COURS DE L'INSTITUT FOURIER

ARMAND BRUMER

II- Séries de Dirichlet et séries *L*

Cours de l'institut Fourier, tome 10 (1975), p. 52-113

<http://www.numdam.org/item?id=CIF_1975__10__A3_0>

II - séries de Dirichlet et séries L

1. *SERIE DE DIRICHLET ASSOCIEE A UNE FORME MODULAIRE* ' (cf.[26])

1.1. FORMES PARABOLIQUES DE TYPE (k,N,ε) .

1.1.1. Nous allons généraliser la notion de forme parabolique, introduite en (I.2.2). Soit N un entier ≥ 1 , ε un caractère de $(\mathbb{Z}/N\mathbb{Z})^*$ dans $\mathbb{C}$. Nous dirons qu'une fonction f de $\mathfrak{H}$ dans $\mathbb{C}$ est une forme parabolique de type (k,N,ε) si f vérifie les 2 conditions suivantes :

(i) f est une forme parabolique de poids k pour $\Gamma(N)$ (au sens de I.2.2).

(ii) Pour toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\Gamma_0(N)$, $f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon(d).f$.

Remarques : Lorsque $\varepsilon = 1$, cela équivaut à dire que f est parabolique de poids k pour $\Gamma_0(N)$. D'autre part, si γ et γ' sont dans $\Gamma_0(N)$, et $\gamma'' = \gamma\cdot\gamma'$, on a $d.d' \equiv d''$ (mod N) (avec des notations évidentes), car $c \equiv 0$ (mod N). Ainsi, ε définit un caractère η de $\Gamma_0(N)$ dans $\mathbb{C}^*$, défini par : $\eta(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \varepsilon(d)$.

Avant de parler de séries de Dirichlet, nous allons démontrer quelques lemmes.

1.1.2. Soit $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in GL_2^+(\mathbb{Z})$; on a : dét. $W_N = N$, $W_N^2 = \begin{pmatrix} -N & 0 \\ 0 & -N \end{pmatrix}$, et $f|_k W_N^2 = (-1)^k f$ pour toute fonction f définie sur $\mathfrak{H}$:

c'est évident si l'on se souvient de la définition :

$$(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(\tau) = (ad-bc)^{k/2}(c\tau+d)^{-k} f(\frac{a\tau+b}{c\tau+d}) \quad \text{(I.2.3.1)}.$$

LEMME. L'opérateur W_N normalise $\Gamma_o(N)$. D'autre part, si f est une forme parabolique de type (k,N,ε) , alors $f|_k W_N$ est parabolique de type $(k,N,\bar{\varepsilon})$.

Ici $\bar{\varepsilon}$ désigne le complexe conjugué de ε .

■ Soit $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_o(N)$, alors

$$W_N \gamma W_N^{-1} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \begin{pmatrix} 0 & 1/N \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -Nb & a \end{pmatrix} = \gamma' \in \Gamma_o(N) ,$$

donc W_N est dans le normalisateur de $\Gamma_o(N)$. Et

$$(f|_k W_N)|_k \gamma = f|_k W_N \gamma = f|_k \gamma' W_N = \varepsilon(a) f|_k W_N .$$

Or $ad \equiv \det \gamma = 1 \pmod N$: ainsi $\varepsilon(a) = \overline{\varepsilon(d)} = \bar{\varepsilon}(d)$. ■

1.1.3. Soient m un entier premier à N , f une forme parabolique de type (k,N,ε) , de développement de Fourier $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$ et χ un caractère primitif modulo m , c'est-à-dire un caractère de $(\mathbb{Z}/m\mathbb{Z})^*$ dans $\mathbb{C}$ qui ne peut se factoriser par aucun $(\mathbb{Z}/d\mathbb{Z})^*$, $(d|m)$. Définissons la fonction f_χ sur $\mathcal{H}$ par :

$$f_\chi(\tau) = \sum_{n\geq 1} a_n \chi(n) e^{2\pi i n\tau} .$$

LEMME. On a la formule suivante : $f|_k \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \overline{\chi(u)} \begin{pmatrix} m & u \\ 0 & m \end{pmatrix} = \mathcal{G}(\bar{\chi}) f_\chi$

où $\mathcal{G}$ est la somme de Gauss :

$$\mathcal{G}(\bar{\chi}) = \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u) e^{2\pi i u/m} \qquad \text{(cf.[17],4.3)}$$

et où l'action notée "$|_k$" de $GL_2^+(\mathbf{R})$ sur les fonctions sur $\mathcal{H}$ est étendue par linéarité à $M_2(\mathbf{R})$.

■ Avec ces notations,

$$(f|_k \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u)\begin{pmatrix} m & u \\ 0 & m\end{pmatrix})(\tau) = (\sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u) f|_k \begin{pmatrix} 1 & u/m \\ 0 & 1\end{pmatrix})(\tau)$$

$$= \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u)\, f(\tau+u/m) \ .$$

Mais le développement de Fourier de f donne $f(\tau) = \sum_{n\geq 1} a_n q^n$ où $q = e^{2\pi i\tau}$, et l'expression précédente vaut :

$$\sum_{n\geq 1} a_n e^{2\pi i n\tau} \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u) e^{2\pi i n u/m} \ .$$

Or, d'après une propriété simple des sommes de Gauss (cf.[17],4.3), on a

$$\sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar{\chi}(u)\, e^{2\pi i n u/m} = \chi(n)\, G(\bar{\chi}) \ .$$

La définition de f_χ donne alors le lemme. ∎

LEMME. Soit α une matrice de $GL_2^+(\mathbb{Z})$, de déterminant ℓ, et N un entier ≥ 1. Alors $\Gamma(N\ell) \subset \alpha^{-1}\Gamma(N)\alpha$.

∎ Soit $\beta \in \Gamma(N\ell)$, i.e. $\beta \equiv 1 \pmod{N\ell}$; alors $\alpha.\beta.\ell\alpha^{-1} \equiv \ell \pmod{N\ell}$, d'où $\alpha\beta\alpha^{-1} \in \Gamma(N)$. ∎

PROPOSITION. La fonction f_χ est une forme parabolique de type $(k, Nf^2, \varepsilon\chi^2)$ et vérifie : $f_\chi|_k W_{Nm^2} = \varepsilon(m)\,\chi(-N)\,\frac{G(\chi)}{G(\bar{\chi})}\, g_{\bar{\chi}}$, où $g = f|_k W_N$.

∎ D'abord, f est modulaire pour $\Gamma(N)$, c'est-à-dire $f|_k\gamma = f$ pour tout γ dans $\Gamma(N)$. Soit $\alpha \in GL_2^+(\mathbb{Z})$; alors $(f|_k\alpha)|_k\alpha^{-1}\gamma\alpha = f|_k\alpha$ autrement dit $f|_k\alpha$ est modulaire pour $\alpha^{-1}\Gamma(N)\alpha$, et a fortiori pour $\Gamma(N\ell)$ d'après le lemme qui précède, si $\ell = \det\alpha$. En particulier, si $\alpha = \begin{pmatrix} m & u \\ 0 & m\end{pmatrix}$, on a $\ell = m^2$, et le lemme (1.1.3) montre que f_χ est modulaire de poids k pour $\Gamma(Nm^2)$.

Montrons que $f_\chi|_k\gamma = \varepsilon\chi^2(d).f_\chi$ si $\gamma = \begin{pmatrix} a & b \\ cNm^2 & d \end{pmatrix} \in \Gamma_o(Nm^2)$:

d'après le lemme (1.1.3), $G(\bar\chi)f_\chi|_k\gamma = \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(u)\, f|_k \begin{pmatrix} m & u \\ 0 & m \end{pmatrix}\gamma$.

Or $\begin{pmatrix} m & u \\ 0 & m \end{pmatrix}\gamma \begin{pmatrix} m & -ud^2 \\ 0 & m \end{pmatrix} = m^2\gamma'$ où $\gamma' \in \Gamma_o(Nm^2)$, d'où $\gamma' \in \Gamma_o(N)$ et $d' \equiv d \pmod N$. Donc $f|_k\begin{pmatrix} m & u \\ 0 & m \end{pmatrix}\gamma = (f|_k\gamma')|_k\begin{pmatrix} m & ud^2 \\ 0 & m \end{pmatrix} = \varepsilon(d)\, f|_k\begin{pmatrix} m & ud^2 \\ 0 & m \end{pmatrix}$.

Ainsi

$$G(\bar\chi)\, f_\chi|_k\gamma = \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(u)\,\varepsilon(d)\, f|_k\begin{pmatrix} m & ud^2 \\ 0 & m \end{pmatrix}$$

$$= \chi(d)^2\varepsilon(d) \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(ud^2)\, f|_k\begin{pmatrix} m & ud^2 \\ 0 & m \end{pmatrix} .$$

Comme d est premier à m , l'application $u \longmapsto ud^2$ est un automorphisme de $(\mathbb{Z}/m\mathbb{Z})^*$; et le lemme (1.1.3) donne :

$$G(\bar\chi)\, f_\chi|_k\gamma = \varepsilon\chi^2(d)\, G(\bar\chi) f_\gamma ;$$

Donc f_χ est de type $(k, Nm^2, \varepsilon\chi^2)$.

Calculons $G(\bar\chi)\, f_\chi|_k W_{Nm^2}$. D'après le lemme (1.1.3), cette fonction est égale à $\sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(u) f|_k \begin{pmatrix} m & u \\ 0 & m \end{pmatrix} W_{Nm^2}$. Or, si u et v vérifient $-Nuw + mv = 1$ (ce qui est possible car N et u sont premiers à m), alors

$$\begin{pmatrix} 1 & u/m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ Nm^2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\begin{pmatrix} m & -w \\ -Nu & v \end{pmatrix}\begin{pmatrix} m & w \\ 0 & m \end{pmatrix} ,$$

d'où

$$G(\bar\chi) f_\chi|_k W_{Nm^2} = \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(u) g|_k \begin{pmatrix} m & -w \\ -Nu & v \end{pmatrix}\begin{pmatrix} m & w \\ 0 & m \end{pmatrix} .$$

Mais d'après le lemme (1.1.2), g est de type $(k, N, \bar\varepsilon)$; or $\bar\varepsilon(v) = \varepsilon(m)$ puisque $mv \equiv 1 \pmod N$, d'où

$$G(\bar\chi) f_\chi|_k W_{Nm^2} = \varepsilon(m) g|_k \sum_{u\in(\mathbb{Z}/m\mathbb{Z})^*} \bar\chi(u)\begin{pmatrix} m & w \\ 0 & m \end{pmatrix} .$$

Enfin, comme $-Nuw \equiv 1 \pmod m$, $\bar\chi(u) = \chi(-N).\chi(w)$, et w parcourt $(\mathbb{Z}/m\mathbb{Z})^*$ lorsque u parcourt $(\mathbb{Z}/m\mathbb{Z})^*$. Le lemme (1.1.3) permet de conclure :

$$G(\bar\chi) f_\chi|_k W_{Nm^2} = \varepsilon(m)\chi(-N) g|_k \sum_{w\in(\mathbb{Z}/m\mathbb{Z})^*} \chi(w)\begin{pmatrix} m & w \\ 0 & m \end{pmatrix} = \varepsilon(m)\chi(-N) G(\chi) g_{\bar\chi} . \blacksquare$$

1.1.5. *LEMME*. Soit f une forme parabolique de poids k pour un sous-groupe G d'indice fini de Γ . Pour τ dans $\mathcal{H}$, posons $\tau = x+iy$ et $q = e^{2\pi i\tau}$. Soit $f(\tau) = \sum_{n\geq 1} a_n q^n$ le développement de Fourier de f . Alors :

(i) il existe une constante M telle que $|f(\tau)| \leq M.y^{-k/2}$.

(ii) $a_n = O(n^{k/2})$.

▪ La fonction $h(\tau) = |f(\tau)|y^{k/2}$ vérifie, pour tout γ dans G :

$$h(\gamma\tau) = |f(\gamma\tau)|\,(\mathrm{Im}(\gamma\tau))^{k/2} = |c\tau+d|^k\,|f(\tau)|\left(\frac{\mathrm{Im}\,\tau}{|c\tau+d|^2}\right)^{k/2} = h(\tau)$$

donc h est continue sur $\bar{G}\backslash\mathcal{H}$. Comme $e^{-2\pi y}$ décroît plus vite que $y^{-k/2}$, h est défini par une série convergente à l'infini. Ainsi h est continue sur le compact $\widehat{\bar{G}\backslash\mathcal{H}}$, d'où l'existence de M .

D'autre part, $a_n = \int_0^1 f(\tau)e^{-2\pi in\tau}dx$, donc

$$|a_n| \leq \int_0^1 |f(\tau)|e^{2\pi ny}dx \leq My^{-k/2}e^{2\pi ny}$$

pour tout $y > 0$, en particulier pour $y = 1/n$. D'où

$$|a_n| \leq Mn^{k/2}e^{2\pi} \quad . \quad \blacksquare$$

1.2. - SERIES DE DIRICHLET.

1.2.1. Soient f une forme parabolique de type (k,N,ϵ) , de développement de Fourier $f(\tau) = \sum_{n\geq 1} a_n q^n$ (où $q = e^{2\pi i\tau}$) , m un entier premier à N , χ un caractère primitif modulo m , s une variable complexe. Définissons les séries de Dirichlet :

$$L(s,f,\chi) = \sum_{n\geq 1} a_n\chi(n)n^{-s}$$

et

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

où Γ est la fonction d'Euler : $\Gamma(s) = \int_0^{+\infty} e^{-t}t^{s-1}dt$.

THEOREME.

(i) La série L est convergente pour $\mathrm{Re}(s) > 1 + k/2$.

(ii) La série L se prolonge analytiquement en une fonction entière (encore notée L).

(iii) La série L vérifie l'équation fonctionnelle :

$$\Lambda(s,f,\chi) = i^k \epsilon(m)\,\chi(-N)\,\frac{G(\chi)}{G(\bar{\chi})}\,\Lambda(k-s,g,\bar{\chi})$$

où $g = f\,|_k\, W_N$.

■ D'après le lemme (1.1.5), $a_n = O(n^{k/2})$, d'où (i) .

Montrons qu'il suffit de démontrer (ii) et (iii) lorsque $\chi = 1$ et $m = 1$: en effet, $f_\chi = \sum a_n \chi(n) q^n$ est de type $(k, Nm^2, \epsilon\chi^2)$ d'après la proposition (1.1.4), donc $L(s,f,\chi) = L(s,f_\chi,1)$ et $\Lambda(s,f,\chi) = m^s \Lambda(s,f_\chi,1)$.

Supposons (ii) et (iii) démontrés pour $\chi = 1$, $m = 1$. Alors (ii) est vrai pour m et χ quelconques, et l'équation fonctionnelle nous donne :

$$\Lambda(s,f_\chi,1) = i^k \Lambda(k-s, f_\chi\,|_k\, W_{Nm^2}, 1) .$$

Or la proposition (1.1.4) montre que $f_\chi\,|_k\, W_{Nm^2} = c_\chi g_{\bar{\chi}}$ si on pose

$$c_\chi = \epsilon(m)\,\chi(-N)\,\frac{G(\chi)}{G(\bar{\chi})} .$$

D'où : $m^s \Lambda(s,f_\chi,1) = i^k c_\chi m^s \Lambda(k-s,g_{\bar{\chi}},1)$ c'est-à-dire

$$\Lambda(s,f,\chi) = i^k c_\chi \Lambda(k-s,g,\bar{\chi}) .$$

Supposons donc maintenant que $m = 1$ et $\chi = 1$, et utilisons la transformation de Mellin : soit $I(s) = \int_0^\infty f(iy) y^s \frac{dy}{y}$. Pour tout s tel que $\mathrm{Re}(s) > 1 + k/2$, cette intégrale est convergente, et même $\int_{1/\sqrt{N}}^\infty f(iy)\, y^s \frac{dy}{y}$ est une fonction entière de s . Mais

$$\int_0^{1/\sqrt{N}} f(iy) y^s \frac{dy}{y} = N^{-s} \int_{1/\sqrt{N}}^\infty f(i/Nu) u^{-s} \frac{du}{u}$$

par le changement de variable $y = 1/Nu$; et $f(i/Nu) = f(W_N(iu))$,

alors que $g(iu) = (f|_k W_N)(iu) = N^{k/2}(Niu)^{-k} f(W_N(iu))$. Ainsi,

$$I(s) = \int_{1/\sqrt{N}}^{\infty} f(iy)\, y^s \frac{dy}{y} + i^k N^{k/2-s} \int_{1/\sqrt{N}}^{\infty} g(iy)\, y^{k-s} \frac{dy}{y}$$

est une fonction entière de s . Or

$$I(s) = \sum_{n\geq 1} a_n \int_0^{\infty} e^{-2\pi n y} y^s \frac{dy}{y} = (2\pi)^{-s} L(s,f,1)\Gamma(s) = N^{-s/2}\Lambda(s,f,1) ,$$

et $\Gamma(s)$ n'a pas de zéro dans $\mathbb{C}$; donc $L(s) = (2\pi)^s I(s)/\Gamma(s)$, et l'assertion (ii) est démontrée.

Enfin, remplaçons (f,s) par $(g,k-s)$ dans l'égalité :

$$\Lambda(s,f,1) = N^{s/2} \int_{1/\sqrt{N}}^{\infty} f(iy) y^s \frac{dy}{y} + i^k N^{k/2-s/2} \int_{1/\sqrt{N}}^{\infty} g(iy) y^{k-s} \frac{dy}{y} .$$

Cela donne :

$$\Lambda(k-s,g,1) = N^{k/2-s/2} \int_{1/\sqrt{N}}^{\infty} g(iy) y^{k-s} \frac{dy}{y} + i^k N^{s/2} \int_{1/\sqrt{N}}^{\infty} f|_k W_N^2 (iy) y^s \frac{dy}{y} .$$

Comme $f|_k W_N^2 = (-1)^k f$ (cf. 1.1.2), nous obtenons :

$$\Lambda(s,f,1) = i^k \Lambda(k-s,g,1)$$

c'est-à-dire (iii) . ∎

1.2.2. En guise de réciproque, Weil a démontré le résultat suivant (cf. [26] , théorème 17) :

Soient N un entier ≥ 1 , $\mathcal{M}$ un ensemble de nombres entiers premiers à N , chacun étant égal à 4 ou à un nombre premier > 2 , $\mathcal{M}$ rencontrant toute progression arithmétique de la forme $\{a+nb\}_n$ où $(a,b) = 1$; soient ϵ un caractère de $(\mathbb{Z}/N\mathbb{Z})^*$ dans $\mathbb{C}$, C une constante égale à ± 1 et $a_1, a_2, \ldots, a_n, \ldots$ des nombres tels que $a_n = O(n^{\sigma})$ pour un certain $\sigma > 0$. Pour tout entier m premier à N et tout caractère χ primitif modulo m , posons

$$L_\chi(s) = \sum a_n \chi(n) n^{-s}$$

et

$$\Lambda_\chi(s) = N^{s/2} m^s (2\pi)^{-s}\, L_\chi(s) .$$

Soit

$$f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n \tau} .$$

THEOREME. Si, pour tout m dans $\mathcal{M}$ et tout χ primitif modulo m, $\Lambda_\chi(s)$ se prolonge analytiquement en une fonction entière de s bornée dans toute bande verticale, et vérifie l'équation fonctionnelle :

$$\Lambda_\chi(s) = C_\chi \Lambda_{\bar\chi}(k-s)$$

où $C_\chi = C\,\varepsilon(m)\,\chi(-N)\,\frac{\mathcal{G}(\chi)}{\mathcal{G}(\bar\chi)}$, et si $L(s)$ est absolument convergente en un point $s = k-\delta$ (avec $\delta > 0$), alors f est une forme parabolique de type (k,N,ε) et vérifie l'équation fonctionnelle : $f = c\,i^k f\,|_k W_N$.

