

**Travaux dirigés de M2**

**La fonction de Ramanujan et représentations galoisiennes**

**Alain Kraus**

**Université de Paris VI**

**Janvier 2005**



# Introduction

L'objectif de ces notes est de présenter, sous forme d'exercices, certains liens existant entre les formes modulaires et les représentations galoisiennes de dimension 2, en caractéristique finie, du groupe de Galois absolu de  $\mathbb{Q}$ . On se limitera au cas des formes modulaires paraboliques pour le groupe  $\mathrm{SL}_2(\mathbb{Z})$  et principalement de la fonction  $\Delta$  de Ramanujan. Soit  $\mathfrak{H}$  le demi-plan de Poincaré. La fonction  $\Delta$  est définie sur  $\mathfrak{H}$  par le produit

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} \quad \text{avec} \quad q = e^{2\pi iz}, \quad z \in \mathfrak{H},$$

qui est normalement convergent sur tout compact de  $\mathfrak{H}$ . C'est à un coefficient multiplicatif près l'unique forme modulaire parabolique de poids 12 pour  $\mathrm{SL}_2(\mathbb{Z})$ . Elle admet un développement de Fourier, convergent pour tout  $z \in \mathfrak{H}$ ,

$$\Delta(z) = \sum_{n \geq 1} \tau(n) q^n = q - 24q^2 + \cdots,$$

où les coefficients  $\tau(n)$  sont des entiers relatifs. S. Ramanujan a démontré vers 1920 que les  $\tau(n)$  vérifient certaines congruences modulo les nombres premiers 2, 3, 5, 7, 23 et 691 (cf. [Ra]). À titre indicatif, pour tout nombre premier  $p$  on a

$$(1) \quad \tau(p) \equiv p + p^4 \pmod{7}.$$

Ces congruences s'interprètent en termes de représentations galoisiennes du groupe de Galois  $G_{\mathbb{Q}}$  de  $\overline{\mathbb{Q}}$  sur  $\mathbb{Q}$  ([Se1]). En effet, d'après les travaux de P. Deligne en 1969 (cf. [De]), pour tout nombre premier  $\ell$ , on peut associer à  $\Delta$  une représentation linéaire continue semi-simple, unique à isomorphisme près,

$$\rho_{\Delta, \ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{\ell})$$

possédant les deux propriétés suivantes :

- 1)  $\rho_{\Delta, \ell}$  est non ramifiée en dehors de  $\ell$ .
- 2) Pour tout nombre premier  $p \neq \ell$ , un élément de Frobenius en  $p$  dans l'image de  $\rho_{\Delta, \ell}$  est de trace  $\tau(p) \pmod{\ell}$  et de déterminant  $p^{11} \pmod{\ell}$ .

Si  $\ell$  est l'un des entiers 2, 3, 5, 7, 23 et 691, les congruences obtenues par Ramanujan permettent alors de décrire la classe d'isomorphisme de  $\rho_{\Delta, \ell}$ . Par exemple, si  $\ell = 7$ , on déduit de (1) que  $\rho_{\Delta, 7}$  est représentable sous la forme

$$\begin{pmatrix} \chi & 0 \\ 0 & \chi^4 \end{pmatrix},$$

où  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_7^*$  est le caractère donnant l'action de  $G_{\mathbb{Q}}$  sur le groupe des racines 7-ièmes de l'unité. En fait, H. P. F. Swinnerton-Dyer a démontré en 1976 que l'image de  $\rho_{\Delta, \ell}$  contient  $\mathrm{SL}_2(\mathbb{F}_{\ell})$  excepté si  $\ell$  est l'un des entiers ci-dessus ([Sw]). Cela explique l'absence de congruences des  $\tau(p)$  modulo d'autres nombres premiers (cf. [Se3]).

Dans le chapitre I on énonce le théorème de Deligne concernant certaines formes modulaires paraboliques pour  $\mathrm{SL}_2(\mathbb{Z})$ , dont les coefficients de Fourier à l'infini sont des entiers relatifs. On rappelle les résultats connus concernant les images possibles des représentations galoisiennes dont l'existence est affirmée par ce théorème. On décrit en particulier les notions de sous-groupes de Cartan de  $\mathrm{GL}_2(\mathbb{F}_{\ell})$  et de leurs normalisateurs. Il se trouve par ailleurs quelques rappels sur la fonction  $\Delta$  et les séries d'Eisenstein. On démontre dans le chapitre II les congruences relatives à  $\Delta$  modulo les nombres premiers exceptionnels mentionnés précédemment. Le chapitre III est consacré à la description des représentations galoisiennes associées. On pourra trouver dans le chapitre IV quelques généralisations dans le cas où les coefficients de Fourier à l'infini des formes modulaires considérées ne sont pas des entiers relatifs.

## Table des matières

Chapitre I. <b>Préliminaires</b>	3
1. Énoncé du théorème de Deligne	3
2. Description de l'image de $\rho_{f, \ell}$	5
3. La fonction $\Delta$ de Ramanujan	11
4. Les séries d'Eisenstein	12
Chapitre II. <b>Congruences relatives à <math>\Delta</math></b>	15
1. Congruences modulo $2^3, 3^3, 5^2, 7$ et 691	15
2. Formule du produit triple de Jacobi	17
3. Congruences modulo 23	19
Chapitre III. <b>Représentations galoisiennes associées</b>	25
1. Les représentations modulo 2, 3, 5, 7 et 691	25
2. La représentation modulo 23	25
3. Les nombres premiers exceptionnels pour $\Delta$	26
Chapitre IV. <b>Généralisations</b>	29
1. Les représentations $\rho_{f, \mathcal{L}}$	29
2. Un exemple en poids 24	30
Bibliographie	33

# Chapitre I — Préliminaires

## 1. Énoncé du théorème de Deligne

Dans toute la suite, on note  $\overline{\mathbb{Q}}$  la clôture algébrique de  $\mathbb{Q}$  dans  $\mathbb{C}$  et  $G_{\mathbb{Q}}$  le groupe de Galois de  $\overline{\mathbb{Q}}$  sur  $\mathbb{Q}$ . Pour tout nombre premier  $\ell$ , on désigne par  $\mathrm{GL}_2(\mathbb{F}_{\ell})$  le groupe des matrices  $(2, 2)$  inversibles à coefficients dans  $\mathbb{F}_{\ell}$ . Le groupe  $G_{\mathbb{Q}}$  est muni de la topologie de Krull et  $\mathrm{GL}_2(\mathbb{F}_{\ell})$  de la topologie discrète.

### 1.1. Rappels sur les représentations linéaires

Soit  $\ell$  un nombre premier. Considérons une représentation linéaire de  $G_{\mathbb{Q}}$  de dimension 2 en caractéristique  $\ell$

$$\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{\ell}).$$

Par définition,  $\rho$  est un homomorphisme de groupes que l'on supposera implicitement continu. Son noyau est donc ouvert. Le sous-corps  $K$  de  $\overline{\mathbb{Q}}$  laissé fixe par ce noyau est une extension galoisienne finie  $K$  de  $\mathbb{Q}$  et  $\rho$  se factorise à travers le groupe de Galois de  $K$  sur  $\mathbb{Q}$ . Étant donné un nombre premier  $p$ , rappelons que  $\rho$  est dite non ramifiée en  $p$  si elle est triviale sur le groupe d'inertie d'une place de  $\overline{\mathbb{Q}}$  prolongeant  $p$ , c'est-à-dire si  $p$  est non ramifié dans  $K$ . Soit  $p$  un tel nombre premier. Pour tout idéal premier  $\mathfrak{P}$  au-dessus de  $p$  dans l'anneau d'entiers de  $K$ , soit  $\sigma_{\mathfrak{P}}$  la substitution de Frobenius en  $\mathfrak{P}$  dans l'extension  $K/\mathbb{Q}$ . En notant encore  $\sigma_{\mathfrak{P}}$  un de ses relèvements à  $G_{\mathbb{Q}}$ , l'élément  $\rho(\sigma_{\mathfrak{P}})$  est appelé le Frobenius en  $\mathfrak{P}$  dans la représentation  $\rho$ . Sa classe de conjugaison ne dépend que de  $p$ . On peut ainsi considérer l'élément

$$\rho(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbb{F}_{\ell}),$$

qui est appelé le Frobenius en  $p$  dans la représentation  $\rho$  et qui est bien défini à conjugaison près. En particulier, la trace et le déterminant de cet élément sont bien définis.

On dit que  $\rho$  est semi-simple si elle est somme directe de représentations simples (ou irréductibles). Tel est par exemple le cas si  $\rho$  est irréductible. Il est en général facile de se convaincre si deux représentations semi-simples sont ou non isomorphes. En effet, la classe d'isomorphisme d'une représentation linéaire semi-simple est déterminée par les polynômes caractéristiques des éléments de Frobenius en les nombres premiers où la représentation est non ramifiée ([De-Se], p. 513). Cela étant, il est parfois difficile de démontrer que deux représentations données sont isomorphes si tel est le cas.

### Exercice 1

- 1) Construire une représentation linéaire  $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_2)$  surjective et non ramifiée en dehors de 2 et 3.

- 2) Expliciter deux représentations linéaires vérifiant les conditions de la question 1 qui ne soient pas isomorphes.

### Exercice 2

Rappelons qu'étant donné un corps de nombres de degré  $n$  sur  $\mathbb{Q}$  et de discriminant  $D$ , on a l'inégalité ([Sa], p. 70) :

$$|D| \geq \left(\frac{3\pi}{4}\right)^{n-1} \times \frac{\pi}{3}.$$

En déduire qu'il n'existe pas de représentation linéaire de  $G_{\mathbb{Q}}$  dans  $\mathrm{GL}_2(\mathbb{F}_2)$  qui soit non ramifiée en dehors de 2 et dont l'image soit d'ordre  $\geq 3$ .

