

# Formes modulaires modulo 2 : structure de l'algèbre de Hecke

Jean-Louis NICOLAS<sup>a</sup>, Jean-Pierre SERRE<sup>b</sup>

<sup>a</sup>CNRS, Université de Lyon, Institut Camille Jordan, Mathématiques, F-69622 Villeurbanne Cedex, France.

<sup>b</sup>Collège de France, 3 rue d'Ulm, F-75231 Paris Cedex 05, France.

## Abstract

### Modular forms mod 2 : structure of the Hecke ring

We show that the Hecke algebra for modular forms mod 2 of level 1 is isomorphic to the power series ring  $\mathbf{F}_2[[x, y]]$ , where  $x = T_3$  and  $y = T_5$ .

**Keywords:** modular forms, Hecke operators, Macaulay.

**Mathematics Subject Classification 2000:** 11F33, 11F25.

## 1. Notations

Nous conservons les notations de la Note précédente [2]. En particulier, nous notons  $\Delta$  l'élément de  $\mathbf{F}_2[[q]]$  défini par :

$$\Delta = \sum_{n=1}^{\infty} \tau(n)q^n = \sum_{m=1}^{\infty} q^{(2m+1)^2},$$

et  $\mathcal{F}$  désigne le sous-espace vectoriel de  $\mathbf{F}_2[[q]]$  engendré par les puissances impaires de  $\Delta$  :

$$\mathcal{F} = \langle \Delta, \Delta^3, \Delta^5, \dots \rangle.$$

L'espace  $\mathcal{F}$  est stable par les opérateurs de Hecke  $T_p$ ,  $p$  premier  $\neq 2$ .

## 2. Les espaces $\mathcal{F}(n)$ et les algèbres $A(n)$

Soit  $n$  un entier  $> 0$ . Soit  $\mathcal{F}(n)$  le sous-espace de  $\mathcal{F}$  de base  $\{\Delta, \Delta^3, \dots, \Delta^{2n-1}\}$ . On a  $\dim \mathcal{F}(n) = n$ . Soit  $A(n)$  la  $\mathbf{F}_2$ -sous-algèbre de  $\text{End}(\mathcal{F}(n))$  engendrée par  $\mathbf{F}_2$  et les  $T_p$ . On a  $A(n) = \mathbf{F}_2 \oplus \mathfrak{m}(n)$ , où  $\mathfrak{m}(n)$

*Email addresses:* jlnicola@in2p3.fr, <http://math.univ-lyon1.fr/~nicolas/> (Jean-Louis NICOLAS),  
jpserre691@gmail.com (Jean-Pierre SERRE).

est l'unique idéal maximal de  $A(n)$  (à savoir le sous-espace vectoriel de  $A(n)$  engendré par les  $T_p$  et leurs produits); cet idéal est nilpotent.

Soit  $\mathcal{F}(n)^*$  le dual de l'espace vectoriel  $\mathcal{F}(n)$ , muni de sa structure naturelle de  $A(n)$ -module, et soit  $e_n$  l'élément de  $\mathcal{F}(n)^*$  défini par :

$$\langle e_n, \Delta \rangle = 1 \quad \text{et} \quad \langle e_n, \Delta^{2i+1} \rangle = 0 \quad \text{si} \quad 1 \leq i < n.$$

Si  $f = \sum a_m(f)q^m$  est un élément de  $\mathcal{F}(n)$ , on a :

$$\langle e_n, f \rangle = a_1(f) \quad \text{et} \quad \langle T_p e_n, f \rangle = a_p(f) \quad \text{pour tout } p.$$

On en déduit par récurrence sur  $r$  la formule :

$$\langle T_{p_1} \dots T_{p_r} e_n, f \rangle = a_{p_1 \dots p_r}(f), \tag{1}$$

où les  $p_i$  sont des nombres premiers  $\neq 2$ .

**Lemme 2.1** - Soit  $f \in \mathcal{F}(n)$ ,  $f \neq 0$ . Il existe  $u \in A(n)$  tel que  $\langle e_n, uf \rangle = 1$ .