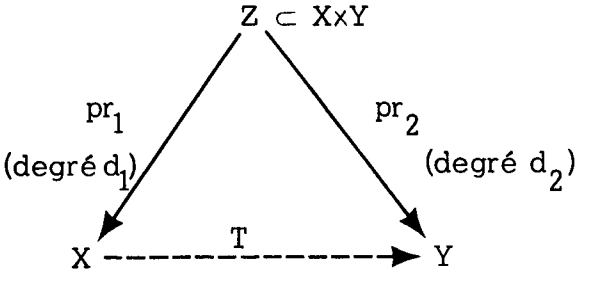
2. *PRODUIT EULERIEN*

2.1. - CORRESPONDANCES DE HECKE.

2.1.1. Soient X et Y deux courbes définies sur un corps K. Une application T de X dans l'ensemble $\mathcal{D}_n(Y)$ des diviseurs de degré n sur Y est appelée une correspondance de X dans Y définie sur K s'il existe une courbe Z définie sur K, contenue dans $X \times Y$, telle que

$$T(x) = \sum_{i=1}^{d_1} (y_i) \quad \text{si} \quad \{(x,y_i)\}_{1\le i\le d_1} = pr_1^{-1}(x)$$

(on note pr_1 (resp. pr_2) la projection de Z sur X (resp. sur Y), et d_1 (resp. d_2) son degré) ;



Remarquons que, pour presque tout x, les d_1 valeurs des y_i sont distinctes. Par linéarité, T induit une application de $\mathcal{D}(X)$ dans $\mathcal{D}(Y)$ telle que pour tout $d \in \mathbb{N}$, $\mathcal{D}_d(X)$ est envoyé dans $\mathcal{D}_{nd}(Y)$, et en particulier $\mathcal{D}_o(X)$ dans $\mathcal{D}_o(Y)$.

Lorsque Z est une variété irréductible, on dit que T est une correspondance irréductible.

2.1.2. Correspondance de Hurwitz (ou Hecke) .

C'est une correspondance de $X_0(N)$ dans lui-même : pour tout entier $n \geq 1$, définissons T_n sur $Y_0(N)$ par

$$T_n((E,C)) = \sum_{\substack{F \text{ sous-groupe de } E \\ |F| = n \\ C \cap F = \{0\}}} (E/F, C+F/F) .$$

Rappelons que $Y_0(N)$ est formé des classes de $\mathbb{C}$-isomorphisme des couples (E,C) où E est une courbe elliptique sur $\mathbb{C}$ et C un sous-groupe cyclique d'ordre N de E . D'après (I.4.3.3), E/F est une courbe elliptique. Et $C+F/F \simeq C/C \cap F \simeq C$ est un sous-groupe de E/F d'ordre N .

On vérifie (cf. [43] ,7.2) que T_n est une correspondance sur $Y_0(N)$, et on la prolonge à $X_0(N)$.

T_n est rationnelle sur $\mathbb{Q}$, car, si (E,C) est rationnel sur $\mathbb{Q}$, les sous-groupes F de E d'ordre n tels que $C \cap F = \{0\}$ sont permutés par l'action du groupe de Galois.

2.1.3. Calcul de T_n : Calculons T_n à partir des T_ℓ (ℓ premier) (cf. [38] , proposition 10, ou [26] , théorème 6).

PROPOSITION.

(i) Si $(n,m) = 1$, alors $T_{nm} = T_n \cdot T_m = T_m \cdot T_n$.

(ii) Si ℓ est premier et $r \geq 1$, alors

$$T_{\ell^r} \cdot T_\ell = \begin{cases} T_{\ell^{r+1}} & \text{si } \ell | N \\ T_{\ell^{r+1}} + \ell T_{\ell^{r-1}} & \text{si } \ell \nmid N \end{cases} .$$

(iii) Pour tous les entiers n et $m \geq 1$, on a :

$$T_n \cdot T_m = \sum_{\substack{d | (n,m) \\ (d,N)=1}} d\, T_{nm/d^2} .$$

■ (i) On a :

$$T_n \cdot T_m((E,C)) = T_n\Big(\sum_{\substack{F\subset E\\ |F|=m\\ F\cap C=\{0\}}} (E/F, C+F/F)\Big)$$

$$= \sum_{\substack{F\subset E\\ |F|=m\\ F\cap C=\{0\}}} \ \sum_{\substack{F'\subset E/F\\ |F'|=m\\ F'\cap(C+F/F)=\{0\}}} (E/F/F', (C+F/F)+F'/F') \quad .$$

Posons $F'' = F+F'$. Alors $F \subset F'' \subset E$, $|F''| = nm$, et $F'' \cap C = \{0\}$. Or $(m,n) = 1$, et donc, pour tout sous-groupe F'' de E d'ordre nm tel que $F'' \cap C = \{0\}$, il existe un et un seul sous-groupe F de F'' d'ordre n , et $F \cap C = \{0\}$. D'où :

$$T_n T_m((E,C)) = \sum_{\substack{F''\subset E\\ |F''|=nm\\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') = T_{nm}((E,C)) \quad .$$

(ii) De manière analogue,

$$T_{\ell^r} T_\ell((E,C)) = \sum_{\substack{F\subset E\\ |F|=\ell\\ F\cap C=\{0\}}} \ \sum_{\substack{F\subset F''\subset E\\ |F''|=\ell^{r+1}\\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') \quad .$$

Notons, pour tout groupe abélien A , A_ℓ le sous-groupe des éléments dont l'ordre divise ℓ .

Partons d'un sous-groupe F'' de E d'ordre ℓ^{r+1} d'intersection nulle avec C , et cherchons les sous-groupes F de F'' d'ordre ℓ . Si $\ell | N$, F''_ℓ et C_ℓ sont deux sous-groupes non nuls de $E_\ell \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ d'intersection nulle. Donc F'' a un seul sous-groupe d'ordre ℓ , égal à F''_ℓ , et

$$T_{\ell^r} T_\ell((E,C)) = \sum_{\substack{F''\subset E\\ |F''|=\ell^{r+1}\\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') = T_{\ell^{r+1}}((E,C)) \quad .$$

Si $\ell \nmid N$, ou bien F'' est cyclique et a un seul sous-groupe d'ordre ℓ égal à F''_ℓ , ou bien F'' n'est pas cyclique, F''_ℓ non plus, et alors $F''_\ell = E_\ell \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ a $(\ell+1)$ sous-groupes d'ordre ℓ . D'où :

$$T_{\ell^r} T_\ell((E,C)) = \sum_{\substack{F''\subset E \\ |F''|=\ell^{r+1} \\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') + \ell \sum_{\substack{E_\ell\subset F''\subset E \\ |F''|=\ell^{r+1} \\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') .$$

Or, lorsque F'' contient E_ℓ , $(E/F'', C+F''/F'')$ est $\overline{K}$-isomorphe à $\Big((E/E_\ell)/(F''/E_\ell)\,,\,(C+E_\ell/E_\ell)+(F''/E_\ell)/(F''/E_\ell)\Big)$. Comme la multiplication par ℓ donne la suite exacte $0 \longrightarrow E_\ell \longrightarrow E \xrightarrow{\ell} E \longrightarrow 0$ et induit un isomorphisme de E/E_ℓ sur E , dans lequel $C+E_\ell/E_\ell$ est transformé en C , et les sous-groupes F'' de E d'ordre ℓ^{r+1} contenant E_ℓ en les sous-groupes F de E d'ordre ℓ^{r-1} , on a dans $Y_o(N)$:

$$\sum_{\substack{E_\ell\subset F''\subset E \\ |F''|=\ell^{r+1} \\ F''\cap C=\{0\}}} (E/F'', C+F''/F'') = \sum_{\substack{F\subset E \\ |F|=\ell^{r-1} \\ F\cap C=\{0\}}} (E/F, C+F/F) = T_{\ell^{r-1}}((E,C)) .$$

Ainsi $T_{\ell^r} T_\ell = T_{\ell^{r+1}} + \ell\, T_{\ell^{r-1}}$ si $\ell \nmid N$.

(iii) est une simple combinaison de (i) et (ii) . ∎

COROLLAIRE. Les correspondances T_ℓ (pour ℓ premier) engendrent une algèbre commutative, qui contient tous les T_n .

2.2. - OPERATEURS DE HECKE.

2.2.1. Lorsque $E = \mathbb{C}/L$, la base $\{\omega_1, \omega_2\}$ de L peut être choisie de telle sorte que $C = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2/N/L$. Un tel choix étant fait, il y a une bijection entre les sous-groupes F de E d'ordre n et les réseaux L' de $\mathbb{C}$ contenant L et tels que $[L':L] = n$, bijection définie par : $F = L'/L$. Ainsi,

$$T_n((E,C)) = \sum_{\substack{L'\supset L \\ [L':L]=n \\ (\mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2/N)+L'/L' \text{ cyclique d'ordre } N}} (\mathbb{C}/L', (\mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2/N)+L'/L') .$$

Or, les conditions $L' \supset L$ et $[L':L] = n$ sont équivalents à l'existence d'une matrice A dans $M_2(\mathbb{Z})$, de déterminant n, telle que $L' = A^{-1}L$. De plus, un changement de base dans L' correspond à la multiplication à droite de A par un élément de Γ. Donc les réseaux L' tels que $L' \supset L$ et $[L':L] = n$ sont classifiés par n'importe qu'el système de représentants de l'ensemble des matrices de $M_2(\mathbb{Z})$ de déterminant n, modulo l'action à droite de Γ, par exemple $\{\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \mid ad = n\ ,\ a > 0\ ,\ 0 \leq b < d\}$.

Soit $A = \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$, alors $A^{-1} = \begin{pmatrix} a/n & b/n \\ 0 & d/n \end{pmatrix}$ et

$$L' = \mathbb{Z}(a\omega_1 + b\omega_2)/n \oplus \mathbb{Z}\, d\omega_2/n\ .$$

Donc

$$(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2/N) + L'/L' = \mathbb{Z}(a\omega_1 + b\omega_2)/n \oplus \mathbb{Z}(\tfrac{d}{n} + \tfrac{1}{N})\omega_2/L' \simeq (\tfrac{d}{n} + \tfrac{1}{N})\mathbb{Z}/\tfrac{d}{n}\mathbb{Z}$$
$$= (\tfrac{1}{a} + \tfrac{1}{N})\mathbb{Z}/\tfrac{1}{a}\mathbb{Z}\ ;$$

ce groupe est cyclique d'ordre N si et seulement si $(N,a) = 1$, d'où le résultat :

PROPOSITION. Soit $(E,C) \in Y_0(N)(\mathbb{C})$ défini par : $E = \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, $C = \mathbb{Z}\omega_1 \oplus \mathbb{Z}(\omega_2/N)/L$. Alors :

$$T_n((E,C)) = \sum_{\substack{A=\left(\begin{smallmatrix} d & -b \\ 0 & a \end{smallmatrix}\right) \\ ad=n,\ a>0 \\ 0\leq b<d,\ (a,n)=1}} \left(\mathbb{C}/A^{-1}L\ ,\ \mathbb{Z}((a\omega_1 + b\omega_2)/n) \oplus \mathbb{Z}(d\omega_2/nN)/A^{-1}L\right)$$

2.2.2. L'identification de $Y_0(N)(\mathbb{C})$ avec $\overline{\Gamma_0(N)}\backslash\mathcal{H}$ (cf. I-4.2.1) permet de définir T_n sur $\overline{\Gamma_0(N)}\backslash\mathcal{H}$ par :

$$T_n(\tau) = \sum_{\substack{ad=n \\ a>0 \\ 0\leq b<d \\ (a,N)=1}} \frac{a\tau + b}{d}\ .$$

PROPOSITION. Soit $\Sigma_n = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})/ad-bc=n\ ,\ (a,N) = 1\ ,\ c \equiv 0 \pmod N\}$. Alors (i) $\Gamma_o(N)$ opère par multiplication à droite et à gauche sur Σ_n, (ii) on a $\Gamma_o(N).\Sigma_n = \Sigma_n.\Gamma_o(N) = \Sigma_n$ et (iii)

$$\Sigma_n = \coprod_{\substack{ad=n \\ a>0 \\ 0\le b<d \\ (a,N)=1}} \Gamma_o(N)\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \coprod_{\substack{ad=n \\ a>0 \\ a\mid d \\ (a,N)=1}} \Gamma_o(N)\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\Gamma_o(N)$$

(où le symbole $\coprod$ indique la réunion disjointe).

■ La vérification de (i) et (ii) est immédiate. Etant donné une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de Σ_n, essayons de déterminer $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_o(N)$ et $\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ telle que $a'd' = n$, $a' > 0$, $0 \le b' < d'$, $(a',N) = 1$, de sorte qu'on ait $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ c'est-à-dire :

$$\begin{cases} \gamma a + \delta c = 0 \\ \gamma b + \delta d = d' \\ \alpha a + \beta c = a' \\ \alpha b + \beta d = b' \ . \end{cases}$$

Notons $e = (a,c)$ le pgcd de a et c, et remarquons que e divise $n = ad - bc$ et est premier à N ; alors les solutions (γ,δ) de la 1ère équation : $\gamma a + \delta c = 0$, sont les couples $(-k\frac{c}{e}, k\frac{a}{e})$ où $k \in \mathbb{Z}$ et l'on a : $\gamma \equiv 0 \pmod N$. Comme $\alpha\delta - \beta\gamma$ est à la fois égal à 1 et divisible par k, on voit que $k = \pm 1$. La 2e équation donne alors : $d' = k\,\frac{ad-bc}{e} = k\,\frac{n}{e}$: on veut $d' > 0$, ce qui impose $k = +1$ et alors $a' = \frac{n}{d'} = e$. Ainsi, nous avons déterminé de manière unique les nombres γ, δ, a', d'. Restent α, β, b'. Le système formé par les 2 dernières équations, où l'on prend b' comme paramètre et (α,β) comme inconnues, est un système de Cramer, et a une solution unique, dans $\mathbb{Q}^2$, pour chaque valeur entière de b', à savoir $(\alpha,\beta) = (\frac{ed-b'c}{n}, \frac{ab'-eb}{n})$. Les valeurs de b' pour lesquelles $(\alpha,\beta) \in \mathbb{Z}^2$ forment une progression arithmétique dont la raison k' est le plus petit entier tel que $\frac{k'c}{n}$ et $\frac{k'a}{n}$ soient entiers ; autrement dit $k' = \frac{n}{2} = d'$. Ainsi, il existe une seule valeur de b' telle que $0 \le b' < d'$ et que $(\alpha,\beta) \in \mathbb{Z}^2$. En résumé, nous avons montré la 1ère formule de (iii).

Pour la 2e formule, remarquons que (a,d) divise toutes les matrices de $\Gamma_o(N)\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\Gamma_o(N)$, et que $(a,d) = a$. Cela nous permet de nous ramener à démontrer que les matrices primitives de Σ_n , c'est-à-dire les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de Σ_n telles que $(a,b,c,d) = 1$ forment la double classe $\Gamma_o(N)\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\Gamma_o(N)$. Et la 1ère formule permet de supposer que $c = 0$. Ainsi, il s'agit de montrer que toute matrice de Σ_n de la forme $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ s'écrit $\tau\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\tau'$ pour deux matrices τ et τ' de $\Gamma_o(N)$. Etant donnés 4 entiers $\alpha,\beta,\gamma,\delta$, posons $\tau_1 = \begin{pmatrix} a\alpha & b\alpha+d\beta \\ \gamma & \delta \end{pmatrix}$ et $\tau_2 = \begin{pmatrix} \alpha & \beta \\ d\gamma & a\delta-b\gamma \end{pmatrix}$: alors $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\tau_1 = \tau_2\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ car $ad = n$. Reste à déterminer $(\alpha,\beta,\gamma,\delta)$ de sorte que τ_1 et τ_2 soient dans $\Gamma_o(N)$, c'est-à-dire de sorte que $\gamma \equiv 0 \pmod N$ et $a\alpha\delta - b\alpha\gamma - d\beta\gamma = 1$. Or $(a,N) = 1$ et $(a,b,d) = 1$, donc $(a,Nb,Nd) = 1$. Le théorème de la progression arithmétique (cf.[38] ,6) appliqué aux nombres $\frac{a}{(a,bN)}$ et $\frac{-bN}{(a,bN)}$ prouve qu'il y a une infinité de nombres premiers congrus à $\frac{-bN}{(a,bN)}$ modulo $\frac{a}{(a,bN)}$. Soit $p = \frac{a}{(a,bN)}\delta - \frac{bN}{(a,bN)}$ un de ceux-ci, tel que $p > dN$. Alors $(p,dN) = 1$, et comme $(a,bN,dN)=1$ nous obtenons $((a,bN)p,dN) = (a\delta-bN,dN) = 1$. Le théorème de Bezout prouve alors l'existence de α,β tels que $a\alpha\delta - b\alpha N - d\beta N = 1$, et il suffit de poser $\gamma = N$. ∎

2.2.3. Maintenant, nous pouvons définir <u>l'opérateur de Hecke</u> T_n sur les formes modulaires de poids k pour $\Gamma_o(N)$ par :

$$f|_k T_n = n^{k/2-1} \sum_{i\in I} f|_k \alpha_i$$

où $\{\alpha_i\}_{i\in I}$ est un système de représentants des classes à gauche de Σ_n modulo $\Gamma_o(N)$ (par exemple $\{\alpha_i\}_{i\in I} = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) / ad=n\ ,\ a>0\ ,\ 0 \le b < d\ ,\ (a,N) = 1\}$, cf.2.2.2).

<u>Remarques</u> : (i) T_1 est l'identité ; (ii) la définition de $f|_k T_n$ est indépendante du choix des α_i : en effet, si $\gamma \in \Gamma_o(N)$, alors

$$f|_k \gamma\alpha_i = (f|_k \gamma)|_k \alpha_i = f|_k \alpha_i \ .$$

2.2.4. *PROPOSITION*. Si la fonction f est une forme modulaire (resp. parabolique) de poids k pour $\Gamma_o(N)$, il en est de même pour la fonction $f|_k T_n$.