### Exercice 3

Soit  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{\ell})$  une représentation linéaire. Notons  $c$  la conjugaison complexe de  $G_{\mathbb{Q}}$ . C'est un automorphisme d'ordre 2, donc le déterminant de  $\rho(c)$  est  $\pm 1$ . On suppose qu'il vaut  $-1$  ; une telle représentation est dite impaire.

- 1) Montrer que si  $\ell \neq 2$ , alors  $\rho(c)$  est conjugué à la matrice  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ .
- 2) Trouver un contre-exemple à cette assertion si  $\ell = 2$ .

## 1.2. Énoncé du théorème

Soient  $k \geq 2$  un entier pair et  $S_k$  le  $\mathbb{C}$ -espace vectoriel des formes modulaires paraboliques de poids  $k$  pour  $\mathrm{SL}_2(\mathbb{Z})$ . Soit  $f$  un élément de  $S_k$  vérifiant les deux conditions suivantes :

- 1)  $f$  est fonction propre de tous les opérateurs de Hecke  $T_n$  avec  $n \geq 1$ .
- 2) Le développement de Fourier de  $f$  est de la forme

$$f = q + \sum_{n \geq 2} a_n q^n \quad \text{avec} \quad a_n \in \mathbb{Z} \quad (q = e^{2\pi iz}, z \in \mathfrak{H}).$$

Ces conditions entraînent l'égalité  $T_n(f) = a_n f$  pour tout  $n \geq 1$ . On obtient des exemples de telles formes modulaires par exemple si la dimension de  $S_k$  vaut 1, autrement dit si  $k = 12, 16, 18, 20, 22$  et  $26$ .

**Théorème 1 (Deligne).** *Soit  $\ell$  un nombre premier. Il existe une représentation linéaire semi-simple, unique à isomorphisme près,*

$$\rho_{f,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{\ell}),$$

*réalisant les deux conditions suivantes :*

- 1)  $\rho_{f,\ell}$  est non ramifiée en dehors de  $\ell$ .

2) Pour tout nombre premier  $p \neq \ell$ , on a

$$(1) \quad \text{Tr } \rho_{f,\ell}(\text{Frob}_p) = a_p \bmod \ell \quad \text{et} \quad \det \rho_{f,\ell}(\text{Frob}_p) = p^{k-1} \bmod \ell.$$

Comme on le signalait dans le paragraphe précédent, une représentation semi-simple de  $G_{\mathbb{Q}}$  dans  $\text{GL}_2(\mathbb{F}_{\ell})$  vérifiant les deux conditions de cet énoncé est unique à isomorphisme près.

#### Exercice 4

Soient  $\mu_{\ell}$  le groupe des racines  $\ell$ -ièmes de l'unité dans  $\overline{\mathbb{Q}}$  et  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$  le caractère donnant l'action de  $G_{\mathbb{Q}}$  sur  $\mu_{\ell}$ . Notons  $\det(\rho_{f,\ell}) : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$  le caractère qui à  $\sigma \in G_{\mathbb{Q}}$  associe le déterminant de  $\rho_{f,\ell}(\sigma)$ .

- 1) Montrer que l'on a  $\det(\rho_{f,\ell}) = \chi^{k-1}$ .
- 2) Soit  $c$  la conjugaison complexe de  $G_{\mathbb{Q}}$ . En déduire que l'on a  $\det(\rho_{f,\ell})(c) = -1$ , autrement dit, que  $\rho_{f,\ell}$  est une représentation impaire.

## 2. Description de l'image de $\rho_{f,\ell}$

On va s'intéresser dans ce paragraphe à l'image de  $\rho_{f,\ell}$  en rappelant, sans démonstration, les résultats connus à ce sujet. Soit  $\text{SL}_2(\mathbb{F}_{\ell})$  le sous-groupe de  $\text{GL}_2(\mathbb{F}_{\ell})$  formé des matrices de déterminant 1. Tout d'abord, l'image de  $\rho_{f,\ell}$  est presque toujours aussi grosse que possible. Plus précisément :

**Théorème 2.** *Pour presque tout  $\ell$  (au sens tous sauf un nombre fini) l'image de  $\rho_{f,\ell}$  contient  $\text{SL}_2(\mathbb{F}_{\ell})$ .*

#### Exercice 5

Supposons que l'image  $G_{\ell}$  de  $\rho_{f,\ell}$  contienne  $\text{SL}_2(\mathbb{F}_{\ell})$ .

- 1) Montrer que  $G_{\ell}$  est le sous-groupe de  $\text{GL}_2(\mathbb{F}_{\ell})$  formé des éléments dont le déterminant est une puissance  $k-1$ -ième dans  $\mathbb{F}_{\ell}^*$ .
- 2) En déduire une condition nécessaire et suffisante pour que  $G_{\ell} = \text{GL}_2(\mathbb{F}_{\ell})$ .

**Définition.** *On dira que  $\ell$  est exceptionnel pour  $f$  si l'image de  $\rho_{f,\ell}$  ne contient pas  $\text{SL}_2(\mathbb{F}_{\ell})$ .*

D'après le théorème 2, l'ensemble des nombres premiers exceptionnels pour  $f$  est fini. Il se pose alors naturellement le problème de déterminer cet ensemble. Dans le cas où  $\ell$  est exceptionnel pour  $f$ , on va décrire dans la suite les différentes possibilités pour l'image de  $\rho_{f,\ell}$ .

## 2.1. Sous-groupes de Cartan

Considérons un plan vectoriel  $V$  sur  $\mathbb{F}_\ell$ . Soient  $\text{End}(V)$  la  $\mathbb{F}_\ell$ -algèbre des endomorphismes de  $V$ , qui est de dimension 4 sur  $\mathbb{F}_\ell$ , et  $\text{GL}(V)$  son groupe des éléments inversibles, qui est d'ordre  $(\ell^2 - 1)(\ell^2 - \ell)$ . On va définir la notion de sous-groupe de Cartan de  $\text{GL}(V)$ . Rappelons que le polynôme minimal d'un élément  $g \in \text{GL}(V)$ , qui n'est pas une homothétie, est de degré 2 et coïncide avec son polynôme caractéristique  $X^2 - \text{Tr}(g)X + \det(g) \in \mathbb{F}_\ell[X]$ . Un élément de  $\text{GL}(V)$  est dit semi-simple si son polynôme minimal est séparable. Dans ce cas, il est irréductible sur  $\mathbb{F}_\ell$  ou bien est de la forme  $(X - a)(X - b)$ , où  $a$  et  $b$  sont deux éléments distincts de  $\mathbb{F}_\ell$ .

### Exercice 6

Montrer qu'un élément de  $\text{GL}(V)$  est semi-simple si et seulement si son ordre est premier à  $\ell$ .

### Exercice 7

Soient  $g$  un élément de  $\text{GL}(V)$  qui ne soit pas une homothétie et  $k$  le commutant de  $g$  dans  $\text{End}(V)$ .

1) Montrer que l'on a  $k = \mathbb{F}_\ell[g]$ .

Supposons  $g$  semi-simple. Soit  $P$  le polynôme minimal de  $g$ .

2) Si  $P$  réductible sur  $\mathbb{F}_\ell$ , montrer que  $k$  est isomorphe à  $\mathbb{F}_\ell \times \mathbb{F}_\ell$ .

3) Si  $P$  est irréductible sur  $\mathbb{F}_\ell$ , montrer que  $k$  est un corps isomorphe à  $\mathbb{F}_{\ell^2}$ .

4) En déduire l'ordre du centralisateur de  $g$  dans  $\text{GL}(V)$  dans les deux cas ci-dessus.

Cela motive la définition suivante :

**Définition.** Soit  $H$  un sous-groupe de  $\text{GL}(V)$ . On dit que  $H$  est un sous-groupe de Cartan de  $\text{GL}(V)$  s'il existe un élément semi-simple  $g \in \text{GL}(V)$ , qui ne soit pas une homothétie, tel que  $H$  soit le centralisateur de  $g$ . On dit que  $H$  est déployé ou non déployé suivant que le commutant de  $g$  dans  $\text{End}(V)$  soit isomorphe à  $\mathbb{F}_\ell \times \mathbb{F}_\ell$  ou à  $\mathbb{F}_{\ell^2}$ .

D'après l'exercice 7, un sous-groupe de Cartan de  $\text{GL}(V)$  est isomorphe à  $\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$  s'il est déployé ou à  $\mathbb{F}_{\ell^2}^*$  s'il est non déployé. Il est en particulier abélien d'ordre respectivement  $(\ell - 1)^2$  ou  $\ell^2 - 1$ .

### Exercice 8

1) Si  $\ell = 2$ , montrer qu'il n'existe pas de sous-groupes de Cartan déployés dans  $\text{GL}(V)$ .

Supposons  $\ell \geq 3$ .

2) Soient  $D$  et  $D'$  deux droites distinctes de  $V$ . Montrer que le fixateur de  $\{D, D'\}$  sous  $\text{GL}(V)$  est un sous-groupe de Cartan déployé de  $\text{GL}(V)$ .



- 3) Soit  $H$  un sous-groupe de Cartan déployé de  $\mathbb{GL}(V)$ . Montrer qu'il existe exactement deux droites  $D_1$  et  $D_2$  de  $V$  telles que  $H$  soit le fixateur de  $\{D_1, D_2\}$ .
- 4) Montrer que l'ensemble des sous-groupes de Cartan déployés de  $\mathbb{GL}(V)$  forme une classe de conjugaison.
- 5) Quel est le nombre de sous-groupes de Cartan déployés de  $\mathbb{GL}(V)$  ?

