ANNALES SCIENTIFIQUES DE L'É.N.S.

MICHEL BROUÉ
MICHEL ENGUEHARD

Polynômes des poids de certains codes et fonctions thêta de certains réseaux

Annales scientifiques de l'É.N.S. 4^e série, tome 5, n° 1 (1972), p. 157-181
<http://www.numdam.org/item?id=ASENS_1972_4_5_1_157_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 5, 1972, p. 157 à 181.

POLYNÔMES DES POIDS DE CERTAINS CODES ET FONCTIONS THÊTA DE CERTAINS RÉSEAUX

PAR MICHEL BROUÉ ET MICHEL ENGUEHARD

Deux théories apparemment fort éloignées, celle des polynômes des poids des codes sur le corps $\mathbf{F}_2$ et celle des fonctions thêta des réseaux sur $\mathbf{Z}$ se ressemblent trop pour être étrangères l'une à l'autre. La similitude la plus frappante est sans doute la suivante : les polynômes des poids de certains codes, codes totalement singuliers maximaux relativement à une forme quadratique convenable (1), engendrent l'algèbre graduée des polynômes à deux variables fixes par l'opération d'un sous-groupe fini H de GL (2, $\mathbf{C}$) [théorèmes 1 (ii) et 2 (ii)]; les fonctions thêta des réseaux unimodulaires pairs sont des formes modulaires qui engendrent une algèbre visiblement isomorphe à la précédente [théorèmes 4 et 5 (ii)].

Nous donnons ici la clé de la ressemblance en construisant des réseaux à partir de codes. Par exemple, l'isomorphisme entre les deux algèbres est défini canoniquement (théorème 8). Le passage des codes aux réseaux fait apparaître un homomorphisme d'un revêtement du groupe unimodulaire sur le groupe H déjà cité (2). L'étude des codes et des réseaux unimodulaires, mais non nécessairement pairs conduit à des résultats analogues (théorèmes 1, 2, 4 et 5).

La théorie des polynômes des poids de codes est présentée au paragraphe 1. Elle a été brièvement exposée par Gleason au Congrès international des Mathématiciens, à Nice, en 1970. La théorie des fonctions thêta est bien connue; elle est rappelée au paragraphe 2. Le lien est établi

(1) Codes que nous appelons unimodulaires pairs car ils permettent de construire des réseaux unimodulairs pairs, *cf.* la proposition 2. La terminologie employée ici est définie en 1.1 et 2.1.

(2) Cet homomorphisme nous a été signalé par M. J.-P. Serre, que nous tenons à remercier de ses conseils.

au paragraphe 3, consacré également à quelques applications. Un essai de généralisation pour d'autre corps que $\mathbf{F}_2$, avec ses applications, mais aussi ses limites, est exposé au paragraphe 4.

1. Codes sur $\mathbf{F}_2$ et polynômes des poids

Notations. — Si a est un ensemble, $|a|$ désigne son cardinal. Dans tout ce qui suit, Ω est un ensemble fini de cardinal n et n est supposé pair. Un corps fini de cardinal q est noté $\mathbf{F}_q$.

1.1. Codes dans $\mathfrak{P}(\Omega)$. — *a. Définitions.* — L'ensemble des parties de Ω muni de l'opération « différence symétrique » $(a + b = a \cup b - a \cap b)$ est un espace vectoriel sur $\mathbf{F}_2$, naturellement isomorphe à $\mathbf{F}_2^{\Omega}$. On munit cet espace de la forme bilinéaire définie comme suit :

$$(a, b) \mapsto \langle a, b \rangle = \begin{cases} 0 & \text{si } |a \cap b| \text{ est pair,} \\ 1 & \text{si } |a \cap b| \text{ est impair} \end{cases}$$

et appelée *produit scalaire naturel.* On note $\mathfrak{P}(\Omega)$ l'espace des parties de Ω muni de son produit scalaire naturel. La base $\{\{j\} : j \in \Omega\}$ est orthonormale.

Un Ω-code est un sous-espace vectoriel de $\mathfrak{P}(\Omega)$. Si $\mathcal{C}$ est un Ω-code, nous noterons $\mathcal{C}^0$ son orthogonal : $\mathcal{C}^0$ est l'ensemble des $a \subset \Omega$ dont l'intersection avec tout élément de $\mathcal{C}$ est de cardinal pair. Nous dirons qu'un Ω-code est *unimodulaire* s'il est égal à son orthogonal. Nous dirons qu'un Ω-code $\mathcal{C}$ est *pair* si tout élément de $\mathcal{C}$ a un cardinal divisible par 4.

Désignons par $\mathcal{H}(\Omega)$ l'hyperplan des parties de cardinal pair de Ω, et définissons sur $\mathcal{H}(\Omega)$ la fonction q suivante :

$$a \mapsto q(a) = \begin{cases} 0 & \text{si } |a| \equiv 0 \bmod 4, \\ 1 & \text{si } |a| \equiv 2 \bmod 4. \end{cases}$$

Alors q est une forme quadratique sur $\mathcal{H}(\Omega)$, car

$$\text{si } a, b \in \mathcal{H}(\Omega), \quad q(a + b) = q(a) + q(b) + \langle a, b \rangle.$$

Un code pair est un sous-espace de $\mathcal{H}(\Omega)$ totalement singulier pour la forme quadratique q; un tel code est contenu dans son orthogonal.

b. Polynôme des poids. — Soit $\mathcal{C}$ un Ω-code. Le polynôme des poids de $\mathcal{C}$ est

$$P_{\mathcal{C}}(X, Y) = \sum_{a \in \mathcal{C}} X^{|a|} Y^{n-|a|}.$$

c. Exemples. — Posons $n = 2m$ et $\Omega = \{ a_1, \ldots, a_m, b_1, \ldots, b_m \}$.

Désignons par $\mathfrak{A}_n$ le code engendré par les $\{ a_j, b_j \}$ $(1 \leq j \leq m)$. C'est un code unimodulaire dont le polynôme des poids est

$$A_n(X, Y) = (X^2 + Y^2)^{\frac{n}{2}}.$$

Supposons maintenant n multiple de 8. Désignons par $\mathfrak{B}_n$ le code engendré par les $\{ a_j, b_j, a_k, b_k \}$ $(j \neq k, 1 \leq j, k \leq m)$ et par $\{ a_1, \ldots, a_m \}$. C'est un code unimodulaire pair, dont le polynôme des poids est

$$B_n(X, Y) = \frac{1}{2}\left((X^2 + Y^2)^{\frac{n}{2}} + (X^2 - Y^2)^{\frac{n}{2}} + (2XY)^{\frac{n}{2}}\right).$$

Citons enfin un code en dimension 24, noté ici $\mathfrak{L}_{24}$, d'une certaine importance en théorie des groupes. C'est un code unimodulaire pair, engendré dans $\mathfrak{X}(\Omega)$ par les octades d'un système de Steiner de type (5, 8, 24) [*cf.* [11], [1]). Le polynôme des poids de $\mathfrak{L}_{24}$ est

$$Q_{24}(X, Y) = X^{24} + 759\, X^{16} Y^8 + 2\,576\, X^{12} Y^{12} + 759\, X^8 Y^{16} + Y^{24} \quad (cf.\ [4]).$$

Ce code est élément d'une famille infinie de codes $\mathfrak{L}_n$, unimodulaires pairs, les « codes quadratiques étendus », définis (*voir* [1]) pour $n = p + 1$, où p est un nombre premier congru à -1 modulo 8.

1.2. ALGÈBRES DE POLYNÔMES ASSOCIÉES. — *Notations.* — Le groupe linéaire GL (2, $\mathbf{C}$) opère à droite sur $\mathbf{C}[X, Y]$:

— si $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbf{C})$ et si $P(X, Y) \in \mathbf{C}[X, Y]$, nous posons

$$(P\,\alpha)(X, Y) = P(aX + bY, cX + dY).$$

a. Propriétés d'invariance des polynômes de certains codes. — Soit π_2 la matrice de symétrie

$$\pi_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

Il résulte des *formules de Mac-Williams* (*voir*, par exemple, [10], 6.1.2) que, pour tout code $\mathcal{C}$, de dimension k,

$$P_{\mathcal{C}^0} = 2^{\frac{n}{2}-k}(P_{\mathcal{C}}\,\pi_2). \tag{1}$$

Supposons que tous les éléments de $\mathcal{C}$ soient de cardinal pair. Alors $P_{\mathcal{C}}$ est fixe par l'opération de la matrice

$$\rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si, de plus, $\mathcal{C}$ est pair, $P_{\mathcal{C}}$ est fixe par l'opération de la matrice

$$\sigma = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}.$$

Désignons par G le groupe engendré par π_2 et ρ, et par H le groupe engendré par π_2 et σ; puisque $\rho = \sigma^2$, on a $G \subset H$. Si le code $\mathcal{C}$ est unimodulaire, sa dimension k est égale à $\frac{n}{2}$, et $P_{\mathcal{C}}$ est fixe par l'opération de π_2. D'où le

THÉORÈME 1. — *Soit $\mathcal{C}$ un code unimodulaire :*

(i) $P_{\mathcal{C}}$ *est fixe par les opérations de* G;

(ii) *si, de plus, $\mathcal{C}$ est pair, $P_{\mathcal{C}}$ est fixe par les opérations de* H.

b. Algèbres associées. — Soit $\mathcal{V}$ (resp. $\mathcal{W}$) l'algèbre des polynômes fixes par l'opération de G (resp. H) dans $\mathbf{C}[X, Y]$; on a $\mathcal{W} \subset \mathcal{V}$ car $G \subset H$. Posons

$$\mathcal{V}_{\mathbf{Z}} = \mathcal{V} \cap \mathbf{Z}[X, Y] \qquad \text{et} \qquad \mathcal{W}_{\mathbf{Z}} = \mathcal{W} \cap \mathbf{Z}[X, Y].$$

D'après le théorème 1, si $\mathcal{C}$ est un code unimodulaire, on a $P_{\mathcal{C}} \in \mathcal{V}_{\mathbf{Z}}$; si, de plus, $\mathcal{C}$ est pair, alors $P_{\mathcal{C}} \in \mathcal{W}_{\mathbf{Z}}$.

