2$, pour $g \in GL_2(\mathbb{A})$, $g \begin{pmatrix} \vec{e_1} \\ \vec{e_2} \end{pmatrix}$ est une base d'un réseau de $\mathbb{A}^2$. Les réseaux ainsi associés à $g \begin{pmatrix} \vec{e_1} \\ \vec{e_2} \end{pmatrix}$ et $g' \begin{pmatrix} \vec{e_1} \\ \vec{e_2} \end{pmatrix}$ coïncident si, et seulement si $g' \in GL_2(\mathbb{Q})g$.

Conclusion : Les réseaux de $\mathbb{A}^2$ sont en bijection avec $GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A})$.

Un réseau de $\mathbb{A}^2$ donne lieu à un réseau de $\mathbb{R}^2$, c'est l'image dans $\mathbb{R}^2$ de $\Lambda \cap (\mathbb{R}^2 \times \prod_p \mathbb{Z}_p^2)$ (on utilise la projection $\mathbb{A}^2 \twoheadrightarrow \mathbb{R}^2$). Donc toute fonction sur les réseaux de $\mathbb{R}^2$ donne lieu à une fonction sur les réseaux de $\mathbb{A}^2$. Deux réseaux Λ et Λ' de $\mathbb{A}^2$ donnent lieu à un même réseau de $\mathbb{R}^2$ si, et seulement si, en écrivant que Λ et Λ' sont associés à g et $g' \in GL_2(\mathbb{A})$, on a $g' \in gGL_2(\prod_p \mathbb{Z}_p)$ (car il faut que $g(\mathbb{Z}_p^2) = g'(\mathbb{Z}_p^2)$ pour tout p). L'espace des réseaux de $\mathbb{R}^2$ coïncide avec $GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A}) / \prod_p GL_2(\mathbb{Z}_p)$.

Remarque : On pourrait s'intéresser aux réseaux de $\mathbb{A}^n$ pour $n \geq 1$. En particulier, pour $n = 1$, l'espace des réseaux de $\mathbb{A}$ est $GL_1(\mathbb{Q})\backslash GL_1(\mathbb{A}) \simeq \mathbb{Q}^*\backslash\mathbb{A}^*$ (groupe des classes d'idèles), et l'espace des réseaux de $\mathbb{R}$ s'identifie à

$$GL_1(\mathbb{Q})\backslash GL_1(\mathbb{A}) / \prod_p GL_1(\mathbb{Z}_p) \simeq \mathbb{Q}^*\backslash\mathbb{A}^* / \prod_p \mathbb{Z}_p^*.$$

Il est intéressant de remplacer $\prod_p \mathbb{Z}_p^*$ par un sous-groupe d'indice fini, voir notamment les idèles de rayon n.

2.10 Le groupe $GL_2(\mathbb{A})$

À un anneau commutatif A, on peut associer les groupes algébriques $(G_a(A),+)$ (groupe additif), $(G_m(A),\cdot)$ (groupe multiplicatif), $(GL_n(A),\cdot)$, *etc.* On examine le groupe $GL_2(\mathbb{Q}_p)$, pour p premier. C'est un groupe topologique. Une base de voisinages de 1 est formée par les

$$K(p^n)=\left\{g\in GL_2(\mathbb{Z}_p)|g\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\mod p^n\right\},n\geq 0$$

qui sont des sous-groupes de $GL_2(\mathbb{Z}_p)$.

Posons $K_1(p^n)=\left\{g\in GL_2(\mathbb{Z}_p)|g\equiv\begin{pmatrix}1&*\\0&1\end{pmatrix}\mod p^n\right\}$, lui aussi un sous-groupe de $GL_2(\mathbb{Z}_p)$ pour tout $n\geq 0$, et $K_0(p^n)=\left\{g\in GL_2(\mathbb{Z}_p)|g\equiv\begin{pmatrix}*&*\\0&*\end{pmatrix}\mod p^n\right\}$ (même remarque). On a $K\subseteq K_1\subseteq K_0$.

$GL_2(\mathbb{Z}_p)$ est un sous-groupe compact maximal de $GL_2(\mathbb{Q}_p)$ (à comparer à la situation $O_2(\mathbb{R})\subseteq GL_2(\mathbb{R})$).