### Exercice 9

- 1) Montrer que les sous-groupes de Cartan non déployés de  $\mathbb{GL}(V)$  sont exactement les groupes multiplicatifs des sous-algèbres de  $\text{End}(V)$  qui sont des corps de cardinal  $\ell^2$ .
- 2) Soit  $P$  un polynôme unitaire de degré 2 dans  $\mathbb{F}_\ell[X]$ . Montrer que l'ensemble des éléments de  $\mathbb{GL}(V)$  ayant  $P$  pour polynôme minimal forme une classe de conjugaison.
- 3) En déduire que l'ensemble des sous-groupes de Cartan non déployés de  $\mathbb{GL}(V)$  forme une classe de conjugaison.
- 4) Quel est le nombre de sous-groupes de Cartan non déployés de  $\mathbb{GL}(V)$  ? (Utiliser le fait que l'ordre du normalisateur d'un sous-groupe de Cartan non déployé est  $2(\ell^2 - 1)$ . Cette assertion est démontrée dans l'exercice 12.)

On définit alors les sous-groupes de Cartan de  $\mathbb{GL}_2(\mathbb{F}_\ell)$  en identifiant ce groupe à  $\mathbb{GL}(V)$  par le choix d'une base de  $V$  sur  $\mathbb{F}_\ell$ . Il existe en fait des représentants privilégiés des deux classes de conjugaison de sous-groupes de Cartan de  $\mathbb{GL}_2(\mathbb{F}_\ell)$ .

1) Si  $\ell \geq 3$ , les sous-groupes de Cartan déployés de  $\mathbb{GL}_2(\mathbb{F}_\ell)$  sont les conjugués du sous-groupe constitué des éléments de la forme

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Ce dernier est appelé le sous-groupe de Cartan déployé standard de  $\mathbb{GL}_2(\mathbb{F}_\ell)$ .

2) En ce qui concerne le cas non déployé : il existe un unique sous-groupe de Cartan non déployé de  $\mathbb{GL}_2(\mathbb{F}_2)$  qui est son sous-groupe d'ordre 3. Supposons  $\ell \geq 3$ . Pour chaque élément de  $\mathbb{F}_\ell$  qui n'est pas un carré, on peut lui associer un sous-groupe de Cartan non déployé de  $\mathbb{GL}_2(\mathbb{F}_\ell)$ . On procède comme suit. Posons  $V = \mathbb{F}_{\ell^2}$ . La représentation régulière du  $\mathbb{F}_\ell$ -espace  $V$  est un isomorphisme de  $\mathbb{F}_{\ell^2}$  sur une sous-algèbre  $k$  de  $\text{End}(V)$  et  $k^*$  est donc un sous-groupe de Cartan non déployé de  $\mathbb{GL}(V)$ . Soient  $\alpha \in \mathbb{F}_\ell$  qui ne soit pas un carré dans  $\mathbb{F}_\ell$  et  $t \in \mathbb{F}_{\ell^2}$  tels que  $\alpha = t^2$ . Au moyen de la base  $(1, t)$  du  $\mathbb{F}_\ell$ -espace vectoriel  $V$ , on constate que  $k^*$  s'identifie au sous-groupe  $C_\alpha$  de  $\mathbb{GL}_2(\mathbb{F}_\ell)$  formé des matrices

$$\begin{pmatrix} a & b\alpha \\ b & a \end{pmatrix},$$

où  $a, b \in \mathbb{F}_\ell$  ne sont pas tous deux nuls. On dit que  $C_\alpha$  est le sous-groupe de Cartan non déployé standard de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  associé à  $\alpha$ .

### Exercice 10

Soient  $\alpha$  et  $\beta$  deux éléments de  $\mathbb{F}_\ell$  qui ne sont pas des carrés. Démontrer directement que les sous-groupes  $C_\alpha$  et  $C_\beta$  sont conjugués dans  $\mathrm{GL}_2(\mathbb{F}_\ell)$ .

## 2.2. Normalisateurs des sous-groupes de Cartan

Soit  $C$  un sous-groupe de Cartan de  $\mathrm{GL}(V)$ . Si  $H$  est déployé, on suppose  $\ell \geq 3$ . Notons  $N$  son normalisateur dans  $\mathrm{GL}(V)$ .

### Exercice 11

Supposons  $C$  déployé. Soient  $D_1$  et  $D_2$  les deux droites de  $V$  telles que  $C$  soit le fixateur de  $\{D_1, D_2\}$  (exercice 8).

- 1) Montrer que  $N - C$  est formé des éléments  $s \in \mathrm{GL}(V)$  tels que  $sD_1 = D_2$  et  $sD_2 = D_1$ .
- 2) En déduire que  $C$  est d'indice 2 dans  $N$ .
- 3) En déduire que le complémentaire du sous-groupe de Cartan déployé standard de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  dans son normalisateur est l'ensemble des matrices de la forme  $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$ .

### Exercice 12

Supposons  $C$  non déployé. On a  $C = k^*$  où  $k$  est une sous-algèbre de  $\mathrm{End}(V)$  qui est un corps à  $\ell^2$  éléments (exercice 9). Soit  $F$  le Frobenius de  $k$  i.e. l'automorphisme de  $k$  qui à  $x$  associe  $x^\ell$ .

- 1) Soit  $g$  un générateur de  $k^*$ . Montrer que  $g$  et  $F(g)$  ont le même polynôme minimal comme endomorphismes de  $V$ .
- 2) En déduire que  $g$  et  $F(g)$  sont conjugués dans  $\mathrm{GL}(V)$ .
- 3) Soit  $\phi : N \rightarrow \mathrm{Aut}(k)$  l'application qui à  $s$  associe l'automorphisme de  $k$  défini par  $u \mapsto sus^{-1}$ . Montrer que  $s$  est un morphisme de groupes surjectif. Déterminer le noyau de  $\phi$ . En déduire que  $C$  est d'indice 2 dans  $N$ .

Le plan  $V$  est muni d'une structure de  $k$ -espace vectoriel de dimension 1 donnée par  $(u, x) \in k \times V \mapsto u(x)$ .

- 4) Montrer que les automorphismes  $k$ -linéaires de  $V$  sont les éléments de  $C$ .
- 5) Montrer que  $N - C$  est formé des éléments  $s \in \mathrm{GL}(V)$  tels que pour tous  $x \in V$  et  $u \in k$ , on ait  $s(u.x) = u^p.s(x)$ . Autrement dit,  $N - C$  est constitué des éléments de  $\mathrm{GL}(V)$  qui sont semi-linéaires pour la structure du  $k$ -espace vectoriel  $V$ .
- 6) Soit  $\alpha$  un élément de  $\mathbb{F}_\ell$  qui n'est pas un carré dans  $\mathbb{F}_\ell$ . Soit  $N_\alpha$  le normalisateur du sous-groupe  $C_\alpha$  de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  défini ci-dessus. Montrer que les matrices de  $N_\alpha$  qui ne

sont pas dans  $C_\alpha$  sont celles de la forme  $\begin{pmatrix} a & -b\alpha \\ b & -a \end{pmatrix}$ , où  $a, b \in \mathbb{F}_\ell$  ne sont pas tous deux nuls.

### Exercice 13

Montrer que les éléments de  $N - C$  ont une trace nulle.

### 2.3. L'image de $\rho_{f,\ell}$ si $\ell$ est exceptionnel

Soit  $\mathrm{PGL}_2(\mathbb{F}_\ell)$  le groupe  $\mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^*$ . La description de l'image de  $\rho_{f,\ell}$  se déduit de la classification des sous-groupes de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  que l'on peut trouver dans [Se2]. Rappelons à ce sujet le résultat suivant concernant les sous-groupes de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  d'ordre premier à  $\ell$ .

**Proposition.** *Soit  $H$  un sous-groupe de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  d'ordre premier à  $\ell$ . On est dans l'un des cas suivants :*

- 1)  $H$  est contenu dans le normalisateur d'un sous-groupe de Cartan.
- 2) L'image de  $H$  dans  $\mathrm{PGL}_2(\mathbb{F}_\ell)$  est isomorphe à  $\mathbb{A}_4$ ,  $\mathbb{S}_4$  ou  $\mathbb{A}_5$ .

On en déduit l'énoncé suivant (cf. *loc. cit.*) :

**Théorème 3.** *Supposons que  $\ell$  soit exceptionnel pour  $f$ . On est dans l'un des cas suivants :*

- 1) la représentation  $\rho_{f,\ell}$  est réductible.
- 2) L'image de  $\rho_{f,\ell}$  est contenue dans le normalisateur d'un sous-groupe de Cartan  $C$  de  $\mathrm{GL}_2(\mathbb{F}_\ell)$  sans être contenue dans  $C$ .
- 3) L'image de  $\rho_{f,\ell}$  dans  $\mathrm{PGL}_2(\mathbb{F}_\ell)$  est isomorphe à  $\mathbb{S}_4$ .

L'exercice qui suit est une réciproque du théorème 3.

### Exercice 14

- 1) Si  $\rho_{f,\ell}$  est réductible montrer que  $\ell$  est exceptionnel pour  $f$ .
- 2) Supposons que  $\rho_{f,\ell}$  vérifie la condition 2 du théorème. Montrer que  $\ell$  est exceptionnel pour  $f$  si et seulement si  $\ell \neq 2$ .
- 3) Supposons que  $\rho_{f,\ell}$  vérifie la condition 3. Montrer que  $\ell$  est exceptionnel pour  $f$  si et seulement si  $\ell \neq 3$  (on pourra utiliser le fait que le sous-groupe dérivé de  $\mathrm{GL}_2(\mathbb{F}_3)$  est  $\mathrm{SL}_2(\mathbb{F}_3)$ ).

### Exercice 15

Démontrer directement les deux assertions suivantes :

- 1) si  $\ell$  est impair, l'image de  $\rho_{f,\ell}$  n'est pas contenue dans un sous-groupe de Cartan non déployé.
- 2) L'image de  $\rho_{f,\ell}$  dans  $\mathrm{PGL}_2(\mathbb{F}_\ell)$  n'est pas isomorphe à  $\mathbb{A}_4$  ni  $\mathbb{A}_5$ .