■ Soit $\gamma \in \Gamma_o(N)$; alors $\{\alpha_i\gamma\}_{i\in I}$ forme un autre système de représentants des classes à gauche de Σ_n modulo $\Gamma_o(N)$, donc

$$(f|_k T_n)|_k \gamma = n^{k/2-1} \sum_{i\in I} f|_k \alpha_i = f|_k T_n .$$

D'autre part, $f|_k T_n$ est holomorphe dans $\mathcal{H}$. Vérifions qu'elle est holomorphe aux pointes ; tout d'abord, calculons son développement de Fourier à l'infini, à partir de celui de f :

$$f(\tau) = \sum_{\nu\geq 0} a_\nu e^{2\pi i\nu\tau} ,$$

et choisissons $\{\alpha_i\}_{i\in I} = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = n \ , \ a > 0 \ , \ 0 \leq b < d \ , \ (a,N)=1\}$. Alors

$$(f|_k T_n)(\tau) = n^{k/2-1} \sum_{(a,d)} \sum_{\substack{ad=n \\ a>0 \\ (a,N)=1}} \sum_{0\leq b<d} n^{k/2} d^{-k} f\left(\frac{a\tau+b}{d}\right)$$

$$= n^{-1} \sum_{(a,d)} \sum_{\substack{ad=n \\ a>0 \\ (a,N)=1}} a^k \sum_{\nu\geq 0} a_\nu e^{2\pi i\nu\frac{a}{d}\tau} \sum_{0\leq b<d} e^{2\pi i\nu\frac{b}{d}} .$$

Or

$$\sum_{0\leq b<d} e^{2\pi i\nu\frac{b}{d}} = \begin{cases} 0 & \text{si } \nu \not\equiv 0 \bmod d \\ d & \text{si } \nu \equiv 0 \bmod d \end{cases} .$$

D'où :

$$(f|_k T_n)(\tau) = \sum_{\nu\geq 0} a_\nu(n) e^{2\pi i\nu\tau}$$

où $a_\nu(n) = \sum_{a:\ \substack{a|(\nu,n) \\ a>0 \\ (a,N)=1}} a\, a_{n\nu/a^2}\, a^{k-1}$. Ainsi $f|_k T_n$ est holomorphe à l'infini, et $a_o(n) = a_o\left(\sum_{a:\ \substack{a|(\nu,n) \\ a>0 \\ (a,N)=1}} a^{k-1}\right)$ est nul dès que a_o est

nul . Par conjugaison, $f|_k T_n$ est holomorphe à toutes les pointes de $\overline{\Gamma(nN)\backslash \mathfrak{H}}$, et parabolique dès que f l'est. Comme

$$\alpha_i^{-1}\Gamma_o(N)\alpha_i \supset \alpha_i^{-1}\Gamma(N)\alpha_i \supset \Gamma(nN)$$

d'après le lemme (1.1.4), la proposition est démontrée. ∎

Remarque : $\Gamma(N)$ est un sous-groupe distingué de Γ , ce qui permet de comparer les pointes à la pointe infinie.

2.3. - PRODUIT EULERIEN.

2.3.1. *THEOREME* . Soit f une forme parabolique de poids k pour Γ , de développement de Fourier :

$$f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau} .$$

Supposons que f est fonction propre pour tous les opérateurs de Hecke, c'est-à-dire qu'il existe, pour tout entier n , un nombre complexe c_n tel que : $f|_k T_n = c_n f$. Alors a_1 est non nul, et l'on peut remplacer f par $1/a_1 \cdot f$. On obtient alors : $a_n = c_n$ pour tout n , et :

$$L(s,f,1) = \prod_{\ell | N} (1-a_\ell \ell^{-s})^{-1} \prod_{\ell \nmid N} (1-a_\ell \ell^{-s} + \ell^{k-1-2s})^{-1} .$$

∎ Comme $f|_k T_n = c_n f$, leurs développements de Fourier coïncident, c'est-à-dire $a_\nu(n) = c_n a_\nu$ pour tout $\nu \in \mathbb{N}$. Or (cf. 2.2.4),

$$a_\nu(n) = \sum_{a \begin{cases} a|(\nu,n) \\ a>0 \\ (a,N)=1 \end{cases}} a_{n\nu/a^2}\, a^{k-1} = a_n(\nu) ,$$

donc $c_n a_\nu = c_\nu a_n$ et en particulier $c_1 a_n = c_n a_1$. Mais T_1 agit trivialement sur f , donc $c_1 = 1$; supposons a_1 nul : alors a_n est nul pour tout n , et f est nulle, ce qui est impossible pour une fonction propre. Ainsi a_1 est non nul, et, quitte à remplacer f par $\frac{1}{a_1} f$, on peut supposer que $a_1 = 1$. Alors, pour tout n , $c_n = a_n$, et

$$L(s,f,1) = \sum_{n\geq 1} a_n/n^s = \sum_{n\geq 1} c_n/n^s \ .$$

Reste à vérifier que $\sum_{n\geq 1} a_n/n^s$ a le produit eulérien indiqué. Mais le calcul des T_n (cf. 2.1.3) se traduit sur les c_n, donc sur les a_n, par : $a_{nm} = a_n \cdot a_m$ si $(n,m) = 1$, $a_{\ell^i} = (a_\ell)^i$ si $\ell | N$, et $a_{\ell^{i+1}} + \ell^{k-1} a_{\ell^{i-1}} - a_{\ell^i} \cdot a_\ell = 0$ si $\ell \nmid N$. La 1ère formule prouve que

$$\sum_{n\geq 1} a_n/n^s = \prod_{\ell} \sum_{i\geq 0} a_{\ell^i}/\ell^{is} \ ,$$

la 2e que

$$(1-a_\ell \ell^{-s})^{-1} = \sum_{i\geq 0} a_{\ell^i}/\ell^{is} \quad \text{si} \quad \ell | N \ ,$$

et la 3e que

$$(1-a_\ell \ell^{-s} + \ell^{k-1-2s})(\sum_{i\geq 0} a_{\ell^i}\ell^{-is}) = 1 + \sum_{i\geq 1} (a_{\ell^{i+1}} - a_\ell a_{\ell^i} + \ell^{k-1} a_{\ell^{i-1}})\ell^{-is}$$

$$= 1 \quad \text{si} \quad \ell \nmid N \ ,$$

d'où le théorème. ∎

2.3.2. Exemple. L'espace des formes paraboliques de poids 12 pour Γ est stable par T_n. Comme il est de dimension 1 sur $\mathbb{C}$, tous ses éléments non nuls sont fonctions propres des T_n, en particulier

$$\Delta = q \prod_{n\geq 1} (1-q^n)^{24} = \sum_{n\geq 1} \tau(n) q^n \ ,$$

à laquelle on peut appliquer le théorème (N = 1) :

$$\sum_{n\geq 1} \frac{\tau(n)}{n^s} = \prod_{\ell} \frac{1}{1 - \tau(\ell)\ell^{-s} + \ell^{11-2s}} \ .$$

Nous avons aussi, par la proposition (2.1.3) :

$$\tau(nm) = \tau(n).\tau(m) \quad \text{si} \quad (n,m) = 1$$

et

$$\tau(p)\cdot\tau(p^r) = \tau(p^{r+1}) + p^{11}\,\tau(p^{r-1}) \ .$$

2.3.3. Remarque : Il existe au plus une forme modulaire non parabolique, de poids donné k, qui soit fonction propre des opérateurs de Hecke, (à une constante multiplicative près) :

D'après (2.3.1), $a_o c_n = \sum_{\substack{a \mid n \\ a>0 \\ (a,N)=1}} a_o a^{k-1}$; si on suppose a_o non nul, la valeur propre c_n vaut $\sum_{\substack{a \mid n \\ a>0 \\ (a,N)=1}} a^{k-1}$; enfin $a_n = c_n \cdot a_1$.

3. *FONCTIONS PROPRES DES OPERATEURS DE HECKE*

Il s'agit ici de déterminer les formes f auxquelles s'applique le théorème (2.3.1).

3.1. - PRODUIT SCALAIRE DE PETERSSON. (cf. [26], 3 ou [12], 3).

3.1.1. *LEMME* . Soient D un ensemble mesurable de $\mathbf{R}^2$, f et g deux fonctions holomorphes dans $\mathcal{H}$, et α un élément de $GL_2^+(\mathbf{R})$. Alors

$$\iint_D (f|_k\alpha)\,(\overline{g|_k\alpha})\,y^k\,\frac{dx\,dy}{y^2} = \iint_{\alpha(D)} f\bar{g}\,y^k\,\frac{dx\,dy}{y^2} \quad .$$

■ D'après (I,2.2.1),

$$(f|_k\alpha)\cdot(\overline{g|_k\alpha})(\tau) = (\det\alpha)^k\cdot|c\tau+d|^{-2k} f(\alpha\tau)\cdot\overline{g(\alpha\tau)} \ ;$$

Or

$$\mathrm{Im}(\alpha\tau) = (\det\alpha)\,|c\tau+d|^{-2}\,\mathrm{Im}(\tau) \ ,$$

et

$$d(\alpha\tau)\wedge d(\overline{\alpha\tau}) = (\det\alpha)^2\,|c\tau+d|^{-4}\,d\tau\wedge d\bar{\tau} \ ,$$

d'où :

$$(f|_k\alpha)(\overline{g|_k\alpha})(\tau)\cdot(\mathrm{Im}(\tau))^{k-2}d\tau\wedge d\bar{\tau} = f(\alpha\tau)\cdot\overline{g(\alpha\tau)}\cdot(\mathrm{Im}(\alpha\tau))^{k-2}\,d(\alpha\tau)\wedge d(\overline{\alpha\tau}) \ .$$

Comme $d\tau\wedge d\bar{\tau} = -2i\,dx\wedge dy$, cela démontre le lemme. ■

3.1.2. *DEFINITION* . Soit G un sous-groupe de Γ , f et g deux formes modulaires de poids k pour G , et D un domaine fondamental de $\overline{G}\backslash\mathcal{H}$. Le produit scalaire de Petersson de f et g est défini par :

$$\langle f,g\rangle_G = \frac{1}{[\overline{\Gamma}:\overline{G}]} \iint_D f\bar{g}\, y^k \frac{dx\,dy}{y^2} \quad .$$

Remarques :

(i) Comme f et g sont deux formes modulaires de poids k pour G , cette définition ne dépend pas de D , d'après le lemme (3.1.1). Par exemple, si D_o est un domaine fondamental de $\overline{\Gamma}\backslash\mathcal{H}$, et si $\overline{\Gamma} = \bigsqcup_{i=1}^{\mu} \overline{G}\alpha_i$, on peut prendre $D = \cup\ \alpha_i(D_o)$, et alors

$$\langle f,g\rangle_G = \frac{1}{\mu} \sum_{i=1}^{\mu} \iint_{\alpha_i(D_o)} f\bar{g}\, y^k \frac{dx\,dy}{y^2} \quad .$$

(ii) Il peut y avoir des problèmes de convergence de l'intégrale aux pointes de $\widehat{\overline{G}\backslash\mathcal{H}}$. A l'infini, soient $f(\tau) = \sum_{n\geq 0} a_n q^n$ et $g(\tau) = \sum_{n\geq 0} b_n q^n$ les développements de Fourier de f et g . Si a_o et b_o sont non nuls, l'intégrale est de même nature que celle de y^k et ne converge pas. Par contre, si l'une au moins des 2 formes est parabolique, l'intégrale converge à l'infini et (par conjugaison) aux autres pointes.

(iii) Le produit scalaire de Petersson est un produit scalaire hermitien non dégénéré (car f et g sont holomorphes).

(iv) Si f et g sont modulaires pour 2 sous-groupes H et G d'indice fini de Γ , et si l'intersection de H et G est d'indice fini dans Γ , alors, la définition montre que :

$$\langle f,g\rangle_H = \langle f,g\rangle_{H\cap G} = \langle f,g\rangle_G \ .$$

Nous noterons désormais $\langle f,g\rangle$ cette valeur.

3.1.3. *PROPOSITION* . Si n est premier à N , l'opérateur T_n est hermitien pour le produit de Petersson.

Cela signifie que $\langle f|_k T_n, g\rangle = \langle f, g|_k T_n\rangle$.

■ D'après (2.1.3), l'algèbre engendrée par les opérateurs T_ℓ (pour ℓ premier, $\ell \nmid N$) contient tous les T_n (pour n premier à N), donc il suffit de vérifier que les opérateurs T_ℓ sont hermitiens. D'après (2.2.2) :

$$\Sigma_\ell = \Gamma_o(N)\begin{pmatrix}1 & 0\\ 0 & \ell\end{pmatrix}\Gamma_o(N) = \coprod_{i=1}^{p+1} \Gamma_o(N)\alpha_i = \coprod_{j=1}^{p+1} \beta_j\Gamma_o(N) \quad .$$

Nous avons vu certaines valeurs possibles des α_i (cf. 2.2.2) mais ici nous allons en utiliser d'autres : comme Σ_ℓ est égal à une seule classe double modulo $\Gamma_o(N)$, toute classe à droite rencontre toute classe à gauche, et en choisissant $\gamma_i \in \Gamma_o(N)\alpha_i \cap \beta_i\Gamma_o(N)$ pour tout i, on obtient un système de représentants des classes à droite et à gauche.

Montrons maintenant que $\langle f|_k T_\ell, g\rangle = \langle f, g|_k T_\ell\rangle$ lorsque f et g sont modulaires pour $G = \Gamma_o(N)$. Appliquons la remarque (3.1.2.(iv))

$$\langle f|_k T_\ell, g\rangle = \frac{1}{[\overline{\Gamma}:\overline{\Gamma_o(N)}]} \sum_{i=1}^{p+1} \iint_D (f|_k\gamma_i)\,\bar{g}\,y^k \frac{dx\,dy}{y^2}$$

$$= \sum_{i=1}^{p+1} \frac{1}{[\overline{\Gamma}:\overline{G}_i]} \iint_{D_i} (f|_k\gamma_i)\bar{g}\,y^k\,\frac{dx\,dy}{y^2}$$

où D est un domaine fondamental pour $\overline{\Gamma_o(N)}\backslash\mathcal{H}$, D_i pour $\overline{G}_i\backslash\mathcal{H}$, et où $G_i = \Gamma_o(N) \cap \gamma_i\Gamma_o(N)\gamma_i^{-1}$. Appliquons le lemme (3.1.1) à $\gamma_i^{-1} \in GL_2^+(\mathbb{R})$, pour chaque i. Cela donne :

$$\langle f|_k T_\ell, g\rangle = \sum_{i=1}^{p+1} \frac{1}{[\overline{\Gamma}:\overline{G}_i]} \iint_{\gamma_i^{-1}(D_i)} f.\overline{(g|_k\gamma_i^{-1})}\,y^k\,\frac{dx\,dy}{y^2} \quad .$$

Or $\gamma_i^{-1}(D_i)$ est un domaine fondamental pour

$$\gamma_i^{-1}G_i\gamma_i = \Gamma_o(N) \cap \gamma_i^{-1}\Gamma_o(N)\gamma_i \quad ,$$

et les indices $[\overline{\Gamma}:\overline{G}_i]$ et $[\overline{\Gamma}:\overline{\gamma_i^{-1}G_i\gamma_i}]$ sont égaux. Le système $\{(\text{dét}.\gamma_i)\gamma_i^{-1}\}$ forme, comme $\{\gamma_i\}$, un système de représentants à droite et à gauche de Σ_ℓ pour l'action de $\Gamma_o(N)$; ainsi

$$\langle f|_k T_\ell, g\rangle = \langle f, g|_k T_\ell\rangle \quad . \quad ■$$

3.2. INVOLUTION D'ATKIN-LEHNER (cf.[2],[19]) .

3.2.1. Soient N , N_1 , N_2 , des entiers ≥ 1 tels que $N = N_1N_2$ et $(N_1,N_2) = 1$. Définissons une application, notée $W_{N_1}^N$, de $X_o(N)$ dans lui-même, en posant, pour tout $(E,C) \in Y_o(N)$:

$$W_{N_1}^N((E,C)) = (E/C_{N_1}, E_{N_1}+C_{N_2}/C_{N_1})$$

où C_{N_i} est l'unique sous-groupe cyclique de C d'ordre N_i $(i=1,2)$ (ainsi $C = C_{N_1}+C_{N_2}$) , et où E_{N_1} est le groupe des points d'ordre N_1 dans E .

PROPOSITION . L'application $W_{N_1}^N$ est un automorphisme de $X_o(N)$, défini sur $\mathbb{Q}$, et c'est une involution.

▪ Si (E,C) est défini sur $\mathbb{Q}$, alors $W_{N_1}^N((E,C))$ l'est aussi. Calculons $W_{N_1}^N((E',C'))$ où $(E',C') = W_{N_1}^N((E,C)) = (E/C_{N_1}, E_{N_1}+C_{N_2}/C_{N_1})$. Comme $E_{N_1}+C_{N_2}/C_{N_1} = E_{N_1}/C_{N_1} + (C_{N_2}+C_{N_1})/C_{N_1}$, nous avons : $C'_{N_1} = E_{N_1}/C_{N_1}$, et $C'_{N_2} = C_{N_2} + C_{N_1}/C_{N_1}$. D'autre part, $E'_{N_1} = F/C_{N_1}$ si F désigne le sous-groupe des éléments x de E tels que $N_1x \in C_{N_1}$. Ainsi, $W_{N_1}^N((E',C')) = (E/E_{N_1}, F+C_{N_2}/E_{N_1})$. Or la multiplication par N_1 induit un isomorphisme de $(E/E_{N_1}, F+C_{N_2}/E_{N_1})$ sur (E,C) , d'où : $(W_{N_1}^N)^2 = 1$. ▪

3.2.2. Soient $E = \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ et $C = \mathbb{Z}\omega_1 \oplus \frac{1}{N}\mathbb{Z}\omega_2/L$. Alors $C_{N_i} = \mathbb{Z}\omega_1 \oplus \frac{1}{N_i}\mathbb{Z}\omega_2/L$ $(i = 1,2)$; posons $L' = \mathbb{Z}\omega_1 \oplus \frac{1}{N_1}\mathbb{Z}\omega_2$; ainsi $C_{N_1} = L'/L$ et $E/C_{N_1} = \mathbb{C}/L'$. Comme $E_{N_1} = \frac{1}{N_1}\mathbb{Z}\omega_1 \oplus \frac{1}{N_1}\mathbb{Z}\omega_2/L$, nous avons $E_{N_1}+C_{N_2}/C_{N_1} = \frac{1}{N_1}\mathbb{Z}\omega_1 \oplus \frac{1}{N}\mathbb{Z}\omega_2/L'$. Cherchons une base $\{\omega'_1,\omega'_2\}$ de L' telle que $E_{N_1}+C_{N_2} = \mathbb{Z}\omega'_1 \oplus \frac{1}{N}\mathbb{Z}\omega'_2/L'$, c'est-à-dire

une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$, de déterminant N_1 , telle que $L' = A^{-1}L$ et que la base $\{\omega'_1 = (d\omega_1 - b\omega_2)/N_1 \ , \ \omega'_2 = (-c\omega_1 + a\omega_2)/N_1\}$ de L' vérifie $E_{N_1} + C_{N_2}/C_{N_1} = \mathbb{Z}\omega'_1 \oplus \frac{1}{N}\mathbb{Z}\omega'_2/L'$. Cette dernière condition équivaut à la congruence :

$$\mathbb{Z}\omega'_1 + \frac{1}{N}\mathbb{Z}\omega'_2 \equiv \frac{1}{N_1}\mathbb{Z}\omega_1 + \frac{1}{N}\mathbb{Z}\omega_2 \pmod{L'}$$

c'est-à-dire $\mathbb{Z}(d\omega_1 - b\omega_2) + \frac{1}{N}\mathbb{Z}(-c\omega_1 + a\omega_2) \equiv \mathbb{Z}\omega_1 + \frac{1}{N_2}\mathbb{Z}\omega_2$ $(\text{mod.} N_1 L' = N_1\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2)$. Donc N doit diviser c , et N_1 diviser a . D'autre part, $\omega'_1 = (d\omega_1 - b\omega_2)/N_1$ est dans $L' = \mathbb{Z}\omega_1 \oplus \frac{1}{N_1}\mathbb{Z}\omega_2$, donc N_1 doit diviser d .