*Démonstration.* Ecrivons  $f$  sous la forme  $f = q^m + \sum_{i>m} a_i q^i$  et soit  $m = p_1 \dots p_r$  une décomposition de  $m$  en produit de nombres premiers. Comme  $m$  est impair, il en est de même des  $p_i$ . Soit  $u = T_{p_1} \dots T_{p_r}$ . La formule (1) montre que  $\langle ue_n, f \rangle = 1$ . Comme  $\langle ue_n, f \rangle = \langle e_n, uf \rangle$ , cela démontre le lemme.

### 3. Quelques propriétés de $\mathcal{F}(n)$ et de $A(n)$

**Proposition 3.1** - Le  $A(n)$ -module  $\mathcal{F}(n)^*$  est libre de base  $e_n$ .

*Démonstration.* Soit  $E$  le sous- $A(n)$ -module de  $\mathcal{F}(n)^*$  engendré par  $e_n$ . Si  $E$  était distinct de  $\mathcal{F}(n)^*$ , il existerait  $f \in \mathcal{F}(n)$ ,  $f \neq 0$ , tel que  $\langle ue_n, f \rangle = 0$  pour tout  $u \in A(n)$ , ce qui contredirait le lemme 1. On a donc  $E = \mathcal{F}(n)^*$ , ce qui montre que  $\mathcal{F}(n)^*$  est engendré par  $e_n$ . D'où la proposition.

*Remarque.* Si  $n > 2$ , le  $A(n)$ -module  $\mathcal{F}(n)$  n'est pas un module libre.

**Corollaire 3.2** - L'application  $A(n) \rightarrow \mathcal{F}(n)^*$  donnée par  $u \mapsto ue_n$  est bijective.

Ce n'est qu'une reformulation de la proposition. Noter que, par dualité, on obtient ainsi une bijection de  $\mathcal{F}(n)$  sur le dual  $A(n)^*$  de l'espace vectoriel  $A(n)$ .

**Corollaire 3.3** - On a  $\dim A(n) = n$ .

Cela résulte du Corollaire précédent et du fait que  $\dim \mathcal{F}(n) = n$ .

**Corollaire 3.4** - Le commutant de  $A(n)$  dans  $\text{End}(\mathcal{F}(n))$  est égal à  $A(n)$ .

Par dualité, cela revient à dire que le commutant de  $A(n)$  dans  $\text{End}(\mathcal{F}(n)^*)$  est égal à  $A(n)$ , ce qui résulte de la proposition.

**Proposition 3.5** - L'algèbre  $A(n)$  est engendrée par  $T_3$  et  $T_5$ .

*Démonstration.* Soit  $A'$  la sous-algèbre de  $A(n)$  engendrée par  $T_3$  et  $T_5$ . C'est une algèbre locale; soit  $\mathfrak{m}'$  son idéal maximal. Supposons que  $A' \neq A(n)$ , i.e.  $\dim A' < n$ . Le  $A'$ -module  $\mathcal{F}(n)^*$  n'est pas monogène: sinon, sa dimension serait  $< n$ . D'après le lemme de Nakayama, cela signifie que le quotient  $V = \mathcal{F}(n)^* / \mathfrak{m}' \mathcal{F}(n)^*$  est de dimension  $> 1$ . Par dualité, cela équivaut à dire que le sous-espace de  $\mathcal{F}(n)$  annulé par  $\mathfrak{m}'$  est de dimension  $> 1$ . Il existe donc  $f \in \mathcal{F}(n)$ , avec  $f \neq 0, \Delta$ , tel que  $T_3 f = T_5 f = 0$ , ce qui contredit le cor.5.3 au th.5.1 de [2].

#### 4. Passage à la limite : l'algèbre $A$

On a  $\mathcal{F}(n) \subset \mathcal{F}(n+1)$  et la restriction à  $\mathcal{F}(n)$  d'un élément de  $A(n+1)$  appartient à  $A(n)$ . On obtient ainsi un homomorphisme surjectif  $A(n+1) \rightarrow A(n)$ . D'où un système projectif

$$\dots \rightarrow A(n+1) \rightarrow A(n) \rightarrow \dots \rightarrow A(2) \rightarrow A(1) = \mathbf{F}_2.$$

Nous noterons  $A$  la limite projective de ce système. C'est un anneau local commutatif; il est compact pour la topologie limite projective. Son idéal maximal  $\mathfrak{m}$  est la limite projective des  $\mathfrak{m}(n)$ . L'anneau  $A$  opère de façon naturelle sur  $\mathcal{F}$ .