### Exercice 16

On admettra pour la question 1 que toute extension abélienne de degré fini de  $\mathbb{Q}$  est contenue dans un corps cyclotomique (cf. [Wa], p. 319).

1) Montrer que les conditions suivantes sont équivalentes :

- (i) la représentation  $\rho_{f,\ell}$  est réductible.
- (ii) Il existe un entier  $m \geq 0$  tel que  $\rho_{f,\ell}$  soit représentable sous la forme

$$\begin{pmatrix} \chi^m & 0 \\ 0 & \chi^{k-1-m} \end{pmatrix},$$

où  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$  est le caractère cyclotomique donnant l'action de  $G_{\mathbb{Q}}$  sur le groupe des racines  $\ell$ -ièmes de l'unité.

- (iii) Il existe un entier  $m \geq 0$  tel que pour tout nombre premier  $p \neq \ell$  on ait

$$(2) \quad a_p \equiv p^m + p^{k-1-m} \pmod{\ell}.$$

2) Supposons que l'on soit dans le deuxième cas du théorème 3 et que l'on ait  $\ell \geq 3$ . Montrer que pour tout nombre premier  $p \neq \ell$  on a l'implication

$$(3) \quad \left(\frac{p}{\ell}\right) = -1 \implies a_p \equiv 0 \pmod{\ell}.$$

3) Supposons que l'on soit dans le troisième cas du théorème 3. Montrer que pour tout nombre premier  $p \neq \ell$  on a

$$(4) \quad \frac{a_p^2}{p^{k-1}} \equiv 0, 1, 2, 4 \pmod{\ell}.$$

L'ensemble des nombres exceptionnels peut en principe être déterminé. En fait la démonstration du théorème 2 est effective, autrement dit elle fournit une majoration explicite des nombres premiers exceptionnels pour  $f$  ([Sw] et [Se3]). Tout d'abord, remarquons qu'il est facile majorer les nombres premiers  $\ell$  pour lesquels la congruence (4) soit réalisée. En effet, il suffit de choisir un nombre premier  $p \geq 3$  tel que  $a_p \neq 0$ . En posant  $\nu = 0, 1, 2$  ou 4, on a (cf. la valuation en  $p$  et le fait que  $k$  soit pair)

$$a_p^2 - \nu p^{k-1} \neq 0,$$

et  $\ell$  divise cet entier. On a par ailleurs le résultat suivant (*loc. cit.*) :

**Théorème 4.**

- 1) Si  $\rho_{f,\ell}$  est réductible, on a  $\ell < k$ , ou bien  $\ell$  divise le numérateur du  $k$ -ième nombre de Bernoulli  $B_k$ .
- 2) Si pour tout nombre premier  $p \neq \ell$  l'implication (3) est satisfaite, on a  $\ell < 2k$ .

On va illustrer dans le reste de ces notes les résultats précédents avec la fonction de Ramanujan pour laquelle  $k = 12$ . On va déterminer les nombres premiers exceptionnels qui lui sont associés et les représentations galoisiennes correspondantes.

**3. La fonction  $\Delta$  de Ramanujan**

Rappelons qu'il s'agit de la fonction définie pour tout  $z \in \mathfrak{H}$  par le produit

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} \quad \text{où} \quad q = e^{2\pi iz}.$$

À un facteur constant près,  $\Delta$  est l'unique forme modulaire de  $S_{12}$ . Son développement de Fourier à l'infini,

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

est normalement convergent sur tout demi-plan  $\Im(z) \geq T > 0$  de  $\mathfrak{H}$ . Pour tout entier  $n \geq 1$ ,  $\tau(n)$  est le coefficient de  $q^n$  dans le produit

$$q \prod_{j=1}^m (1 - q^j)^{24},$$

ceci pour tout entier  $m \geq n$ . On a ainsi

$$(5) \quad \Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + \dots$$

Pour chaque nombre premier  $p$ ,  $\Delta$  est fonction propre des opérateurs de Hecke  $T_n$  avec pour valeur propre  $\tau(n)$ . Cela entraîne les formules

$$(6) \quad \tau(mn) = \tau(m)\tau(n) \quad \text{si} \quad \text{pgcd}(m, n) = 1,$$

$$(7) \quad \tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1}) \quad \text{si } p \text{ est premier.}$$

Par ailleurs, on a

$$\tau(n) = O(n^6).$$

On a en fait un résultat plus précis. En effet, Deligne a démontré la conjecture de Ramanujan selon laquelle pour tout nombre premier  $p$ , on a

$$|\tau(p)| < 2p^{11/2}.$$

La série de Dirichlet associée à  $\Delta$ ,

$$\Phi(s) = \sum_{n \geq 1} \frac{\tau(n)}{n^s},$$

est absolument convergente dès que  $\Re(s) > 7$ . Dans cette région, on a un développement en produit Eulérien

$$\Phi(s) = \prod_{p \text{ premier}} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}},$$

qui se prolonge en une fonction holomorphe dans tout le plan complexe.

Signalons la conjecture de Lehmer (1947) sur les coefficients de Fourier de  $\Delta$  ([Le]) :

**Conjecture.** *Pour tout  $n \geq 1$ , on a  $\tau(n) \neq 0$ .*

Il se trouve dans [Se5] une démonstration du fait que tel est le cas pour  $n \leq 10^{15}$ .

#### 4. Séries d'Eisenstein

Soit  $k$  un entier pair  $\geq 4$ . Notons  $M_k$  le  $\mathbb{C}$ -espace vectoriel des formes modulaires de poids  $k$  pour  $\mathbb{SL}_2(\mathbb{Z})$ . C'est un  $\mathbb{C}$ -espace vectoriel de dimension finie. On a

$$\dim M_k = \begin{cases} \left[ \frac{k}{12} \right] & \text{si } k \equiv 2 \pmod{12} \\ \left[ \frac{k}{12} \right] + 1 & \text{si } k \not\equiv 2 \pmod{12}. \end{cases}$$

La multiplication par  $\Delta$  induit un isomorphisme de  $\mathbb{C}$ -espaces vectoriels de  $M_{k-12}$  sur  $S_k$ . En effet, l'application  $M_{k-12} \rightarrow S_k$  qui à  $f$  associe  $\Delta f$  est  $\mathbb{C}$ -linéaire. Elle est injective car  $\Delta$  est partout non nulle sur  $\mathfrak{H}$ . Par ailleurs, si  $g \in S_k$ , la fonction  $g/\Delta$  appartient à  $M_{k-12}$ , d'où l'assertion.

##### Exercice 17

Déterminer le polynôme caractéristique de l'opérateur de Hecke  $T_2$  agissant sur  $S_{24}$ .

La série d'Eisenstein  $G_k$  de poids  $k$  est définie pour tout  $z \in \mathfrak{H}$ , par l'égalité

$$G_k(z) = \sum' \frac{1}{(m + nz)^k},$$

où le symbole  $\sum'$  signifie que la sommation porte sur les couples  $(m, n) \neq (0, 0)$ .

##### Exercice 18

Montrer que cette série est normalement convergente dans toute bande verticale de la forme  $\{x + iy ; |x| \leq A, y \geq \delta > 0\}$  et en déduire que  $G_k$  est une fonction holomorphe sur  $\mathfrak{H}$ .

En fait,  $G_k$  appartient à  $M_k$  et l'on a

$$M_k = S_k \bigoplus \mathbb{C}.G_k.$$

Par ailleurs, le  $\mathbb{C}$ -espace  $M_k$  admet pour base la famille des monômes  $G_4^a G_6^b$  où  $a$  et  $b$  sont des entiers naturels tels que  $4a + 6b = k$ . Posons pour tous  $j$  et  $n \geq 1$

$$\sigma_j(n) = \sum_{d|n} d^j.$$

Soit  $B_k$  le  $k$ -ième nombre de Bernoulli, qui est défini à partir du développement (valable pour  $0 < |z| < 2\pi$ )

$$\frac{z}{e^z - 1} = \sum_{n \geq 1} \frac{B_n}{n!} z^n.$$

Les  $B_n$  sont dans  $\mathbb{Q}$ , on a  $B_{2n+1} = 0$  pour tout  $n \geq 1$  et l'on vérifie que

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, \dots, B_{12} = -\frac{691}{2730}, \dots, B_{16} = -\frac{3617}{510} \dots$$

Notons  $\zeta$  la fonction zeta de Riemann classique. Pour tout  $z \in \mathfrak{H}$ , on a

$$G_k(z) = 2\zeta(k) \left( 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n \right).$$

On normalise  $G_k$  en posant

$$E_k(z) = \frac{G_k(z)}{2\zeta(k)}.$$

On a les développements suivants :

$$(8) \quad E_4(z) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n, \quad E_6(z) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n,$$

$$(9) \quad E_8(z) = 1 + 480 \sum_{n \geq 1} \sigma_7(n) q^n, \quad E_{10}(z) = 1 - 264 \sum_{n \geq 1} \sigma_9(n) q^n,$$

$$(10) \quad E_{12}(z) = 1 + \frac{65520}{691} \sum_{n \geq 1} \sigma_{11}(n) q^n.$$

On a la formule de Jacobi :

$$(11) \quad E_4^3 - E_6^2 = 1728\Delta.$$

Rappelons que l'on dispose aussi d'une fonction  $E_2$  définie pour  $z \in \mathfrak{H}$  par l'égalité

$$(12) \quad E_2(z) = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n.$$

La fonction  $E_2$  est holomorphe sur  $\mathfrak{H}$ . Elle n'est pas modulaire et vérifie l'équation fonctionnelle

$$(13) \quad E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{6z}{\pi i} \quad \text{pour } z \in \mathfrak{H}.$$





## Chapitre II — Congruences relatives à $\Delta$

On va expliciter dans ce chapitre des congruences satisfaites par les coefficients de Fourier de  $\Delta$ . Les nombres premiers intervenant dans ces congruences sont précisément ceux qui sont exceptionnels pour  $\Delta$ .