Et on vérifie facilement que ces trois conditions sont suffisantes. En résumé :

PROPOSITION . Soient $(E,C) = (\mathbb{C}/L, \mathbb{Z}\omega_1 \oplus \frac{1}{N}\mathbb{Z}\omega_2/L)$, où $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ et $(E',C') = (\mathbb{C}/L' \ , \ \mathbb{Z}\omega'_1 + \frac{1}{N}\mathbb{Z}\omega'_2/L')$, où $L' = \mathbb{Z}\omega'_1 \oplus \mathbb{Z}\omega'_2$. Alors $(E',C') = W_{N_1}^N((E,C))$ si et seulement si la matrice de passage de $\{\omega'_1, \omega'_2\}$ à $\{\omega_1, \omega_2\}$ est de la forme $\begin{pmatrix} N_1 a & b \\ Nc & N_1 d \end{pmatrix}$ et de déterminant N_1 .

Notons encore $W_{N_1}^N$ cette matrice. Elle vérifie les propriétés suivantes :

(i) $W_{N_1}^N (W_{N_1}^{'N})^{-1} \in \Gamma_o(N)$ si $W_{N_1}^{'N}$ est une matrice du même type,

(ii) $\frac{1}{N_1}(W_{N_1}^N)^2 \in \Gamma_o(N)$;

(iii) $W_{N_1}^N$ normalise $\Gamma_o(N)$.

La matrice $W_{N_1}^N$ permet de définir un opérateur, encore noté $W_{N_1}^N$, sur l'espace des formes modulaires de poids k pour $\Gamma_o(N)$ grâce à :

$$(f|_k W_{N_1}^N)(\tau) = N_1^{k/2}(Nc\tau + N_1 d)^{-k} f\left(\frac{N_1 a\tau + b}{Nc\tau + N_1 d}\right) .$$

En particulier, si $N_1 = N$, $N_2 = 1$, $W_N^N = W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$: nous retrouvons ainsi l'opérateur étudié en (1.1) .

La propriété (ii) prouve que l'opérateur $W_{N_1}^N$ est involutif.

3.3. FORMES PRIMITIVES ET THEOREME D'ATKIN.

3.3.1. Remarques :

(i) Si f est une forme modulaire pour $\Gamma_o(M)$ et si M divise N , alors f est une forme modulaire pour $\Gamma_o(N)$, puisque $\Gamma_o(N) \subset \Gamma_o(M)$.

(ii) Si f est une forme modulaire pour $\Gamma_o(M)$, si M divise N , et si m divise N/M , alors $f|\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$ est modulaire pour $\Gamma_o(N)$: en effet,

$$\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} a & mb \\ cN/m & d \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$$

et M divise N/m , donc $\begin{pmatrix} a & mb \\ cN/m & d \end{pmatrix} \in \Gamma_o(M)$, et

$$f \mid \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \mid \begin{pmatrix} a & b \\ cN & d \end{pmatrix} = f \mid \begin{pmatrix} a & mb \\ cN/m & d \end{pmatrix} \mid \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = f \mid \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} .$$

(iii) Rappelons que $f|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}(\tau) = m^{k/2} f(m\tau)$.

3.3.2. Ces remarques justifient la définition suivante : une forme modulaire de poids k pour $\Gamma_o(N)$ est dite <u>ancienne</u> ("oldform") si c'est une combinaison linéaire de fonctions de la forme $\tau \to f(m\tau)$, où f est une forme modulaire de poids k pour $\Gamma_o(M)$, M divise N , $M \neq N$, et où m divise M/N .

Notons $S(N,k)$ l'espace des formes paraboliques de poids k pour $\Gamma_o(N)$, et $S^a(N,k)$ le sous-espace des formes anciennes.

LEMME . <u>L'espace</u> $S^a(N,k)$ <u>est stable par les opérateurs</u> T_n <u>pour tout</u> n <u>premier à</u> N , <u>et</u> $W_{N_1}^N$ <u>pour tout</u> N_1 <u>divisant</u> N <u>tel que</u> $(N_1, N/N_1) = 1$.

■ Rappelons que $f|_k T_n = n^{k/2-1} \sum_{\substack{ad=n \\ a>0 \\ 0\le b<d \\ (a,N)=1}} f|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ (cf. 2.2.3)

et que $S(N,k)$ est stable par T_n (cf. 2.2.4). Or $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & mb \\ 0 & d \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$, et $(m,d) = 1$ car $m|N$, $d|n$, et $(n,N) = 1$. Ainsi, si b' désigne le reste de la division euclidienne de mb par d, nous obtenons :

$$f|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}|_k T_n = \left[n^{k/2-1} \sum_{\substack{ad=n \\ a>0 \\ 0\le b'<d \\ (a,N)=1}} f|_k \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix} \right]|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$$

et $S^a(N,k)$ est stable par T_n.

Rappelons que $f|_k W_{N_1}^N = f|_k \begin{pmatrix} N_1 a & b \\ Nc & N_1 d \end{pmatrix}$ pour n'importe quels entiers a,b,c,d tels que $N_1 ad - N_2 bc = 1$ (si $N_2 = N/N_1$). Comme $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} W_{N_1} = \begin{pmatrix} N_1 a & mb \\ cN/m & N_1 d \end{pmatrix} \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$, on montre (de même que pour T_n) que $S^a(N,k)$ est stable par $W_{N_1}^N$. ■

3.3.3. Par définition, l'espace des formes paraboliques de poids k <u>primitives</u> pour $\Gamma_o(N)$ ("newforms") est l'orthogonal de $S^a(N,k)$ dans $S(N,k)$ pour le produit scalaire de Petersson, et il est noté $S^o(N,k)$.

LEMME. <u>L'espace</u> $S^o(N,k)$ <u>est stable par les opérateurs</u> T_n <u>pour tout</u> n <u>premier à</u> N, <u>et par</u> $W_{N_1}^N$ <u>pour tout</u> N_1 <u>divisant</u> N.

■ Vu le lemme (3.3.2), il suffit de vérifier que T_n et $W_{N_1}^N$ sont des opérateurs hermitiens pour le produit scalaire de Petersson. Nous l'avons déjà montré pour T_n (proposition (3.1.3)), et pour $W_{N_1}^N$ nous allons utiliser les propriétés (ii) et (iii) de (3.2.2) : $W_{N_1}^N$ est un opérateur involutif sur $S(N,k)$, et il normalise $\Gamma_o(N)$. Ainsi, si W

désigne $W_{N_1}^N$,

$$\langle f,g \mid W\rangle = \iint_D f.\overline{g|W} = \iint_{W^{-1}(D)} f|W^{-1}.\bar{g} = \iint_D f|W.\bar{g} = \langle f|W,g\rangle \ . \ \blacksquare$$

Si $M \mid N$, $\Gamma_o(N)$ est un sous-groupe de $\Gamma_o(M)$; choisissons un système $\{\alpha_i\}$ de représentants des classes à gauche de $\Gamma_o(M)$ modulo $\Gamma_o(N)$, c'est-à-dire $\Gamma_o(M) = \bigsqcup_i \Gamma_o(N)\alpha_i$, puis définissons une application notée tr_M^N de $S(N,k)$ dans $S(M,k)$ par : $tr_M^N(f) = \sum_i f|_k \alpha_i$. Alors tr_M^N est indépendante du choix des α_i .

PROPOSITION . Soit $f \in S(N,k)$. Alors f est primitive pour $\Gamma_o(N)$ si et seulement si, pour tout nombre premier ℓ divisant N , on a : $tr_{N/\ell}^N(f) = 0$ et $tr_{N/\ell}^N(f|_k W_N) = 0$.

Ce théorème est démontré dans [19] (théorème 4) .

3.3.4. *PROPOSITION* . Tous les opérateurs T_n $((n,N)=1)$ et $W_{N_1}^N$ $(N_1|N$, et $(N_1, N/N_1) = 1)$ commutent.

■ Nous avons vu (cf.2.1.3) que les T_n commutent entre eux et il est évident que les $W_{N_1}^N$ commutent entre eux. Montrons que $T_n \circ W_N = W_N \circ T_n$: soit $(E,C) \in Y_o(N)$; alors

$$T_n \circ W_N((E,C)) = T_n(E/C, E_N/C) = \sum_{\substack{F' \subset E/C \\ |F'|=n}} ((E/C)/F', (E_N/C+F')/F')$$

et

$$W_N \circ T_n((E,C)) = W_N\Big(\sum_{\substack{F\subset E \\ |F|=n}} (E/F, C+F/F)\Big) = \sum_{\substack{F\subset E \\ |F|=n}} (E/C+F, ((E/F)_N)/(C+F)/F) \ .$$

Or l'hypothèse $(n,N) = 1$ montre que $(E/F)_N = E_N+F/F$ et qu'il existe une bijection entre les sous-groupes F de E d'ordre n et les sous-groupes F' de E/C d'ordre n , définie par $F' = F+C/C$. Ainsi

$$T_n \circ W_N((E,C)) = W_N \circ T_n((E,C)) = \sum_{\substack{F \subset E \\ |F|=n}} (E/C+F, (E_N+F)/(C+F)) .$$

Enfin, si N_1 est un diviseur de N tel que $(N_1, N/N_1) = 1$, on montre de manière analogue que $T_n \circ W^N_{N_1} \circ T_n$.

COROLLAIRE . Les opérateurs $W^N_{N_1}$ et T_n pour $(n,N) = 1$ sont diagonalisables simultanément.

■ En effet, ils sont hermitiens et commutent entre eux. ■

3.3.5. L'intérêt de l'involution d'Atkin-Lehner vient du résultat suivant où le symbole $\ell^r \| N$ signifie : $\ell^r | N$ et $\ell^{r+1} \nmid N$:

THEOREME PRINCIPAL D'ATKIN. Sur les formes primitives, l'opérateur T_ℓ est déterminé par W_{ℓ^r} si $\ell^r \| N$, $r \geq 1$. Plus précisément, si f est une forme primitive pour $\Gamma_0(N)$, on a :

$$T_\ell f = 0 \text{ si } \ell^2 | N, \text{ et } T_\ell f = -\ell^{k/2-1} W_\ell f \text{ si } \ell \| N .$$

Pour une démonstration de ce théorème, voir ([19], théorème 3, ou [2]).

COROLLAIRE . Il existe une base de l'espace des formes primitives formée de fonctions propres de TOUS les T_n.

A ces formes s'applique le théorème (2.3.1) sur le produit eulérien des séries de Dirichlet associées.

3.3.6. Exemple : $N = \ell$ et $k = 2$.

PROPOSITION . Si N est un nombre premier noté ℓ, toute forme parabolique de poids 2 pour $\Gamma_0(\ell)$ est primitive, et $T_\ell f = -W_\ell f$.

■ Les fonctions $tr_1^{\ell}(f)$ et $tr_1^{\ell}(f|_2 W_{\ell})$ sont des formes paraboliques de poids 2 pour $\Gamma_o(1) = \Gamma$, donc elle sont nulles (cf.I.2.2.3). D'après la proposition (3.3.3), cela prouve que f est primitive.

D'autre part, $f|_2 T_{\ell}+W_{\ell} = f|_2 (\sum_{a=0}^{\ell-1} \begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix})$, et

$\begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$, donc

$$f|_2 T_{\ell}+W_{\ell}|_2 W_1 = f|_2 W_{\ell}|_2 (\sum_{a=0}^{\ell-1} \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}+\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}) = tr_1^{\ell}(f|_2 W_{\ell}) .$$

D'après ce qui précède, $f|_2 T_{\ell}+W_{\ell} = 0$. ■

COROLLAIRE . Il existe une base de l'espace $S(\ell,2) = S^o(\ell,2)$ telle que $L(s,f,1) = (1-a_{\ell}\ell^{-s})^{-1} \prod_{p\neq\ell} (1-a_p p^{-s}+p^{1-2s})^{-1}$ pour toute forme f de cette base, de développement de Fourier $f(\tau) = \sum_{n\geq 1} a_n e^{2\pi i n\tau}$, normalisée par $a_1 = 1$. De plus, $a_{\ell} = \pm 1$.

■ C'est le théorème (2.3.1). La dernière assertion vient de ce que a_{ℓ} est valeur propre de $T_{\ell} = -W_{\ell}$, qui est une involution. ■

4. *JACOBIENNE*

4.1. JACOBIENNE D'UNE COURBE.

4.1.1. Diviseurs sur une courbe.

Soient K un corps égal à $\mathbb{C}$ ou à un corps local, X une courbe projective non singulière définie sur K , munie d'un point O défini sur K , L une extension algébrique de K . Rappelons les définitions suivantes : $\mathcal{D}(X)(L)$ désigne le groupe des diviseurs de X définis sur L , c'est-à-dire le $\mathbb{Z}$-module libre engendré par les "cycles" de la forme $e((P_1)+(P_2)+\ldots+(P_s))$ où $P_1, P_2, \ldots, P_s$ sont des points de X , où

$P_2,\ldots,P_s$ sont les conjugués de P_1 sur L, et où e est le degré d'inséparabilité de $L(P_1)/L$; $\mathcal{D}_o(X)(L)$ est le sous-groupe de $\mathcal{D}(X)(L)$ formé des diviseurs de degré nul, le <u>degré</u> étant l'application d de $\mathcal{D}(X)(\overline{K})$ dans $\mathbb{Z}$ définie par linéarité à partir de :

$$d(e((P_1)+(P_2)+\ldots+(P_s))) = s.e\ ;$$

$\mathcal{D}_\ell(X)(L)$ est le sous-groupe de $\mathcal{D}_o(X)(L)$ formé des <u>diviseurs de fonctions</u> de $K(X)$.

Nous noterons $\mathcal{D}(X)$, $\mathcal{D}_o(X)$, $\mathcal{D}_\ell(X)$, pour $\mathcal{D}(X)(\overline{K})$, $\mathcal{D}_o(X)(\overline{K})$, $\mathcal{D}_\ell(X)(\overline{K})$.

4.1.2. <u>Jacobienne</u> ([52]).

En faisant correspondre à L le groupe quotient $\mathcal{D}_o(X)(L)/\mathcal{D}_\ell(X)(L)$ on définit un foncteur de la catégorie des extensions de K dans celle des groupes abéliens.

PROPOSITION. <u>Il existe une variété abélienne définie sur</u> K, <u>notée</u> $J(X)$, <u>telle que</u> $J(X)(L) = \mathcal{D}_o(X)(L)/\mathcal{D}_\ell(X)(L)$ <u>pour toute extension</u> L <u>de</u> K. <u>La dimension de</u> $J(X)$ <u>est égale au genre de</u> X.

Rappelons qu'une variété abélienne définie sur K est une variété projective définie sur K, munie d'une loi de groupe abélien telle que l'addition s'exprime sur les coordonnées par des fonctions rationnelles à coefficients dans K. D'autre part, $J(X)(K)$ désigne les points de $J(X)$ à coordonnées dans K.

On peut trouver une démonstration de la proposition, avec une construction de $J(X)$, dans [6].

PROPOSITION. <u>Si le genre de</u> X <u>est non nul, pour tout point</u> P_o <u>de</u> X, <u>l'application de</u> X <u>dans</u> $J(X)$ <u>qui associe au point</u> P <u>la classe du diviseur</u> $(P) - (P_o)$ <u>est une injection</u>.

■ Si les diviseurs $(P) - (P_o)$ et $(Q) - (Q_o)$ sont équivalents, pour deux points P et Q distincts de X, alors $(P) - (Q)$ est le diviseur d'une fonction f sur X. Mais alors f définit un revêtement de

degré un : $X \to \mathbb{P}^1$, donc X est de genre nul. ∎

Remarques :

- Si P_o est rationnel sur L , alors l'injection l'est aussi.
- Si $X = X_o(N)$, on pose $P_o = \infty$, et alors l'injection est rationnelle sur $\mathbb{Q}$.

4.1.3. Courbes elliptiques.

PROPOSITION 1. Si X est une courbe elliptique E , les variétés abéliennes E et $J(E)$ sont isomorphes.

∎ Remarquons que $J(E)$ est une courbe, puisque $g = 1$. A tout point P de E , associons la classe de $(P) - (O)$ dans $\mathcal{D}_o(E)/\mathcal{D}_\ell(E)$. Cette application est injective : en effet, si $(P) - (O) = (Q) - (O)$, le diviseur $(P) - (Q)$ est un diviseur de fonctions sur E , ce qui est impossible sur une courbe de genre 1 ($K(E)/K$ serait monogène).

Surjectivité : si $d \in \mathcal{D}_o(E)$, le diviseur $d+(O)$ est de degré $1 > 2g - 2$, et le théorème de Riemann-Roch donne

$$\ell(d+(O)) = \deg(d+(O)) - g + 1 = 1 :$$

autrement dit, il existe un diviseur positif linéairement équivalent à $d + (O)$, i.e. un point P de E tel que $d \equiv (P) - (O) \pmod{\mathcal{D}_\ell(E)}$.

Cette application est un homomorphisme de groupes : écrivons l'équation de E sous la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, et considérons trois points P,Q,R de E de somme nulle, i.e. trois points alignés dans le plan (x,y) . Soit $f(x,y) = ux + vy + w = 0$ l'équation de la droite PQR . La fonction f a 3 zéros en P,Q,R , et un seul pôle en O , donc son diviseur est $(f) = (P) + (Q) + (R) - 3(O)$. ∎

4.1.4. Cas complexe.

Sur $\mathbb{C}$, une courbe projective non singulière de genre g peut être considérée comme une surface de Riemann compacte ; l'espace des formes différentielles holomorphes sur cette surface est de dimension g .

Soit $\{\omega_1,\omega_2,\ldots,\omega_g\}$ une base de l'espace des formes différentielles holomorphes sur cette surface de Riemann (notée X) ; soit Λ le réseau de $\mathbb{C}$ engendré par les g-uples $(\int_\gamma \omega_1, \int_\gamma \omega_2,\ldots,\int_\gamma \omega_g)$, où γ parcourt l'ensemble des lacets sur X ; soit P_o un point fixé de X. Considérons l'application de X dans $\mathbb{C}^g/\Lambda$ définie par :

$$P \longmapsto (\int_{P_o}^{P} \omega_1, \int_{P_o}^{P} \omega_2,\ldots, \int_{P_o}^{P} \omega_g) .$$

PROPOSITION . L'application qui fait correspondre au diviseur (P) - (Q) (sur X) le g-uple $(\int_Q^P \omega_1 , \int_Q^P \omega_2,\ldots,\int_Q^P \omega_g)$ définit un isomorphisme de la jacobienne de X sur $\mathbb{C}^g/\Lambda$.

Remarque : Cette proposition prouve que $\mathbb{C}^g/\Lambda$ est une variété abélienne ; on peut le montrer directement : $\mathbb{C}^g/\Lambda$ est un groupe abélien, et il faut vérifier que c'est une variété projective.

En fait, on montre qu'il existe une forme de Riemann sur $\mathbb{C}^g/\Lambda$, c'est-à-dire une application E de $\mathbb{C}^g \times \mathbb{C}^g$ dans $\mathbf{R}$, vérifiant les conditions suivantes :

(i) E est $\mathbf{R}$-bilinéaire ;

(ii) $E(x,y) = -E(y,x)$;

(iii) si $(x,y) \in \Lambda \times \Lambda$ alors $E(x,y) \in \mathbb{Z}$;

(iv) la forme $\mathbf{R}$-bilinéaire : $(x,y) \mapsto E(x,iy)$ est symétrique définie positive.

Or l'existence d'une forme de Riemann sur $\mathbb{C}^g/\Lambda$ est une condition nécessaire et suffisante pour que $\mathbb{C}^g/\Lambda$ soit une variété abélienne. (cf. [43], App.11 ; [46], thm.38).