Proposition 23 *On a* $GL_2(\mathbb{Q}_p)=GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)GL_2(\mathbb{Z}_p)$.

Preuve : Soit $g\in GL_2(\mathbb{Q}_p)$. $GL_2(\mathbb{Q}_p)$ opère transitivement sur $\mathbb{P}^1(\mathbb{Q}_p)$ par homographies (on peut même prendre $GL_2(\mathbb{Z}_p)$, voire $SL_2(\mathbb{Z}_p)$) : soit $\frac{u}{v}\in\mathbb{P}^1(\mathbb{Q}_p)$ tel que $p\nmid u$ ou $p\nmid v$ avec $u,v\in\mathbb{Z}_p$. Il existe $w,t\in\mathbb{Z}_p$ tels que $wv-tu=1$. Alors, $\begin{pmatrix}u&w\\v&t\end{pmatrix}\in SL_2(\mathbb{Z}_p)$ et $\begin{pmatrix}u&w\\v&t\end{pmatrix}\infty=\frac{u}{v}$, d'où la transitivité.

Considérons $g\infty\in\mathbb{P}^1(\mathbb{Q}_p)$. Il existe $\gamma\in SL_2(\mathbb{Z}_p)$ tel que $g^{-1}\infty=\gamma^{-1}\infty$. Donc $g\gamma^{-1}\infty=\infty$, et $g\gamma^{-1}$ appartient au stabilisateur sous $GL_2(\mathbb{Q}_p)$ de ∞, et est donc triangulaire supérieure dans $GL_2(\mathbb{Q}_p)$. Posons $g\gamma^{-1}=\begin{pmatrix}p^r\alpha&t\\0&p^s\beta\end{pmatrix}=\begin{pmatrix}p^r&t\\0&p^s\end{pmatrix}\underbrace{\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}}_{\in GL_2(\mathbb{Z}_p)}$, avec $\alpha,\beta\in\mathbb{Z}_p^*$, $t\in\mathbb{Q}_p$ et $r,s\in\mathbb{Z}$.

Posons encore $\begin{pmatrix}p^r&t\\0&p^s\end{pmatrix}=\begin{pmatrix}p^r&t-up^r\\0&p^s\end{pmatrix}\underbrace{\begin{pmatrix}1&u\\0&1\end{pmatrix}}_{\in GL_2(\mathbb{Z}_p)}$, avec $u\in\mathbb{Z}_p$ tel que $t-up^r\in\mathbb{Z}\left[\frac{1}{p}\right]$ (c'est possible, car $\mathbb{Q}_p=\mathbb{Z}\left[\frac{1}{p}\right]+\mathbb{Z}_p$). Donc

$$g\gamma^{-1}=\underbrace{\begin{pmatrix}p^r&t-up^r\\0&p^s\end{pmatrix}}_{\in GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)}\underbrace{\begin{pmatrix}1&u\\0&1\end{pmatrix}\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}}_{\in GL_2(\mathbb{Z}_p)}.\square$$

Corollaire 12 *Soit K un sous-groupe compact ouvert de $GL_2(\mathbb{Z}_p)$ tel que* $\det(K)=\mathbb{Z}_p^*$. *On a* $GL_2(\mathbb{Q}_p)=GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)K$.

Preuve : En effet, montrons que $GL_2(\mathbb{Q}_p)/(GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)K) = \{1\}$; or c'est

$$GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)GL_2(\mathbb{Z}_p)/(GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)K) = GL_2(\mathbb{Z}_p)/(\underbrace{(GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)\cap GL_2(\mathbb{Z}_p))}_{=GL_2(\mathbb{Z})}K).$$

L'ensemble $GL_2(\mathbb{Z})K$ contient $SL_2(\mathbb{Z})K$. Or $SL_2(\mathbb{Z})$ est dense dans $SL_2(\mathbb{Z}_p)$ (on le montrera plus tard, indépendamment des résultats ici démontrés), donc cet ensemble contient $SL_2(\mathbb{Z}_p)$. Comme $\det(K) = \mathbb{Z}_p^*$, cet ensemble est $GL_2(\mathbb{Z}_p)$. □