### 1. Congruences modulo $2^3$ , $3^3$ , $5^2$ , 7 et 691

Le premier exercice fournit une application linéaire de  $M_k$  dans  $M_{k+2}$ , dont la restriction à  $S_k$  a une image contenue dans  $S_{k+2}$ .

#### Exercice 1

Soient  $k$  un entier naturel et  $f$  une forme modulaire de  $M_k$ . Pour tout  $z \in \mathfrak{H}$ , on pose

$$g(z) = \frac{1}{2\pi i} f'(z) - \frac{k}{12} E_2(z) f(z).$$

- 1) Montrer que  $g$  appartient à  $M_{k+2}$ .
- 2) Montrer que  $f$  est parabolique si et seulement si tel est le cas de  $g$ .

#### Exercice 2

Démontrer les égalités suivantes (où  $q = e^{2\pi iz}$ ,  $z \in \mathfrak{H}$ ) :

$$(1) \quad E_2 E_4 - E_6 = 720 \sum_{n \geq 1} n \sigma_3(n) q^n,$$

$$(2) \quad E_4^2 - E_2 E_6 = 1008 \sum_{n \geq 1} n \sigma_5(n) q^n.$$

Dans chacun des exercices 3 à 6 qui suivent, il figure une proposition concernant une congruence pour  $\Delta$ . L'exercice en fournit une démonstration.

#### Exercice 3 - Congruences de $\tau(n)$ modulo 8

**Proposition.** Pour tout  $n \geq 1$ , on a

$$(1) \quad \tau(n) \equiv \sigma_1(n) \pmod{8} \quad \text{si} \quad n \equiv 1 \pmod{2},$$

$$(2) \quad \tau(n) \equiv 0 \pmod{8} \quad \text{si} \quad n \equiv 0 \pmod{2}.$$

En particulier, pour tout nombre premier  $p$  impair, on a  $\tau(p) \equiv 1 + p \pmod{8}$ .

1) Pour tout  $n \geq 1$ , montrer l'égalité

$$(3) \quad \sigma_7(n) = \sigma_3(n) + 120 \sum_{k=1}^{n-1} \sigma_3(k) \sigma_3(n-k).$$

Considérons les  $q$ -développements des fonctions  $E_4^3$  et  $E_6^2$  :

$$E_4^3 = 1 + \sum_{n \geq 1} a_n q^n \quad \text{et} \quad E_6^2 = 1 + \sum_{n \geq 1} b_n q^n \quad (a_n, b_n \in \mathbb{Z}).$$

2) Pour tout  $n \geq 1$ , montrer que l'on a

$$(4) \quad a_n \equiv 208(2\sigma_7(n) - \sigma_3(n)) \pmod{2^9},$$

$$(5) \quad b_n \equiv 16 \sigma_5(n) + \frac{8}{15}(\sigma_7(n) - \sigma_3(n)) \pmod{2^9}.$$

3) En déduire la congruence (1).

4) Démontrer par récurrence la congruence (2).

#### Exercice 4 - Congruences de $\tau(n)$ modulo 27

**Proposition.** Pour tout entier  $n \geq 1$ , on a

$$\tau(n) \equiv n^2 \sigma_7(n) \pmod{27}.$$

En particulier, pour tout nombre premier  $p$ , on a  $\tau(p) \equiv p^2 + p^9 \pmod{27}$ .

1) Soient  $E_8''$  la fonction dérivée seconde de  $E_8$  et  $E_4'$  la fonction dérivée de  $E_4$ . Démontrer que  $2E_8'' - 9E_4'^2$  appartient à  $S_{12}$ .

2) En déduire l'égalité

$$\sum_{n \geq 1} n^2 \sigma_7(n) q^n = \Delta + 540 \left( \sum_{n \geq 1} n \sigma_3(n) q^n \right)^2.$$

3) En déduire la proposition.

#### Exercice 5 - Congruences de $\tau(n)$ modulo 25

**Proposition.** Pour tout  $n \geq 1$ , on a

$$\tau(n) \equiv n \sigma_9(n) \pmod{25}.$$

En particulier, pour tout nombre premier  $p$ , on a  $\tau(p) \equiv p + p^{10} \pmod{25}$ .

- 1) Montrer qu'une base du  $\mathbb{C}$ -espace vectoriel  $M_{12}$  est  $(\Delta, E_4^3)$ .
- 2) En utilisant l'exercice 1, en déduire l'égalité

$$2(E_4^3 - E_6^2) = -1584 \sum_{n \geq 1} n \sigma_9(n) q^n + 5E_4^3 - 5E_2 E_4 E_6.$$

- 3) En utilisant l'égalité (2) de l'exercice 2, en déduire la proposition.

### Exercice 6 - Congruences de $\tau(n)$ modulo 7

**Proposition.** Pour tout entier  $n \geq 1$ , on a

$$\tau(n) \equiv n \sigma_3(n) \pmod{7}.$$

En particulier, pour tout nombre premier  $p$ , on a  $\tau(p) \equiv p + p^4 \pmod{7}$ .

Posons

$$E_4^2 = \sum_{n \geq 0} a_n q^n \quad \text{et} \quad E_4^3 = \sum_{n \geq 0} b_n q^n \quad (a_n, b_n \in \mathbb{Z}).$$

- 1) Montrer que l'on a  $a_n \equiv 4\sigma_1(n) \pmod{7}$ .
- 2) En utilisant l'égalité (1) de l'exercice 2, en déduire que l'on a  $b_n \equiv 6n\sigma_3(n) \pmod{7}$ .
- 3) En déduire la proposition.
- 4) Montrer que si  $n \equiv 0, 3, 5 \pmod{7}$ , alors  $\tau(n)$  est multiple de 7.

### Exercice 7 - Congruences de $\tau(n)$ modulo 691

En utilisant le fait que  $(E_{12}, \Delta)$  est une base du  $\mathbb{C}$ -espace vectoriel  $M_{12}$ , démontrer que pour tout  $n \geq 1$ , on a

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

## 2. Formule du produit triple de Jacobi

Il s'agit de la formule suivante due à Jacobi (1828) :

**Théorème 1.** Soient  $q \in \mathbb{C}$  tel que  $|q| < 1$  et  $w \in \mathbb{C}^*$ . On a l'égalité

$$\sum_{m \in \mathbb{Z}} q^{m^2} w^m = \prod_{n \geq 1} (1 - q^{2n})(1 + q^{2n-1}w)(1 + q^{2n-1}w^{-1}).$$

L'exercice qui suit en fournit une démonstration (cf. [Ha-Wr], p. 282 et [Go], p. 303).

### Exercice 8

- 1) Vérifier l'énoncé du théorème si  $q = 0$ .

On supposera désormais  $q$  non nul.

- 2) Montrer que la série  $\sum_{m \in \mathbb{Z}} q^{m^2} w^m$  est convergente en vrac, autrement dit que la famille  $(q^{m^2} w^m)_{m \in \mathbb{Z}}$  est absolument sommable.

- 3) Montrer que le produit est convergent.

Notons  $A(q, w)$  le produit et  $J(q, w)$  la série.

- 4) Pour  $q$  fixé, vérifier que la fonction définie sur  $\mathbb{C}^*$  par  $w \mapsto A(q, w)$  est holomorphe.

On en déduit un développement en série de Laurent pour tout  $w \in \mathbb{C}^*$

$$A(q, w) = \sum_{n \in \mathbb{Z}} a_n(q) w^n \quad (a_n(q) \in \mathbb{C}).$$

- 5) Vérifier que l'on a  $qwA(q, q^2w) = A(q, w)$ .

- 6) En déduire que pour tout  $n \in \mathbb{Z}$ , on a  $a_n(q) = q^{n^2} a_0(q)$  puis l'égalité

$$A(q, w) = a_0(q) J(q, w).$$

Tout revient donc à prouver que  $a_0(q) = 1$ .

- 7) Soit  $B$  la boule ouverte de centre 0 et de rayon  $1/2$ . Soit  $w \in \mathbb{C}^*$  fixé. Montrer que les fonctions

$$q \mapsto J(q, w) \quad \text{et} \quad q \mapsto A(q, w),$$

sont continues sur  $B$ . En déduire que l'on a

$$\lim_{q \rightarrow 0} a_0(q) = 1.$$

- 8) Montrer que l'on a

$$J(q, i) = J(q^4, -1) \quad \text{et} \quad A(q, i) = A(q^4, -1).$$

- 9) En déduire que  $a_0(q) = a_0(q^4)$  et le théorème.

On déduit du théorème le résultat suivant qui est dû à Euler :

**Corollaire.** *Pour tout nombre complexe  $q$  tel que  $|q| < 1$ , on a*

$$\prod_{n \geq 1} (1 - q^n) = \sum_{n \in \mathbb{Z}} (-1)^n q^{(3n^2+n)/2}.$$

Il suffit en effet de remplacer  $q$  par  $q^{3/2}$  et  $w$  par  $-q^{1/2}$  dans l'énoncé du théorème pour obtenir le corollaire.

### Exercice 9

Démontrer que pour tout nombre complexe  $q$  tel que  $|q| < 1$ , on a

$$\prod_{n \geq 1} (1 - q^n)^3 = \sum_{n \geq 0} (-1)^n (2n + 1) q^{n(n+1)/2}.$$

## 3. Congruences modulo 23

L'objectif de ce paragraphe est de démontrer le résultat suivant (cf. [Wi]) :

**Théorème 2.** *Soit  $p$  un nombre premier distinct de 23. On a*

$$\begin{cases} \tau(p) \equiv 0 \pmod{23} & \text{si } \left(\frac{p}{23}\right) = -1 \\ \tau(p) \equiv 2 \pmod{23} & \text{si } p \text{ est de la forme } x^2 + 23y^2 \\ \tau(p) \equiv -1 \pmod{23} & \text{si } \left(\frac{p}{23}\right) = 1 \text{ et } p \text{ n'est pas de la forme } x^2 + 23y^2. \end{cases}$$

Signalons que l'on a  $\tau(23) = 18643272$  qui est congru à 1 modulo 23. Commençons par rappeler quelques propriétés de l'anneau d'entiers du corps  $\mathbb{Q}(\sqrt{-23})$ .