4.1.5. Formes différentielles (cf.[43], Appendix ; [44], 1.2) .

Pour définir les formes différentielles sur un corps de base quelconque K, on procède ainsi : soient V une variété définie sur K de dimension n, et Ω un domaine universel pour K (cf.[43]). Notons L(V) le corps des fonctions rationnelles de V dans L, pour toute extension L de K .

PROPOSITION . Il existe un espace vectoriel $\mathrm{Dif}(V)$ sur $\Omega(V)$ de dimension n , et une application Ω-linéaire d de $\Omega(V)$ dans $\mathrm{Dif}(V)$ telle que :

(i) $d(fg) = fdg + gdf$ (quels que soient f,g dans $\Omega(V)$) ;

(ii) $\{df_1, df_2, \ldots, df_n\}$ est une base de $\mathrm{Dif}(V)$ sur $\Omega(V)$ si et seulement si $\{f_1, f_2, \ldots, f_n\}$ est une base de transcendance séparante de $\Omega(V)$ sur Ω .

$\mathrm{Dif}(V)$ est l'espace des formes différentielles sur V . Une forme différentielle ω sur V est dite holomorphe si, en tout point de V , on peut écrire $\omega = \sum_i f_i dg_i$, avec des fonctions f_i et g_i holomorphes en ce point. Nous noterons $\mathrm{Dif}_o(V)$ l'espace des formes différentielles holomorphes sur V .

De façon analogue, ω est dite définie sur L $(K \subset L \subset \Omega)$ si en tout point de V , on peut écrire $\omega = \sum_i f_i dg_i$ avec f_i et g_i dans $L(V)$. L'espace des formes différentielles sur V définies sur L est noté $\mathrm{Dif}(V;L)$. On définit de même $\mathrm{Dif}_o(V;L)$.

Soit W une autre variété sur K , et λ un morphisme de V dans W . On définit une application λ_* de $\mathrm{Dif}(W)$ dans $\mathrm{Dif}(V)$ par :

$$\lambda_*(\sum_i f_i dg_i) = \sum_i (f_i \circ \lambda) d(g_i \circ \lambda) ,$$

et alors $\lambda_*(\mathrm{Dif}_o(W))$ est inclus dans $\mathrm{Dif}_o(V)$.

En particulier, si $K = \mathbb{C}$, $V = X$, $W = J(X) = \mathbb{C}^g/\Lambda$ pour une courbe X sur $\mathbb{C}$, et si λ est défini par : $z \mapsto (\int_{z_o}^{z} \omega_1, \int_{z_o}^{z} \omega_2, \ldots, \int_{z_o}^{z} \omega_g)$, l'application λ_* est un isomorphisme de $\mathrm{Dif}_o(J(X))$ sur $\mathrm{Dif}_o(X)$. Décrivons λ_* : soient $z_1, z_2, \ldots, z_g$ les applications coordonnées de $J(X)$ dans $\mathbb{C}$. Alors $\{dz_1, dz_2, \ldots, dz_g\}$ est une base de $\mathrm{Dif}(J(X))$, et λ_* est défini par : $\lambda_*(dz_i) = \omega_i$. En fait, on a un résultat plus général :

En caractéristique quelconque, $\mathrm{Dif}_0(J(X))$ et $\mathrm{Dif}_0(X)$ sont isomorphes.

En particulier, sur $\mathbb{C}$, si X est une courbe modulaire $X_0(N)$, l'application $f \mapsto \omega = f(\tau)d\tau$ est un isomorphisme entre l'espace des formes paraboliques de poids 2 pour $\Gamma_0(N)$ et l'espace des formes différentielles holomorphes sur $X_0(N)$. Ces deux espaces sont aussi isomorphes à l'espace des formes différentielles holomorphes sur $J(X_0(N))$, et ils sont de dimension g sur $\mathbb{C}$, si g désigne le genre de $X_0(N)$.

4.2. CORRESPONDANCES.

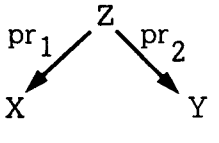
4.2.1. Correspondance et jacobienne. Soient X et Y deux courbes définies sur K, et T une correspondance de X dans Y. La linéarité permet de supposer T irréductible : cela signifie, (avec les notations de 2.1.1), qu'il existe une sous-variété irréductible Z de $X \times Y$, telle que

$$T(x) = \sum_{i=1}^{d_1} (y_i) \quad \text{si} \quad \{(x,y_i)\}_{1\le i\le d_1} = \mathrm{pr}_1^{-1}(x) .$$

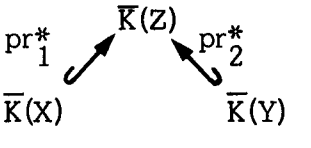
Par linéarité, cela définit un homomorphisme T de $\mathcal{D}_0(X)$ dans $\mathcal{D}_0(Y)$.

PROPOSITION. L'image par T de $\mathcal{D}_\ell(X)$ est dans $\mathcal{D}_\ell(Y)$.

■ Soit f une fonction rationnelle sur X. Les projections :



définissent des injections :



Soit N la norme de $\bar{K}(Z)$ dans $\bar{K}(Y)$, et $f \mid T = N(\mathrm{pr}_1^*(f))$. Montrons que $T((f)) = (f \mid T)$. Pour tout y dans Y, nous avons :

$$f \mid T(y) = N(\mathrm{pr}_1^*(f))(y) = \prod_{i=1}^{d_2} \mathrm{pr}_1^*(f)\ (x_i, y)$$

où les x_i sont définis par : $\mathrm{pr}_2^{-1}(y) = \{(x_i,y)\}_{1\le i\le d_2}$. Comme $\mathrm{pr}_1^*(f)(x,y) = f(x)$, nous obtenons : $f \mid T(y) = \prod_{i=1}^{d_2} f(x_i)$. Et en désignant par $v_x(f)$ l'ordre d'une fonction f en un point x :

$$(f \mid T) = \sum_{y\in Y} v_y(f \mid T).(y) = \sum_{y\in Y} \Big(\sum_{\substack{x\in X \\ (x,y)\in Z}} v_x(f)\Big)(y)$$

$$= \sum_{x\in X} v_x(f) \Big(\sum_{\substack{y\in Y \\ (x,y)\in Z}} (y)\Big) = \sum_{x\in X} v_x(f).(T(x)) = T((f)) \ . \ \blacksquare$$

COROLLAIRE 1. Toute correspondance T de X dans Y définit un homomorphisme de $J(X)$ dans $J(Y)$.

Nous noterons encore cet homomorphisme T .

4.2.2. Transposée. Soit T une correspondance de X dans Y , définie par $T(x) = \sum_{i=1}^{d_1} y_i$ comme précédemment. On appelle correspondance transposée de T la correspondance T' de Y dans X définie par $T'(y) = \sum_{i=1}^{d_2} x_i$ où $\{(x_i,y)\}_{1\le i\le d_2} = pr_2^{-1}(y)$.

4.2.3. Frobenius. Soit q une puissance d'un nombre premier p , et notons K le corps $\mathbb{F}_q$: alors l'application $x \to x^q$ est un automorphisme de $\overline{K}$. Soit V une variété projective définie sur $\overline{K}$ par des polynômes homogènes $F_i(\underline{X})$ (où $\underline{X} = (X_0,X_1,\ldots,X_r)$) , soit $F_i^{\pi_q}(\underline{X})$ le polynôme obtenu en faisant agir $x \mapsto x^q$ sur les coefficients de F_i , et soit V^{π_q} la variété définie par les $F_i^{\pi_q}(\underline{X})$. L'application $(x_0,x_1,\ldots,x_r) \mapsto (x_0^q,x_1^q,\ldots,x_r^q)$ envoie V dans V^{π_q} et est appelée l'application de Frobenius.

Lorsque V est définie sur $\mathbb{F}_q$, on a $V^{\pi_q} = V$. Si V est une courbe X , on peut définir une correspondance de X dans elle-même, appelée correspondance de Frobenius et notée π_q , par : $\pi_q(x) = (x^q)$. La correspondance transposée π_q' est alors définie par : $\pi_q'(x) = q(x^{1/q})$, et nous avons :

$$\pi_q\pi_q'(x) = \pi_q'\pi_q(x) = q(x) \ .$$

5. *ENDOMORPHISMES D'UNE COURBE ELLIPTIQUE*

5.1. ENDOMORPHISMES D'UNE VARIETE ABELIENNE.

5.1.1. Soit A une variété abélienne sur un corps quelconque K, A_n le groupe des points dont l'ordre divise n, ℓ un nombre premier différent de la caractéristique de K. La multiplication par ℓ envoie A_{ℓ^n} dans $A_{\ell^{n-1}}$, et l'ensemble des A_{ℓ^n} $(n \in \mathbb{N})$ forme un système projectif. Par définition, le module de Tate $T_\ell(A)$ est égal à $\varprojlim_{n\in\mathbb{N}} A_{\ell^n}$.

5.1.2. En caractéristique nulle, A est un tore $\mathbb{C}^g/\Lambda$ muni d'une forme de Riemann (cf 4.1.4), et $\mathrm{End}(A)$ est isomorphe à l'anneau des endomorphismes de $\mathbb{C}^g$ qui laissent Λ stables ; comme $\Lambda \simeq \mathbb{Z}^{2g}$, on a : $\mathrm{End}(A) \subset M_{2g}(\mathbb{Z})$.

D'autre part, $A_{\ell^n} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, $T_\ell(A) \simeq (\mathbb{Z}_\ell)^{2g}$ et même $T_\ell(A)$ est canoniquement isomorphe à $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ (utiliser l'isomorphisme canonique $A_{\ell^n} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^n\mathbb{Z}$).

L'anneau $\mathrm{End}(A)$ opère sur A, donc sur $T_\ell(A)$, et on obtient ainsi une représentation R_ℓ de $\mathrm{End}(A)$ dans $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) = \mathrm{End}_{\mathbb{Z}_\ell}(\Lambda\otimes_{\mathbb{Z}}\mathbb{Z}_\ell)$ appelée <u>représentation ℓ-adique</u> de $\mathrm{End}(A)$.

5.1.3. Ces résultats se généralisent ainsi :

THEOREME (Weil) (cf.[52]). <u>Soient</u> A, K, ℓ <u>comme dans</u> (5.1.1), <u>et</u> g <u>la dimension de</u> A. <u>Alors</u> :

(i) $A_{\ell^n} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$;

(ii) <u>Il existe une injection</u> R_ℓ <u>de</u> $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ <u>dans</u> $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$;

(iii) $\mathrm{End}(A)$ <u>est un</u> $\mathbb{Z}$-<u>module libre de rang</u> $\leq (2g)^2$.

5.2. ISOGENIE TRANSPOSEE.

5.2.1. Soient E,F , deux courbes elliptiques sur K , et λ une isogénie définie sur K , de E dans F (cf.I,4.3.1). On peut considérer λ comme une correspondance de E dans F , et définir sa transposée λ' de F dans E (cf.4.2.2) ; alors $\lambda'(Q) = \sum_{\substack{P\in E \\ \lambda(P)=Q}} e_P(P)$

où e_P est la "multiplicité" de P .

D'après le corollaire (4.2.1), λ' définit un homomorphisme de $J(F)$ dans $J(E)$. Mais la jacobienne d'une courbe elliptique s'identifie à cette courbe (cf. 4.1.3), donc λ' définit un homomorphisme, encore noté λ', de F dans E .

Décrivons l'homomorphisme λ' : soient d le degré de λ et d_s son degré de séparabilité (cf.I.4.3.1), $\{f_i\}_{1\le i\le d} = \lambda^{-1}(Q)$, $\{a_i\}_{1\le i\le d} = \lambda^{-1}(0) = \operatorname{Ker}\lambda$. Alors λ' est composée des 3 applications :

$$F \xrightarrow{\sim} J(F) \xrightarrow{\lambda'} J(E) \xrightarrow{\sim} E$$

$$Q \longmapsto (Q)-(O) \longmapsto \sum_{i=1}^{d} (P_i)-(a_i) \longmapsto Q'$$

où Q' est défini par : $\sum_{i=1}^{d} (P_i) - (a_i) \equiv (Q') - (O) \pmod{\mathcal{D}_\ell(E)}$; ainsi, λ' est un homomorphisme non nul de F dans E , c'est-à-dire une isogénie.

5.2.2. *PROPOSITION* (cf.[5] ,2.8) : L'application $\lambda \mapsto \lambda'$ transforme toute isogénie de E dans F en une isogénie de F dans E , et vérifie les propriétés suivantes :

(i) $\lambda.\lambda' = \deg \lambda$;

(ii) si $n \in \mathbb{Z}$, alors $n' = n$;

(iii) $(\lambda_2\lambda_1)' = \lambda_1'\lambda_2'$;

(iv) $\lambda'' = \lambda$;

(v) $(\lambda_1+\lambda_2)' = \lambda_1' + \lambda_2'$ si $\lambda_1+\lambda_2 \neq 0$.

■ Il suffit de vérifier ces propriétés en considérant λ et λ' comme des homomorphismes entre $\mathcal{D}(E)$ et $\mathcal{D}(F)$. Si $Q \in F$, alors

$$\lambda\lambda'((Q)) = \lambda\Big(\sum_{\substack{P\in E\\ \lambda(P)=Q}} (P)\Big) = \sum_{\substack{P\in E\\ \lambda(P)=Q}} (Q) = (\deg \lambda).(Q) ,$$

d'où (i) . De plus, si $\lambda = n \in \mathbb{Z}$, $\deg \lambda = n^2$ (cf.I,4.3.2) , et (i) implique $n' = n$, c'est-à-dire (ii).

Pour (iii), soient E,F,G trois courbes elliptiques sur K , λ_1 une isogénie de E dans F , λ_2 de F dans G , alors la description de λ' donne :

$$(\lambda_2\lambda_1)'((R)) = \sum_{\substack{P\in E\\ \lambda_2\lambda_1(P)=R}} (P) = \lambda_1'\lambda_2'((R)) ,$$

c'est-à-dire (iii).

Or pour montrer (iv), il suffit de montrer que $\lambda"\lambda' = \lambda\lambda'$, puisque λ' est surjective. Utilisons successivement (iii), (i), (ii), (i) : cela donne $\lambda"\lambda' = (\lambda\lambda')' = (\deg \lambda)' = \deg \lambda = \lambda\lambda'$, d'où (iv).

Enfin, soit Z_1 (resp.Z_2) la courbe de $E \times F$ définissant la correspondance λ_1 (resp. λ_2) de E dans F (cf.2.1.1) ; la correspondance $\lambda_3 = \lambda_1+\lambda_2$ correspond donc à la courbe Z_3 , "réunion" de Z_1 et Z_2 . Rappelons que $\lambda_i'(y) = \sum_{(x,y)\in Z_i} (x)$ $(i=1,2)$; ainsi,

$$\lambda_3'(y) = \sum_{(x,y)\in Z_3} (x) = \sum_{(x,y)\in Z_1} (x) + \sum_{(x,y)\in Z_2} (x) = \lambda_1'(y) + y_2'(y)$$

et (v) est démontré. (on trouvera dans [5] , Appendix C, une autre démonstration de (v)). ■

Remarque : En posant $O' = O$, pour l'homomorphisme nul, on obtient une application de $\mathrm{Hom}(E,F)$ dans $\mathrm{Hom}(F,E)$ qui vérifie les propriétés (i) à (v).

COROLLAIRE . L'application $\lambda \mapsto \lambda'$ définit une involution sur $\mathrm{End}(E)$.

5.2.3. *PROPOSITION* (cf.[18],13.2). Soit λ un endomorphisme de E, λ non entier rationnel. Alors $\mathbb{Q}(\lambda)$ est une extension quadratique imaginaire de $\mathbb{Q}$, le conjugué de λ sur $\mathbb{Q}$ est l'isogénie transposée λ', et le polynôme minimal de λ sur $\mathbb{Q}$ est à coefficients entiers.

■ Considérons l'égalité : $(1-\lambda)(1-\lambda') = 1-(\lambda+\lambda') + \lambda\lambda'$, dans laquelle $(1-\lambda)(1-\lambda')$ et $\lambda\lambda'$ sont des entiers naturels (on utilise 5.2.2, (i)). Elle montre que $\lambda + \lambda'$ est entier, donc que le polynôme $P(x) = (x-\lambda)(x-\lambda') = x^2 - x(\lambda+\lambda') + \lambda\lambda'$ est à coefficients entiers, et que λ et λ' sont algébriques sur $\mathbb{Q}$, de degré inférieur à 2. Comme $n^2 - nm(\lambda+\lambda') + \lambda\lambda'm^2 = (n-m\lambda)(n-m\lambda') \in \mathbb{N}$ si $n,m \in \mathbb{Z}$, le polynôme $P(x)$ prend des valeurs positives ou nulles en tout point de $\mathbb{Q}$, donc de $\mathbb{R}$, et son discriminant est négatif ou nul. S'il est nul, $\lambda = \lambda'$ est rationnel, donc entier, ce qui est contraire à l'hypothèse. S'il est strictement négatif, $\mathbb{Q}(\lambda)/\mathbb{Q}$ est imaginaire quadratique, et la proposition est démontrée. ■

COROLLAIRE. L'isogénie λ est égale à sa transposée λ' si et seulement si $\lambda \in \mathbb{Z}$.

5.2.4. L'application $\lambda \to \lambda'$ correspond à l'involution d'Atkin-Lehner sur $X_o(N)$:

PROPOSITION. Si N est premier, $W_N((E,\mathrm{Ker}\ \lambda)) = (\lambda(E),\mathrm{Ker}\ \lambda')$.

■ Nous avons vu que $Y_o(N)$ est en bijection avec l'ensemble des couples (E,λ) où λ est une isogénie sur E de degré N, par : $(E,\lambda) \to (E,\mathrm{Ker}\ \lambda)$ (cf.I,4.3.3).

Puisque $\lambda\lambda' = N$, le groupe $\lambda(E_N)$ est inclus dans $\mathrm{Ker}\ \lambda'$; or ces 2 groupes ont le même ordre N. Donc

$$W_N((E,\mathrm{Ker}\ \lambda)) = (E/\mathrm{Ker}\ \lambda, E_N/\mathrm{Ker}\ \lambda) = (\lambda(E),\mathrm{Ker}\ \lambda')$$

sur $Y_o(N)$. ■

5.3. COURBES ELLIPTIQUES SUR $\mathbb{C}$ AVEC MULTIPLICATION COMPLEXE (cf.[48]).

5.3.1. Une courbe elliptique E sur un corps K est dite à multiplication complexe si $\mathrm{End}\, E \neq \mathbb{Z}$. Supposons maintenant que $K = \mathbb{C}$, $E = \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, et $\tau = \omega_2/\omega_1$; alors $\mathrm{End}(E)$ est un $\mathbb{Z}$-module libre de rang au plus égal à 2, et la proposition (5.2.3) prouve que, si E a de la multiplication complexe, $\mathrm{End}\, E$ est un ordre dans un corps quadratique imaginaire. On démontre alors les résultats suivants :

5.3.2. *PROPOSITION*. La courbe elliptique $\mathbb{C}/L$ a de la multiplication complexe si et seulement si le corps $\mathbb{Q}(\tau)$ est quadratique imaginaire. Et alors, $\mathrm{End}(\mathbb{C}/L)$ est un ordre dans $\mathbb{Q}(\tau)$. (cf.[48] prop.4.5).