PROPOSITION 1. — (i) *L'élément $(\pi_2 \rho)^4$ est la matrice d'homothétie de rapport* -1, *et* G *est un groupe diédral d'ordre* 16, *engendré par des réflexions.*

(ii) *L'élément $(\pi_2 \sigma)^3$ est la matrice d'homothétie d'ordre* 8 *et de rapport* $\frac{i+1}{\sqrt{2}}$, *et* $\frac{H}{\langle (\pi_2 \sigma)^3 \rangle}$ *est un groupe fini d'ordre* 24 *isomorphe au groupe symétrique de degré* 4. *Ainsi* H *est un groupe fini d'ordre* $8.24 = 192$ *engendré par des pseudo-réflexions.*

(Si x est élément d'un groupe, le groupe cyclique engendré par x est noté $\langle x \rangle$.)

Démonstration de la proposition 1. — On a effectivement

$$(\pi_2 \rho)^4 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad (\pi_2 \sigma)^3 = \frac{i+1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(i) Comme G est engendré par les réflexions π_2 et ρ dont le produit est d'ordre 8, c'est un groupe diédral d'orde 16.

(ii) Le groupe symétrique de degré m, $\mathfrak{S}_m$, opérant sur l'ensemble $\{1, \ldots, m\}$, admet la présentation suivante relativement aux générateurs $A = (1, 2)$ et $B = (1, \ldots, m)$ (*cf.* [5], 6.22, p. 64).

$$B^m = (AB)^{m-1}, \qquad A^2 = (A, B^j)^2 = 1 \quad \left(\text{pour } 2 \leq j \leq \frac{m}{2}\right).$$

Alors $B^m = 1$. On en déduit la présentation suivante de $\mathfrak{S}_4$:

$$A^2 = B^4 = (AB)^3 = 1.$$

En effet, si ces relations sont vérifiées dans un groupe, on a

$$AB^2 = (AB)B = (B^{-1}A)^2 B = B^{-1}AB^{-1}AB$$

est conjugué de B^{-1}; alors $(A, B^2) = (AB^2)^2$ est conjugué de B^{-2} et la relation $(A, B^2)^2 = 1$ est vérifiée.

Le quotient $\frac{H}{\langle (\pi_2 \sigma)^3 \rangle}$ est engendré par les images de π_2 et de σ, d'ordres respectifs 2 et 4, le produit étant d'ordre 3. Donc $\frac{H}{\langle (\pi_2 \sigma)^3 \rangle}$ est isomorphe à une image de $\mathfrak{S}_4$ d'ordre au moins 12, nécessairement $\mathfrak{S}_4$ lui-même.

L'application σ fixe point par point une droite de $\mathbf{C}^2$, c'est donc une pseudo-réflexion (*cf.* [2], § 2, n° 1). Le groupe H est d'ordre $8.24 = 192$.

THÉORÈME 2. — (i) $\mathcal{V}$ *est une algèbre graduée de polynômes, engendrée par deux éléments algébriquement indépendants homogènes* A_2 *et* B_8 *de degrés respectifs* 2 *et* 8.

(ii) $\mathcal{W}$ *est une algèbre graduée de polynômes, engendrée par deux éléments algébriquement indépendants homogènes* B_8 *et* Q_{24}, *de degrés respectifs* 8 *et* 24.

Démonstration du théorème 2. — D'après ([2], chap. V, § 5), l'algèbre $\mathcal{V}$ (resp. $\mathcal{W}$) est une algèbre de polynômes homogènes engendrée par deux éléments algébriquement indépendants de degrés respectifs a_1 et a_2 (resp. b_1 et b_2) tels que $a_1 a_2 = |G| = 16$ (resp. $b_1 b_2 = |H| = 192$).

Puisque G contient la matrice scalaire $-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ [resp. H contient $\frac{i+1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$], le degré de tout polynôme de $\mathcal{V}$ (resp. $\mathcal{W}$) est multiple de 2 (resp. 8). Or il existe, d'après les exemples ci-dessus (1.1.*c*), un polynôme A_2 de degré 2 dans $\mathcal{V}$ (resp. B_8 de degré 8 dans $\mathcal{W}$). Donc nécessairement $a_1 = 2$ et $a_2 = \frac{16}{2} = 8$ $\left(\text{resp. } b_1 = 8 \text{ et } b_2 = \frac{192}{8} = 24\right)$. En outre, le polynôme B_8 de degré 8 appartient à $\mathcal{V}$ et est algébriquement indépendant de A_2 (resp. le polynôme Q_{24} de degré 24 appartient à $\mathcal{W}$ et est algébriquement indépendant de B_8).

Remarque. — Ce résultat montre en particulier qu'il ne peut exister un code unimodulaire pair dans $\mathcal{R}(\Omega)$ que si $n = |\Omega|$ est multiple de 8.

Pour étudier les algèbres $\mathcal{V}_{\mathbf{Z}}$ et $\mathfrak{W}_{\mathbf{Z}}$, nous utiliserons l'existence de certains polynômes de valuation nulle en Y; posant

$$C = \frac{1}{4}(A_2^4 - B_8) \qquad \text{et} \qquad D = \frac{1}{42}(B_8^3 - Q_{24}),$$

on a

$$C(X, Y) = X^2 Y^2 (X^2 - Y^2)^2 \qquad \text{et} \qquad C \in \mathcal{V}_{\mathbf{Z}},$$
$$D(X, Y) = X^4 Y^4 (X^4 - Y^4)^4 \qquad \text{et} \qquad D \in \mathfrak{W}_{\mathbf{Z}}.$$

THÉORÈME 3.

(i) $\mathcal{V}_{\mathbf{Z}} = \mathbf{Z}[A_2, C]$;

(ii) $\mathfrak{W}_{\mathbf{Z}} = \mathbf{Z}[B_8, D]$.

Démonstration du théorème 3. — D'après le théorème 2,

$$\mathcal{V} = \mathbf{C}[A_2, B_8] \qquad \text{et} \qquad \mathfrak{W} = \mathbf{C}[B_8, Q_{24}].$$

Or $B_8 = A_2^4 - 4C$ et $Q_{24} = B_8^3 - 42D$. Donc on a aussi

$$\mathcal{V} = \mathbf{C}[A_2, C] \qquad \text{et} \qquad \mathfrak{W} = \mathbf{C}[B_8, D].$$

Il suffit donc, pour démontrer le théorème 3, de vérifier que

$$\mathbf{C}[A_2, C] \cap \mathbf{Z}[X, Y] = \mathbf{Z}[A_2, C]$$

et

$$\mathbf{C}[B_8, D] \cap \mathbf{Z}[X, Y] = \mathbf{Z}[B_8, D].$$

Les polynômes A_2 et C, B_8 et D sont à coefficients entiers rationnels. On a donc les inclusions

$$\mathbf{C}[A_2, C] \cap \mathbf{Z}[X, Y] \supset \mathbf{Z}[A_2, C]$$

et

$$\mathbf{C}[B_8, D] \cap \mathbf{Z}[X, Y] \supset \mathbf{Z}[B_8, D].$$

Les inclusions dans l'autre sens se déduisent du fait que les termes de plus bas degré en Y de A_2 et C — tout comme ceux de B_8 et D — ont des coefficients 1, mais des degrés en Y différents :

Supposons que, pour un certain entier d, il existe un polynôme $R(A_2, C)$, homogène de degré d en (X, Y), appartenant à

$$\mathcal{V}_{\mathbf{Z}} = \mathbf{C}[A_2, C] \cap \mathbf{Z}[X, Y]$$

et non à $\mathbf{Z}[A_2, C]$, et choisissons-le avec la plus grande valuation possible en Y. Le terme le plus bas degré en Y de $R(A_2(X, Y), C(X, Y))$ provient uniquement du terme de plus bas degré en C de $R(A_2, C)$, soit $a A_2^k C^{k'}$ $(k, k' \in \mathbf{N})$. Son coefficient est a, donc $a \in \mathbf{Z}$. Alors

$$(R(A_2, C) - a A_2^k C^{k'}) \in \mathcal{V}_{\mathbf{Z}}$$

et est de valuation en Y supérieure à celle de $R(A_2, C)$. Le choix de R implique donc

$$(R - a A_2^k C^{k'}) \in \mathbf{Z}[A_2, C], \qquad \text{soit} \quad R \in \mathbf{Z}[A_2, C]$$

et l'hypothèse sur R est contredite, ce qui est absurde.

Tous les polynômes homogènes de $\mathcal{V}_{\mathbf{Z}}$ appartiennent donc à $\mathbf{Z}[A_2, C]$. Par conséquent, $\mathcal{V}_{\mathbf{Z}} \subset \mathbf{Z}[A_2, C]$. De même, $\mathcal{W}_{\mathbf{Z}} \subset \mathbf{Z}[B_8, D]$.

2. Réseaux de $\mathbf{Q}^n$ et fonctions thêta

La lettre n désigne toujours un entier naturel pair. L'espace $\mathbf{Q}^n$ est supposé muni de son produit scalaire naturel, noté

$$(x, y) \mapsto xy.$$

2.1. Réseaux dans $\mathbf{Q}^n$. — *a. Définitions.* — Un réseau de $\mathbf{Q}^n$ est un sous-$\mathbf{Z}$-module libre de rang n de $\mathbf{Q}^n$. Si L est un réseau de $\mathbf{Q}^n$, nous désignons par L^0 son *réseau dual*, c'est-à-dire l'ensemble des vecteurs de $\mathbf{Q}^n$ qui ont un produit scalaire entier avec tous les vecteurs de L. Nous dirons qu'un réseau L est *unimodulaire* s'il est égal à son dual. Nous dirons qu'un réseau L de $\mathbf{Q}^n$ est *pair* si tout vecteur de L a un carré scalaire entier et pair. Un réseau pair est contenu dans son dual. Enfin le *volume* d'un réseau L, noté vol (L), est la valeur absolue du déterminant d'une base de L par rapport à une base orthonormale de $\mathbf{Q}^n$. Un réseau unimodulaire est de volume 1.

b. Fonctions thêta. — Soit L un réseau de $\mathbf{Q}^n$. La *fonction thêta de* L est une fonction holomorphe, noté Θ_L, définie sur le demi-plan supérieur $\mathfrak{H}$ et telle que

$$\Theta_L(z) = \sum_{x \in L} e^{\pi i z(xx)} \qquad \text{si} \quad z \in \mathfrak{H}.$$

c. Exemples. — Le réseau $\mathbf{Z}^n \subset \mathbf{Q}^n$ est unimodulaire et sa fonction thêta est

$$\Theta_{\mathbf{Z}^n}(z) = \left(\sum_{m=-\infty}^{+\infty} e^{\pi i m^2 z} \right)^n.$$

Pour n multiple de 8, nous noterons $\Lambda(n)$ le réseau unimodulaire pair défini et noté $\Gamma(n)$ au chapitre V, § 1 de [8], et E_4 la fonction $\Theta_{\Lambda(8)}$ [3]. La fonction thêta du réseau $\Lambda(n)$ sera donnée plus loin.