Le groupe $GL_2(\mathbb{A})$ est un groupe topologique qui contient diagonalement $GL_2(\mathbb{Q})$ et les groupes $GL_2(\mathbb{R})$ et $GL_2(\mathbb{Q}_p)$ pour p premier. La topologie de $GL_2(\mathbb{A})$ est la topologie du produit restreint de $GL_2(\mathbb{R})$ et des $GL_2(\mathbb{Q}_p)$, vis-à-vis des sous-groupes compacts $GL_2(\mathbb{Z}_p)$, p premier. Une base de voisinages de 1 est formée par les $V_\infty \times \prod_p K(p^{n_p})$, où $n_p \geq 0$ et $\tilde{\forall} p n_p = 0$, et où V_∞ parcourt une base de voisinages de 1 dans $GL_2(\mathbb{R})$.

Théorème 21 *On a $GL_2(\mathbb{A}) = GL_2(\mathbb{Q}) \cdot (GL_2(\mathbb{R}) \times \prod_p GL_2(\mathbb{Z}_p))$.*

Preuve : On aura besoin du lemme suivant :

Lemme 8 *Soient $p_1, \ldots, p_n \in \mathbb{P}$ distincts. Soit $(g_1, \ldots, g_n) \in GL_2(\mathbb{Q}_{p_1}) \times \cdots \times GL_2(\mathbb{Q}_{p_n})$. Il existe $\gamma \in GL_2(\mathbb{Q})$ (mieux : $\gamma \in GL_2\left(\mathbb{Z}\left[\frac{1}{p_1 \cdots p_n}\right]\right)$) tel que $(\gamma g_1, \ldots, \gamma g_n) \in GL_2(\mathbb{Z}_{p_1}) \times \cdots \times GL_2(\mathbb{Z}_{p_n})$.*

Preuve du lemme : On raisonne par récurrence sur n. Pour $n = 1$, on l'a déjà fait. Étudions $n > 1$. Par hypothèse de récurrence, il existe $\gamma' \in GL_2(\mathbb{Q})$ tel que $(\gamma' g_1, \ldots, \gamma' g_n) \in GL_2(\mathbb{Z}_{p_1}) \times \cdots \times GL_2(\mathbb{Z}_{p_{n-1}}) \times GL_2(\mathbb{Q}_{p_n})$. Il existe $\gamma_n \in GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ tel que $\gamma_n \gamma' \gamma_n \in GL_2(\mathbb{Z}_p)$. On a $\gamma_n \in GL_2(\mathbb{Z}_{p_i})$ pour $i \neq n$. On a donc $\gamma_n \gamma' \gamma_i \in GL_2(\mathbb{Z}_{p_i})$ pour $i \neq n$: tout va bien.

Revenons au théorème. Soit $g = (g_v)_{v \in \mathscr{S}} \in GL_2(\mathbb{A})$. On a $g_p \in GL_2(\mathbb{Z}_p)$ pour presque tout p. Soit $S = \{p \in \mathscr{S} | g_p \notin GL_2(\mathbb{Z}_p)\}$ (ensemble fini). D'après le lemme, il existe $\gamma \in GL_2\left(\mathbb{Z}\left[\frac{1}{p_1 \cdots p_n}\right]\right)$ teel que $\gamma g_p \in GL_2(\mathbb{Z}_p)$ pour $p \in S$. Mais le résultat est à l'évidence vrai aussi pour $p \notin S$ (car $GL_2\left(\mathbb{Z}\left[\frac{1}{p_1 \cdots p_n}\right]\right) \subseteq GL_2(\mathbb{Z}_p)$ pour $p \notin S$), donc on a le résultat : $\gamma g \in GL_2(\mathbb{R}) \times \prod_p GL_2(\mathbb{Z}_p)$. □

Corollaire 13 *Soit K un sous-groupe compact ouvert de $\prod_p GL_2(\mathbb{Z}_p)$ tel que $\det(K) = \prod_p \mathbb{Z}_p^*$. Alors $GL_2(\mathbb{A}) = GL_2(\mathbb{Q})(GL_2(\mathbb{R}) \times K)$.*