5.3.3. Soient K un corps de nombres, $\mathcal{O}$ un ordre de K, $\mathfrak{a}$ un réseau de K. On dit que $\mathfrak{a}$ est un $\mathcal{O}$-idéal propre si $\mathcal{O} = \{x \in K / x\mathfrak{a} \subset \mathfrak{a}\}$. L'ensemble des $\mathcal{O}$-idéaux propres forme un groupe, d'élément neutre $\mathcal{O}$, et l'on définit le groupe des classes de $\mathcal{O}$-idéaux propres (modulo la relation : $\mathfrak{a}$ équivaut à $\mathfrak{a}'$ s'il existe un $x \in K^*$ tel que $\mathfrak{a} = x\mathfrak{a}'$).

PROPOSITION. Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K. Il existe une bijection entre les classes de courbes elliptiques sur $\mathbb{C}$ telles que $\mathrm{End}\, E \simeq \mathcal{O}$, et les classes de $\mathcal{O}$-idéaux propres.

Dans cet isomorphisme, à la classe d'un $\mathcal{O}$-idéal propre $\mathfrak{a}$ correspond la classe de la courbe elliptique $\mathbb{C}/\mathfrak{a}$. (cf.[48] prop.4.8). On note $j(\mathfrak{a})$ l'invariant de $\mathbb{C}/\mathfrak{a}$.

COROLLAIRE. Si $\mathcal{O}$ est l'ordre maximal de K, c'est-à-dire l'anneau des entiers de K, le nombre de classes de courbes elliptiques E sur $\mathbb{C}$ telles que $\mathrm{End}\, E \simeq \mathcal{O}$ est égal au nombre de classes du corps K. (cf.[48] prop.4.10).

(Dans ce cas, un $\mathcal{O}$-idéal propre est un idéal fractionnaire de K).

5.3.4. La théorie du corps de classes permet de démontrer le résultat suivant :

THEOREME . Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire K , et soit $\mathfrak{a}$ un $\mathcal{O}$-idéal propre. Alors :

(i) Tout conjugué de $j(\mathfrak{a})$ sur K (resp. sur $\mathbb{Q}$) est de la forme $j(\mathfrak{b})$, pour un $\mathcal{O}$-idéal propre $\mathfrak{b}$.

(ii) L'extension $K(j(\mathfrak{a}))/K$ est galoisienne, et l'on définit un isomorphisme du groupe de Galois de $K(j(\mathfrak{a}))/K$ sur le groupe des classes de $\mathcal{O}$-idéaux propres, en associant à tout $\sigma \in \mathrm{Gal}(K(j(\mathfrak{a}))/K)$ la classe d'un $\mathcal{O}$-idéal propre $\mathfrak{b}$ tel que $j(\mathfrak{a})^{\sigma} = j(\mathfrak{b}^{-1}\mathfrak{a})$.

(iii) Les extensions $K(j(\mathfrak{a}))/K$ et $\mathbb{Q}(j(\mathfrak{a}))/\mathbb{Q}$ sont de même degré.

(iv) Si $\mathcal{O}$ est l'ordre maximal de K , alors $K(j(\mathfrak{a}))$ est l'extension abélienne non ramifiée maximale de K .

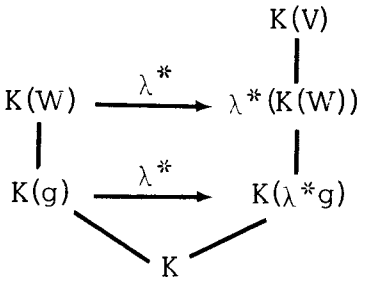
([48] , theorem 5.7).

5.4. SEPARABILITE DES MORPHISMES.

5.4.1. Soient deux courbes V et W sur K , et λ un morphisme non constant de V dans W défini sur K . Nous avons vu en (4.1.5) que λ induit un homomorphisme λ_* de $\mathrm{Dif}(W;K)$ dans $\mathrm{Dif}(V;K)$, et aussi (cf.I,4.3.1) un homomorphisme λ^* de $K(W)$ dans $K(V)$. Par définition, λ est séparable (resp. inséparable, purement inséparable), si l'extension $K(V)/\lambda^*(K(W))$ est séparable (resp. inséparable, purement inséparable).

PROPOSITION (cf.[48] ,5.1). Soit $\omega \in \mathrm{Dif}(W;K)$, $\omega \neq 0$; alors λ est séparable si et seulement si $\lambda_*(\omega)$ est non nul.

■ Considérons le diagramme ci-dessous, où $\{g\}$ forme une base de transcendance séparante de $K(W)/K$. Alors $\lambda^*(K(W)/K(\lambda^* g)$ est séparable comme $K(W)/K(g)$, et $K(V)/\lambda^*(K(W))$ est séparable si et seulement



si $K(V)/K(\lambda^*g)$ l'est aussi, c'est-à-dire si et seulement si $\{\lambda^*g\}$ forme une base de transcendance séparante de $K(V)/K$. D'après (4.1.5), cela équivaut à dire que $\{d(\lambda^*g)\}$ forme une base de $Dif(V)$ sur $\Omega(V)$, ou encore que $d(\lambda^*g) \neq 0$, alors que l'hypothèse sur g signifie que $\{dg\}$ forme une base de $Dif(W)$ sur $\Omega(W)$. Ainsi, ω s'écrit $h \cdot dg$ avec $h \neq 0$, et λ est séparable si et seulement si $\lambda_*(\omega) = (\lambda^*h) \cdot d(\lambda^*g)$ est non nul. ∎

COROLLAIRE . Les conditions suivantes sont équivalentes : λ est séparable ; λ_* est non nulle ; λ_* est injective.

5.4.2. Soit p un nombre premier et $q = p^f$. Si $K = \mathbb{F}_q$ et $V = W$, considérons l'application de Frobenius π_q définie en (4.2.3).

PROPOSITION . Le Frobenius est purement inséparable de degré q .

∎ Le degré de π_q est égal à $\pi_q \pi'_q$ d'après (5.2.2), qui est égal à q d'après (4.2.3). D'autre part,

$$(\pi_p)_*(df) = d(\pi_p^* f) = d(f \circ \pi_p) = (f' \circ \pi_p) \cdot d(\pi_p) = 0 ,$$

donc $(\pi_p)_*$ est nul et π_p inséparable d'après (5.3.1). Comme p est premier, π_p est purement inséparable, et $\pi_q = (\pi_p)^f$ aussi. ∎

5.4.3. Hypothèse de Riemann (cf.[16] ,8) .

PROPOSITION . Si E est une courbe elliptique sur $\mathbb{F}_q$, on a :

$$\left| \#(E(\mathbb{F}_q)) - (1+q) \right| \leq 2q^{1/2} .$$

∎ L'isogénie $1 - \pi_q$ est séparable (d'après (5.4.1) et (5.4.2)), donc il n'y a pas de problème de multiplicité, et

$$\deg(1-\pi_q) = \# \operatorname{Ker}(1-\pi_q) = \# E(\mathbb{F}_q) .$$

D'autre part,

$$\deg(1-\pi_q) = (1-\pi_q)(1-\pi'_q) = 1 - (\pi_q+\pi'_q) + \pi_q\pi'_q = 1-\mathrm{tr}(\pi_q) + q \ .$$

Et enfin, si $n,m \in \mathbb{Z}$, $\deg(n+m\lambda) = n^2 + mn\,\mathrm{tr}(\lambda) + m^2 \deg \lambda$ est un entier positif, autrement dit le trinôme $X^2 + X\,\mathrm{tr}(\lambda) + \deg(\lambda)$ est positif sur $\mathbb{Q}$, donc sur $\mathbf{R}$, et le discriminant $\mathrm{tr}(\lambda)^2 - 4 \deg \lambda$ est négatif ou nul. Ainsi $|\mathrm{tr}(\lambda)| \leq 2\sqrt{\deg \lambda}$, et en particulier $|\mathrm{tr}(\pi_q)| \leq 2q^{1/2}$. ∎

Remarque : Cette proposition est un cas particulier du résultat suivant, dû à Weil (cf.[16] ,8) : si X est une courbe projective non singulière de genre g définie sur $\mathbb{F}_q$, on a :

$$|\#X(\mathbb{F}_q) - (1+q)| \leq 2gq^{1/2} \ .$$

Ce résultat équivaut au suivant (cf.[16] ,9.3): Tous les zéros de la fonction zêta de Riemann sur X ont une partie réelle égale à $1/2$.

Il est généralisé par les conjectures de Weil et Petersson (cf.[16],9.4) récemment démontrées par Deligne ([6a] ,[6b] ,[40]) dont nous reparlerons en (7.4.2).

5.5. SUPERSINGULARITE.

Soit K un corps de caractéristique $p \neq 0$, et E une courbe elliptique sur K .

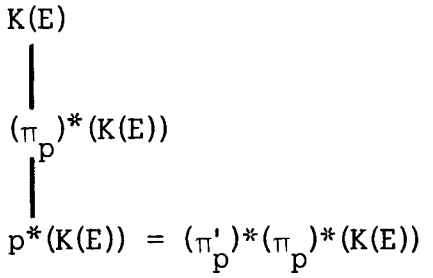
5.5.1. *LEMME* . La multiplication par p est une isogénie inséparable de E .

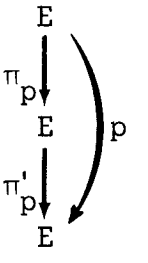
∎ L'application p_* est la multiplication par p des différentielles ; donc $p_* = 0$. ∎

Cela signifie que l'extension $K(E)/p^*(K(E))$ est inséparable.

Remarque : Nous savons, d'après (5.4.2), que π_p est inséparable et de degré $p = \pi_p\pi'_p$. Ainsi, l'extension $K(E)/p^*(K(E))$ se décompose en 2 extensions successives de degré p : $K(E)/(\pi_p)^*(K(E))$ qui est toujours

inséparable, et $(\pi_p)^*(K(E))/p^*(K(E)) = (\pi'_p)^*(\pi_p)^*(K(E))$ qui est inséparable si et seulement si π'_p est inséparable.





5.5.2. La courbe E est dite <u>non-supersingulière</u> si π'_p est séparable. Dans ce cas, $\mathrm{Ker}(p) \simeq \mathbb{Z}/p\mathbb{Z}$, chaque élément étant compté avec la multiplicité p .

Dans le cas contraire, π'_p est inséparable, p est purement inséparable, Ker(p) est réduit à l'élément 0 avec la multiplicité p^2, et E est dite <u>supersingulière</u>.

PROPOSITION . <u>Si</u> E <u>est supersingulière</u>, <u>son invariant</u> j <u>est dans</u> $\mathbb{F}_{p^2}$ (<u>même si</u> E <u>n'est pas défini sur</u> $\mathbb{F}_{p^2}$) . (cf.[18],12.2).

■ La courbe E est supersingulière si et seulement si p est purement inséparable, et alors $p^*(\overline{K}(E))$ est une extension de $(\overline{K}(E))^{p^2}$. Or $[\overline{K}(E) : p^*(\overline{K}(E))] = \deg(p) = p^2$, et d'autre part $(\overline{K}(E))^{p^2} = \overline{K}(E^{p^2})$ puisque $\overline{K}$ est algébriquement clos, d'où $[K(E):(\overline{K}(E))^{p^2}] = \deg(\pi_p^2) = p^2$. Ainsi, $p^*(\overline{K}(E)) = (\overline{K}(E))^{p^2}$, et $pE \simeq E^{p^2}$. Comme on a ici $E \simeq pE$, on en déduit que $j(E) = j(E^{p^2}) = j(E)^{p^2}$. ■

Ainsi, le nombre des invariants des courbes supersingulières est fini, donc le nombre des classes de $\overline{K}$ isomorphisme de courbes supersingulières sur K est fini.

5.5.3. Nous admettrons le résultat suivant, dû à Deuring (cf.[7]):

THEOREME . Soit E une courbe elliptique sur un corps K de caractéristique $p \neq 0$. Alors :

(i) Si j est transcendant sur $\mathbb{F}_p$, $\mathrm{End}(E) = \mathbb{Z}$;

(ii) Si E est supersingulière, End(E) est l'ordre maximal de l'algèbre de quaternions ramifiée en p et ∞ seulement.

(iii) Si E est non supersingulière et si K est un corps fini, End(E) est un ordre dans un corps quadratique imaginaire, et p est complètement décomposé dans ce corps quadratique.

On trouvera une démonstration de ce théorème dans [18] ,13.2, théorème 5 (pour (iii)), théorèmes 7,8,9 (pour (ii)) . L'assertion (i) provient de l'assertion analogue en caractéristique nulle ([18] ,3.3), jointe à un résultat de Deuring sur la réduction (mod.p) des invariants algébriques sur $\mathbb{Q}$ ([18] ,13.4, théorème 13).

5.5.4. Exemple 1.

PROPOSITION . Sur $\mathbb{F}_2$ ou $\mathbb{F}_4$, la courbe elliptique E d'équation $y^2+y = x^3$ est supersingulière, et $\pi_4 = -2$.

■ On peut le voir en utilisant le théorème de Deuring (iii) et la remarque (I,1.2.3) : End E contient Aut $E \simeq SL_2(\mathbb{F}_3)$, donc ne peut pas être contenu dans un corps quadratique imaginaire.

On peut aussi revenir à la définition, en montrant que la multiplication par 2 est purement inséparable : nous allons montrer que $2 = -\pi_4$, qui est purement inséparable d'après (5.3.2). Soit P un point de E , de coordonnées (x,y) , P' le 3e point d'intersection de la tangente à E en P et de E . Par définition, $2P = -P'$. Or, un calcul élémentaire donne l'équation de la tangente en P : $Y = x^2X + y^2$, et les coordonnées de P' : $x' = x^4$, $y' = y^4$; d'où $-2P = \pi_4(P)$ pour tout P de E . ■

5.5.5. Exemple 2.

PROPOSITION. Sur $\mathbb{F}_p((q))$, la courbe de Tate est non singulière.

▪ Ici, q désigne un élément d'un corps de caractéristique p , et E(q) la courbe de Tate d'équation $Y^2 - XY = X^2 - h_2X - h_3$ (cf.I.3.3). Les points d'ordre p de E(q) forment le groupe $q^{(1/p)\mathbb{Z}}/q^{\mathbb{Z}}$ cyclique d'ordre p , d'où la proposition. ▪

6. *REDUCTION*

Nous donnons ici quelques définitions, exemples et résultats dont nous aurons besoin. Pour plus de précision, voir [5] ou [42 a] , par exemple.

6.1. REDUCTION DES VARIETES PROJECTIVES.

6.1.1. Soient K un corps de nombres ou un corps p-adique, $\mathfrak{P}$ un idéal premier de K , R l'anneau des entiers en $\mathfrak{P}$, et $\tilde{K} = R/\mathfrak{P}$ le corps résiduel en $\mathfrak{P}$. Soit V une variété projective définie sur K , plongée dans $\mathbb{P}^{n+1}(\bar{K})$. On définit une variété projective sur $\tilde{K}$, appelée réduction de V (modulo $\mathfrak{P}$) , et notée $\tilde{V}$, de la façon suivante : on choisit pour tout point P de V , un système de coordonnées homogènes $(a_o, a_1, \ldots, a_n)$ tel que toutes les coordonnées soient dans R , et que l'une au moins ne soit pas dans $\mathfrak{P}$. Alors le n-uple $(\tilde{a}_o, \tilde{a}_1, \ldots, \tilde{a}_n)$ (où $\tilde{a}_i$ est la réduction modulo $\mathfrak{P}$ de a_i) , définit un point noté $\tilde{P}$ de $\mathbb{P}^{n+1}(\tilde{K})$. La variété $\tilde{V}$ est formée de l'ensemble des points $\tilde{P}$ lorsque P parcourt V .

6.1.2. En particulier, considérons une courbe elliptique E sur $\mathbb{Q}$. Nous verrons (cf.III.2) que, si le nombre premier p ne divise pas le

discriminant de E , alors la réduction $\tilde{E}$ de E modulo p est encore une courbe elliptique ; dans ce cas, la réduction modulo p est un homomorphisme de groupes de E sur $\tilde{E}$, dont le noyau est formé des points P admettant un système de coordonnées homogènes (x,y,z) tel que : p divise z , mais p ne divise pas les trois coordonnées.

6.2. POINTS D'ORDRE FINI SUR UNE COURBE ELLIPTIQUE.

6.2.1. Soit E une courbe elliptique sur un corps de nombres ou sur un corps p-adique, noté K .

PROPOSITION . La réduction modulo p induit un homomorphisme surjectif de E_N sur $(\tilde{E})_N$; autrement dit, $(\widetilde{E_N}) = (\tilde{E})_N$.

■ Pour démontrer ce résultat, on peut utiliser le fait que la réduction modulo p commute avec les opérations de la géométrie algébrique, et décrire E_N de la manière suivante : E_N est le noyau de la multiplication par N dans E ; considérons le graphe Γ_N de la multiplication par N (c'est un sous-ensemble de $E \times E$) ; l'intersection de Γ_N avec $E \times \{O\}$, projetée sur la première composante, nous donne le noyau de la multiplication par N : i.e. $E_N = pr_1(\Gamma_N \cap (E \times \{O\}))$ (cf.[18] ,9.1). ■

6.2.2. *COROLLAIRE* . Si $p \nmid N$, la réduction modulo p induit un isomorphisme de E_N sur $(\tilde{E})_N$. Par contre, si $p = N$, l'homomorphisme de réduction mod.p de E_p sur $\tilde{E}_p$ n'est pas injectif.

■ Il suffit de comparer les cardinaux de ces ensembles finis : or $\#E_N = N^2$ pour tout N , $\#\tilde{E}_N = N^2$ si $p \nmid N$, $\#\tilde{E}_p = p$ ou 1 selon que E est non supersingulière ou supersingulière. ■

6.3. REDUCTION DES HOMOMORPHISMES.

6.3.1. Soient E et F deux courbes elliptiques sur le corps de nombres K ayant bonne réduction modulo p .

PROPOSITION . Il existe un homomorphisme injectif de $\mathrm{Hom}(E,F)$ dans $\mathrm{Hom}(\tilde{E},\tilde{F})$.

▪ Considérons le graphe d'un homomorphisme λ dans la variété $E \times F$, et réduisons modulo p . Nous obtenons le graphe d'un homomorphisme $\tilde{\lambda}$ de $\tilde{E}$ dans $\tilde{F}$, de même degré que λ . Cette dernière propriété prouve que l'homomorphisme : $\lambda \to \tilde{\lambda}$ est injectif. ▪

6.3.2. Remarque : λ est toujours séparable, mais $\tilde{\lambda}$ peut ne pas l'être, par exemple si $\lambda = p$.

6.3.3. *PROPOSITION* . Soient ℓ un nombre premier différent de p , et λ un endomorphisme de E . Alors les endomorphismes $R_\ell(\lambda)$ de $T_\ell(E)$ et $R_\ell(\tilde{\lambda})$ de $T_\ell(\tilde{E})$ ont même polynôme caractéristique.

▪ Rappelons que le module de Tate $T_\ell(E) = \varprojlim E_{\ell^n}$, ainsi que la représentation R_ℓ , ont été définis en (5.1). Comme $p \nmid \ell$, on a un isomorphisme de $T_\ell(E)$ sur $T_\ell(\tilde{E})$, et un diagramme commutatif :

$$\begin{array}{ccc} T_\ell(E) & \xrightarrow{R_\ell(\lambda)} & T_\ell(E) \\ \downarrow \wr & & \downarrow \wr \\ T_\ell(\tilde{E}) & \xrightarrow{R_\ell(\tilde{\lambda})} & T_\ell(\tilde{E}) \end{array} \quad .$$

Ainsi, $R_\ell(\lambda)$ et $R_\ell(\tilde{\lambda})$ ont même polynôme caractéristique. ▪

Remarque : La définition de $\tilde{\lambda}$, ainsi que cette proposition, se généralisent à une variété abélienne quelconque (cf.[42 a]).