---

[3] C'est la fonction notée E_2 dans ([8], p. 150) identifiée à $\Theta_{\Lambda(8)}$ au chapitre VII, n° 6.6 du même ouvrage.

2.2. Algèbres de fonctions associées. — *a. Propriétés d'invariance des fonction thêta de certains réseaux.* — Soit L un réseau de $\mathbf{Q}^n$. Il résulte de la formule de Poisson (*voir* [8], chap. VII, § 6) que

$$\Theta_{L^\circ}(z) = \left(\frac{z}{i}\right)^{-\frac{n}{2}} \mathrm{vol}(L)\, \Theta_L\left(-\frac{1}{z}\right). \tag{2}$$

Si tous les carrés scalaires des vecteurs de L sont entiers, Θ_L est invariante par la transformation $z \mapsto z + 2$. Si, de plus, L est pair, Θ_L est invariante par la transformation $z \mapsto z + 1$. Par conséquent,

Théorème 4. — (i) *Soit* U *un réseau unimodulaire de* $\mathbf{Q}^n$. *Alors*

$$\Theta_U\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{n}{2}} \Theta_U(z) \qquad \text{et} \qquad \Theta_U(z+2) = \Theta_U(z).$$

(ii) *Si, de plus,* U *est pair,*

$$\Theta_U(z+1) = \Theta_U(z).$$

b. Algèbres associées. — Soit $\mathfrak{N}_n$ l'espace vectoriel des fonctions θ, définies et holomorphes sur $\mathfrak{P}$, et telles que

1° pour tout $z \in \mathfrak{P}$,

$$\theta\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{n}{2}} \theta(z) \quad \text{et} \quad \theta(z+2) = \theta(z);$$

2° θ est « holomorphe aux pointes », c'est-à-dire qu'il existe $a_m \in \mathbf{C}$ $(m \geqq 0)$ et un réel $c > 0$, tels que

$$\theta(z) = \sum_{m \geqq 0} a_m e^{\pi i m z} \qquad \text{et} \qquad a_m = 0(m^c).$$

Le sous-espace de $\mathfrak{N}_n$ des fonctions qui satisfont en outre à l'identité

$$\theta(z+1) = \theta(z)$$

sera noté $\mathfrak{M}_n$ (4).

Posons $\mathfrak{N} = \bigoplus_{n \geqq 2} \mathfrak{N}_n$ et $\mathfrak{M} = \bigoplus_{n \geqq 2} \mathfrak{M}_n$: les fonctions de $\mathfrak{N}_n$ et de $\mathfrak{M}_n$ sont dites de « degré n ». Ce degré est le double du « poids » usuel. Soit $\mathfrak{N}_{\mathbf{Z}}$ (resp. $\mathfrak{M}_{\mathbf{Z}}$) l'ensemble des fonctions de $\mathfrak{N}$ (resp. de $\mathfrak{M}$) telles que, avec les notations employées ci-dessus, $a_m \in \mathbf{Z}$ pour tout m.

---

(4) Les espaces $\mathfrak{N}_n$ et $\mathfrak{M}_n$ sont étudiés entre autres dans [7] et y sont notés respectivement $\mathfrak{M}_0\left(2, \frac{n}{2}, 1\right)$ et $\mathfrak{M}_0\left(1, \frac{n}{2}, 1\right)$ (*cf.* [7], p. XIV et Chap. I).

Si U est un réseau unimodulaire, le théorème 4 exprime que Θ_U est un élément de degré n de $\mathfrak{N}$, donc de $\mathfrak{N}_{\mathbf{Z}}$. Si, de plus, U est pair, on a $\Theta_U \in \mathfrak{M}_{\mathbf{Z}}$.

THÉORÈME 5. — (i) *$\mathfrak{N}$ est une algèbre graduée, engendrée par deux éléments algébriquement indépendants de degrés respectifs* 2 *et* 8.

(ii) *$\mathfrak{M}$ est une algèbre graduée, engendrée par deux éléments algébriquement indépendants de degrés respectifs* 8 *et* 24.

Démonstration du théorème 5. — Il résulte des définitions de $\mathfrak{N}_n$ et de $\mathfrak{M}_n$ que si $\theta_1 \in \mathfrak{N}_{n_1}$ et $\theta_2 \in \mathfrak{N}_{n_2}$ (resp. $\theta_1 \in \mathfrak{M}_{n_1}$ et $\theta_2 \in \mathfrak{M}_{n_2}$), $\theta_1\,\theta_2 \in \mathfrak{N}_{n_1+n_2}$ (resp. $\theta_1\,\theta_2 \in \mathfrak{M}_{n_1+n_2}$).

(i) Les dimensions des espaces $\mathfrak{N}_n$ sont calculées dans [7] précisément grâce à l'existence d'une telle génération de $\mathfrak{N}$.

On a ([7], théor. 4), pour tout n pair,

$$\dim \mathfrak{N}_n = 1 + \left[\frac{n}{8}\right] \quad (5)$$

et les générateurs utilisés sont (p. I.41)

$$\Theta_{\mathbf{Z}^2} = (\Theta_{\mathbf{Z}})^2 = \left(\sum_{m \in \mathbf{Z}} e^{\pi i m^2 z}\right)^2 \quad (cf.\ 2.1.c)$$

et

$$\Theta_{\Lambda(8)} = E_4 = 1 + 240 \sum_{m \geq 1} \frac{m^3\, e^{2\pi i m z}}{1 - e^{2\pi i m z}}.$$

Remarquons que si θ appartient à $\mathfrak{N}_2$ et ζ à $\mathfrak{N}_8$, et si ζ et θ^4 ne sont pas proportionnelles, $\mathfrak{N}$ est engendrée par θ et ζ. En effet, $\theta^{\frac{n}{2}-4j}\zeta^j$ appartient à $\mathfrak{N}_n$ quel que soit l'entier j entre 0 et $\left[\frac{n}{8}\right]$. Si la fonction méromorphe $\frac{\zeta}{\theta^4}$ n'est pas constante, elle ne vérifie aucune équation algébrique. Les fonctions $\theta^{\left(\frac{n}{2}\right)-4j}\zeta^j$ sont donc linéairement indépendantes et engendrent $\mathfrak{N}_n$, ceci quel que soit n pair. Ainsi $\mathfrak{N}$ s'identifie à l'algèbre des polynômes en θ et ζ.

(ii) De même, l'espace $\mathfrak{M}_n$ est de dimension non nulle si et seulement si n est multiple de 8 ([7], théor. 3), auquel cas ([4], théor. 3′ : $\dim \mathfrak{M}_n = \partial(1) + \left[\frac{n}{24}\right]$ et p. I.27, $\partial(1) = 1$) :

$$\dim \mathfrak{M}_n = 1 + \left[\frac{n}{24}\right].$$

(5) $[m]$ désigne la partie entière de m.

On en conclut comme dans le premier cas que si $\theta \in \mathfrak{M}_8$, $\zeta \in \mathfrak{M}_{24}$ et si θ^3 et ζ engendrent $\mathfrak{M}_{24}$, $\mathfrak{M}$ est isomorphe à l'algèbre des polynômes en θ et ζ.

Remarque. — Des théorèmes 4 et 5 on déduit qu'il ne peut exister de réseau unimodulaire pair dans $\mathbf{Q}^n$ que si n est multiple de 8.

Pour déterminer $\mathfrak{N}_{\mathbf{Z}}$ et $\mathfrak{M}_{\mathbf{Z}}$, nous utiliserons les éléments qui « prennent la valeur 0 à la pointe $i\infty$ », c'est-à-dire dont le développement en série en $e^{\pi i z}$ n'a pas de terme constant, et de degré minimum.

(i) Les valeurs pour $i\infty$ de $\Theta_{\mathbf{Z}}$ et de E_4 sont égales à 1. Donc $\Theta_{\mathbf{Z}}^8 - E_4$, qui appartient à $\mathfrak{N}_8$, est de valeur nulle en $i\infty$. En outre, les coefficients du développement en $e^{\pi i z}$ de $\zeta = \dfrac{\Theta_{\mathbf{Z}} - 1}{2}$ sont entiers. Il en résulte que ceux de $\dfrac{(\Theta_{\mathbf{Z}})^8 - 1}{16}$ le sont aussi :

$$(\Theta_{\mathbf{Z}})^8 - 1 = \sum_1^8 2^k \binom{8}{k} \zeta^k = 16\,(e^{\pi i z} + \ldots).$$

Comme $\dfrac{E_4 - 1}{16}$ est aussi à coefficients entiers, nous poserons

$$\Delta_4 = \frac{(\Theta_{\mathbf{Z}})^8 - E_4}{16}.$$

On a donc

$$\Delta_4 \in \mathfrak{N}_{\mathbf{Z}}.$$

Nous verrons (*cf.* 3.3) que

$$\Delta_4(z) = e^{\pi i z} \prod_{m \geq 1} ((1 - e^{\pi i m z})\,(1 + e^{2\pi i m z}))^8$$

$$= e^{\pi i z} \prod_{m \geq 1} ((1 - e^{4\pi i m z})\,(1 - e^{\pi i (2m-1) z}))^8.$$

Comme $(\Theta_{\mathbf{Z}})^8$ et Δ_4 engendrent $\mathfrak{N}_8$, $\mathfrak{M} = \mathbf{C}[(\Theta_{\mathbf{Z}})^2, \Delta_4]$.

