*Actes, Congrès intern. Math.*, 1970. Tome 2, p. 291 à 299.

# GROUPES FORMELS, FONCTIONS AUTOMORPHES ET FONCTIONS ZETA DES COURBES ELLIPTIQUES

par P. CARTIER

A ANDRÉ WEIL et JEAN DIEUDONNÉ,
*dont les travaux ont été notre source d'inspiration constante et féconde*

## 1. Congruences pour les coefficients des fonctions automorphes.

Nous allons rappeler quelques-unes des remarquables congruences satisfaites par les coefficients des formes modulaires, et qui ont été découvertes par Ramanujan, Newman, Atkin, O'Brien et Swinnerton-Dyer (voir Atkin [1] pour les détails). Considérons d'abord la forme modulaire $\Delta$ de poids 12 (discriminant) :

$$\Delta(\tau) = e^{2\pi i\tau} \prod_{n=1}^{\infty} (1 - e^{2\pi i n\tau})^{24} = \sum_{n=1}^{\infty} \tau(n) \, e^{2\pi i n\tau} \tag{1}$$

Soit $p$ un nombre premier ; les coefficients $\tau(n)$ de $\Delta$ satisfont à la relation de Ramanujan-Mordell(1) :

$$\tau(np) - \tau(p) \, \tau(n) + p^{11} \, \tau(n/p) = 0 \tag{2}$$

pour tout entier $n \geqslant 1$. Sous l'hypothèse $\tau(p) \not\equiv 0 \bmod p$, on déduit de cette égalité des congruences comme suit : définissons par récurrence les nombres rationnels $p$-entiers $B_\alpha$ par $B_1 = \tau(p)$ et $B_{\alpha+1} = \tau(p) - p^{11}/B_\alpha$ ; on a alors

$$\tau(np^\alpha) \equiv B_\alpha \, \tau(np^{\alpha-1}) \mod p^{11\alpha} \tag{3}$$

pour $n \geqslant 1$ et $\alpha \geqslant 1$. On notera qu'il existe une unique unité $p$-adique $B$ satisfaisant à l'équation $B^2 - \tau(p) \, B + p^{11} = 0$ et qu'on a $B_\alpha \equiv B \bmod p^{11\alpha}$ pour tout $\alpha \geqslant 1$ ; on peut donc remplacer $B_\alpha$ par $B$ dans (3), à condition de se placer dans le domaine des nombres $p$-adiques.

Considérons par ailleurs les coefficients $c(n)$ définis par $j(\tau) = \sum_{n=-1}^{\infty} c(n) \, e^{2\pi i n\tau}$, où $j$ est l'invariant modulaire elliptique de poids 0 bien connu. En 1968, Atkin a obtenu le résultat suivant, qui généralise et résume une longue suite de résultats partiels : étant donné un entier $\alpha \geqslant 1$, on pose $t(n) = c(\ell^\alpha n)/c(\ell^\alpha)$ ; on a alors les relations

---

(1) Nous faisons la convention que $\tau(a)$ est nul si $a$ n'est pas entier ; on fera des conventions analogues pour $t(a)$ dans (4), pour $\beta(a)$ dans (9), etc . . .

$$t(np) - t(p).t(n) + p^{-1}.t(n/p) \equiv 0 \mod \ell^{\alpha} \tag{4}$$

$$t(n\ell) = t(n).t(\ell) \tag{5}$$

($n \geqslant 1$, $p$ premier $\neq \ell$) lorsque $\ell = 13$ et $\alpha$ quelconque ou lorsque $\ell = 17, 19, 23$ et $\alpha$ assez petit. Atkin a formulé une conjecture précise pour le cas des nombres premiers $\ell$ quelconques [1].