Soient  $x$  et  $y$  deux indéterminées. Pour chaque  $n$ , il existe un unique homomorphisme  $\psi_n : \mathbf{F}_2[x, y] \rightarrow A(n)$  tel que  $\psi_n(x) = T_3$  et  $\psi_n(y) = T_5$ . Par passage à la limite, on en déduit un homomorphisme

$$\psi : \mathbf{F}_2[[x, y]] \rightarrow A$$

tel que  $\psi(x) = T_3$  et  $\psi(y) = T_5$ .

**Théorème 4.1** - *L'homomorphisme  $\psi$  défini ci-dessus est un isomorphisme.*

*Démonstration.* La surjectivité de  $\psi$  résulte de la prop. 3.5. Pour prouver l'injectivité, il suffit de montrer que, pour tout élément  $u = \sum \lambda_{ij} x^i y^j$  non nul de  $\mathbf{F}_2[[x, y]]$ , il existe  $f \in \mathcal{F}$  tel que :

$$\sum \lambda_{ij} T_3^i T_5^j f = \Delta. \quad (2)$$

[Noter que la somme est une somme finie, car  $T_3^i T_5^j f = 0$  quand  $i + j$  est assez grand (par exemple  $i + j > \deg f$ ).]

Si  $\lambda_{00} = 1$  on prend  $f = \Delta$ . Supposons donc  $\lambda_{00} = 0$ . Soit  $\Sigma$  l'ensemble des couples  $(i, j)$  avec  $\lambda_{ij} = 1$ ; considérons ceux pour lesquels l'entier  $i + j$  est minimal, et parmi ceux-là, soit  $(a, b)$  le couple où  $a$  est maximum. Soit  $k$  l'entier impair de code  $[a, b]$ , au sens de [2, §4.1] et soit  $f = \Delta^k$ . On montre, en utilisant les Propositions 4.3 et 4.4 de [2, §4], que l'on a  $T_3^a T_5^b f = \Delta$  et  $T_3^i T_5^j f = 0$  pour tout  $(i, j) \in \Sigma$  distinct de  $(a, b)$ . D'où (2).

**Corollaire 4.2** - *L'algèbre  $A$  est un anneau local régulier de dimension 2. En particulier, c'est un anneau intègre.*

A partir de maintenant, nous identifierons les algèbres  $A$  et  $\mathbf{F}_2[[x, y]]$  au moyen de  $\psi$ ; cela nous permettra d'écrire  $x$  et  $y$  à la place de  $T_3$  et  $T_5$ .

#### 5. Structure des $A$ -modules $\mathcal{F}$ et $\mathcal{F}^*$

L'algèbre  $A$  opère sur  $\mathcal{F}$ . Par dualité, elle opère aussi sur le dual  $\mathcal{F}^*$  de  $\mathcal{F}$ , qui est la limite projective des  $\mathcal{F}(n)^*$ . Soit  $e \in \mathcal{F}^*$  la forme linéaire sur  $\mathcal{F}$  définie par :

$$\langle e, f \rangle = a_1(f) \text{ pour tout } f \in \mathcal{F}, \text{ où } a_1(f) \text{ désigne le coefficient de } q \text{ dans } f.$$

**Théorème 5.1** - *a) Le  $A$ -module  $\mathcal{F}^*$  est libre de base  $e$ .*

*b) Le  $A$ -module  $\mathcal{F}$  est isomorphe à l'espace  $A_{\text{cont}}^*$  des formes linéaires continues sur  $A$ .*

[Une forme linéaire sur  $A$  est continue si et seulement si elle s'annule sur une puissance de l'idéal maximal de  $A$ .]

*Démonstration.* L'assertion a) résulte de la prop.3.1 par dualité; il en est de même de b) car  $A_{\text{cont}}^* = \cup_{n \geq 1} A(n)^*$ .

**Corollaire 5.2** - *Le  $A$ -module  $\mathcal{F}$  est divisible: pour tout  $u \in A, u \neq 0$ , la multiplication par  $u$  est un endomorphisme surjectif de  $\mathcal{F}$ . En particulier, les endomorphismes  $T_p : \mathcal{F} \rightarrow \mathcal{F}$  sont surjectifs.*

*Démonstration.* Par dualité, cela revient à dire que  $u : \mathcal{F}^* \rightarrow \mathcal{F}^*$  est injectif, ce qui est clair puisque  $A$  est un anneau intègre.