(ii) on sait ([7], démonstration du théorème 4, car $\mathfrak{M}_0\left(1, \frac{n}{2}, 1\right)$ est égal à $\mathfrak{M}\left(1, \frac{n}{2}, 1\right)$ — ou bien [8], chap. VII, § 2) que $\mathfrak{M}_{\mathbf{Z}}$ contient une forme parabolique remarquable de degré 24, Δ_{12}, qui s'écrit également sous forme de produit infini :

$$\Delta_{12}(z) = e^{2\pi i z} \prod_{m \geq 1} (1 - e^{2\pi i m z})^{24}.$$

Là encore, $\mathfrak{M} = \mathbf{C}[E_4, \Delta_{12}]$.

Notons enfin que

$$\Delta_4(z) = \Delta_{12}(z)^{-\frac{1}{3}} \Delta_{12}(2z)^{\frac{1}{3}} \Delta_{12}\left(\frac{z}{2}\right)^{\frac{1}{3}}.$$

THÉORÈME 6.

(i) $\mathcal{M}_{\mathbf{Z}} = \mathbf{Z}[(\Theta_{\mathbf{Z}})^8, \Delta_4]$;

(ii) $\mathcal{M}_{\mathbf{Z}} = \mathbf{Z}[E_4, \Delta_{12}]$.

La démonstration de ce théorème est en tout point semblable à celle du théorème 3; le rôle joué par la valuation en Y des polynômes des poids l'est ici par la valuation en $e^{\pi i z}$ des développements à la pointe $i\infty$ des fonctions considérées.

3. Codes et réseaux, polynômes et fonctions thêta

Ω désigne toujours un ensemble fini de cardinal pair, n.

3.1. CODES ET RÉSEAUX. — A tout Ω-code $\mathcal{C}$, nous associons un réseau $U(\mathcal{C})$ de $\mathbf{Q}^n$, de la manière suivante :

Soit $\{v_j\}_{j\in\Omega}$ une base orthogonale de $\mathbf{Q}^n$ telle que, pour tout $j \in \Omega$, $v_j^2 = \frac{1}{2}$. Le réseau $U(\mathcal{C})$ est l'ensemble des $x = \sum_{j\in\Omega} x_j v_j$ tels que :

1° les x_j soient entiers;

2° $\{j \mid x_j \equiv 1 \bmod 2\} \in \mathcal{C}$.

PROPOSITION 2. — 1° *Si $\mathcal{C}$ est de dimension k,*

$$\mathrm{vol}(U(\mathcal{C})) = 2^{\frac{n}{2}-k};$$

2° $U(\mathcal{C})^0 = U(\mathcal{C}^0)$;

3° *Pour que les carrés scalaires des vecteurs de $U(\mathcal{C})$ soient entiers, il faut et il suffit que $\mathcal{C} \subset \mathcal{H}(\Omega)$. Pour que $U(\mathcal{C})$ soit pair, il faut et il suffit que $\mathcal{C}$ soit pair.*

C'est évident.

Exemples :

Si n est pair, $U(\mathcal{A}_n)$ est isomorphe à $\mathbf{Z}^n$.

Si n est divisible par 8, $U(\mathcal{B}_n)$ est isomorphe à $\Lambda(n)$.

3.2. POLYNÔMES ET FONCTIONS THÊTA. — La fonction $\Theta_{U(\mathcal{C})}$ se calcule à l'aide des fonctions thêta de Jacobi. Nous utiliserons les notations

classiques de [9] :

$$\theta_2(v \mid z) = \sum_{m=-\infty}^{+\infty} \exp\left(\pi i\left(m+\frac{1}{2}\right)^2 z + \pi i\,(2m+1)\,v\right),$$

$$\theta_3(v \mid z) = \sum_{m=-\infty}^{+\infty} \exp(\pi i m^2 z + 2\pi i m v),$$

$$\theta_4(v \mid z) = \sum_{m=-\infty}^{+\infty} (-1)^m \exp(\pi i m^2 z + 2\pi i m v) \qquad (v \in \mathbf{C} \text{ et } z \in \mathfrak{P})$$

ainsi que les suivantes :

$$\theta_j(z) = \theta_j(0 \mid z) \qquad \text{pour } j = 2,\ 3 \text{ et } 4$$

et

$$\varphi_j(z) = \theta_j(2z) \qquad \text{pour } j = 2,\ 3 \text{ et } 4.$$

THÉORÈME 7. — *Soit $\mathcal{C}$ un Ω-code. On a*

$$\Theta_{U(\mathcal{C})} = P_{\mathcal{C}}(\varphi_2, \varphi_3).$$

Démonstration du théorème 7. — Conservons les notations introduites en 3.1 pour définir $U(\mathcal{C})$. Soit λ l'application de $U(\mathcal{C})$ dans $\mathcal{C}$, qui à x appartenant à $U(\mathcal{C})$ associe

$$a = \{j \mid x_j \equiv 1 \pmod 2\}.$$

Si $\lambda(x) = a$, il existe $k_j \in \mathbf{Z}$ $(j \in \Omega)$ tels que

$$x = \sum_{\in \Omega} 2k_j v_j + \sum_{j \in a} v_j$$

et x parcourt $\lambda^{-1}(a)$ quand (k_j) parcourt $\mathbf{Z}^\Omega$. On a

$$x^2 = \sum_{j \in a} 2\left(k_j + \frac{1}{2}\right)^2 + \sum_{j \notin a} 2k_j^2.$$

D'où

$$\sum_{\lambda(x)=a} e^{\pi i z (xx)} = \sum_{(k_j) \in \mathbf{Z}^\Omega} \left(\prod_{j \in a} e^{2\pi i z \left(k_j + \frac{1}{2}\right)^2}\right)\left(\prod_{j \notin a} e^{2\pi i z k_j^2}\right)$$

$$= \left(\prod_{j \in a}\left(\sum_{k_j \in \mathbf{Z}} e^{2\pi i z \left(k_j + \frac{1}{2}\right)^2}\right)\right)\left(\prod_{j \notin a}\left(\sum_{k_j \in \mathbf{Z}} e^{2\pi i z k_j^2}\right)\right)$$

$$= \varphi_2(z)^{|a|}\,\varphi_3(z)^{n-|a|}.$$

On a donc

$$\Theta_{U(\mathcal{C})}(z) = \sum_{a \in \mathcal{C}} \left(\sum_{\lambda(x)=a} e^{\pi i z(xx)} \right)$$
$$= \sum_{a \in \mathcal{C}} \varphi_2(z)^{|a|} \varphi_3(z)^{n-|a|}$$
$$= P_{\mathcal{C}}(\varphi_2(z), \varphi_3(z)).$$

Exemples :

a. La fonction Θ du réseau $\mathbf{Z}^n$ est θ_3^n. Si n est pair, $\mathbf{Z}^n$ est isomorphe à $U(\mathcal{A}_n)$, dont la fonction Θ, d'après le théorème précédent, est $A_n(\varphi_2, \varphi_3) = (\varphi_2^2 + \varphi_3^2)^{\frac{n}{2}}$. On retrouve ici l'une des relations quadratiques classiques entre les fonctions de Jacobi ([9], form. XLVIII (3)) :

$$\theta_3(z)^2 = \theta_2(2z)^2 + \theta_4(2z)^2.$$

b. De même, la fonction Θ du réseau $\Lambda(n) = U(\mathcal{B}_n)$ est $B_n(\varphi_2, \varphi_3)$. Outre la relation précédente, on a

$$\theta_2(z)^2 = 2\,\theta_2(2z)\,\theta_3(2z),$$
$$\theta_4(z)^2 = \theta_3^2(2z) - \theta_2^2(2z).$$

Donc

$$\Theta_{\Lambda(n)} = \frac{1}{2}(\theta_2^n + \theta_3^n + \theta_4^n)$$

(pour $n = 8$, c'est XXXVI (8) de [9]).

3.3. Isomorphisme entre les algèbres associées.

Théorème 8. — *L'application qui, à un polynôme* $P(X, Y) \in \mathbf{C}[X, Y]$ *associe la fonction* $P(\varphi_2, \varphi_3)$, *définit des isomorphismes d'algèbres entre* $\mathcal{V}$ (*resp.* $\mathfrak{W}$) *et* $\mathfrak{A}$ (*resp.* $\mathfrak{M}$).

Démonstration. — Nous savons que $\mathcal{V} = \mathbf{C}[A_2, B_8]$ (§ 1, théor. 2) et que $\mathfrak{A} = \mathbf{C}[\Theta_{U(\mathcal{A}_2)}, \Theta_{U(\mathcal{B}_8)}]$ (§ 2, théor. 5). De même,

$$\mathfrak{W} = \mathbf{C}[B_8, Q_{24}] \quad \text{et} \quad \mathfrak{M} = \mathbf{C}[\Theta_{U(\mathcal{B}_8)}, \Theta_{U(\mathcal{Q}_{24})}].$$

Le théorème 8 est donc une conséquence immédiate du théorème 7.

Toute fonction appartenant à $\mathfrak{A}$ (resp. $\mathfrak{M}$) s'écrit donc sous la forme $P(\varphi_2, \varphi_3)$, où P appartient à $\mathcal{V}$ (resp. $\mathfrak{W}$), et cela d'une manière unique, car les fonctions φ_2 et φ_3 sont algébriquement indépendantes.