Le troisième exemple que nous considérerons se réfère à des formes modulaires de poids 2, c'est-à-dire à des formes différentielles de première espèce sur des courbes modulaires. D'une manière plus générale (cf. n° 5 pour le rapport entre ces deux points de vue), considérons une cubique plane $C$ d'équation non homogène $Y^2 = X^3 - aX - b$ avec $a$ et $b$ entiers. Choisissons au voisinage du point à l'infini de $C$ un paramètre local $\xi$ tel que l'on ait $X = \xi^{-2} + \sum_{n=-1}^{\infty} \alpha(n).\xi^n$ avec des coefficients $\alpha(n)$ entiers ; la forme différentielle de première espèce $\omega = -dX/2Y$ sur $C$ se développe sous la forme $\omega = \sum_{n=1}^{\infty} \beta(n).\xi^{n-1}d\xi$ avec des coefficients $\beta(n)$ entiers, et $\beta(1) = 1$. Soit $p$ un nombre premier différent de 2 et 3 ; Atkin et Swinnerton-Dyer(1) ont établi les congruences suivantes :

$$\beta(np) \equiv \beta(n).\beta(p) \mod p \tag{6}$$

$$\beta(p) \equiv \sum_{t \bmod p} -\left(\frac{t^3-at-b}{p}\right) \mod p\ , \tag{7}$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre. Supposons qu'on ait $\beta(p) \not\equiv 0 \bmod p$, c'est-à-dire que la réduction de $C$ modulo $p$ soit d'invariant de Hasse-Witt non nul ; il existe alors une suite $(k_\alpha)_{\alpha \geqslant 1}$ de nombres entiers tels que

$$\beta(np^{\alpha}) \equiv k_{\alpha}\beta(np^{\alpha-1}) \mod p^{\alpha} \text{ pour tout } n \geqslant 1\ . \tag{8}$$

L'analogie avec la démonstration de (3) à partir de (2) a conduit Atkin et Swinnerton-Dyer à postuler une congruence de la forme

$$\beta(np) - \beta(p).\beta(n) + p.\beta(n/p) \equiv 0 \mod p^{\alpha} \tag{9}$$

pour tout entier $n \equiv 0 \bmod p^{\alpha-1}$, y compris lorsque $\beta(p) \equiv 0 \bmod p$.

Il semble prématuré de faire des conjectures précises contenant tous ces cas particuliers (et d'autres analogues). Le schéma général semble être le suivant : on considère une certaine forme modulaire de poids $2g$, soit $h(\tau) = \sum_{n=1}^{\infty} r(n).e^{2\pi i n\tau}$, avec des coefficients $r(n)$ entiers, normalisée par $r(1) = 1$ ; on est en droit d'attendre des congruences de la forme

(1) A notre connaissance, les résultats d'Atkin et Swinnerton-Dyer n'ont pas encore été publiés et sont contenus dans la correspondance échangée entre ces auteurs et Serre. Nous remercions Serre qui, en nous communiquant cette correspondance et en nous obligeant à répondre à ses questions pertinentes, a été à l'origine des résultats exposés ici.

(10) $\quad r(np) - r(p) \cdot r(n) + p^{2g-1} \cdot r(n/p) \equiv 0 \mod p^{(2g-1)\alpha}$

lorsque $p$ est premier et $n \equiv 0 \mod p^{\alpha-1}$. Rappelons que la relation (2) de Ramanujan-Mordell signifie que $\Delta$ est fonction propre de l'opérateur de Hecke $T_p$. Par analogie, les résultats sur l'invariant modulaire elliptique $j$ suggèrent la possibilité suivante : soit $\ell$ premier ; à l'aide des coefficients de Fourier de certaines formes modulaires de poids 0, on pourrait définir une "cohomologie étale $\ell$-adique" qui serait un module libre $H_\ell$ de rang $[\ell/12]$ sur l'anneau $\mathbf{Z}_\ell$ des entiers $\ell$-adiques et un opérateur de Hecke $T_{p,\ell}$ dans $H_\ell$ pour tout nombre premier $p \neq \ell$. Par contre, les congruences sur les courbes elliptiques suggèrent la possibilité dans certains cas de définir un opérateur de Hecke $T_{p,p}$ dans un module de cohomologie $p$-adique $H'_p$ analogue à la cohomologie de Washnitzer-Monsky.