*Remarque.* D'après [3],  $\mathcal{F}$  est un  $A$ -module *injectif*, à savoir l'enveloppe injective du corps résiduel  $\mathbf{F}_2$  de  $A$ . C'est là une propriété plus forte que la propriété de divisibilité.

## 6. Une base de $\mathcal{F}$ adaptée à $T_3$ et $T_5$

**Théorème 6.1** - *Il existe une base  $m(a, b)_{a, b \geq 0}$  de  $\mathcal{F}$  et une seule qui a les quatre propriétés suivantes :*

- i)  $m(0, 0) = \Delta$ .
- ii)  $\langle e, m(a, b) \rangle = 0$  si  $a + b > 0$ .
- iii)  $T_3 | m(a, b) = \begin{cases} m(a-1, b) & \text{si } a > 0 \\ 0 & \text{si } a = 0. \end{cases}$
- iv)  $T_5 | m(a, b) = \begin{cases} m(a, b-1) & \text{si } b > 0 \\ 0 & \text{si } b = 0. \end{cases}$

*Démonstration.* D'après le th.5.1, il suffit de prouver le même énoncé pour le  $A$ -module  $A_{\text{cont}}^*$ , et dans ce cas on définit  $m(a, b)$  comme la forme linéaire sur  $A$  donnée par :

$$\sum n_{ij} x^i y^j \mapsto n_{ab}.$$

Les propriétés i) à iv) sont évidentes. L'unicité se démontre par récurrence sur  $a + b$ .

*Exemples* (cf. [5]) :

$$\begin{aligned} m(0, 0) &= \Delta; \quad m(1, 0) = \Delta^3; \quad m(0, 1) = \Delta^5; \\ m(2, 0) &= \Delta^9; \quad m(1, 1) = \Delta^7; \quad m(0, 2) = \Delta^{17}; \\ m(3, 0) &= \Delta^{11}; \quad m(2, 1) = \Delta^{13}; \quad m(1, 2) = \Delta^{11} + \Delta^{19}; \quad m(0, 3) = \Delta^{13} + \Delta^{21}; \\ m(2^r, 0) &= \Delta^{1+2^{2r+1}}, \quad m(2^r - 1, 0) = \Delta^{(1+2^{2r+1})/3} \quad \text{et} \quad m(0, 2^r) = \Delta^{1+2^{2r+2}}. \end{aligned}$$

*Remarques.*

1) L'exposant dominant de  $m(a, b)$  au sens de [2, §4.3] est l'entier impair de code  $(a, b)$ ; cela se déduit des résultats énoncés dans [2, §4]. En particulier, l'ordre de nilpotence de  $m(a, b)$  est égal à  $a + b + 1$ .

2) D'après Macaulay ([1], voir aussi [3]) il est commode de noter les  $m(a, b)$  comme des monômes  $x^{-a}y^{-b}$ , avec la convention que  $x^{-a}y^{-b} = 0$  si  $a$  ou  $b$  est  $< 0$ . Les formules du th.6.1 s'écrivent alors simplement

$$x \cdot x^{-a}y^{-b} = x^{1-a}y^{-b} \quad \text{et} \quad y \cdot x^{-a}y^{-b} = x^{-a}y^{1-b}.$$

## 7. Développement des $T_p$ comme séries en $x = T_3$ et $y = T_5$

D'après le th.4.1, tout  $T_p$  peut s'écrire comme une série formelle en  $x = T_3$  et  $y = T_5$  :

$$T_p = \sum_{i+j \geq 1} a_{ij}(p) x^i y^j, \quad \text{avec} \quad a_{ij}(p) \in \mathbf{F}_2. \quad (3)$$

De façon plus précise, on a :

$$T_p \in \mathbf{F}_2[[x^2, y^2]] \quad \text{si } p \equiv 1 \pmod{8}, \quad (4)$$

$$T_p \in x \cdot \mathbf{F}_2[[x^2, y^2]] \quad \text{si } p \equiv 3 \pmod{8}, \quad (5)$$

$$T_p \in y \cdot \mathbf{F}_2[[x^2, y^2]] \quad \text{si } p \equiv 5 \pmod{8}, \quad (6)$$

$$T_p \in xy \cdot \mathbf{F}_2[[x^2, y^2]] \quad \text{si } p \equiv 7 \pmod{8}. \quad (7)$$