### 3.1. Sur l'anneau d'entiers du corps $\mathbb{Q}(\sqrt{-23})$

Soit  $\omega = \sqrt{-23}$  une racine carrée de  $-23$ . Posons  $K = \mathbb{Q}(\omega)$  et notons  $A$  l'anneau d'entiers de  $K$ .

1) Une  $\mathbb{Z}$ -base de  $A$  est  $\left(1, \frac{1+\omega}{2}\right)$ . L'anneau  $A$  est l'ensemble des éléments de la forme  $\frac{a+b\omega}{2}$ , où  $a$  et  $b$  sont des entiers relatifs de même parité.

2) Le discriminant de  $K$  est  $-23$ , de sorte que 23 est le seul nombre premier ramifié dans  $K$ .

3) Le groupe des unités de  $A$  est  $\{\pm 1\}$ .

4) Le nombre de classes de  $K$  est 3.

5) Les nombres premiers 2 et 3 sont décomposés dans  $A$ . On a

$$(1) \quad 2A = \mathfrak{P}_2 \mathfrak{P}'_2 \quad \text{et} \quad 3A = \mathfrak{P}_3 \mathfrak{P}'_3,$$

où

$$\mathfrak{P}_2 = \left(2, \frac{1+\omega}{2}\right), \quad \mathfrak{P}'_2 = \left(2, \frac{1-\omega}{2}\right), \quad \mathfrak{P}_3 = \left(3, \frac{1-\omega}{2}\right), \quad \mathfrak{P}'_3 = \left(3, \frac{1+\omega}{2}\right).$$

Vérifions la première égalité de (1). On remarque pour cela que  $\mathfrak{P}_2\mathfrak{P}'_2 = (4, 1-\omega, 1+\omega, 6)$ . Par ailleurs,  $1-\omega$  et  $1+\omega$  appartiennent à  $2A$ , donc  $\mathfrak{P}_2\mathfrak{P}'_2$  est contenu dans  $2A$ . Inversement  $2$  appartient à  $\mathfrak{P}_2\mathfrak{P}'_2$ , d'où l'assertion. La preuve de la deuxième égalité est la même.

6) Les idéaux  $\mathfrak{P}_2$  et  $\mathfrak{P}_3$  ne sont pas principaux (donc il en est de même de  $\mathfrak{P}'_2$  et  $\mathfrak{P}'_3$ ). En effet, supposons par exemple que  $\mathfrak{P}_2$  soit principal. Il existe deux entiers  $a$  et  $b$  de même parité tels que l'on ait

$$\mathfrak{P}_2 = \left( \frac{a + b\omega}{2} \right).$$

La norme de  $K$  sur  $\mathbb{Q}$  de  $\mathfrak{P}_2$  est 2. Il en résulte que  $a^2 + 23b^2 = 8$ , ce qui conduit à une contradiction. La démonstration est la même en ce qui concerne l'idéal  $\mathfrak{P}_3$ . On en déduit que la classe de  $\mathfrak{P}_2$  (ou de  $\mathfrak{P}_3$ ) est un générateur du groupe des classes de  $K$ .

7) Les classes de  $\mathfrak{P}_2$  et  $\mathfrak{P}_3$  sont égales. En effet, dans le groupe des idéaux fractionnaires non nuls de  $K$ , on a l'égalité

$$\mathfrak{P}_2 = \left( \frac{1 + \omega}{6} \right) \mathfrak{P}_3.$$

8) Les classes de  $\mathfrak{P}_2$  et  $\mathfrak{P}'_2$  sont distinctes. Sinon il existerait  $x \in K$  tel que

$$2A = \mathfrak{P}_2^2(x),$$

par suite,  $\mathfrak{P}_2^2$ , et donc  $\mathfrak{P}_2$ , serait principal, ce qui n'est pas.

9) On a les égalités

$$(2) \quad (1 + \omega)A = \mathfrak{P}_2^2\mathfrak{P}'_2\mathfrak{P}'_3 \quad \text{et} \quad (1 - \omega)A = \mathfrak{P}_2'^2\mathfrak{P}_2\mathfrak{P}_3.$$

En effet, on a

$$\mathfrak{P}_2^2\mathfrak{P}'_2\mathfrak{P}'_3 = \left( \frac{1 + \omega}{6} \right) (\mathfrak{P}_2\mathfrak{P}'_2)(\mathfrak{P}_3\mathfrak{P}'_3),$$

ce qui entraîne la première égalité. La deuxième se déduit de la première par conjugaison par le groupe de Galois de  $K$  sur  $\mathbb{Q}$ .

10) On a le résultat suivant :

**Lemme.** *Supposons  $\left(\frac{p}{23}\right) = 1$ . Il existe deux idéaux premiers distincts  $\mathfrak{P}$  et  $\mathfrak{P}'$  de  $A$  tels que  $pA = \mathfrak{P}\mathfrak{P}'$ . Les idéaux  $\mathfrak{P}$  et  $\mathfrak{P}'$  sont principaux si et seulement si il existe des entiers naturels  $x$  et  $y$  tels que  $p = x^2 + 23y^2$ .*

Démonstration : Notons que l'on a  $\left(\frac{p}{23}\right) = \left(\frac{-23}{p}\right)$ , de sorte que  $p$  est décomposé dans  $K$ . On remarque d'abord que  $\mathfrak{P}$  est principal si et seulement si tel est le cas de  $\mathfrak{P}'$  (car ils sont conjugués par Galois). Supposons qu'il existe  $x, y \in \mathbb{N}$  tels que  $p = x^2 + 23y^2$ . On a

$$pA = (x + \omega y)(x - \omega y),$$

ce qui entraîne que  $(x + \omega y)$  et  $(x - \omega y)$  sont les deux idéaux premiers au-dessus de  $p$ , ils sont donc principaux. Inversement, supposons  $\mathfrak{P}$  principal. Il existe  $a, b \in \mathbb{Z}$  de même parité tels que

$$\mathfrak{P} = \left( \frac{a + b\omega}{2} \right).$$

La norme de  $\mathfrak{P}$  vaut  $p$ , d'où

$$4p = a^2 + 23b^2.$$

Si  $a$  et  $b$  sont impairs, on a  $a^2 \equiv b^2 \equiv 1 \pmod{8}$ , d'où  $4p \equiv 0 \pmod{8}$ , puis  $p = 2$ . Or les idéaux premiers de  $A$  au-dessus de 2 ne sont pas principaux. Par suite  $a$  et  $b$  sont pairs et l'on a

$$p = \left( \frac{a}{2} \right)^2 + 23 \left( \frac{b}{2} \right)^2,$$

d'où le résultat.

### Exercice 10

Posons  $F = X^3 - X - 1 \in \mathbb{Z}[X]$ . Soit  $\alpha \in \mathbb{C}$  une racine de  $F$ .

- 1) Montrer que le corps de classes de Hilbert de  $K$  est le corps  $H := K(\alpha)$ .
- 2) Soit  $p$  un nombre premier distinct de 23. Montrer que  $p$  est totalement décomposé dans  $H$  si et seulement si il existe  $x$  et  $y$  dans  $\mathbb{Z}$ , avec  $x \neq 0$ , tels que  $p = x^2 + 23y^2$  (utiliser le théorème de réciprocité pour les corps de classes de Hilbert).

### 3.2. Démonstration du théorème 2

On part de l'identité d'Euler, valable pour tout nombre complexe  $q$  tel que  $|q| < 1$  (corollaire de l'exercice 8) :

$$\Phi(q) := \prod_{n \geq 1} (1 - q^n) = \sum_{n \geq 0} a_n q^n,$$

avec

$$(3) \quad a_n = \begin{cases} (-1)^m & \text{s'il existe } m \geq 0 \text{ tel que } n = \frac{1}{2}m(3m \pm 1) \\ 0 & \text{sinon.} \end{cases}$$

Il existe des entiers  $c_n \in \mathbb{Z}$  tels que l'on ait

$$q \Phi(q) \Phi(q^{23}) = \sum_{n \geq 1} c_n q^n.$$

### Exercice 11

Soit  $n$  un entier naturel non nul.

- 1) Montrer que l'on a  $\tau(n) \equiv c_n \pmod{23}$ .
- 2) Soit  $h$  est la partie entière de  $\frac{n-1}{23}$ . Montrer que l'on a

$$c_n = a_{n-1} + a_1 a_{n-24} + \cdots + a_h a_{n-1-23h}.$$

**Exercice 12**

Soit  $n \geq 1$  un entier qui ne soit pas un résidu quadratique modulo 23. Montrer que l'on a  $c_n = 0$  et en déduire que  $\tau(n) \equiv 0 \pmod{23}$ .

En particulier, si  $\left(\frac{p}{23}\right) = -1$ , on a  $\tau(p) \equiv 0 \pmod{23}$ .

Considérons l'ensemble  $S$  formé des couples  $(u, v) \in \mathbb{N}^2$  tels que

$$(4) \quad u^2 + 23v^2 = 24p.$$

**Exercice 13**

Soit  $(u, v)$  un élément de  $S$ .

- 1) Montrer qu'il existe un unique couple  $(m, n) \in \mathbb{N}^2$  tel que, les deux signes étant indépendants, on ait

$$u = 6m \pm 1 \quad \text{et} \quad v = 6n \pm 1.$$

On obtient ainsi une application  $\psi : S \rightarrow \mathbb{N}$  telle que  $\psi((u, v)) = m + n$ , où  $(m, n)$  est le couple d'entiers vérifiant la condition ci-dessus.