## 2. Groupes $p$-adiques rigides.

La suite de cet exposé est motivée par les congruences d'Atkin et Swinnerton-Dyer pour les différentielles de première espèce sur les courbes elliptiques. Le cadre naturel semble celui des groupes $p$-adiques rigides, dont nous empruntons la définition (en la simplifiant pour notre usage) à Tate [6]. Notons $p$ un nombre premier, $\mathfrak{o}$ ou $\mathbf{Z}_p$ l'anneau des entiers $p$-adiques et $K$ ou $\mathbf{Q}_p$ le corps des fractions de $\mathfrak{o}$. Pour tout entier $n \geqslant 0$, on note $D^n$ l'ensemble des vecteurs à $n$ composantes dans $\mathfrak{o}$ divisibles par $p$, et $\mathfrak{A}_n$ la $\mathfrak{o}$-algèbre des fonctions sur $D^n$ de la forme

$$f(x) = \sum_{i_1, \ldots, i_n} a(i_1, \ldots, i_n) \cdot x_1^{i_1} \ldots x_n^{i_n}$$

(les coefficients $a(i_1, \ldots, i_n)$ étant pris dans $\mathfrak{o}$). Une *variété rigide de dimension n* est un couple $(X, \mathfrak{A}(X))$ isomorphe à $(D^n, \mathfrak{A}_n)$ ; un système de coordonnées rigide sur $X$ est une suite $(\xi_1, \ldots, \xi_n)$ d'éléments de $\mathfrak{A}(X)$ telle que l'application $x \mapsto (\xi_1(x), \ldots, \xi_n(x))$ soit un isomorphisme de $X$ sur $D^n$. Une variété rigide $X$ porte une structure de variété analytique sur le corps $K$ pour laquelle tout système de coordonnées rigide est un système de coordonnées analytique ; les éléments de $\mathfrak{A}(X)$ sont *certaines* fonctions analytiques sur $X$, qualifiées de *rigides*(1). A partir des fonctions analytiques rigides sur $X$, on pourra définir les champs de vecteurs (ou les formes différentielles) rigides.

Les variétés rigides forment une catégorie avec produit, et l'on peut par suite définir la notion de groupe $p$-adique rigide. Deux exemples de tels groupes sont le groupe additif $\mathbf{G}_a$, ayant $D^1$ pour variété sous-jacente, et l'addition pour opération, et le groupe multiplicatif $\mathbf{G}_m$ qui se compose du groupe multiplicatif des $x \equiv 1 \mod p$ dans $\mathfrak{o}$, avec la coordonnée rigide $\xi$ donnée par $\xi(x) = x - 1$.

Dans la suite, nous désignerons par $G$ un groupe $p$-adique rigide de dimension 1 (nécessairement commutatif) ; les formes différentielles rigides de degré 1 sur $G$

---

(1) Rappelons qu'une fonction qui est localement égale à une fonction analytique est analytique. Par contre, une fonction qui appartient localement à $\mathfrak{A}(X)$ n'appartient pas nécessairement à $\mathfrak{A}(X)$, d'où la terminologie : "rigide".

invariantes par translation forment un $o$-module libre de rang 1, dont nous choisirons une base $\omega_0$. Alors $\omega_0$ est la différentielle $d\ell$ d'une fonction analytique $\ell$ sur $G$, appelée le *logarithme de G*. Ce logarithme est un isomorphisme de groupes de Lie $p$-adiques de $G$ sur $G_a$, mais n'est pas en général une fonction analytique rigide. Pour préciser ce point, introduisons les opérateurs de Lazard $\Psi_n (n \geqslant 1)$ dans $\mathfrak{A}(G)$ par

$$\Psi_n f(x) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x^i) \quad ; \tag{11}$$

si $\xi$ est une coordonnée rigide dans $G$, normalisée par $\omega_0 = d\xi$ à l'origine, on a

$$\ell(x) = \sum_{n=1}^{\infty} (-1)^{n-1} \Psi_n \xi(x)/n. \tag{12}$$

Cette formule de Lazard permet le contrôle des dénominateurs dans $\ell$ ; lorsque $G = \mathbf{G}_m$, $\xi(x) = x - 1$ et $\omega_0 = dx/x$, on a $\Psi_n \xi = \xi^n$ et (12) redonne le développement en série classique du logarithme usuel.