Exemples :

(i) La dimension de l'espace des éléments « de valeur nulle en $i\infty$ » de $\mathfrak{M}_8$ est égale à 1 (*cf.* la démonstration du théorème 5). Un calcul de coefficients montre que

$$4\,\Delta_4 = C(\varphi_2, \varphi_3) = (\varphi_2\,\varphi_3\,(\varphi_2^2 - \varphi_3^2))^2.$$

Tenant compte des relations quadratiques signalées en 3.2, on obtient

$$\Delta_4 = 2^{-4}\,(\theta_2\,\theta_4)^4.$$

Or θ_2 et θ_4 admettent des développements en produits infinis ([9], XXXII (6) et (8))

$$\theta_2(z) = 2\,e^{\frac{\pi i z}{4}} \prod_{m\geq 1} (1 - e^{2\pi i m z})\,(1 + e^{2\pi i m z})^2,$$

$$\theta_4(z) = \prod_{m\geq 1} (1 - e^{2\pi i m z})\,(1 - e^{\pi i (2m-1) z})^2.$$

Les développements de Δ_4 données en 2.2 s'en déduisent immédiatement.

(ii) De même, dans l'espace des formes paraboliques de degré 24 de $\mathfrak{M}$, qui est de dimension 1, on a

$$16\,\Delta_{12} = D(\varphi_2, \varphi_3),$$

soit

$$\Delta_{12} = 2^{-8}\,(\theta_2\,\theta_3\,\theta_4)^8.$$

3.4. Homomorphismes entre groupes d'opérateurs. — *a. Formules de transformation des fonctions φ_2 et φ_3.* — Il est évident que

$$(3) \qquad \begin{cases} \varphi_2(z+1) = i\,\varphi_2(z) \\ \varphi_3(z+1) = \varphi_3(z) \quad \text{pour tout } z \in \mathfrak{H}. \end{cases}$$

D'autre part, on a (*cf.* [6], appendice au chapitre I)

$$\varphi_2\left(-\frac{1}{z}\right) = \left(\frac{z}{2i}\right)^{\frac{1}{2}} \theta_4\left(\frac{z}{2}\right) \qquad \text{et} \qquad \varphi_3\left(-\frac{1}{z}\right) = \left(\frac{z}{2i}\right)^{\frac{1}{2}} \theta_3\left(\frac{z}{2}\right) \quad (6)$$

La comparaison des développements montre immédiatement que

$$\theta_4\left(\frac{z}{2}\right) = -\varphi_2(z) + \varphi_3(z) \qquad \text{et} \qquad \theta_3\left(\frac{z}{2}\right) = \varphi_2(z) + \varphi_3(z);$$

---

(6) Dans cette formule, la détermination de la racine $\left(\frac{z}{i}\right)^{\frac{1}{2}}$ est réelle positive quand $\frac{z}{i}$ est réel positif.

donc

$$(4)\qquad \begin{cases} \varphi_2\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{1}{2}} \left(\frac{1}{\sqrt{2}}\right)(-\varphi_2(z) + \varphi_3(z)), \\ \varphi_3\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{1}{2}} \left(\frac{1}{\sqrt{2}}\right)(\varphi_2(z) + \varphi_3(z)) \qquad (z \in \mathfrak{P}). \end{cases}$$

Ces relations s'écrivent

$$(3')\qquad \begin{pmatrix} \varphi_2(z+1) \\ \varphi_3(z+1) \end{pmatrix} = \sigma \begin{pmatrix} \varphi_2(z) \\ \varphi_3(z) \end{pmatrix},$$

$$(4')\qquad \begin{pmatrix} \left(\frac{z}{i}\right)^{\frac{1}{2}} \varphi_2\left(-\frac{1}{z}\right) \\ \left(\frac{z}{i}\right)^{\frac{1}{2}} \varphi_3\left(-\frac{1}{z}\right) \end{pmatrix} = \pi_2 \begin{pmatrix} \varphi_2(z) \\ \varphi_3(z) \end{pmatrix} \qquad (z \in \mathfrak{P}),$$

où σ et π_2 sont les matrices définies en 1.2.*a*).

Soit P un élément homogène de degré n appartenant à $\mathbf{C}[X, Y]$. Des formules (4) on déduit immédiatement

$$(5)\qquad P\left(\varphi_2\left(-\frac{1}{z}\right), \varphi_3\left(-\frac{1}{z}\right)\right) = \left(\frac{z}{i}\right)^{\frac{n}{2}} (P\,\pi_2)(\varphi_2(z), \varphi_3(z)),$$

où $z \in \mathfrak{P}$ et GL (2, $\mathbf{C}$) opère à droite sur $\mathbf{C}[X, Y]$ selon les conventions adoptées au paragraphe 1.2.

b. Formule de Mac Williams et formule de Poisson. — Si $\mathcal{C}$ est un Ω-code de dimension k (où $|\Omega| = n$) et $P_{\mathcal{C}}$ le polynôme des poids de $\mathcal{C}$, et si $L = U(\mathcal{C})$ est le réseau associé selon la procédure définie en 3.1, la fonction thêta de L est $P(\varphi_2, \varphi_3)$ (théor. 7). Le code orthogonal $\mathcal{C}^0$ conduit au réseau dual L^0. Tenant compte de la formule de Poisson [form. (2) rappelée en 2.2.*a*] et de la formule (5), utilisant une nouvelle fois le théorème 7, on obtient

$$2^{\frac{n}{2}-k} (P_{\mathcal{C}}\,\pi_2)(\varphi_2, \varphi_3) = P_{\mathcal{C}^0}(\varphi_2, \varphi_3).$$

Ainsi la formule de Mac Williams [(1) en 1.2.*a*] est une traduction en théorie des codes de la formule de Poisson, ou inversement, la formule de Poisson est une traduction en théorie des réseaux de la formule de Mac Williams.

c. Le groupe $\tilde{H}$. — Les formules (3') et (4') peuvent s'interpréter en termes d'homomorphisme de groupes. Définissons pour cela un revêtement H du groupe unimodulaire SL (2, $\mathbf{Z}$).

Les éléments de H sont, par définition, les couples (ε, τ), où $\tau \in \mathrm{SL}(2, \mathbf{Z})$ et ε est une fonction holomorphe sur $\mathfrak{H}$ telle que $\varepsilon^8 = \left(\frac{d\tau^{-1}}{dz}\right)^2$.

Le produit est défini ainsi

$$(\tau, \varepsilon)(\tau', \varepsilon') = (\varepsilon_1, \tau \circ \tau'), \qquad \text{où} \quad \varepsilon_1 = \varepsilon(\varepsilon' \circ \tau^{-1}).$$

Cette définition est admissible car

$$\varepsilon_1^8 = \left(\frac{d\tau^{-1}}{dz}\right)^2 \left(\frac{d\tau'^{-1}}{dz} \circ \tau^{-1}\right)^2 = \left(\frac{d(\tau \circ \tau')^{-1}}{dz}\right)^2.$$

L'application $(\varepsilon, \tau) \to \tau$ est un homomorphisme de $\tilde{\mathrm{H}}$ sur $\mathrm{SL}(2, \mathbf{Z})$. Le noyau de cet homomorphisme est

$$\tilde{\mathrm{K}} = \{(\varepsilon, \mathrm{Id});\ \varepsilon^8 = 1\};$$

donc $\tilde{\mathrm{K}}$ est isomorphe au groupe des racines huitièmes de l'unité.

Le groupe $\tilde{\mathrm{H}}$ opère linéairement à gauche sur l'espace des fonctions complexes sur $\mathfrak{H}$ de la façon suivante, qui correspond à l'action « de poids $\frac{1}{2}$ » au sens de la théorie des formes modulaires (7) :

Si $\varphi : \mathfrak{H} \to \mathbf{C}$, posons, pour $(\varepsilon, \tau) \in \tilde{\mathrm{H}}$,

$$(\varepsilon, \tau)\varphi = \varepsilon(\varphi \circ \tau^{-1}).$$

Posons également

$$\mu = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \qquad \omega = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad \varepsilon_0(z) = \left(\frac{z}{i}\right)^{-\frac{1}{2}},$$

fonction holomorphe réelle positive si $\frac{z}{i}$ est réel positif. Alors $(1, \mu)$ et (ε_0, ω) appartiennent à $\tilde{\mathrm{H}}$ et les formules (3') et (4') s'écrivent maintenant

$$\begin{pmatrix} (1, \mu)\varphi_2 \\ (1, \mu)\varphi_3 \end{pmatrix} = \sigma \begin{pmatrix} \varphi_2 \\ \varphi_3 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} (\varepsilon_0, \omega)\varphi_2 \\ (\varepsilon_0, \omega)\varphi_3 \end{pmatrix} = \pi_2 \begin{pmatrix} \varphi_2 \\ \varphi_3 \end{pmatrix}.$$

d. Un homomorphisme de $\tilde{\mathrm{H}}$ *sur* H. — Si n est entier, notons $\Gamma(n)$ le groupe de congruence de niveau n ainsi défini.

$\Gamma(n)$ est l'ensemble des éléments $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ tels que

$$a \equiv d \equiv \pm 1 \pmod{n} \qquad \text{et} \qquad b \equiv c \equiv 0 \pmod{n}.$$

$\mathrm{SL}(2, \mathbf{Z}) = \Gamma(1)$ sera plus simplement noté Γ.

---

(7) L'action de poids n est définie par une formule analogue, le multiplicateur devenant ε^{2n}.

THÉORÈME 9. — (*a*) *Le groupe* $\tilde{H}$ *est engendré par* $(1, \mu)$ *et* (ε_0, ω).

(*b*) *L'espace* $\mathbf{C}\varphi_2 + \mathbf{C}\varphi_3$ *est stable par* $\tilde{H}$.

(*c*) *Cette représentation définit un homomorphisme h de* $\tilde{H}$ *sur* H *et induit un homomorphisme h' sur* Γ *sur* $H/K \cong \mathfrak{S}_4$, *de noyau* $\Gamma(4)$.

(Rappelons que $\mathfrak{S}_4$ est le groupe symétrique de degré 4.)