*Exemples* (cf. [5]) :

$$T_{17} = x^2 + y^2 + x^2y^2 + x^6 + x^4y^2 + y^6 + x^6y^2 + x^4y^4 + x^2y^6 + x^{10} + x^{10}y^2 + x^6y^6 + x^4y^8 + x^2y^{10} + \dots$$

$$T_{11} = x(1 + x^2 + y^2 + x^4 + x^2y^2 + y^4 + x^2y^4 + y^6 + x^6y^2 + x^8y^2 + x^6y^4 + x^2y^8 + y^{10} + x^{10}y^2 + \dots)$$

$$T_{13} = y(1 + x^2 + y^2 + x^4 + y^4 + x^6 + x^4y^2 + x^2y^4 + x^6y^2 + x^2y^6 + y^8 + x^{10} + x^8y^2 + x^6y^4 + y^{10} + \dots)$$

$$T_7 = xy(1 + x^2 + x^4 + x^2y^2 + y^6 + x^6y^2 + y^8 + x^{10} + x^8y^2 + x^6y^4 + x^{12} + x^4y^8 + x^2y^{10} + \dots)$$

Dans des cas simples, on peut donner explicitement la valeur du coefficient  $a_{ij}(p)$ . Par exemple :

$$a_{10}(p) = 1 \iff p \equiv 3 \pmod{8} \quad (8)$$

$$a_{01}(p) = 1 \iff p \equiv 5 \pmod{8} \quad (9)$$

$$a_{11}(p) = 1 \iff p \equiv 7 \pmod{16} \quad (10)$$

$$a_{20}(p) = 1 \iff p \text{ est de la forme } a^2 + 8b^2 \text{ avec } a, b \in \mathbf{Z}, b \text{ impair} \quad (11)$$

$$a_{02}(p) = 1 \iff p \text{ est de la forme } a^2 + 16b^2 \text{ avec } a, b \in \mathbf{Z}, b \text{ impair}. \quad (12)$$

Les formules (5) et (8) montrent que, si  $p \equiv 3 \pmod{8}$ , alors  $T_p$  est le produit de  $x$  par une série inversible en  $x^2$  et  $y^2$ ; en particulier,  $T_p$  et  $T_3$  ont le même noyau. Même chose si  $p \equiv 5 \pmod{8}$  avec  $x$  et  $T_3$  remplacé par  $y$  et  $T_5$ . On en déduit que l'algèbre  $A$  est topologiquement engendrée par n'importe quel couple  $(T_p, T_{p'})$  avec  $p \equiv 3 \pmod{8}$  et  $p' \equiv 5 \pmod{8}$ . Notons aussi que la proposition 4.3 (resp. 4.4) de [2] reste valable si l'on remplace  $T_3$  par  $T_p$  avec  $p \equiv 3 \pmod{8}$  (resp.  $T_5$  par  $T_{p'}$  avec  $p' \equiv 5 \pmod{8}$ ).

*Remarques.*

1) Pour  $i$  et  $j$  fixés, la fonction  $p \mapsto a_{ij}(p)$  est *frobénienne* au sens de [4, §3.3]. De façon plus précise, sa valeur ne dépend que de la substitution de Frobenius de  $p$  dans une certaine extension galoisienne finie de  $\mathbf{Q}$ , qui est non ramifiée en dehors de  $\{2\}$  et dont le groupe de Galois est un 2-groupe. Dans les deux premiers exemples ci-dessus, on peut prendre pour extension galoisienne le corps  $\mathbf{Q}(\mu_8)$  des racines huitièmes de l'unité; dans les trois autres, les corps  $\mathbf{Q}(\mu_8, \sqrt{uv})$ ,  $\mathbf{Q}(\mu_8, \sqrt{u})$  et  $\mathbf{Q}(\mu_8, \sqrt{v})$  avec  $u = 1 + i$  et  $v = \sqrt{2}$ ; le premier de ces corps est le corps  $\mathbf{Q}(\mu_{16})$  des racines 16-ièmes de l'unité; les deux autres ont des groupes de Galois sur  $\mathbf{Q}$  qui sont diédraux d'ordre 8.

2) Si  $p > 5$ , on peut se demander si la série donnant  $T_p$  peut être un polynôme en  $x$  et  $y$ . La réponse est "non" : d'après un résultat récent de J. Bellaïche, les  $T_p$  sont *algébriquement indépendants* sur  $\mathbf{F}_2$ .