Le lien avec les groupes formels est le suivant. Choisissons une coordonnée rigide $\xi$ sur $G$ ; il existe alors une série formelle $F \in o[[X, X']]$ caractérisée par $\xi(xx') = F(\xi(x) ; \xi(x'))$ pour $x, x'$ dans $G$ ("Théorème d'addition"). Cette série satisfait aux identités

$$F(X ; 0) = F(0 ; X) = X \quad , \quad F(X ; Y) = F(Y ; X) \quad , \tag{13}$$

$$F(F(X ; Y) ; Z) = F(X ; F(Y ; Z)) \quad ;$$

autrement dit, c'est une loi de groupe formel commutatif à coefficients dans $o$.

### 3. Classification des groupes $p$-adiques rigides.

Le théorème de classification repose sur deux notions essentielles : la hauteur et le module différentiel. Soit $G$ un groupe $p$-adique rigide de dimension 1. L'anneau $\mathfrak{A} = \mathfrak{A}(G)$ est local, et son idéal maximal $\mathfrak{m}$ se compose des fonctions analytiques rigides dont les valeurs sont divisibles par $p$ en tout point de $G$. La *hauteur* de $G$ est la borne supérieure (finie ou non) $ht(G)$ des entiers $h \geqslant 1$ tels que

$$\Psi_p(\mathfrak{A}) \subset p \cdot \mathfrak{A} + \mathfrak{m}^{p^h}.$$

On a $ht(\mathbf{G}_m) = 1$ et $ht(\mathbf{G}_a) = \infty$ ; la formule (12) montre facilement que tout groupe de hauteur infinie est isomorphe, comme groupe $p$-adique rigide, à $\mathbf{G}_a$.

Une *courbe* dans $G$ est un morphisme de variétés rigides $\gamma : D^1 \to G$, normalisé par $\gamma(0) = e$ (élément neutre de $G$). Les courbes forment un groupe commutatif $C(G)$ pour l'addition définie par $(\gamma + \gamma')(t) = \gamma(t) \cdot \gamma'(t)$. Pour tout nombre premier $\ell$, l'opérateur de décalage dans $C(G)$ est défini par $V_\ell \gamma(t) = \gamma(t^\ell)$, et l'opérateur de Frobenius par $F_\ell \gamma(t) = \prod_{i=1}^{\ell} \gamma(\zeta^i t^{1/\ell})$. Dans cette dernière formule, $\zeta$ est une racine $\ell$-ième de l'unité, distincte de 1, que l'on adjoint à $o$ ainsi que la racine $t^{1/\ell}$ de $t$, mais le résultat de la multiplication se trouve définit sur 0.

Notons maintenant $t$ la coordonnée naturelle sur $D^1$ et $\Omega$ le $\mathfrak{o}$-module des formes différentielles rigides sur $D^1$ ; nous représenterons toujours celles-ci sous la forme

$$(14) \qquad \omega = \sum_{n=1}^{\infty} a(n) \cdot t^{n-1} dt \qquad (a(n) \in \mathfrak{o} \text{ pour tout } n \geqslant 1) \quad ;$$

enfin, soit $d\mathfrak{A}_1$ l'ensemble des différentielles des fonctions $f \in \mathfrak{A}_1$. L'application $\gamma \mapsto \gamma^*(\omega_0)$ définit un isomorphisme $u$ du groupe $C(G)$ des courbes de $G$ sur un sous-groupe $\mathfrak{D}(G)$ de $\Omega$. On dit que $\mathfrak{D}(G)$ est le *module différentiel* de $G$ ; il caractérise $G$ à un isomorphisme rigide près. De plus, $u$ transforme $V_\ell$ et $F_\ell$ en les opérateurs suivants sur $\mathfrak{D}(G)$ :

$$(15) \qquad V_\ell \omega = \sum_{n=1}^{\infty} \ell \cdot a(n/\ell) \cdot t^{n-1} dt \quad , \quad F_\ell \omega = \sum_{n=1}^{\infty} a(n\ell) \cdot t^{n-1} dt$$

(pour $\omega$ de la forme (13)).