Démonstration du théorème 9. — Les formules de transformation de φ_2 et φ_3 montrent que le groupe engendré par $(1, \mu)$ et (ε_0, ω) stabilise $\mathbf{C}\varphi_2 + \mathbf{C}\varphi_3$ et y opère comme le groupe engendré par σ et π_2, c'est-à-dire H. Or il est bien connu (*cf.* [8], chap. VII, n° 1.2) que μ et ω engendrent Γ. Par ailleurs, $\nu = ((\varepsilon_0, \omega)(1, \mu))^3$ opère sur l'espace de représentation selon la matrice $(\pi_2\sigma)^3$, laquelle est d'ordre 8 (propos. 1); comme $\omega\mu$ est d'ordre 3 dans Γ, ν est de la forme (δ, Id), où δ est une racine primitive huitième de l'unité $\left(\text{évidemment } \frac{i+1}{\sqrt{2}}\right)$. Donc ν engendre $\tilde{K}$. La suite

$$1 \to \tilde{K} \to \tilde{H} \to \Gamma \to 1 \tag{E}$$

étant exacte, le groupe engendré par $(1, \mu)$ et (ε_0, ω) est $\tilde{H}$ tout entier. Ceci démontre (*a*), (*b*) et la première assertion de (*c*).

Soit h l'homomorphisme ainsi obtenu de $\tilde{H}$ sur H. On a

$$h((1, \mu)) = \sigma \qquad \text{et} \qquad h((\varepsilon_0, \omega)) = \pi_2 \qquad \text{et} \qquad h(\tilde{K}) = h(\langle \nu \rangle) = \langle (\pi_2\sigma)^3 \rangle = K.$$

La suite exacte (E) est donc transformée par h en la suite exacte

$$1 \to K \to H \to H/K \to 1 \tag{F}$$

et h induit un homomorphisme h' de Γ sur H/K, isomorphe à $\mathfrak{S}_4$ (prop. 1).

Le noyau de h' contient ω^2, μ^4 et $(\omega\mu)^3$, qui appartiennent aussi à $\Gamma(4)$. Il résulte de la présentation de $\mathfrak{S}_4$ utilisée pour démontrer la proposition 1, et du fait que ω et μ engendrent Γ, que $\frac{\Gamma}{\Gamma(4) \cap \mathrm{Ker}\, h'}$ est une image homomorphe de $\mathfrak{S}_4$. Mais l'indice de $\Gamma(4)$ dans Γ est connu (*cf.* [7], p. IV-1) et égal à 24, ordre de $\mathfrak{S}_4$; c'est aussi l'indice de Ker h'. Donc $\Gamma(4) = \mathrm{Ker}\, h'$ ce que nous voulions démontrer.

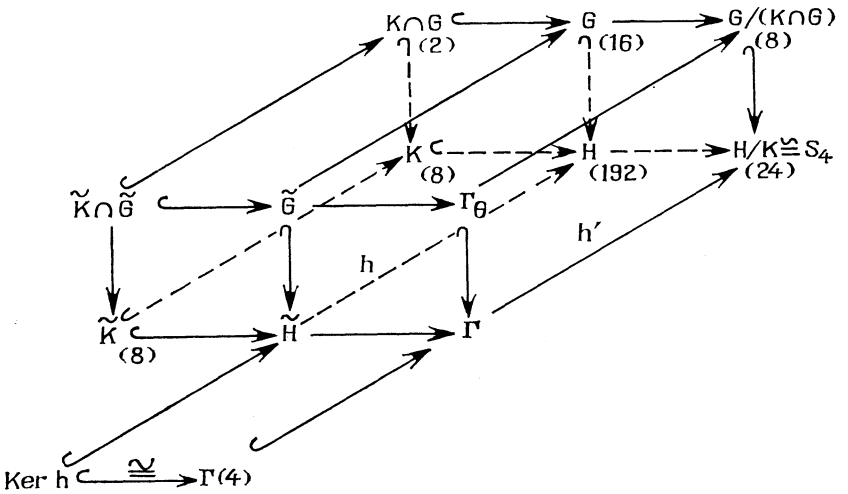
e. Un sous-groupe $\tilde{G}$ *de* $\tilde{H}$. — Soient $\tilde{G}$ le sous-groupe de $\tilde{H}$ engendré par (ε_0, ω) et $(1, \mu)^2$ et Γ_0 le sous-groupe de Γ engendré par ω et μ^2; Γ_0 est l'image de $\tilde{G}$ par l'homomorphisme canonique de $\tilde{H}$ sur Γ. On sait (*cf.* [7], p. I.32) que Γ_0 est un sous-groupe non invariant d'indice 3 de Γ. La suite exacte (E) se restreint en

$$1 \to \tilde{K} \cap \tilde{G} \to \tilde{G} \to \Gamma_0 \to 1. \tag{E'}$$

Il est clair que la restriction de h à $\tilde{G}$ a pour image G le groupe diédral d'ordre 16 défini en 1.2.*a*. Donc $\frac{\tilde{G}}{\mathrm{Ker}\, h \cap \tilde{G}}$ est isomorphe à G. La restriction de h' à Γ_θ a pour image le 2-groupe de Sylow de H/K, qui est diédral d'ordre 8. Donc $\frac{\tilde{G}}{(\mathrm{Ker}\, h.\tilde{K}) \cap \tilde{G}}$ est isomorphe à $G/\langle -\mathrm{Id} \rangle$. Or $\tilde{K}$ opère fidèlement sur l'espace $\mathbf{C}\varphi_2 + \mathbf{C}\varphi_3$. Autrement dit, $\tilde{K} \cap \mathrm{Ker}\, h = \{1\}$. C'est donc que $\tilde{K} \cap \tilde{G}$ est d'ordre 2.

Ainsi $\tilde{G}$ est un sous-groupe d'indice 12 de $\tilde{H}$.

Les résultats exposés dans ce paragraphe sont résumés dans le diagramme commutatif ci-dessous. Toutes les lignes sont exactes. Les monomorphismes sont représentés par des flèches « à poignées », style parapluie, et, lorsque les groupes considérés sont finis, leurs ordres sont indiqués entre parenthèses.



3.5 Compléments. — *a. Intégralité des coefficients.* — L'isomorphisme établi entre $\mathfrak{W}$ et $\mathfrak{M}$ n'induit pas un isomorphisme entre $\mathfrak{W}_\mathbf{Z}$ et $\mathfrak{M}_\mathbf{Z}$. En effet,

$$\mathfrak{W}_\mathbf{Z} = \mathbf{Z}[B_8, D] \quad (\S\,1, \text{théor. } 3) \qquad \text{et} \qquad \mathfrak{M}_\mathbf{Z} = \mathbf{Z}[E_4, \Delta_{12}].$$

Or $E_4 = B_8(\varphi_2, \varphi_3)$, mais $\Delta_{12} = 2^{-4} D(\varphi_2, \varphi_3)$.

La situation est la même en ce qui concerne $\mathfrak{V}$ et $\mathfrak{N}$: on a

$$\mathfrak{V}_\mathbf{Z} = \mathbf{Z}[A_2, C] \qquad \text{et} \qquad \mathfrak{N}_\mathbf{Z} = \mathbf{Z}[\theta_3^2, \Delta_4];$$

si $\theta_3^2 = A_2(\varphi_2, \varphi_3)$, par contre, $\Delta_4 = 2^{-2} C(\varphi_2, \varphi_3)$.

Si U est un réseau unimodulaire de $\mathbf{Q}^n$, et si P_U est le polynôme tel que $\Theta_U = P_U(\varphi_2, \varphi_3)$, il est faux que P_U soit à coefficients entiers; on peut

seulement affirmer que $P_U \in \mathbf{Z}[A_2, C)$. Par exemple, avec $n = 32$, soit $\{e_j\}_{j\in\Omega}$, une base orthonormale de $\mathbf{Q}^n$, et soit $U = \bigoplus_{j\in\Omega} \mathbf{Z}\, e_j$; soit η la symétrie par rapport au vecteur $\sum_{j\in\Omega} e_j$. Nous avons défini dans [3] un réseau unimodulaire pair $\Gamma_4(U, \eta)$. Soit T son polynôme, $T(\varphi_2, \varphi_3)$ sa fonction Θ. Si T est à coefficients entiers, $T \in \mathbf{Z}[B_8, D]$ et par conséquent, $T(\varphi_2, \varphi_3) \in \mathbf{Z}[E_4, 16\,\Delta_{12}]$. Il en résulte alors que le nombre u_a de vecteurs du réseau de carré a est divisible par 16. On voit facilement que $u_2 = 994$. Donc certains coefficients de T ne sont pas entiers.

b. Calcul des polynômes de certains réseaux. — Soit n un entier multiple de 8, et soient Ω de cardinal n, $\mathcal{C}$ un Ω-code unimodulaire pair. Soit $V(\mathcal{C})$ le réseau obtenu de la manière suivante [3] :

Sur une base orthogonale $\{\nu_j\}_{j\in\Omega}$ de $\mathbf{Q}^n$ donnée, et telle que, pour tout $j \in \Omega$, $\nu_j^2 = \frac{1}{8}$, un vecteur $x = \sum_{j\in\Omega} x_j \nu_j$ appartient à $V(\mathcal{C})$ si et seulement si

1° les x_j sont entiers et de même parité;

2° $\forall\, \alpha \in \mathbf{Z}$, $\{j \mid x_j \equiv \alpha \bmod 4\} \in \mathcal{C}$;

3° $\sum_{j\in\Omega} x_j \equiv \left(\frac{n}{2}\right) x_{j_0} \pmod 8$, pour $j_0 \in \Omega$.