6.4. REDUCTION DES JACOBIENNES.

PROPOSITION (cf.[15], Igusa) :

(i) Les variétés $X_0(N)$ et $X(N)$ ont bonne réduction en tout p ne divisant pas N ;

(ii) Si X est une courbe projective non singulière ayant bonne réduction en p, alors sa jacobienne a bonne réduction en p, et $\widetilde{J(X)} = J(\widetilde{X})$.

7. *SERIE L ASSOCIEE A UNE COURBE MODULAIRE*

7.1. CONGRUENCE DE KRONECKER (cf.[18], 5.2).

7.1.1. Principe du q-développement.

PROPOSITION . Soit f une fonction modulaire de poids nul pour Γ, holomorphe sur $\mathfrak{H}$, et soit $f(\tau) = \sum_{i \geq m} b_i q^i$ (où $q = e^{2\pi i \tau}$) le développement de Fourier de f. Alors f est un polynôme en j à coefficients dans $\sum_{i \geq m} b_i \mathbb{Z}$.

■ Si $m \geq 1$, f est une forme parabolique de poids nul pour Γ, donc $f = 0$ (cf.I,2.2.3). Si $m \leq 0$, remplaçons f par la fonction $f_1 = f - b_m j^{-m}$: f_1 est une fonction modulaire de poids nul pour Γ, holomorphe sur $\mathfrak{H}$, et $f_1(\tau) = \sum_{i \geq m+1} b_{1,i} q^i$, où $b_{1,i} \in \sum_{i \geq m} b_i \mathbb{Z}$. Si $m+1 \leq 0$, on itère le procédé, jusqu'à la fonction f_{1-m} qui est nulle (comme forme parabolique de poids nul pour Γ) et dans $f + (\sum_{i \geq m} b_i \mathbb{Z})[j]$ (par construction). ■

7.1.2. Courbes isogènes. Soit E une courbe elliptique sur $\mathbb{C}$ d'invariant j .

PROPOSITION . Les invariants des courbes isogènes à E sont entiers sur $\mathbb{Z}[j]$.

Nous allons démontrer la proposition dans le cas où l'isogénie est de degré premier p . Cette démonstration se généralise aisément au cas d'un degré quelconque (cf.[43],4.6) .

■ Nous avons vu en (I,4.3.3) que les courbes isogènes à E par une isogénie de degré p sont les courbes E/F où F parcourt les $(p+1)$ sous-groupes d'ordre p de E ; si $E = \mathbb{C}/L$, ce sont les courbes $\mathbb{C}/L'$, où $L' = \alpha_i^{-1}L$ et où l'ensemble des α_i forme un système quelconque de représentants des classes à gauche modulo Γ des matrices de déterminant p dans $M_2(\mathbb{Z})$, par exemple

$$\{\alpha_i\}_{1\le i\le p+1} = \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}_{0\le u<p} \cup \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{(cf.2.2.1).}$$

Ainsi, les invariants des courbes p-isogènes à E sont les racines du polynôme $\varphi_p(X) = \prod_{1\le i\le p+1} (X - j\circ\alpha_i(\tau))$. Les coefficients de φ_p sont les fonctions symétriques élémentaires des $j\circ\alpha_i$, c'est-à-dire des fonctions holomorphes sur $\mathfrak{H}$, avec un développement de Fourier en $q^{1/p}$ à coefficients dans $\mathbb{Z}[\zeta_p]$ (si $\zeta_p = e^{2\pi i/p}$) ; car $j(\tau) = \sum_{n\ge -1} c(n)q^n$, avec $c(n) \in \mathbb{Z}$, d'où : $j(p\tau) = \sum_{n\ge -1} c(n)q^{pn}$ et $j(\frac{\tau+u}{p}) = \sum_{n\ge -1} c(n)\zeta^{nu}q^{n/p}$. De plus, si $\gamma \in \Gamma$, l'ensemble $\{\alpha_i\circ\gamma\}$ forme un système de représentants (comme $\{\alpha_i\}$), donc les coefficients de φ_p sont des fonctions modulaires de poids nul pour Γ , holomorphes dans $\mathfrak{H}$, dont le développement de Fourier est à coefficients dans $\mathbb{Z}[\zeta_p]$. D'après le principe de q-développement (7.1.1), ces coefficients sont des polynômes en j , à coefficients dans $\mathbb{Z}[\zeta_p]$. De plus, l'action de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permute les fonctions $j\circ\alpha_i$ (il suffit de regarder les développements de Fourier explicités ci-dessus), donc les coefficients de $\varphi_p(X)$ sont en fait dans $\mathbb{Z}[j]$. Comme $\varphi_p(X)$ est unitaire, ses racines $j\circ\alpha_i$ sont entières sur $\mathbb{Z}[j]$. ■

7.1.3. Polynôme modulaire. D'après ce qui précède, on peut considérer $\varphi_p(X)$ comme un polynôme en 2 variables $\Phi_p(X,j) \in \mathbb{Z}[X,j]$.

PROPOSITION .

(i) Le polynôme $\Phi_p(X,j)$ est symétrique ; considéré comme polynôme en 1 seule variable (X ou j), il est irréductible de degré p+1 ;

(ii) Et $\Phi_p(j,j)$ est un polynôme en j unitaire de degré 2p .

■ Comme Γ permute transitivement les $j\circ\alpha_i$ $(1 \le i \le p+1)$, les racines de $\varphi_p(X)$ sont conjuguées sur $\mathbb{Q}(j)$, donc le polynôme $\Phi_p(X,j)$ considéré comme polynôme en X est irréductible (sur $\mathbb{Q}(j)$) .

D'autre part, on peut prendre les 2 matrices $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ parmi les α_i , autrement dit , $\Phi_p(j(p\tau),j(\tau))$ et $\Phi_p(j(\tau/p),j(\tau))$ -ou $\Phi_p(j(\tau),j(p\tau))$- sont nuls pour tout $\tau \in \mathcal{H}$. Cela équivaut à dire que $\Phi_p(X,j)$ et $\Phi_p(j,X)$ ont pour racine commune $X = j\circ p$. Comme $\Phi_p(X,j)$ est un polynôme en X irréductible, il existe (par le lemme de Gauss) un polynôme $g(X,j) \in \mathbb{Z}[X,j]$ tel que $\Phi_p(j,X) = g(X,j)\Phi_p(X,j)$; on en déduit $\Phi_p(j,X) = g(X,j)g(j,X)\Phi_p(j,X)$, donc $g(X,j) = \pm 1$. Si $g(X,j) = -1$, alors $\Phi_p(j,j) = -\Phi_p(j,j)$, et j serait une racine $\Phi_p(X,j)$, ce qui est faux. Ainsi $\Phi_p(X,j) = \Phi_p(j,X)$ et (i) est démontré.

Le développement de Fourier de $\Phi_p(j,j) = \prod_{1\le i\le p+1} (j-j\circ\alpha_i)$ a pour terme de plus bas degré $(-1/q^p) \times (1/q)^p = -1/q^{2p}$ d'après les formules rappelées en (7.1.2), donc le polynôme en j , $\Phi_p(j,j)$ a pour terme de plus haut degré $-j^{2p}$. ■

7.1.4. Congruence de Kronecker.

PROPOSITION . Les polynômes $\Phi_p(X,j)$ et $(X-j^p)(X^p-j)$ sont congrus modulo p .

■ Les développements de Fourier donnés en (7.1.2) montrent que $j\circ\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right) - j^p \in p\mathbb{Z}((q))$ et que $j\circ\left(\begin{smallmatrix}1 & u\\ 0 & p\end{smallmatrix}\right) - j^{1/p} \in (1-\xi_p)\mathbb{Z}[\xi_p]((q))$, d'où $\Phi_p(X,j) \equiv (X-j^p)(X-j^{1/p})^p \bmod (1-\xi_p)\mathbb{Z}[\xi_p]$. Mais $\Phi_p(X,j) \in \mathbb{Z}[X,j]$ et $(X-j^p)(X-j^{1/p})^p$ est congru à $(X-j^p)(X^p-j)$ mod.$(1-\xi_p)\mathbb{Z}[\xi_p]$, donc $\Phi_p(X,j)$ est congru à $(X-j^p)(X^p-j)$ modulo $(1-\xi_p)\mathbb{Z}[\xi_p] \cap \mathbb{Z} = p\mathbb{Z}$. ■

La congruence $\Phi_p(X,j) \equiv (X-j^p)(X-j^{1/p})^p$ signifie que l'une des courbes p-isogènes à $\tilde{E}$ (réduction modulo p de E) a pour invariant j^p , et que les p autres ont pour invariant $j^{1/p}$. Or j^p est l'invariant de $\pi_p(\tilde{E})$, et si $\tilde{E}'$ est une courbe d'invariant $j^{1/p}$, $\pi_p(\tilde{E}')$ et $\tilde{E}$ ont même invariant j : donc $\pi_p(\tilde{E}') \approx \tilde{E}$.

7.2. THEOREME D'EICHLER-SHIMURA.

7.2.1. Comme $X_o(N)$ est définie sur $\mathbb{Q}$, sa réduction $\widetilde{X_o(N)}$ (mod.p) est définie sur $\mathbb{F}_p$, et π_p est une correspondance sur $\widetilde{X_o(N)}$.

THEOREME . Si $p \nmid N$, la correspondance de Hecke T_p sur $X_o(N)$ a une réduction $\tilde{T}_p$ modulo p qui vérifie : $\tilde{T}_p = \pi_p + \pi'_p$.

■ Il suffit de vérifier la formule sur $Y_o(N)$. On peut même se limiter aux couples (E,C) de $Y_o(N)$ tels que E ait bonne réduction non supersingulière modulo p . On a alors la suite exacte :

$$0 \to D \to E_p \to (\tilde{E})_p \to 0$$

où $\#E_p = p^2$, $\#(\tilde{E})_p = p$, donc $\#D = p$, et la projection : $E \to E/D$ est une isogénie de degré p .

En réduction mod.p , cette isogénie reste de degré p (cf. 6.3.1) mais son noyau $\tilde{D}$ est trivial, c'est donc une isogénie inséparable de $\tilde{E}$. Les p autres isogénies de degré p de E sont de la forme : $E \to E/F$, où F parcourt les sous-groupes de E d'ordre p distincts de D ; donc $\tilde{F} \approx \tilde{E}_p$ et en réduction les p couples $(E/F, C+F/F)$ sont

tous égaux à $(\tilde{E}/\tilde{E}_p, \tilde{C}+\tilde{E}_p/\tilde{E}_p)$: ils sont isogènes à $(\tilde{E},\tilde{C})$ par une isogénie de degré p séparable.

D'après (7.1.4), la 1ère isogénie est le Frobenius π_p, et l'on a : $\pi_p(\tilde{E}/\tilde{E}_p, \tilde{C}+\tilde{E}_p/\tilde{E}_p) = (\tilde{E},\tilde{C})$. Ainsi,

$$\begin{aligned}\tilde{T}_p((\tilde{E},\tilde{C})) &= \pi_p((\tilde{E},\tilde{C})) + p(\tilde{E}/\tilde{E}_p, \tilde{C}+\tilde{E}_p/\tilde{E}_p) \\ &= \pi_p((\tilde{E},\tilde{C})) + \pi'_p.\pi_p(\tilde{E}/\tilde{E}_p, \tilde{C}+\tilde{E}_p/\tilde{E}_p) \text{ (d'après 4.2.3)} \\ &= \pi_p((\tilde{E},\tilde{C})) + \pi'_p((\tilde{E},\tilde{C})) ,\end{aligned}$$

et $\tilde{T}_p = \pi_p + \pi'_p$. ∎

7.2.2. Afin de traduire sur les formes paraboliques de poids 2 le théorème d'Eichler-Shimura, nous rappelons ici des résultats obtenus depuis le paragraphe 4 :

L'espace $S(2,N)$ des <u>formes paraboliques de poids</u> 2 <u>pour</u> $\Gamma_o(N)$ est isomorphe à l'espace $\mathrm{Dif}_o(X_o(N))$ des <u>formes différentielles holomorphes sur</u> $X_o(N)$, par : $f \to \omega = f(z)dz$. Et $\mathrm{Dif}_o(X_o(N))$ est isomorphe à l'espace $\mathrm{Dif}_o(J_o(N))$ des <u>formes différentielles holomorphes sur</u> $J_o(N)$ (cf. 4.1.5).

Or $J_o(N)$ est une variété abélienne sur $\mathbb{C}$, de la forme $\mathbb{C}^g/\Lambda$ pour un réseau Λ de $\mathbb{C}^g$ (cf. 4.1.4) : ainsi, tout endomorphisme U de $J_o(N)$ peut être considéré comme un endomorphisme $R(U)$ de $\mathbb{C}^g$ laissant fixe Λ, et R définit la <u>représentation complexe</u> de $\mathrm{End}_{\mathbb{Q}}(J_o(N)) = \mathrm{End}(J_o(N)) \otimes \mathbb{Q}$ dans $M_g(\mathbb{C})$. Puisque Λ est laissé fixe par $R(U)$, on définit aussi la <u>représentation rationnelle</u> R_o de $\mathrm{End}_{\mathbb{Q}}(J_o(N))$ dans $\mathrm{End}_{\mathbb{Q}}(\Lambda\otimes\mathbb{Q}) \simeq M_{2g}(\mathbb{Q})$ et, pour tout nombre premier ℓ, la <u>représentation ℓ-adique</u> R_ℓ de $\mathrm{End}_{\mathbb{Z}_\ell}(J_o(N)) = \mathrm{End}(J_o(N)) \otimes \mathbb{Z}_\ell$ dans $\mathrm{End}_{\mathbb{Z}_\ell}(\Lambda\otimes\mathbb{Z}_\ell) \simeq \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell) \simeq M_{2g}(\mathbb{Z}_\ell)$ (cf.5.1). Si $U \in \mathrm{End}(J_o(N))$, en fait $R_o(U)$, $R_\ell(U)$ et $R(U) \oplus \overline{R(U)}$ sont représentés par des matrices équivalentes, et ont le même polynôme caractéristique à coefficients entiers (cf [43] lemma 3.49). En particulier,

$$\det R_o(U) = \det R_\ell(U) = \det R(U) \times \det \overline{R(U)} = |\det R(U)|^2 .$$

Or l'homomorphisme $U \mapsto U_*$ de $\mathrm{End}(J_o(N))$ dans $\mathrm{End}(\mathrm{Dif}_o(J_o(N)))$ défini en (4.1.5) définit une représentation équivalente à la représentation complexe R, donc $\det. R_\ell(U) = |\det. U_*|^2$.

Soit p un nombre premier différent de ℓ, et réduisons modulo p : d'après (6.3.3), $R_\ell(U)$ et $R_\ell(\tilde{U})$ ont même polynôme caractéristique.

En résumé, nous obtenons :

$$\det. R_\ell(\tilde{U}) = |\det. U_*|^2 .$$

7.2.3. Appliquons ce qui précède à l'endomorphisme $U = 1 - T_p u + pu^2$ de $J_o(N)$, où u est une indéterminée.

PROPOSITION . <u>Si</u> $p \nmid N$, <u>nous avons</u> :

$$\det_{S(2,N)}(1-T_p u+pu^2) = \det_{\widetilde{T_\ell(J_o(N))}}(1-\pi_p u) .$$

■ Le polynôme en u : $\det_{S(2,N)}(1-T_p u+pu^2)$ est à coefficients réels. D'après (7.2.2),

$$\det_{S(2,N)}(1-T_p u+pu^2) = \det(R(1-T_p u+pu^2)) ,$$

et

$$(\det_{S(2,N)}(1-T_p u+pu^2))^2 = \det_{\widetilde{T_\ell(J_o(N))}}\widetilde{(1-T_p u+pu^2)} .$$

Or

$$\widetilde{1 - T_p u + pu^2} = 1- \tilde{T}_p u + pu^2 = 1 - (\pi_p+\pi'_p)u + \pi_p\pi'_p u^2 = (1-\pi_p u)(1-\pi'_p u)$$

d'après le théorème d'Eichler-Shimura (7.2.1), car $p \nmid N$.

D'autre part, $\widetilde{1 - \pi_p u}$ et $1 - \pi'_p u$ sont conjugués, donc leurs déterminants sur $\widetilde{T_\ell(J_o(N))}$ sont égaux ; ainsi

$$(\det_{S(2,N)}(1-T_p u+pu^2))^2 = (\det_{\widetilde{T_\ell(J_o(N))}}(1-\pi_p u))^2 ,$$

et le signe doit être le même (poser $u = 0$ par exemple !), d'où la proposition. ■

7.3. FONCTION ZETA D'UNE VARIETE SUR UN CORPS FINI (cf [16], 9)

7.3.1. Soient p un nombre premier, q une puissance de p, V une variété affine ou projective non singulière définie sur $\mathbb{F}_q$. On appelle fonction zêta de V la fonction d'une variable complexe s définie par :

$$\zeta_V(s) = \prod_{x \in \mathfrak{X}} \left(1 - \frac{1}{q^{s.\deg(x)}}\right)^{-1}$$

où $\mathfrak{X}$ est l'ensemble des cycles premiers de V rationnels sur $\mathbb{F}_q$, c'est-à-dire l'ensemble des diviseurs de la forme $\sum_{i=1}^{d} (P_i)$ où les P_i sont tous les conjugués de P_1 sur $\mathbb{F}_q$ (le degré du cycle $\sum_{i=1}^{d} P_i$ est égal à d).

Lorsque V est affine, l'ensemble M des idéaux maximaux de $\mathbb{F}_q[V]$ est en bijection avec $\mathfrak{X}$, et $\zeta_V(s) = \prod_{m \in M} \left(1 - \frac{1}{Nm^s}\right)^{-1}$, où $Nm = \#(\mathbb{F}_q[V]/m)$. On montre que le produit infini qui définit $\zeta_V(s)$ converge au moins pour $Re(s) > \dim V$. On a :

$$\zeta_V(s) = \prod_{n \geq 1} (1 - q^{-ns})^{-\nu_n}$$

si ν_n est le nombre de cycles $x \in \mathfrak{X}$ de degré n, et :

$\log \zeta_V(s) = \sum_{n \geq 1} \frac{N_n}{n q^{ns}}$ si $N_n = \sum_{d \mid n} d\nu_d$ est le cardinal de $V(\mathbb{F}_{q^n})$, c'est-à-dire le nombre de points de V fixes par π_{q^n}.

Les cohomologies de Weil permettent de déterminer N_n ([16] donne une idée de la méthode et de nombreuses références).

7.3.2. En particulier, lorsque V est une courbe X projective non singulière sur $\mathbb{F}_q$ de genre g, on obtient $N_n = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$ si $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ sont les valeurs propres de π_q sur $T_\ell(J(X))$, numérotées de telle sorte que $\alpha_i \cdot \alpha_{i+g} = q$ $(1 \leq i \leq g)$, d'où le :

THEOREME DE HASSE-WEIL : $\zeta_X(s) = \dfrac{\prod_{i=1}^{2g} (1-\alpha_i q^s)}{(1-q^{-s})(1-q^{1-s})}$.