Soit $F$ la loi de groupe formel définie à la fin du n° 2, et soit $F_{(p)}$ la loi de groupe formel à coefficients dans le corps $\mathbf{F}_p = \mathfrak{o}/p.\mathfrak{o}$ déduite de $F$ par réduction modulo $p$. Sa hauteur au sens de Lazard et Dieudonné est égale à la hauteur $h$ de $G$ ; *nous la supposons désormais finie*(1). Le module de Dieudonné de $F_{(p)}$ est un $\mathfrak{o}$-module libre $\mathfrak{D}_p(G)$ de rang $h$ muni d'un opérateur linéaire $V$, donc un module sur l'anneau de polynômes $\mathfrak{o}[V]$. On démontre qu'il existe un unique polynôme d'Eisenstein $P = V^h + b_1 V^{h-1} + \cdots + b_{h-1} V + b_h$ dans $\mathfrak{o}[V]$ tel que $\mathfrak{D}_p(G)$ soit isomorphe au $\mathfrak{o}[V]$-module $\mathfrak{o}[V]/(P)$. De plus, la théorie résumée dans [2] permet d'identifier $\mathfrak{D}_p(G)$ au quotient de $\mathfrak{D}(G)$ par le sous-groupe formé des différentielles de la forme $p \cdot df + \Sigma_\ell V_\ell \omega_\ell$ avec $f \in \mathfrak{A}_1$ et $\omega_\ell \in \mathfrak{D}(G)$ pour tout nombre premier $\ell$, et $V$ provient de $V_p$ par passage au quotient.

Le polynôme d'Eisenstein $P$, ou ce qui revient au même, les coefficients $b_1, \ldots, b_h$ déterminent entièrement le module différentiel $\mathfrak{D}(G)$ qui se compose des formes différentielles $\omega$ telles que

$$(16) \qquad V_p^h \omega + b_1 \cdot V_p^{h-1} \omega + \cdots + b_{h-1} \cdot V_p \omega + b_h \cdot \omega \equiv 0 \mod p \cdot d\mathfrak{A}_1 .$$

De manière plus explicite, soient $a(1), a(2), \ldots, a(n), \ldots$ des éléments de $\mathfrak{o}$ ; posons

$$(17) \qquad t(n) = a(n) + \frac{p b_{h-1}}{b_h} \cdot a(n/p) + \cdots + \frac{p^{h-1} b_1}{b_h} \cdot a(n/p^{h-1}) + \frac{p^h}{b_h} \cdot a(n/p^h) .$$

*La forme différentielle* $\omega = \sum_{n=1}^{\infty} a(n) \cdot t^{n-1} dt$ *appartient à* $\mathfrak{D}(G)$ *si et seulement si l'on a les congruences* $t(n) \equiv 0 \mod p^\alpha$ *pour tout* $\alpha \geqslant 1$ *et tout entier* $n \equiv 0 \mod p^\alpha$. De plus, tout polynôme d'Eisenstein de degré $h$ provient d'un groupe $p$-adique rigide de dimension 1 et de hauteur $h$.

---

(1) Lorsque $G$ est de hauteur infinie, il est isomorphe (de manière rigide) à $\mathbf{G}_a$, et l'on a $\mathfrak{D}(G) = d\mathfrak{A}_1$.

En résumé, *on peut répartir les groupes p-adiques rigides de hauteur h en familles non vides* $\mathbf{F}(b_1, \ldots, b_h)$ (avec $b_1, \ldots, b_h$ dans $p.\mathfrak{o}$ et $b_h$ non divisible par $p^2$). *Supposons que G soit de type* $\mathbf{F}(b_1, \ldots, b_h)$ *et soient* $\xi$ *une coordonnée rigide dans* $G$, $\omega = \sum_{n=1}^{\infty} a(n) \cdot \xi^{n-1} d\xi$ *une forme différentielle rigide invariante par translations sur G. Alors les coefficients* $a(n) \in \mathfrak{o}$ *satisfont aux congruences* $t(np^\alpha) \equiv 0$ mod. $p^\alpha$ *pour* $\alpha \geqslant 1$ et $n \geqslant 1$, *en définissant* $t(n)$ *comme plus haut*(1).