- 2) Vérifier sur un exemple qu'en général  $\psi$  n'est pas injective.  
3) Montrer que l'on a

$$(5) \quad c_p = \sum_{(u,v) \in S} (-1)^{\psi((u,v))}.$$

Remarquons que si  $\left(\frac{p}{23}\right) = -1$  l'ensemble  $S$  est vide, et la question 3 entraîne que  $c_p = 0$  i.e. que  $\tau(p) \equiv 0 \pmod{23}$ .

**Exercice 14**

On suppose qu'il existe  $(x, y) \in \mathbb{N}^2$  tel que  $p = x^2 + 23y^2$ .

- 1) Montrer qu'un tel couple d'entiers  $(x, y) \in \mathbb{N}^2$  est unique.  
2) Montrer que l'on a

$$S = \left\{ (|x - 23y|, x + y), (x + 23y, |x - y|) \right\}.$$

- 3) En déduire que l'on a  $c_p = 2$ , puis  $\tau(p) \equiv 2 \pmod{23}$ .

**Exercice 15**

On suppose que l'on a  $\left(\frac{p}{23}\right) = 1$  et que  $p$  n'est pas de la forme  $x^2 + 23y^2$ .

D'après le lemme, il existe deux idéaux premiers distincts  $\mathfrak{P}$  et  $\mathfrak{P}'$  de  $A$ , qui ne sont pas principaux, tels que  $pA = \mathfrak{P}\mathfrak{P}'$ . Puisque le groupe des classes d'idéaux de  $K$  est d'ordre



3, les classes de  $\mathfrak{P}$  et  $\mathfrak{P}'$  sont distinctes. D'après les alinéas 6 et 8 du paragraphe 3.1, on peut donc supposer que  $\mathfrak{P}$  est dans la classe de  $\mathfrak{P}_2$  et que  $\mathfrak{P}'$  est dans celle de  $\mathfrak{P}'_2$ .

- 1) Montrer que l'idéal  $\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}$  est principal.
- 2) En déduire que  $S$  est non vide.
- 3) Montrer qu'il existe un unique couple  $(u, v) \in S$ .
- 4) Quitte à changer  $v$  en  $-v$ , montrer qu'il existe des entiers relatifs  $r, s, r'$  et  $s'$  tels que l'on ait

$$(1 + \omega)(u - v\omega) = 4(r + s\omega) \quad \text{et} \quad (1 - \omega)(u - v\omega) = 6(r' - s'\omega).$$

- 5) En déduire que  $c_p = -1$ , puis que  $\tau(p) \equiv -1 \pmod{23}$ .

Cela termine la démonstration du théorème.



## Chapitre III — Représentations galoisiennes associées

### 1. Les représentations modulo 2, 3, 5, 7 et 691

Soit  $\ell$  l'un des nombres premiers 2, 3, 5, 7 et 691. Compte tenu des résultats obtenus précédemment, il est facile de décrire la classe d'isomorphisme de  $\rho_{\Delta, \ell}$ . En effet, dans les exercices 1 à 7 du chapitre II, on a démontré l'existence d'un entier  $m \geq 0$  tel que pour nombre premier  $p \neq \ell$ , on ait

$$\tau(p) \equiv p^m + p^{11-m} \pmod{\ell}.$$

On peut prendre  $m = 0$  si  $\ell \in \{2, 3, 691\}$  et  $m = 1$  si  $\ell \in \{5, 7\}$ . D'après l'exercice 16 du chapitre I, la représentation  $\rho_{\Delta, \ell}$  est donc réductible et est représentable sous la forme

$$\begin{pmatrix} \chi^m & 0 \\ 0 & \chi^{11-m} \end{pmatrix},$$

où  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$  est le caractère cyclotomique donnant l'action de  $G_{\mathbb{Q}}$  sur le groupe des racines  $\ell$ -ièmes de l'unité. Le nombre premier  $\ell$  est donc exceptionnel pour  $\Delta$ . On notera que l'ordre de l'image de  $\rho_{\Delta, \ell}$  est  $\ell - 1$ .

### 2. La représentation modulo 23

On va construire dans ce paragraphe la représentation  $\rho_{\Delta, 23}$  qui, rappelons le, est unique à isomorphisme près. Conformément au théorème de Deligne, il s'agit donc de construire une représentation semi-simple  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{23})$  vérifiant les deux conditions suivantes :

- 1)  $\rho$  est non ramifiée en dehors de 23.
- 2) Pour tout nombre premier  $p \neq 23$ , on a

$$\mathrm{Tr} \rho(\mathrm{Frob}_p) = \tau(p) \pmod{23} \quad \text{et} \quad \det \rho(\mathrm{Frob}_p) = p^{11} \pmod{23}.$$

On considère pour cela le corps de décomposition  $H$  sur  $\mathbb{Q}$  du polynôme  $X^3 - X - 1$  de  $\mathbb{Z}[X]$ . C'est une extension galoisienne de  $\mathbb{Q}$  et le groupe de Galois de  $H$  sur  $\mathbb{Q}$  est isomorphe à  $\mathbb{S}_3$ . Le corps quadratique contenu dans  $H$  est  $K := \mathbb{Q}(\omega)$  où  $\omega = \sqrt{-23}$  et d'après l'exercice 10 du chapitre II,  $H$  est le corps de classes de Hilbert de  $K$ . On dispose de l'homomorphisme de restriction

$$\mathrm{Res} : G_{\mathbb{Q}} \rightarrow \mathrm{Gal}(H/\mathbb{Q}).$$

Choisissons un isomorphisme  $i$  de  $\mathrm{Gal}(H/\mathbb{Q})$  sur  $\mathbb{S}_3$ . On obtient alors par composition avec  $\mathrm{Res}$  un homomorphisme  $G_{\mathbb{Q}} \rightarrow \mathbb{S}_3$ . On va expliciter dans l'exercice qui suit un homomorphisme injectif  $r : \mathbb{S}_3 \rightarrow \mathrm{GL}_2(\mathbb{Z})$  qui correspond en fait à l'unique représentation irréductible de degré 2 de  $\mathbb{S}_3$  :

### Exercice 1

Soit  $V$  l'hyperplan de  $\mathbb{C}^3$  d'équation  $x_1 + x_2 + x_3 = 0$ . Le groupe  $S_3$  opère sur  $V$  par permutation des coordonnées :

$$(\sigma, (x_1, x_2, x_3)) \mapsto (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

On déduit de cette action une représentation  $r : S_3 \rightarrow \mathrm{GL}(V)$ . Posons  $e_1 = (1, -1, 0)$ ,  $e_2 = (1, 0, -1)$  et identifions  $\mathrm{GL}(V)$  à  $\mathrm{GL}_2(\mathbb{C})$  via la base  $(e_1, e_2)$  de  $V$ .

- 1) Expliciter la représentation  $r : S_3 \rightarrow \mathrm{GL}_2(\mathbb{C})$  ainsi obtenue.
- 2) Montrer que  $r$  est irréductible et injective.

On constate que  $r(S_3)$  est contenu dans  $\mathrm{GL}_2(\mathbb{Z})$ . En considérant la surjection canonique  $s : \mathrm{GL}_2(\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{F}_{23})$ , on obtient une représentation

$$\rho := s \circ r \circ i \circ \mathrm{Res} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{23}),$$

dont on va maintenant démontrer qu'elle satisfait les conditions souhaitées.

### Exercice 2

- 1) Vérifier que  $\rho$  est irréductible et non ramifiée en dehors de 23.
- 2) Soit  $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{23}^*$  le caractère cyclotomique. Montrer que l'on a  $\det \rho = \chi^{11}$ .
- 3) Décrire la restriction de  $\rho$  à un sous-groupe d'inertie de  $G_{\mathbb{Q}}$  au-dessus de 23.

### Exercice 3

- 1) Montrer que pour tout nombre premier  $p \neq 23$ , on a  $\mathrm{Tr} \rho(\mathrm{Frob}_p) = \tau(p) \bmod 23$ .
- 2) En déduire que  $\rho_{\Delta, 23}$  est isomorphe à  $\rho$ .
- 3) Montrer que l'image de  $\rho_{\Delta, 23}$  est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé de  $\mathrm{GL}_2(\mathbb{F}_{23})$  qui est isomorphe à  $S_3$ .

Cela termine la description de  $\rho_{\Delta, 23}$ .

### 3. Les nombres premiers exceptionnels pour $\Delta$

On déduit des résultats précédents l'énoncé suivant :

**Théorème.** *Les nombres premiers exceptionnels pour  $\Delta$  sont 2, 3, 5, 7, 23 et 691.*

Il résulte de ce qui précède que ces nombres premiers sont exceptionnels pour  $\Delta$ . Inversement, soit  $\ell$  un nombre premier exceptionnel. D'après le théorème 3 du chapitre I, on est dans l'un des cas suivants :

1)  $\rho_{\Delta,\ell}$  est réductible. On a alors  $\ell \leq 11$  ou bien  $\ell$  divise le numérateur de  $B_{12}$  qui n'est autre que 691 (th. 4). Pour tout entier  $m$  tel que  $0 \leq m \leq 5$ , on vérifie que

$$-24 = \tau(2) \not\equiv 2^m + 2^{11-m} \pmod{11},$$

d'où il résulte que  $\rho_{\Delta,11}$  n'est pas réductible (exercice 16 du chapitre I).

2) L'image  $\rho_{\Delta,\ell}$  est contenue dans le normalisateur d'un sous-groupe de Cartan  $C$  sans être contenue dans  $C$ . On a dans ce cas  $\ell \leq 23$  (*loc. cit.*). Il s'agit de vérifier que pour  $\ell = 11, 13, 17$  et  $19$ , il existe un nombre premier  $p \neq \ell$  tel que l'on ait

$$(1) \quad \left(\frac{p}{\ell}\right) = -1 \quad \text{et} \quad \tau(p) \not\equiv 0 \pmod{\ell}.$$

On utilise les valeurs numériques suivantes :

$$\tau(3) = 252, \quad \tau(5) = 4830 \quad \text{et} \quad \tau(7) = -16744.$$

On constate que la condition (1) est satisfaite avec les couples  $(p, \ell) = (7, 11), (5, 13), (3, 17)$  et  $(3, 19)$ , d'où notre assertion.