## 8. Séries thêta associées à $\mathbf{Q}(\sqrt{-2})$

Soient  $n$  un entier  $\geq 1$  et soit  $t \in \mathbf{Z}/2^n\mathbf{Z}$ . Soit  $\theta_{t,n} \in \mathbf{F}_2[[q]]$  la série définie par :

$$\theta_{t,n} = \sum_{a \text{ impair} > 0} \sum_{b \equiv ta \pmod{2^n}} q^{a^2 + 2b^2}.$$

On a :

$$\theta_{0,n} = \Delta, \quad \theta_{t,n} = \theta_{-t,n}, \quad \theta_{2^{n-1},n} = 0, \quad \theta_{t,n} + \theta_{2^{n-1}-t,n} = \theta_{t,n-1}, \text{ et } \theta_{2^{n-2},n} = \Delta^{1+2^{2n-3}} \text{ si } n \geq 2.$$

Les séries  $\theta_{t,n}$  appartiennent à  $\mathcal{F}$ . De façon plus précise :

**Théorème 8.1** - Pour  $n > 0$  fixé, les  $\theta_{t,n}$  engendrent le même sous-espace vectoriel de  $\mathcal{F}$  que les formes  $m(a, 0)$  avec  $0 \leq a < 2^{n-1}$ .

[Pour la définition des  $m(a, b)$ , voir §6.]

**Corollaire 8.2** - Soit  $f = \sum a_n q^n$  un élément de  $\mathcal{F}$ . Les propriétés suivantes sont équivalentes :

- 1)  $T_5|f = 0$ .
- 2) La série  $f$  est de la forme  $\sum \theta_{t_i, n_i}$ .
- 3)  $a_n = 1 \Rightarrow n$  est de la forme  $a^2 + 2b^2$ , avec  $a, b \in \mathbf{Z}$ .

*Exemples* (la table des  $\theta_{t,n}$  pour  $n \leq 6$  et  $0 \leq t \leq 2^{n-1}$  est sur le site [5]) :

$$\begin{aligned} \theta_{0,1} &= \Delta; \\ \theta_{0,2} &= \Delta; \quad \theta_{1,2} = \Delta^3; \\ \theta_{0,3} &= \Delta; \quad \theta_{1,3} = \Delta^3 + \Delta^{11}; \quad \theta_{2,3} = \Delta^9; \quad \theta_{3,3} = \Delta^{11}. \end{aligned}$$

*Action des opérateurs de Hecke sur les  $\theta_{t,n}$ .*

Si  $p \equiv 5$  ou  $7 \pmod{8}$ , on a  $T_p|\theta_{t,n} = 0$ .

Si  $p \equiv 1$  ou  $3 \pmod{8}$ , on écrit  $p$  sous la forme  $p = a^2 + 2b^2$ , avec  $a, b \in \mathbf{Z}$ ; on définit  $t(p) \in \mathbf{Z}/2^n\mathbf{Z}$  par  $t(p) \equiv b/a \pmod{2^n}$ , et l'on pose  $t^*(p) = -t(p)$ . On a :

$$T_p|\theta_{t,n} = \theta_{t \bullet t(p), n} + \theta_{t \bullet t^*(p), n}$$

où l'on a noté  $x \bullet y$  la loi de composition<sup>1</sup> sur  $\mathbf{Z}/2^n\mathbf{Z}$  définie par la formule  $x \bullet y = (x + y)/(1 - 2xy)$ .

On a en particulier  $\theta_{2^{n-1}-t(p), n} = T_p|\Delta^{1+2^{2n-1}}$ .