Preuve : Il faut montrer que

$$(GL_2(\mathbb{R}) \times \prod_p GL_2(\mathbb{Z}_p))/\underbrace{(GL_2(\mathbb{Q}) \cap (GL_2(\mathbb{R}) \times \prod_p GL_2(\mathbb{Z}_p)))}_{=GL_2(\mathbb{Z})} \cdot (GL_2(\mathbb{R}) \times K) = \{1\}.$$

Les $GL_2(\mathbb{R})$ « s'annulent », il reste donc à montrer que $GL_2(\mathbb{Z})K = \prod_p GL_2(\mathbb{Z}_p)$. Comme $\det(K) = \prod_p \mathbb{Z}_p^*$, il suffit de voir que $GL_2(\mathbb{Z}) \cdot K$ contient $\prod_p SL_2(\mathbb{Z}_p)$. Pour cela, comme K est ouvert, il suffit de voir que $SL_2(\mathbb{Z})$ est dense dans $\prod_p SL_2(\mathbb{Z}_p)$, comme on le verra plus loin. □

Corollaire 14 *On a $SL_2(\mathbb{A}) = SL_2(\mathbb{Q})\cdot(SL_2(\mathbb{R})\times\prod_p SL_2(\mathbb{Z}_p))$, (on peut remplacer $\prod_p SL_2(\mathbb{Z}_p)$ par K, un sous-groupe compact ouvert de $\prod_p SL_2(\mathbb{Z}_p)$).*

Preuve : Soit $g = (g_v)_v \in SL_2(\mathbb{A})$. Utilisons le théorème. On a $g = \underbrace{g_0}_{\in GL_2(\mathbb{Q})} \left(\underbrace{h_\infty}_{\in GL_2(\mathbb{R})} \prod_p \underbrace{h_p}_{\in GL_2(\mathbb{Z}_p)} \right)$.

On a $1 = \det(g) = \det(g_0)\det(h_p)$ (p premier). On a $h_p = \underbrace{\begin{pmatrix} \det(h_p) & 0 \\ 0 & 1 \end{pmatrix}}_{\in GL_2(\mathbb{Z}_p)} \underbrace{h'_p}_{\in SL_2(\mathbb{Z}_p)}$,

et même $\begin{pmatrix} \det(h_p) & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Q})$, car $\det(h_p) = (\det(g_0))^{-1} \in \mathbb{Q}$. On écrit

$$g = \left(\underbrace{g_0 \prod_p \begin{pmatrix} \det(h_p) & 0 \\ 0 & 1 \end{pmatrix}}_{\in SL_2(\mathbb{Q})} \right) \left(\underbrace{h_\infty \prod_p h'_p}_{\in \prod_p SL_2(\mathbb{Z}_p)} \right). \square$$

Il reste à montrer que $SL_2(\mathbb{Z})$ est dense dans $SL_2(\hat{\mathbb{Z}}) = \prod_p SL_2(\mathbb{Z}_p)$. Autrement dit :

Proposition 24 (Approximation faible) *Soit $N \geq 1$. L'application canonique $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ est surjective (c'est faux si on remplace SL_2 par GL_2).*

Preuve : On peut le démontrer en utilisant le fait que S et T engendrent $SL_2(\mathbb{Z})$ (et $SL_2(\mathbb{Z}/N\mathbb{Z})$). Voici une autre preuve : soit $\bar{g} \in SL_2(\mathbb{Z}/N\mathbb{Z})$. Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ telle que $g \mod N = \bar{g}$. On peut s'arranger pour que a et b soient premiers entre eux. On a $\det(g) \neq 0$, car $\det(g) \equiv 1 \mod N$. Donc $g \in GL_2(\mathbb{Q})$. $GL_2(\mathbb{Q})$ opère sur $\mathbb{P}^1(\mathbb{Q})$. On a $g\infty = \frac{a}{c}$. $SL_2(\mathbb{Z})$ opère transitivement sur $\mathbb{P}^1(\mathbb{Q})$. Il existe $\gamma \in SL_2(\mathbb{Z})$ tel que $\gamma\infty = g\infty$. Donc $\gamma^{-1}g\infty = \infty$, et $\gamma^{-1}g = \begin{pmatrix} u & t \\ 0 & v \end{pmatrix} \in M_2(\mathbb{Z})$. On a $\underbrace{\gamma^{-1}}_{=\begin{pmatrix} u \\ 0 \end{pmatrix}} g \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \gamma^{-1} \begin{pmatrix} a \\ c \end{pmatrix}$. Comme $a \wedge c = 1$, *i.e.*