## 4. Courbes elliptiques.

On note $\mathbf{Z}$ l'anneau des entiers rationnels, $\mathbf{Q}$ le corps des nombres rationnels et $\mathbf{F}_p$ le corps fini à $p$ éléments. Soit $H \in \mathbf{Z}[X, Y, Z]$ un polynôme non nul, homogène de degré 3, irréductible et de discriminant non nul. On suppose que la courbe elliptique d'équation homogène $H = 0$ a un point d'inflexion à coordonnées rationnelles. Quitte à faire un changement linéaire de variables à coefficients entiers, on peut ramener $H$ à la forme

$$(18) \quad H(X, Y, Z) = Y^2Z + (aX + bZ)YZ + (X^3 + uX^2Z + vXZ^2 + wZ^3)$$

et supposer que la réduction $H_{(p)}$ de $H$ modulo $p$ est irréductible dans $\mathbf{F}_p[X, Y, Z]$ pour tout nombre premier $p$. Soit $\Gamma$ le schéma projectif sur $\mathbf{Z}$ associé à l'algèbre graduée $\mathbf{Z}[X, Y, Z]/(H)$ ; on pose $C = \mathbf{Q} \otimes_{\mathbf{Z}} \Gamma$ et $C_{(p)} = F_p \otimes_{\mathbf{Z}} \Gamma$, de sorte que $C$ est la courbe elliptique sur $\mathbf{Q}$ d'équation $H = 0$, et que $C_{(p)}$ est la réduction modulo $p$ de $C$, d'équation $H_{(p)} = 0$. On dit que $\Gamma$ est le *modèle de Néron* de $C$ (cf. [4]). On considère $C$ (resp. $C_{(p)}$) comme un groupe algébrique sur $\mathbf{Q}$ (resp. $\mathbf{F}_p$), d'élément neutre le point à l'infini $e$ (resp. $e_p$).

Soit $p$ un nombre premier. Nous associons comme suit un groupe $p$-adique rigide $G_p$ à $\Gamma$ : les points de $G_p$ sont les points de $\Gamma$ dans $\mathbf{Z}_p$ qui se réduisent modulo $p$ en $e_p$, et les fonctions analytiques rigides sur $G_p$ sont les éléments du complété de l'anneau local du schéma $\Gamma$ au point $e_p \in \Gamma(\mathbf{F}_p)$. De manière plus concrète, $G_p$ se compose des points $g = (x, y, z)$ de $C$ dans $\mathbf{Q}_p$ tels que $x/py \in \mathbf{Z}_p$, et l'on définit une coordonnée rigide $\xi$ par $\xi(g) = x/y$. On note $\omega = \sum_{n=1}^{\infty} \beta(n) \cdot \xi^{n-1} d\xi$ la forme différentielle de première espèce sur $C$ normalisée par $\beta(1) = 1$ ; c'est une forme différentielle rigide invariante par translations sur $G_p$.

Supposons d'abord que $C_{(p)}$ soit une courbe elliptique sur $\mathbf{F}_p$, ce qui exclut un nombre fini de valeurs de $p$. Le nombre des points rationnels de $C_{(p)}$ est de la forme $1 - f_p + p$ avec $|f_p| < 2p^{1/2}$ (inégalité de Hasse-Weil). De plus, la réduction modulo $p$ de $\omega$ est une forme de première espèce sur $C_{(p)}$ et "l'opération de Cartier" la multiplie par $f_p$ ; comme cette opération transforme $h^{p^l-1}dh$ en $h^{p^{l-1}-1}dh$, on en déduit les

---

(1) En particulier, le groupe $p$-adique rigide $G$ est défini à isomorphisme près par sa réduction modulo $p$, qui est un groupe formel sur $\mathbf{F}_p = \mathfrak{o}/p.\mathfrak{o}$, et il n'y a donc pas de "modules". Cette situation est particulière au cas envisagé $\mathfrak{o} = \mathbf{Z}_p$ (cf. [2]).

congruences $\beta(np) \equiv f_p . \beta(n)$ et en particulier $\beta(p) \equiv f_p$ mod. $p$. Lorsque $H$ est de la forme $Y^2Z - (X^3 - aXZ^2 - bZ^3)$, on a $f_p = \sum_{t \bmod p} -\left(\frac{t^3-at-b}{p}\right)$ et l'on retrouve ainsi les congruences (6) et (7) du n° 1 (cette démonstration est due à Serre). Enfin, $f_p$ détermine la structure du groupe $p$-adique rigide $G_p$ comme suit(1) :

(a) si $f_p \neq 0$, le groupe $G_p$ est de hauteur 1, associé au polynôme d'Eisenstein $V - pu^{-1}$ où l'unité $p$-adique $u$ satisfait à $u^2 - f_p u + p = 0$ ;

(b) si $f_p = 0$, le groupe $G_p$ est de hauteur 2, associé au polynôme d'Eisenstein $V^2 + p$.