## 9. Séries thêta associées à $\mathbf{Q}(i)$

Les définitions et les résultats sont essentiellement les mêmes que ceux du §8, à cela près que  $a^2 + 2b^2$ ,  $T_5$  et  $m(a, 0)$  sont remplacés par  $a^2 + 4b^2$ ,  $T_3$  et  $m(0, b)$ . De façon plus précise, si  $t$  et  $n$  sont comme ci-dessus, on définit la série thêta d'indice  $(t, n)$  par :

$$\theta'_{t,n} = \sum_{a \text{ impair} > 0} \sum_{b \equiv ta \pmod{2^n}} q^{a^2 + 4b^2}.$$

On a :

$$\theta'_{0,n} = \Delta, \quad \theta'_{t,n} = \theta'_{-t,n}, \quad \theta'_{2^{n-1}, n} = 0, \quad \theta'_{t,n} + \theta'_{2^{n-1}-t, n} = \theta'_{t, n-1}, \quad \text{et} \quad \theta'_{2^{n-2}, n} = \Delta^{1+2^{2n-2}} \quad \text{si } n \geq 2.$$

De plus :

**Théorème 9.1** - Pour  $n > 0$  fixé, les  $\theta'_{t,n}$  engendrent le même sous-espace vectoriel de  $\mathcal{F}$  que les formes  $m(0, b)$  avec  $0 \leq b < 2^{n-1}$ .

**Corollaire 9.2** - Soit  $f = \sum a_n q^n$  un élément de  $\mathcal{F}$ . Les propriétés suivantes sont équivalentes :

- 1)  $T_3|f = 0$ .
- 2) La série  $f$  est de la forme  $\sum \theta'_{t_i, n_i}$ .
- 3)  $a_n = 1 \Rightarrow n$  est de la forme  $a^2 + b^2$ , avec  $a, b \in \mathbf{Z}$ .

*Exemples* (la table des  $\theta'_{t,n}$  pour  $n \leq 6$  et  $0 \leq t \leq 2^{n-1}$  est sur le site [5]) :

$$\begin{aligned} \theta'_{0,1} &= \Delta; \\ \theta'_{0,2} &= \Delta; \quad \theta'_{1,2} = \Delta^5; \\ \theta'_{0,3} &= \Delta; \quad \theta'_{1,3} = \Delta^5 + \Delta^{13} + \Delta^{21}; \quad \theta'_{2,3} = \Delta^{17}; \quad \theta'_{3,3} = \Delta^{13} + \Delta^{21}. \end{aligned}$$

*Action des opérateurs de Hecke sur les  $\theta'_{t,n}$ .*

Si  $p \equiv 3$  ou  $7 \pmod{8}$ , on a  $T_p|\theta'_{t,n} = 0$ .

---

1. Cette loi munit  $\mathbf{Z}/2^n\mathbf{Z}$  d'une structure de groupe abélien; ce groupe est cyclique d'ordre  $2^n$ ; on peut l'interpréter comme le groupe des classes de formes quadratiques binaires primitives de discriminant  $-2^{2n+3}$ , ou encore comme le groupe Pic du sous-anneau de  $\mathbf{Z}[\sqrt{-2}]$  de conducteur  $2^n$ .

Si  $p \equiv 1$  ou  $5 \pmod{8}$ , on écrit  $p$  sous la forme  $p = a^2 + 4b^2$ , avec  $a, b \in \mathbf{Z}$ ; on pose  $t(p)' \equiv b/a \pmod{2^n}$  et  $t^*(p)' = -t_1(p)'$ . On a :

$$T_p | \theta'_{t,n} = \theta'_{t \bullet' t(p)',n} + \theta'_{t \bullet' t^*(p)',n}$$

où l'on a noté  $x \bullet' y$  la loi de composition sur  $\mathbf{Z}/2^n\mathbf{Z}$  définie par la formule  $x \bullet' y = (x + y)/(1 - 4xy)$ .

On a en particulier  $\theta'_{2^{n-1}-t(p)',n} = T_p | \Delta^{1+2^{2n}}$ .

## Références

- [1] F. S. MACAULAY. *Algebraic theory of modular systems*, Cambridge Tract **19**, Cambridge, 1916; seconde édition, avec une introduction par P. Roberts, Cambridge, 1994.
- [2] J-L. NICOLAS et J-P. SERRE. *Formes modulaires modulo 2 : l'ordre de nilpotence des opérateurs de Hecke*, C.R. Acad. Sci. Paris, Ser. I 350 (2012), <http://dx.doi.org/10.1016/j.crma.2012.03.013>
- [3] D. G. NORTHCOTT. *Injective envelopes and inverse polynomials*, J. London Math. Soc. (2), **8** (1974), 290-296.
- [4] J-P. SERRE. *Lectures on  $N_X(p)$* , AK Peters, CRC Press, Taylor & Francis, 2012.
- [5] <http://math.univ-lyon1.fr/~nicolas/polHecke.html>