Le calcul montre alors

Proposition 3 :

$$\Theta_{V(\mathcal{C})} = \frac{1}{2}(P_{\mathcal{C}}(\varphi_2, \varphi_3) + S_n(\varphi_2, \varphi_3)),$$

où

$$S_n(X, Y) = (2\,XY(X^2 + Y^2))^{\frac{n}{4}} + (X^2 - Y^2)^{\frac{n}{4}} + (-1)^{\frac{n}{8}}(2\,XY(X^2 - Y^2)^{\frac{n}{4}},$$

soit encore

$$S_n(\varphi_2, \varphi_3) = (\theta_2\,\theta_3)^{\frac{n}{2}} + (\theta_3\,\theta_4)^{\frac{n}{2}} + (-1)^{\frac{n}{8}}(\theta_2\,\theta_4)^{\frac{n}{2}}.$$

Exemple. — Le réseau de Leech Λ n'est autre que le réseau $V(\mathfrak{L}_{24})$ (*voir* [3] ou [4]). Posant $\Theta_\Lambda = P_\Lambda(\varphi_2, \varphi_3)$, on obtient

$$P_\Lambda(X, Y) = X^{24} - 3.X^{20}Y^4 + 771.X^{16}Y^8 + 2\,558.X^{12}Y^{12}$$
$$+ 771.X^8Y^{16} - 3.X^4Y^{20} + Y^{24}.$$

4. Utilisation des codes sur $\mathbf{F}_3$; une sous-algèbre de $\mathcal{H}$.

4.1. CODES ET POLYNOMES DES POIDS SUR UN CORPS FINI QUELCONQUE. — Les notions de codes sur $\mathbf{F}_2$ et de polynômes des poids se généralisent de la façon suivante :

Soient Ω un ensemble fini de cardinal n et K un corps commutatif. L'espace vectoriel K^Ω est supposé muni du produit scalaire naturel pour lequel la base canonique $\{ e_j \}_{j \in \Omega}$ est orthonormale. Un (K, Ω)-code est un sous-espace vectoriel de K^Ω. Si $\mathcal{C}$ est un (K, Ω)-*code* nous désignerons par $\mathcal{C}^0$ son orthogonal et nous dirons que $\mathcal{C}$ est *unimodulaire* si $\mathcal{C} = \mathcal{C}^0$. Si $x \in K$, le *poids* de x, noté $| x |$, est le nombre de coordonnées non nulles de x dans sa décomposition sur la base canonique de K^Ω. Si K est fini, le *polynôme des poids* d'un (K, Ω)-code $\mathcal{C}$ est

$$P_{\mathcal{C}}(X, Y) = \sum_{x \in \mathcal{C}} X^{|x|} Y^{n-|x|}.$$

Exemples :

1. Soient $\Omega = \{ 1, 2, 3, 4 \}$ et $\{ e_j \}_{1 \leq j \leq 4}$ la base canonique de $\mathbf{F}_3^\Omega$. Nous désignerons par $\mathcal{F}$ le code engendré par les vecteurs $e_1 + e_2 + e_3$ et $e_2 - e_3 + e_4$; c'est un code unimodulaire de polynôme des poids

$$F(X, Y) = Y^4 + 8 X^3 Y.$$

2. Soit $\mathcal{R}_{12}$ le « code quadratique étendu » dans $\mathbf{F}_3^{12}$ (*voir* [1]); c'est un code unimodulaire de polynôme des poids

$$R_{12}(X, Y) = 24.X^{12} + 440.X^9 Y^3 + 264.X^6 Y^6 + Y^{12}.$$

4.2. ALGÈBRE DE POLYNÔMES ASSOCIÉE AUX CODES SUR $\mathbf{F}_3$. — *a. Propriétés d'invariance des polynômes de certains codes.* — Soient q une puissance d'un nombre premier, et $K = \mathbf{F}_q$. Soit π_q la matrice involutive

$$\pi_q = \frac{1}{\sqrt{q}} \begin{pmatrix} -1 & 1 \\ q-1 & 1 \end{pmatrix}.$$

Les formules de Mac Williams [*voir* [10]) impliquent que pour tout (K, Ω)-code $\mathcal{C}$, de dimension k,

$$P_{\mathcal{C}^0} = q^{\frac{n}{2}-k} (P_{\mathcal{C}} \pi_q). \tag{6}$$

Supposons maintenant $q = 3$. Si un vecteur $x = (x_j)_{j \in \Omega}$ de $\mathbf{F}_3^\Omega$ est de carré scalaire nul, alors $| x |$ est un multiple de 3, car le seul carré non nul

de $\mathbf{F}_3$ est 1 : $\sum_{j\in\Omega} x_j^2 \equiv |x| \pmod 3$. Par conséquent, si $\mathcal{C}$ est un (F_3, Ω)-code dont tous les vecteurs sont de carré scalaire nul, $P_{\mathcal{C}}$ est fixe par l'opération de la matrice

$$\rho_3 = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & 1 \end{pmatrix}.$$

Désignons par G_3 le sous-groupe de GL (2, $\mathbf{C}$) engendré par les matrices π_3 et ρ_3. Il résulte de ce qui précède :

THÉORÈME 10. — *Soit $\mathcal{C}$ un $(\mathbf{F}_3, \Omega)$-code unimodulaire. Alors $P_{\mathcal{C}}$ est fixe par les opérations de G_3.*

b. Algèbre associée. — Soit $\mathcal{V}_3$ l'algèbre des polynômes fixes par l'opération de G_3 sur $\mathbf{C}[X, Y]$. Posons

$$\mathcal{V}_{3,\mathbf{Z}} = \mathcal{V}_3 \cap \mathbf{Z}[X, Y].$$

D'après le théorème 10, si $\mathcal{C}$ est un $(\mathbf{F}_3, \Omega)$-code unimodulaire, on a $P_{\mathcal{C}} \in \mathcal{V}_{3,\mathbf{Z}}$.

PROPOSITION 4. — *L'élément $(\pi_3 \rho_3)^3$ est une matrice d'homothétie d'ordre 4 et $\frac{G_3}{\langle (\pi_3 \rho_3)^3 \rangle}$ est isomorphe au groupe alterné $\mathfrak{A}_4$. Ainsi G_3 est un groupe fini d'ordre 48 engendré par des pseudo-réflexions.*

Démonstration de la proposition. — On a, en effet,

$$(\pi_3 \varphi_3)^3 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Dans le quotient de G_3 par le groupe cyclique $\langle (\pi_3 \rho_3)^3 \rangle$, les images de π_3, ρ_3 et $\pi_3\rho_3$ sont d'ordres respectifs 2, 3 et 3. Or le groupe alterné de degré 4 admet la présentation (*cf.* [5], p. 66)

$$A^2 = B^3 = (AB)^3 = 1.$$

La proposition 4 est donc démontrée.

THÉORÈME 11. — *$\mathcal{V}_3$ est une algèbre de polynômes homogènes, engendrée par deux éléments algébriquement indépendants de degrés respectifs 4 et 12, F et R_{12}.*

Démonstration analogue à celle du théorème 2 du paragraphe 1.

L'algèbre $\mathcal{V}_{3,\mathbf{Z}}$ contient un polynôme analogue à C et D dans respectivement $\mathcal{V}$ et $\mathcal{W}$: $\frac{R_{12} - F^3}{24} = C_3$; on a

$$C_3(X, Y) = X^3 (X^3 - Y^3)^3 \qquad \text{et} \qquad C_3 \in \mathcal{V}_{3,\mathbf{Z}}.$$

THÉORÈME 12. — $\mathcal{V}_{3,\mathbf{Z}} = \mathbf{Z}[F, C_3]$.

Démonstration analogue à celle du théorème 3 (§ 1).

4.3. $\mathbf{F}_3$-CODES ET RÉSEAUX, POLYNÔMES ET FONCTIONS THÊTA. — *a. Codes et réseaux.* — Soient Ω un ensemble fini de cardinal n multiple de 4 et p un nombre premier. A tout $(\mathbf{F}_p, \Omega)$-code $\mathcal{C}$, nous associons un réseau $U(\mathcal{C})$ de la façon suivante :

Soit $\{\nu_j\}_{j\in\Omega}$ une base orthogonale de $\mathbf{Q}^n$ telle que, pour tout $j\in\Omega$, $\nu_j^2 = \frac{1}{p}$ (il existe bien une telle base si n est multiple de 4). Soit $R = \bigoplus_{j\in\Omega} \mathbf{Z}\,\nu_j$: $\frac{R}{pR}$ s'identifie naturellement à $\mathbf{F}_p^\Omega$. Soit λ la projection de R sur $\frac{R}{pR} \simeq \mathbf{F}_p^\Omega$. Le réseau $U(\mathcal{C})$ envisagé est $\lambda^{-1}(\mathcal{C})$.

PROPOSITION 5. — (1) *Si $\mathcal{C}$ est de dimension k,* $\mathrm{vol}(U(\mathcal{C})) = p^{\frac{n}{2}-k}$.

(2) $U(\mathcal{C})^0 = U(\mathcal{C}^0)$.

(3) *Pour que les carrés scalaires des vecteurs de $U(\mathcal{C})$ soient entiers, il faut et il suffit que les carrés scalaires des vecteurs de $\mathcal{C}$ soient nuls.*

b. Polynômes et fonctions thêta. — *Reprenant les notations du paragraphe* 3; 3.2, nous poserons

$$\psi_0(z) = \theta_3(3z) \qquad \text{et} \qquad \psi_1(z) = e^{\frac{\pi i z}{3}}\,\theta_3(z \mid 3z),$$

autrement dit,

$$\psi_j(z) = \sum_{m=-\infty}^{+\infty} \exp\left(3\pi i\left(k + \frac{j}{3}\right)^2 z\right) \qquad \text{pour} \quad j = 0, 1.$$

THÉORÈME 13. — *Soit $\mathcal{C}$ un $(\mathbf{F}_3, \Omega)$-code. On a*

$$\Theta_{U(\mathcal{C})} = P_{\mathcal{C}}(\psi_1, \psi_0).$$

Démonstration du théorème 13. —Soient

$$a = (a_j)_{j\in\Omega}\in\mathcal{C} \qquad \text{et} \qquad x = (x_j)_{j\in\Omega}\in U(\mathcal{C})$$

tels que $\lambda(x) = a$. Soit $S(a)$ l'ensemble des indices j tels que $a_j \neq 0$; $S(a)$ est de cardinal $|a|$. On a

$$x = \sum_{j\in\Omega} 3k_j v_j + \sum_{j\in S(a)} \delta_j v_j \quad (\text{où } \delta_j\in\{-1, 1\}),$$

et x parcourt $\lambda^{-1}(a)$ quand $(k_j)_{j\in\Omega}$ parcourt $\mathbf{Z}^\Omega$. On a aussi

$$x^2 = 3\sum_{\in S(a)}\left(k_j + \frac{\delta_j}{3}\right)^2 + \sum_{j\in S(a)} 3k_j^2.$$

Remarquons que

$$\sum_{k\in\mathbf{Z}} e^{3\pi i z\left(k+\frac{1}{3}\right)^2} = \sum_{k\in\mathbf{Z}} e^{3\pi i z\left(k-\frac{1}{3}\right)^2},$$

car la transformation $k \to -k$ échange les deux séries. Un calcul analogue à celui utilisé pour démontrer le théorème 7 montre que

$$\sum_{\lambda(x)=a} e^{\pi i z(x.x)} = \psi_1(z)^{|a|}\,\psi_0(z)^{n-|a|},$$

et donc

$$\Theta_{U(\mathcal{C})} = P_{\mathcal{C}}(\psi_1, \psi_0).$$

Remarque. — Lorsque $p > 3$, $\mathbf{F}_p$ contient d'autres carrés que 0 et 1, il n'est en général pas possible d'exprimer $\Theta_{U(\mathcal{C})}$ comme seule fonction de $P_{\mathcal{C}}$.