Notons $u = q^{-s}$ et $L_X(u)$ l'inverse du numérateur de $\zeta_X(s)$, c'est-à-dire $L_X(u) = \prod_{i=1}^{2g} (1-\alpha_i u)^{-1} = \det_{T_\ell(J(X))}(1-\pi_q u)^{-1}$. Nous utilisons ceci en (7.4.1) en prenant pour X la réduction modulo p de $X_o(N)$.

7.4. SERIES L ET SERIES DE DIRICHLET.

7.4.1. Maintenant, soit X la courbe $X_o(N)$, et $\widetilde{X_o(N)}^{(p)}$ sa réduction modulo p . On définit la série L associée à $X_o(N)$ par :

$$L_{X_o(N)}(u) = \prod_{p \nmid N} L_{\widetilde{X_o(N)}^{(p)}}(u) \times \prod_{p \mid N} \det_{S(N,2)}(1-T_p u)^{-1} .$$

D'autre part, on a vu (3.3.5 et 3.3.6) qu'on peut trouver une base $f_1, f_2, \ldots, f_g$ de l'espace des formes paraboliques de poids 2 pour $\Gamma_o(N)$ qui soit formée de fonctions propres pour tous les opérateurs T_ℓ ; si $f_j(\tau) = \sum_{n \geq 1} a_n^{(j)} e^{2\pi i \tau}$, normalisons ces fonctions par : $a_1^{(j)} = 1$.

THEOREME . Avec ces notations, nous avons la relation suivante entre série L et séries de Dirichlet:

$$L_{X_o(N)}(p^{-s}) = \prod_{i=1}^{g} L(s, f_i, 1) .$$

■ D'après (2.3.1),

$$L(s, f_i, 1) = \prod_{p \mid N} (1-a_p^{(i)} p^{-s})^{-1} \times \prod_{p \nmid N} (1-a_p^{(i)} p^{-s} + p^{k-1-2s})^{-1} ;$$

or d'après (7.2.3), $\det_{T_\ell(\widetilde{J_o(N)}^{(p)})}(1-\pi_p u) = \det_{S(N,2)}(1-T_p u+pu^2)$

c'est-à-dire

$$L_{\widetilde{X_o(N)}^{(p)}}(u) = \prod_{i=1}^{g} (1-a_p^{(i)}u+p^{k-1}u^2)^{-1} \times \prod_{i=1}^{g} (1-a_p^{(i)}u)^{-1} . \quad \blacksquare$$

7.4.2. Hypothèse de Riemann (cf. (5.3.3) et [16] ,9).

PROPOSITION . Si $p \nmid N$, les valeurs propres des T_p vérifient : $|a_p^{(i)}| \leq 2\sqrt{p}$.

■ On a :

$$\prod_{i=1}^{g} (1-a_p^{(i)}u+pu^2) = \prod_{i=1}^{g} (1-\alpha_i u)(1-\bar{\alpha}_i u)$$

$$= \prod_{i=1}^{g} (1-(\alpha_i+\bar{\alpha}_i)u+pu^2) \quad \text{car} \quad \alpha_i\bar{\alpha}_i = p ,$$

d'où $a_p^{(i)} = \alpha_i + \bar{\alpha}_i$; or $|\alpha_i|^2 = |\bar{\alpha}_i|^2 = \alpha_i\bar{\alpha}_i = p$, donc $|a_p^{(i)}| \leq 2\sqrt{p}$. ■

Cette proposition est la démonstration, pour $k = 2$, de la conjecture suivante de Petersson :

Conjecture : Les valeurs propres a_p des opérateurs de Hecke T_p sur les formes paraboliques de poids k pour $\Gamma_o(N)$ vérifient $|a_p| \leq 2p^{k-1/2}$ si $p \nmid N$) . Cette conjecture a été récemment démontrée par Deligne ([6a] ,[6b] ,[40]).

7.4.3. *COROLLAIRE* . Les valeurs propres des opérateurs de Hecke sont des nombres réels.

■ Les valeurs propres des opérateurs de Hecke sont les nombres $a_n^{(i)}$ (cf.2.3.1) ; or nous venons de voir que $a_p^{(i)} = \alpha_i + \bar{\alpha}_i$, donc que $a_p^{(i)}$ est réel. ■

8. *LA COURBE MODULAIRE* $X_o(11)$

8.1. L'ESPACE M(11,2) .

8.1.1. Ici $N = 11$ est premier, et le corollaire (cf. I.4.2.3) donne le genre de $X_o(11)$: $g_o(11) = 1$. La courbe $X_o(11)$ est une courbe elliptique . Nous allons déterminer son équation.

L'espace des formes paraboliques de poids 2 pour $\Gamma_o(11)$, noté $S(11,2)$, est de dimension $g_o(11) = 1$ (cf.4.1.5) . Or la fonction $\varphi(\tau) = \eta^2(\tau)\eta^2(11\tau)$ est une forme parabolique (non nulle) pour $\Gamma_o(11)$ (nous le démontrons dans un cas plus général en (IV.2.1.3)) . Donc $S(11,2)$ est engendré par φ .

D'autre part, il ne peut pas exister deux formes modulaires non paraboliques de poids 2 indépendantes.

Nous allons construire une fonction modulaire ψ de poids 2 pour $\Gamma_o(11)$, non parabolique, et prouver ainsi que l'espace $M(11,2)$ des formes modulaires de poids 2 pour $\Gamma_o(11)$ est de dimension 2.

8.1.2. Tout d'abord, soit $A = (a_{ij})$ une matrice carrée d'ordre pair $n = 2k$, à coefficients entiers, symétrique, définie, positive, et telle que les coefficients a_{ii} de la diagonale soient pairs. Soit Q la forme quadratique à coefficients entiers définie par : $Q(\underline{x}) = \frac{1}{2}\sum_{i=1}^{n} a_{ij}x_ix_j$ si $\underline{x} = (x_1,\ldots,x_n)$, et définissons la fonction θ_Q sur $\mathcal{H}$ par :

$$\theta_Q(\tau) = \sum_{\underline{m}\in\mathbb{Z}^n} e^{2\pi i Q(\underline{m})\tau} .$$

Soit N le plus petit entier tel que NA^{-1} vérifie les mêmes hypothèses que A . Soit ε le caractère quadratique défini par :

$$\varepsilon(d) = \left(\frac{(-1)^k \det A}{d}\right) .$$

PROPOSITION . La fonction θ_Q est une forme modulaire de type (k,N,ε) , non parabolique.

▪ Il s'agit de montrer que $\theta_Q |_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \epsilon(d)\, \theta_Q$ lorsque $c \equiv 0 \pmod N$ et $ad - bc = 1$. C'est une conséquence de la formule sommatoire de Poisson (cf.I.2.3.1). θ_Q n'est pas parabolique : en effet, considérée comme série entière en $q = e^{2\pi i\tau}$, son terme constant correspond à $\underline{m} = 0$ puisque la forme quadratique Q est non dégénérée, et vaut 1 . ▪

8.1.3. Application : Soit $A = \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}$, $\det A = 11$, $N = 11$ et $11.A^{-1} = \begin{pmatrix} 6 & -1 \\ -1 & 2 \end{pmatrix}$. La proposition dit que la fonction ξ , définie sur $\mathcal{H}$ par :

$$\xi(\tau) = \sum_{(n,m)\in\mathbb{Z}^2} e^{2\pi i(m^2+mn+3n^2)\tau}$$

est une forme modulaire de type $(1, 11, (\frac{-11}{\cdot}))$ c'est-à-dire :

$\xi |_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\frac{-11}{d})\xi$ dès que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(11)$. Et ξ n'est pas parabolique.

Posons $\psi = \xi^2$. Alors ψ est une forme modulaire non parabolique de poids 2 pour $\Gamma_o(11)$. D'où le résultat :

PROPOSITION . <u>L'espace</u> $M(11,2)$ <u>est de dimension</u> 2 <u>et</u> $\{\varphi, \psi\}$ <u>en forme une base</u>.

8.2. EQUATION DE $X_o(11)$.

8.2.1. Rappelons que l'involution d'Atkin-Lehner $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ normalise $\Gamma_o(N)$. Soit $\Gamma_+(N)$ le sous-groupe de $GL_2(\mathbb{Z})$ engendré par $\Gamma_o(N)$ et W_N . L'indice de $\Gamma_o(N)$ dans $\Gamma_+(N)$ est égal à 2 , donc le degré du revêtement $X_o(N) \to X_+(N) = \overline{\Gamma}_+(N)\backslash\mathcal{H}$ est égal à 2 .

Les genres $g_o(N)$ et $g_+(N)$ de $X_o(N)$ et $X_+(N)$ sont liés par <u>la formule de Riemann-Hurwitz</u>, qui donne ici :

$$2g_o(N) - 2 = 2(2g_+(N) - 2) + \sum_{P\in X_o(N)} (e_p - 1)$$

où e_p est l'indice de ramification en p . Or $e_p = 1$ ou 2 , et $e_p = 2$ si et seulement si p est un point fixe pour W_N dans $X_o(N)$. Ainsi, ω désignant le nombre de points fixes de W_N , on a :

$$2g_o(N) - 2 = 2(2g_+(N)-2) + \omega \quad .$$

Remarquons que ω est au moins égal à 1 , car $W_N(\frac{i}{\sqrt{N}}) = \frac{i}{\sqrt{N}}$. Lorsque $N = 11$, $g_o(11) = 1$, et $4(g_+(11)-1) + \omega = 0$. Comme $g_+(11)$ et ω sont des entiers, $g_+(11) \geq 0$ et $\omega \geq 1$, la seule solution est : $g_+(11) = 0$ et $\omega = 4$. D'où le résultat :

PROPOSITION . Le revêtement : $X_o(11) \to X_+(11)$ est de degré 2 , la courbe $X_+(11)$ est de genre nul, et W_{11} a quatre points fixes dans $X_o(11)$.

COROLLAIRE . Nous avons $\psi|_2 W_{11} = -\psi$, et $\varphi|_2 W_{11} = -\varphi$.

▪ Nous avons vu que la valeur de ψ à l'infini est égale à 1 . D'autre part, on peut calculer la valeur de $\psi|_2 W_{11}$ à l'infini : elle vaut (-1) . Donc $(\psi + \psi|_2 W_{11})(\tau)d\tau$ et $(\varphi + \varphi|_2 W_{11})(\tau)d\tau$ sont des formes différentielles holomorphes sur $X_+(11)$, qui est de genre nul ; d'après (4.1.5), ces formes différentielles sont nulles. ▪

8.2.2. *LEMME* . Les diviseurs de φ et ψ sont de degré 2 . Plus précisément, $(\psi) = 2(\frac{i}{\sqrt{11}})$ et $(\varphi) = (0) + (\infty)$.

▪ La forme différentielle $\varphi(\tau)d\tau$ est holomorphe sur $X_o(11)$, donc de degré $2g-2 = 0$ (théorème de Riemann-Roch). Or la forme différentielle $d\tau$ a pour diviseur $(d\tau) = -(0)-(\infty)$: d'où $(\varphi) = (0)+(\infty)$ et $\deg(\varphi) = 2$. Le quotient φ/ψ est une fonction sur $X_o(11)$, donc les degrés de (φ) et (ψ) sont égaux. Comme ψ est un carré, tous ses zéros sont d'ordre pair ; et comme ψ est holomorphe, la seule possibilité est la suivante : ψ a un zéro double sur $X_o(11)$. Or la fonction continue : $y \to \psi(iy)$, pour $y \in]0,+\infty[$, est à valeurs réelles ; comme $\psi(0) = -1$ et $\psi(\infty) = +1$, le théorème des valeurs intermédiaires prouve que le zéro de ψ est sur le demi-axe imaginaire ; comme

$\psi|_2 W_{11} = -\psi$, ce zéro doit être fixe par W_{11} . Autrement dit, ψ a un pôle double au point $\frac{i}{\sqrt{11}}$. ∎

8.2.3. Posons $X = \varphi/\psi$; ainsi, X est une fonction sur $X_o(11)$; et $X|_2 W_{11} = X$, donc X induit une fonction sur $X_+(11)$. De plus, X a un pôle double en $\frac{i}{\sqrt{11}}$ et deux zéros simples, en 0 et ∞ (cf. la fonction $\wp$ de Weierstrass). Considérée comme fonction sur $X_+(11)$, X a un pôle simple en $\frac{i}{\sqrt{11}}$ et un zéro simple à la pointe $0 = \infty$.

PROPOSITION . $\mathbb{Q}(X_+(11)) = \mathbb{Q}(X)$.

∎ Le corps $\mathbb{Q}(X)$ est inclus dans $\mathbb{Q}(X_+(11))$, et le degré $[\mathbb{Q}(X_+(11)) : \mathbb{Q}(X)]$ est égal au degré des zéros de X dans $X_+(11)$, c'est-à-dire à 1 . ∎

8.2.4. Considérons la série d'Eisenstein E_4 (définie en I.2.1.1) et posons $f = \frac{-E_4 + E_4|_4 W_{11}}{120}$. Calculons :

$$(E_4|_4 W_{11})(\tau) = 11^2.(11\tau)^{-4} \cdot E_4(\tfrac{-1}{11\tau}) = 11^2 E_4(11\tau)$$

car $\begin{pmatrix} 11 & 0 \\ 0 & 1 \end{pmatrix}.\begin{pmatrix} 0 & -1 \\ 11 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ et E_4 est une fonction modulaire de poids 4 pour $SL_2(\mathbb{Z})$; donc $f(\tau) = \frac{121\, E_4(11\tau) - E_4(\tau)}{120}$. Rappelons que $E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n$ donc $f(q)$ est une série entière en q à coefficients entiers, dont le terme constant est égal à 1 .

De par sa définition, $f|_4 W_{11} = -f$.

Posons $Y = \frac{f}{\psi^2}$; comme $\psi|_2 W_{11} = -\psi$, on a $\psi^2|_4 W_{11} = \psi^2$, et $Y|_4 W_{11} = -Y$.

Enfin, f n'ayant pas de pôle, les pôles de Y sont les zéros de ψ^2 ; or ψ^2 a un seul zéro, d'ordre 4 , en $\frac{i}{\sqrt{11}}$. Donc Y a un pôle d'ordre au plus 4 en $\frac{i}{\sqrt{11}}$. Et même d'ordre au plus 3 car $f(\frac{i}{\sqrt{11}}) = 0$ puisque $f|W_{11} = -f$.

D'autre part, $Y|_4 W_{11} = -Y$ donc les 4 points fixes de W_{11} sont des points "singuliers" (zéros ou pôles) pour Y, et le pôle est d'ordre au moins 3. D'où le résultat suivant :

PROPOSITION. Y a un pôle triple en $\frac{i}{\sqrt{11}}$, et un zéro simple en chacun des 2 autres points fixes de W_{11}.

8.2.5. *THEOREME*. $\mathbb{Q}(X_o(11)) = \mathbb{Q}(X,Y)$.

■ En effet, $[\mathbb{Q}(X_o(11)) : \mathbb{Q}(X_+(11))] = 2$, $\mathbb{Q}(X_+(11)) = \mathbb{Q}(X)$ d'après (8.2.3), et $Y \in \mathbb{Q}(X_o(11))$, $Y \notin \mathbb{Q}(X_+(11))$. ■

De plus, Y^2 (étant invariant par W_{11}) appartient à $\mathbb{Q}(X_+(11)) = \mathbb{Q}(X)$, donc Y^2 est égal à un polynôme en X de degré ≤ 3 car le seul pôle de X (resp. Y) est le point $\frac{i}{\sqrt{11}}$, et il est d'ordre 2 (resp. 3).

En écrivant les premiers termes des développements de Fourier de X et Y, on obtient l'équation : $Y^2 = 1 - 20X + 56X^2 - 44X^3$ et pour se ramener à la forme canonique, on effectue le changement de variable : $Y = \frac{2y+11+10x}{11}$, $X = \frac{-x}{11}$, (cf [9]) qui donne :

$$y^2 + 10xy + 11y = x^3 - 11x^2 .$$

8.2.6. Les formules de (I.1.1.2) donnent alors le discriminant de $X_o(11)$: $\Delta = -11^5$.

Cette dernière équation est une équation minimale pour $X_o(11)$: en effet, tout changement de variable multiplie le discriminant par une puissance douzième, or le nombre -11^5 ne comporte aucun facteur à une puissance 12.

8.3. QUELQUES PROPRIETES DE $X_o(11)$.

8.3.1. Pointes et points rationnels d'ordre fini.

Les pointes ∞ et 0 de $X_o(11)$ correspondent respectivement aux points $(x,y) = (0,0)$ et $(0,-11)$: en effet, X s'annule aux pointes, donc x aussi, et l'on a $y = 11.\frac{Y-1}{2}$; or, à l'infini on a : $f(\infty) = 1$, $\psi(\infty) = 1$, donc $Y(\infty) = 1$ et $y(\infty) = 0$; et en 0 , $f(0) = -1$, $\psi(0) = -1$, donc $Y(0) = -1$ et $y(0) = -11$.

Le point $(x,y) = (0,0)$ est rationnel sur $\mathbb{Q}$, et si on lui applique les formules d'addition sur les courbes elliptiques (cf [31] ,3.4), on constate qu'il est d'ordre 5 . Dans le chapitre IV, nous généraliserons ce résultat, et montrerons que ces 5 points sont les seuls points rationnels de $X_o(11)$.

8.3.2. Réduction de $X_o(11)$.

La courbe elliptique $X_o(11)$ est à bonne réduction modulo p pour tout nombre premier $p \neq 11$.

En 11, les formules de (I.1.1.2) montrent que $-c_6$ est congru à 9 modulo 11, donc $(-c_6/\Delta) = +1$.

Nous verrons en (III, prop.1.1.5 et théorème 1.2.4), que cela prouve que $X_o(11)$ est une courbe de Tate sur $\mathbb{Q}$.

8.3.3. Eichler-Shimura.

Les coefficients c_n du q-développement de $\varphi(\tau) = \eta^2(\tau).\eta^2(11\tau)$ se calculent facilement à partir du q-développement de η :

$$\sum_{n\geq 1} c_n q^n = (q^{1/24} \prod_{n\geq 1} (1-q^n))^2 \, (q^{11/24} \prod_{n\geq 1} (1-q^{11n}))^2$$

$$= q \prod_{n\geq 1} (1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 - 6q^4 + \dots .$$

D'autre part, on peut aussi calculer $N_p = \sharp X_o(11)(\mathbb{F}_p)$ pour tout nombre premier p .

On peut alors vérifier la formule : $N_p = 1 - c_p + p$ (cf. 7.3.2 et 7.4.2) et l'hypothèse de Riemann : $|1+p-N_p| \leq 2\sqrt{p}$ c'est-à-dire : $|c_p| \leq 2\sqrt{p}$.

Pour calculer N_p , on sait que c'est un multiple de 5 , car le point $(0,0)$ est un point d'ordre 5 de $E(\mathbb{F}_p)$, pour tout p différent de 5 et 11 . D'autre part, N_p est inférieur ou égal à $\#P_2(\mathbb{F}_p) = p^2+1$. Par exemple, cela donne immédiatement $N_2 = 5$, alors qu'on avait $c_2 = -2$. Pour $p = 3$, $E(\mathbb{F}_3)$ comporte les points $(x,y) = (0,0),(0,1),(-1,0),(-1,-1)$, et le point à l'infini, donc $N_3 = 5$, alors que $c_3 = -1$ ...