La congruence (9) du n° 1 se déduit immédiatement de là et des résultats du n° 3.

La *fonction zéta* de la courbe elliptique $C$ a été définie par A. Weil comme le produit eulérien $\zeta_C(s) = \prod_p \zeta_p(s)$ ; lorsque $C_{(p)}$ est une courbe elliptique, on a $\zeta_p(s) = (1 - f_p p^{-s} + p^{1-2s})^{-1}$, et l'on a une recette bien définie [7] lorsque $p$ est un nombre premier exceptionnel pour $C$. On peut aussi définir le *schéma formel* $\hat{\Gamma}$ *complété de* $\Gamma$ le long de la section neutre ; c'est un groupe formel sur $\mathbf{Z}$. Le choix du paramètre local $\xi$ permet de représenter $\hat{\Gamma}$ par une loi de groupe formel $F$ à coefficients dans $\mathbf{Z}$, telle que $\xi(xx') = F(\xi(x) ; \xi(x'))$ pour tout nombre premier $p$ et $x$, $x'$ dans $G_p$.

Un de nos résultats fondamentaux (démontré aussi partiellement par Honda [3]) est le suivant : *il existe un paramètre local bien déterminé $t$ dans $\Gamma$ au voisinage de la section neutre tel que la forme différentielle de première espèce $\omega$ s'écrive*

$$\omega = \sum_{n=1}^{\infty} b(n) . t^{n-1} dt$$

*et que la fonction zéta de $C$ s'écrive $\zeta_C(s) = \sum_{n=1}^{\infty} b(n) . n^{-s}$ avec les mêmes coefficients entiers $b(n)$. Le choix usuel des facteurs exceptionnels de $\zeta_C$ est le seul pour lequel ce résultat soit vrai, et l'on peut donc dire que la fonction zéta de $C$ ne dépend que du groupe formel associé à $C$.*

### 5. Relation avec les fonctions automorphes.

Les résultats précédents nous semblent jeter une lumière supplémentaire sur les conjectures de Weil [7], [8] (mais non sur leur démonstration !). Notons $\mathbf{C}$ l'ensemble des nombres complexes, $\mathbf{P}$ le demi-plan de Poincaré et, pour tout entier $N > 0$, soit $\Gamma_0(N)$ le groupe des transformations conformes de $\mathbf{P}$ de la forme $z \mapsto \frac{az+b}{cz+d}$ avec

---

(1) Lorsque $C_{(p)}$ n'est pas une courbe elliptique, elle est isomorphe comme groupe algébrique sur $\mathbf{F}_p$, soit à $\mathbf{G}_a$, soit à $\mathbf{G}_m$, soit à la forme non-déployée de $\mathbf{G}_m$ qui se déploye sur l'extension quadratique de $\mathbf{F}_p$.

$a$ , $b$ , $c$ , $d$ entiers, $ad - bc = 1$ et $c \equiv 0$ mod. $N$. Les coefficients entiers $b(n)$ étant définis comme précédemment, on note $\varphi$ la forme différentielle holomorphe $\sum_{n=1}^{\infty} b(n) . e^{2\pi i n\tau} d\tau$ sur **P**. Enfin, soit $N$ le *conducteur* de $C$ ; c'est un entier $> 0$ dont les diviseurs premiers sont les nombres premiers exceptionnels pour $C$. La conjecture de Weil est que *$\varphi$ est toujours invariante par $\Gamma_0(N)$*.