4.4. Une sous-algèbre de $\mathcal{R}$. — Si $P(X, Y)$ appartient à $\mathcal{V}_3$, $P(X, Y) \in \mathbf{C}[F, R_{12}]$ (théor. 11). Donc $P(\psi_1, \psi_0)$ appartient à $\mathbf{C}[\Theta_{U(\mathcal{F})}, \Theta_{U(\mathcal{R}_{12})}]$ (théor. 13). Les réseaux $U(\mathcal{F})$ et $U(\mathcal{R}_{12})$ sont unimodulaires (propos. 5), leurs fonctions thêta sont des éléments de $\mathcal{R}$ (théor. 4). Quand $P(X, Y)$ parcourt $\mathcal{V}_3$, $P(\psi_1, \psi_0)$ parcourt une sous-algèbre de $\mathcal{R}$ isomorphe à $\mathcal{V}_3$.

On en déduit les identifications suivantes :

a. L'espace $\mathcal{R}_4$ est de dimension 1 (théor. 5) et engendré par $(\theta_3)^4$. Il contient aussi $F(\psi_1, \psi_0)$ (théor. 12). Or ces deux fonctions prennent la valeur 1 à la pointe $i\infty$. Donc

$$\theta_3^4 = \psi_0^4 + 8\,\psi_0\,\psi_1^3.$$

Cette égalité permet de calculer le nombre de décompositions d'un entier k sous la forme

$$k = 3\,m_0^2 + \sum_{j=1}^{3}(3\,m_j^2 - 2\,m_j) \qquad (m_j \in \mathbf{Z})$$

(les nombres $3\,m^2 - 2\,m$ sont dits « nombres octogonaux ».)

b. L'espace $\mathcal{R}_{12}$ est de dimension 2 (théor. 5) et l'espace des éléments « nuls en $i\infty$ » de degré 12 de $\mathcal{R}$ est donc de dimension 1. Cet espace contient la racine carrée Δ_6 de Δ_{12}.

$$\Delta_6(z) = e^{\pi i z}\prod_{m\geq 1}(1 - e^{2\pi i m z})^{12}.$$

L'étude à l'infini montre que

$$\Delta_6 = -\,C_3(\psi_1, \psi_0).$$

Par extraction de la racine cubique, on obtient

$$\psi_1(z).(\psi_0(z)^3 - \psi_1(z)^3) = e^{\frac{\pi i z}{3}} \prod_{m \geq 1} (1 - e^{2\pi i m z})^4.$$

4.5. UN HOMOMORPHISME DE $\tilde{G}$ SUR G_3. — *a. Formules de transformation des fonctions* ψ_1 et ψ_0. — Des calculs analogues à ceux utilisés pour démontrer les formules (3) et (4) conduisent aux formules suivantes :

$$(7) \qquad \begin{cases} \psi_1(z+2) = e^{\frac{2\pi i}{3}} \psi_1(z), \\ \psi_0(z+2) = \psi_0(z) \quad \text{pour tout } z \in \mathfrak{P}; \end{cases}$$

$$(8) \qquad \begin{cases} \psi_1\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{1}{2}} \left(\frac{1}{\sqrt{3}}\right) (-\psi_1(z) + \psi_0(z)), \\ \psi_0\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{1}{2}} \left(\frac{1}{\sqrt{3}}\right) (2.\psi_1(z) + \psi_0(z)). \end{cases}$$

Si P est un polynôme homogène en X et Y de degré n, on en déduit

$$(9) \qquad P\left(\psi_1\left(-\frac{1}{z}\right), \psi_0\left(-\frac{1}{z}\right)\right) = \left(\frac{z}{i}\right)^{\frac{n}{2}} (P\,\pi_3)(\psi_1(z), \psi_0(z)) \qquad (z \in \mathfrak{P}).$$

b. Comme au paragraphe 3.4.*b*, on voit que la proposition 5, le théorème 13 et la formule (9) permettent de considérer la formule de Mac Williams relative aux codes sur $\mathbf{F}_3$ [form. (6), § 4.2.*a*] comme une traduction de la formule de Poisson [form. (2), 2.2.*a*], et inversement.

c. Une représentation de $\tilde{G}$.

THÉORÈME 14. — (*a*) *L'espace* $\mathbf{C}\psi_1 + \mathbf{C}\psi_0$ *est stable par* $\tilde{G}$.

(*b*) *Cette représentation définit un homomorphisme g de* $\tilde{G}$ *sur* G_3 *et induit un homomorphisme g' de* Γ_0 *sur* $\frac{G_3}{\langle -\mathrm{Id} \rangle}$, *de noyau* $\Gamma(6) \cap \Gamma_0$.

Démonstration du théorème 14. — Les formules (7) et (8) montrent que le sous-groupe de $\tilde{H}$ engendré par $(1, \mu)^2$ et (ε_0, ω), à savoir $\tilde{G}$, stabilise $\mathbf{C}\psi_1 + \mathbf{C}\psi_0$ et y opère comme le groupe engendré par ρ_3 et π_3, c'est-à-dire G_3. Ceci démontre (*a*) et la première assertion de (*b*).

Soit g l'homomorphisme ainsi obtenu de $\tilde{G}$ sur G_3. La définition de l'action des éléments de $\tilde{H}$ sur l'espace des fonctions complexes sur $\mathfrak{P}$ implique qu'un élément $(\varepsilon, \mathrm{Id})$ de $\tilde{K}$ opère selon l'homothétie de rapport ε. On a vu (3.4.*e*) que $\tilde{G} \cap \tilde{K}$ est d'ordre 2. Donc g transforme la suite exacte

$$(E') \qquad 1 \to \tilde{K} \cap \tilde{G} \to \tilde{G} \to \Gamma_0 \to 1$$

en la suite exacte

$$(F') \qquad 1 \to \langle (\pi_3 \rho_3)^6 \rangle \to G_3 \to \frac{G_3}{\langle (\pi_3 \rho_3)^6 \rangle} \to 1.$$

Les groupes $\frac{\Gamma_0}{\operatorname{Ker} g'}$ et $\frac{G_3}{\langle (\pi_3 \rho_3)^6 \rangle}$ sont isomorphes d'ordre 24. De la proposition 4 et de la présentation de $\mathfrak{A}_4$ utilisée pour démontrer cette proposition, il résulte immédiatement que $\frac{\Gamma_0}{\operatorname{Ker} g'}$ admet une présentation de la forme

$$A^2 = B^3 = (AB)^6 = 1, \quad (AB)^3 \text{ central.}$$

L'indice de $\Gamma(6)$ dans Γ est égal à 72 (*cf.* [7], P. IV.1). Mais $\Gamma(6)$ est contenu dans Γ_0, et invariant dans Γ_0. On vérifie facilement que les images de μ^2, ω et $\omega\mu^2$ sont d'ordres respectifs 2, 3 et 6 dans $\Gamma_0/\Gamma(6)$, l'image de $(\omega\mu^2)^3$ étant centrale. Donc $\frac{\Gamma_0}{\Gamma(6)}$ est isomorphe à $\frac{\Gamma_0}{\operatorname{Ker} g'}$ et un raisonnement semblable à celui tenu pour démontrer le théorème 10 montre que $\operatorname{Ker} g' = \Gamma(6)$.

BIBLIOGRAPHIE

[1] E. F. Assmus et H. F. Mattson, *New 5-designs* (*J. of Combinatorial theory*, vol. 6, 1969, p. 123-151).

[2] N. Bourbaki, *Groupes et algèbres de Lie;* chap. V; *Groupes engendrés par des réflexions*, Hermann, Paris, 1968.

[3] M. Broué et M. Enguehard, *Sur certains réseaux unimodulaires pairs* (*C. R. Acad. Sc.*, t. 272, série A, 1971, p. 210-213).

[4] J. H. Conway, *A group of order* 8, 315, 553, 613, 086, 720, 000 (*Bull. Lond. Math. Soc.*, vol. 1, 1969, p. 79-88).

[5] H. S. Coxeter et W. O. J. Moser, *Generators and relations for discrete groups* (*Ergebnisse der Mathematik*, t. 14, 1957, Springer Verlag, Berlin).

[6] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York, 1966.

[7] A. Ogg, *Modular forms and Dirichlet Series*, W. Benjamin Publ., New York, 1969.

[8] J.-P. Serre, *Cours d'arithmétique*, Collection « Sup », P. U. F., Paris, 1970.

[9] J. Tannery et J. Molk, *Éléments de la théorie des fonctions elliptiques*, t. 2, Gauthier-Villars, Paris, 1898.

[10] J. H. Van Lint, *Coding Theory* (*Lecture notes in mathematics*, 201, Springer Verlag, Berlin, 1971).

[11] E. Witt, *Uber Steinersche Systeme* (*Abh. Math. Sem. Univ. Hamburg.*, t. 12, 1938, p. 265-274).

(Manuscrit reçu le 26 octobre 1971.)

Michel Broué,
Laval-en-Brie,
77-Salins

et Michel Enguehard,
4, rue Jean-Mermoz,
94-Le Kremlin-Bicêtre,