$\mathbb{Z}a + \mathbb{Z}c = \mathbb{Z}$, et $\gamma^{-1} \in SL_2(\mathbb{Z})$, les coordonnées de $\gamma^{-1} \begin{pmatrix} a \\ c \end{pmatrix}$ sont premières entre elles. Donc u et 0 sont premières entre eux ($u\mathbb{Z} = \mathbb{Z}$), et ceci impose $u \in \{\pm 1\}$. On peut supposer $u = 1$, par exemple. On a alors $g = \begin{pmatrix} 1 & t \\ 0 & v \end{pmatrix} \gamma$ avec $t, v \in \mathbb{Z}$. Comme $\det(\bar{g}) = 1$, on a $v \equiv 1 \mod N$. Bref, $g = \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \gamma$, et $g \equiv \gamma' \mod N$, $\gamma' \in SL_2(\mathbb{Z})$. $\square$

Corollaire 15 (Approximation forte) *$SL_2(\mathbb{Q})SL_2(\mathbb{R})$ et $SL_2(\mathbb{Q})SL_2(\mathbb{Q}_p)$ sont denses dans $SL_2(\mathbb{A})$.*

Preuve : Montrons la densité de $SL_2(\mathbb{Q})SL_2(\mathbb{R})$. Soit $g = (g_v)_v \in SL_2(\mathbb{A})$. Écrivons $g = g_0(h_\infty \prod_p h_p)$ comme d'habitude. Soit $N = \prod_p p^{n_p} \geq 1$ un entier, et posons $K(N) = \prod_p K(p^{n_p}) \subseteq \prod_p SL_2(\mathbb{Z}_p)$. Il existe, d'après la proposition, $\gamma \in SL_2(\mathbb{Z})$ tel que $\gamma^{-1} \prod_p h_p \in K(N)$.

On a $g = (\underbrace{g_0\gamma}_{\in GL_2(\mathbb{Q})})(\underbrace{\gamma^{-1}h_\infty}_{\in SL_2(\mathbb{R})} \prod_p \underbrace{\gamma^{-1}h_p}_{K(N)})$. Donc si on pose $g' = g\gamma$ et $h'_\infty = \gamma^{-1}h_\infty$, alors $g'h'_\infty \in gK(N)$. Pour montrer le deuxième résultat, on procède de façon analogue, en utilisant le fait que $GL_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ est dense dans $GL_2(\mathbb{R})$. □

Soient $k \geq 0$ et $f \in M_k$. Soit $g \in GL_2(\mathbb{A})$. Écrivons $g = \underbrace{g_0}_{\in GL_2(\mathbb{Q})} \left(\underbrace{g_\infty}_{\in GL_2(\mathbb{R})^+} \prod_p \underbrace{g_p}_{\in GL_2(\mathbb{Z}_p)} \right)$, où $g_\infty = \begin{pmatrix} a_\infty & b_\infty \\ c_\infty & d_\infty \end{pmatrix}$, et posons

$$F(g) = f(g_\infty i)(c_\infty i + d)^{-k}$$

($i \in \mathcal{H}$). La décomposition de g est bien définie à $SL_2(\mathbb{Z}) = GL_2(\mathbb{Q}) \cap (GL_2(\mathbb{R})^+ \times \prod_p GL_2(\mathbb{Z}_p))$ près. Si on change g_∞ par γg_∞, $f(g_\infty i)$ ne change pas, car $f \in M_k$. On a ainsi défini $F : GL_2(\mathbb{A}) \to \mathbb{C}$, invariante à gauche par $GL_2(\mathbb{Q})$, invariante à droite par $\prod_p GL_2(\mathbb{Z}_p)$.

Références

[Ser] Jean-Pierre Serre, *Cours d'arithmétique*, chapitre 7, 1970.