Soient $D$ le disque unité ouvert dans **C**, et $C_c$ le tore complexe de dimension 1 formé des points complexes de $C$. Le groupe commutatif $\Lambda$ formé des applications holomorphes $\gamma$ de $D$ dans $C_c$ telles que $\gamma(0) = e$ est l'analogue du groupe $C(G)$ défini au n° 3. On définit pour chaque nombre premier $p$ des opérateurs $V_p$ et $F_p$ par

$$V_p\gamma(q) = \gamma(q^p) \quad , \quad F_p\gamma(q^p) = \sum_{j=1}^{p} \gamma(\zeta^j q) \tag{19}$$

(avec $\zeta^p = 1$ , $\zeta \neq 1$) ; l'opérateur de Hecke associé à $p$ est $T_p = V_p + F_p$. Le paramètre local $t$ auquel il est fait allusion à la fin du n° 4 définit en fait une coordonnée locale holomorphe au voisinage de $e$ dans $C_c$ et il existe un élément $\delta$ de $\Lambda$ caractérisé par $t(\delta(q)) = q$ pour $q$ assez petit dans $D$.

Posons $H(\tau) = \delta(e^{2\pi i\tau})$ ; alors $H$ est une application holomorphe de **P** dans $C_c$, caractérisée par la propriété suivante : *l'image réciproque par $H$ de la forme de première espèce $\omega$ sur $C_c$ est la forme différentielle holomorphe $\varphi$ sur* **P**. Soit $p$ un nombre premier tel que $C_{(p)}$ soit une courbe elliptique ; on peut montrer qu'on a $T_p\delta = f_p\delta$, c'est-à-dire la relation

$$H(p\tau) + \sum_{j \bmod. p} H\Big(\frac{\tau + j}{p}\Big) = f_p . H(\tau) \quad (\tau \text{ dans } \mathbf{P}) \quad . \tag{20}$$

La conjecture de Weil signifie que $H$ se factorise en $\mathbf{P} \to \mathbf{P}/\Gamma_0(N) \xrightarrow{H'} C_c$. De plus, par adjonction à $\mathbf{P}/\Gamma_0(N)$ des points à l'infini correspondant aux "pointes", on obtient une courbe algébrique complète $S_N$ sur **C**. Or Shimura a construit dans [5] un modèle de $S_N$ sur le corps **Q** des nombres rationnels, et l'on peut raffiner sa méthode(1) de manière à obtenir un schéma $\Sigma_N$ sur **Z** tel que $S_N = \mathbf{C} \otimes_{\mathbf{Z}} \Sigma_N$. Nos résultats entraînent que, *si $C$ satisfait à la conjecture de Weil, $H'$ est un morphisme de schémas de $\Sigma_N$ dans $\Gamma$ au-dessus de Spec* (**Z**).

---

(1) Pour tout nombre premier $p$, l'anneau local de $\Sigma_N$ au point de $\Sigma_N$ générique au-dessus de $p$ se compose des fonctions méromorphes sur **P**, invariantes par $\Gamma_0(N)$ et qui se développent en série de Fourier $\sum_{n=-\infty}^{\infty} c_n . e^{2\pi i n\tau}$ avec des coefficients $p$-entiers $c_n$.

## BIBLIOGRAPHIE

[1] ATKIN A.O.L. — Congruences for modular forms, in *Computers in Mathematical Research*, North Holland Publ., 1968.

[2] CARTIER P. — Relèvement des groupes formels commutatifs, *Séminaire Bourbaki*, 21e année, 1968-69, exposé n° 359.

[3] HONDA T. — Formal groups and zeta functions, *Osaka J. Math.*, 5, 1968, p. 199-213.

[4] NÉRON A. — Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, *Publ. Math. I.H.E.S.*, 21, 1964, p. 1-128.

[5] SHIMURA G. — Correspondances modulaires et les fonctions $\zeta$ des courbes algébriques, *Journ. Math. Soc. Japan*, 10, 1958, p. 1-28.

[6] TATE J. — Rigid analytic spaces, à paraître dans *Inventiones Mathematicae*.

[7] WEIL A. — Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Annalen*, 168, 1967, p. 149-156.

[8] WEIL A. — Dirichlet series and automorphic functions, Lecture Notes in Math. *189*, Springer 1971.

Université Louis Pasteur
Dept. de Mathématiques
7, Rue René Descartes,
67 – Strasbourg – France