3) L'image  $\rho_{\Delta,\ell}$  dans  $\mathbb{PGL}_2(\mathbb{F}_\ell)$  est isomorphe à  $\mathbb{S}_4$ . On a dans ce cas

$$\frac{\tau(p)^2}{p^{11}} \equiv \nu \pmod{\ell},$$

avec  $\nu = 0, 1, 2$  ou  $4$ . En explicitant cette condition avec les nombres premiers  $p = 3$  et  $p = 5$ , on constate que cela entraîne  $\ell \leq 7$ .

On en déduit que l'ensemble des nombres premiers exceptionnels pour  $\Delta$  est contenu dans  $\{2, 3, 5, 7, 23, 691\}$ . D'où le théorème.



## Chapitre IV — Généralisations

On se propose ici de faire quelques remarques sur l'énoncé du théorème 1 du chapitre I dans le cas où les coefficients de Fourier de la forme modulaire considérée ne sont pas des entiers relatifs. On illustrera cette situation sur un exemple avec une forme modulaire parabolique de poids 24. On pourra par exemple consulter à ce sujet [Ri] et [Se4].

### 1. Les représentations $\rho_{f,\mathcal{L}}$

Soit  $k$  un entier pair  $\geq 2$ . Considérons une forme modulaire parabolique  $f \in S_k$  vérifiant les deux conditions suivantes :

1) Le développement de Fourier de  $f$  est de la forme

$$f = q + \sum_{n \geq 2} a(n)q^n \quad \text{avec} \quad a(n) \in \mathbb{C} \quad (q = e^{2\pi iz}, z \in \mathfrak{H}).$$

2)  $f$  est fonction propre de tous les opérateurs de Hecke  $T_n$  avec  $n \geq 1$ . On a alors  $T_n f = a(n)f$  pour tout  $n \geq 1$ .

On dit parfois qu'une telle forme modulaire  $f$  est une forme de Hecke (cf. [Za]). Si  $d$  est la dimension du  $\mathbb{C}$ -espace vectoriel  $S_k$ , on démontre qu'il existe exactement  $d$  formes de Hecke dans  $S_k$  et qu'elles constituent une base de  $S_k$  (cf. *loc. cit.*). Rappelons par ailleurs que l'on a les formules suivantes (avec  $a(1) = 1$ ) :

$$(1) \quad a(n)a(m) = a(mn) \quad \text{si} \quad \text{pgcd}(m, n) = 1,$$

$$(2) \quad a(p)a(p^n) = a(p^{n+1}) + p^{k-1}a(p^{n-1}) \quad \text{si } p \text{ est premier et } n \geq 1.$$

Soit  $K = \mathbb{Q}(\dots, a(n), \dots)$  le sous-corps de  $\mathbb{C}$  engendré par les  $a(n)$ . On peut démontrer que  $K$  est une extension finie de  $\mathbb{Q}$  de degré inférieur ou égal à  $d$ . Par ailleurs,  $K$  est un corps totalement réel et les coefficients  $a(n)$  appartiennent à l'anneau d'entiers  $O_K$  de  $K$ .

Le théorème 1 se généralise comme suit :

**Théorème.** Soient  $\ell$  un nombre premier et  $\mathcal{L}$  un idéal premier de  $O_K$  au-dessus de  $\ell$ . Il existe une représentation linéaire semi-simple, unique à isomorphisme près,

$$\rho_{f,\mathcal{L}} : G_{\mathbb{Q}} \rightarrow \text{GL}_2\left(O_K/\mathcal{L}\right)$$

qui est non ramifiée en dehors de  $\ell$ , et telle que pour tout  $p$  premier distinct de  $\ell$ , on ait

$$\text{Tr } \rho_{f,\mathcal{L}}(\text{Frob}_p) = a(p) \bmod. \mathcal{L} \quad \text{et} \quad \det \rho_{f,\mathcal{L}}(\text{Frob}_p) = p^{k-1} \bmod. \mathcal{L}.$$

## 2. Un exemple en poids 24

Illustrons ce résultat dans une situation simple. Supposons  $k = 24$ . On a dans ce cas  $d = 2$ . Une base de  $S_{24}$  s'obtient en multipliant par  $\Delta$  une base de  $M_{12}$ . On peut par exemple prendre  $(\Delta^2, E_4^3\Delta)$ . Explicitons les deux formes de Hecke de  $S_{24}$ . Si  $f$  est l'une de ces deux formes, il existe  $\lambda \in \mathbb{C}$  tel que

$$f = E_4^3\Delta + \lambda\Delta^2.$$

On a

$$\Delta^2 = q^2 - 48q^3 + 1080q^4 - 15040q^5 + \dots,$$

$$E_4^3\Delta = q + 696q^2 + 162252q^3 + 12831808q^4 + 34188270q^5 + \dots.$$

En posant

$$f = q + \sum_{n \geq 2} a(n)q^n,$$

on obtient

$$a(2) = 696 + \lambda \quad \text{et} \quad a(4) = 12831808 + 1080\lambda.$$

Par ailleurs, en utilisant la formule (2), avec  $p = 2$  et  $n = 1$ , on a l'égalité

$$a(2)^2 = a(4) + 2^{23}.$$

On obtient ainsi une équation de degré 2 en  $\lambda$  :

$$\lambda^2 + 312\lambda - 20736000 = 0.$$

Soit  $\alpha$  une racine carrée de 144169. On obtient

$$\lambda = -156 \pm 12\alpha.$$

Il en résulte que les deux formes de Hecke cherchées sont

$$f_1 = E_4^3\Delta + (-156 + 12\alpha)\Delta^2 \quad \text{et} \quad f_2 = E_4^3\Delta + (-156 - 12\alpha)\Delta^2.$$

Leurs coefficients de Fourier appartiennent à  $K := \mathbb{Q}(\alpha)$  et elles sont conjuguées par le groupe de Galois de  $\mathbb{Q}(\alpha)$  sur  $\mathbb{Q}$ . Notons  $a_n(f_1)$  le  $n$ -ième coefficient de Fourier de  $f_1$ . On vérifie que l'on a :

$$(3) \quad a_2(f_1) = 540 + 12\alpha, \quad a_3(f_1) = 169740 - 576\alpha,$$

$$(4) \quad a_5(f_1) = 36534510 - 180480\alpha, \quad a_7(f_1) = -679592200 - 11829888\alpha.$$



Donnons maintenant un exemple de représentation  $\rho_{f_1, \mathcal{L}}$  qui soit surjective dans le cas où  $\ell$  est décomposé dans  $K$ . Admettons pour cela le résultat suivant ([Se2], prop. 19) :

**Proposition.** Soient  $\ell$  un nombre premier  $\geq 5$  et  $G$  un sous-groupe de  $\mathrm{GL}_2(\mathbb{F}_\ell)$ . On suppose que les conditions suivantes sont réalisées :

- 1)  $G$  contient un élément  $s$  tel que  $\mathrm{Tr}(s)^2 - 4\det(s)$  soit un carré non nul dans  $\mathbb{F}_\ell$  et que  $\mathrm{Tr}(s) \neq 0$ .
- 2)  $G$  contient un élément  $s'$  tel que  $\mathrm{Tr}(s')^2 - 4\det(s')$  ne soit pas un carré dans  $\mathbb{F}_\ell$  et que  $\mathrm{Tr}(s') \neq 0$ .
- 3)  $G$  contient un élément  $s''$  tel que  $u = \mathrm{Tr}(s'')^2 / \det(s'')$  soit distinct de 0, 1, 2 et 4 et que  $u^2 - 3u + 1 \neq 0$ .

Alors,  $G$  contient  $\mathrm{SL}_2(\mathbb{F}_\ell)$ . En particulier, si l'homomorphisme  $\det : G \rightarrow \mathbb{F}_\ell^*$  est surjectif, on a  $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ .

Prenons  $\ell = 11$ . Il existe deux idéaux premiers  $\mathcal{L}$  et  $\mathcal{L}'$  dans l'anneau d'entiers  $O_K$  de  $K$  au-dessus de 11. Leurs corps résiduels s'identifient donc à  $\mathbb{F}_{11}$ . Plus précisément, pour tout  $x \in O_K$  il existe un unique entier  $a$  tel que  $0 \leq a \leq 10$  et  $x \equiv a \pmod{\mathcal{L}}$ . Soit  $i : O_K \rightarrow \mathbb{F}_{11}$  l'application définie par  $i(x) = a$ . C'est un homomorphisme surjectif de noyau  $\mathcal{L}$ . L'un des idéaux  $\mathcal{L}$  et  $\mathcal{L}'$ , par exemple  $\mathcal{L}$ , est tel que

$$(5) \quad \alpha \equiv 6 \pmod{\mathcal{L}},$$

et l'on a alors  $\alpha \equiv 5 \pmod{\mathcal{L}'}$ . En effet, on vérifie que pour tout  $a$  tel que  $0 \leq a \leq 10$  et  $a \neq 5, 6$ , la norme de  $K$  sur  $\mathbb{Q}$  de  $\alpha - a$  n'est pas divisible par 11 et que 11 ne divise pas  $\alpha - 5$  ni  $\alpha - 6$ . On a ainsi  $i(\alpha) = 6$ . Les groupes  $\mathrm{GL}_2(O_K/\mathcal{L})$  et  $\mathrm{GL}_2(\mathbb{F}_{11})$  sont isomorphes et l'on obtient ainsi une représentation

$$\rho_{f_1, \mathcal{L}} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{11}),$$

telle que pour tout nombre premier  $p \neq 11$ , on ait

$$(6) \quad \mathrm{Tr} \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_p) = i(a_p(f_1)) \quad \text{et} \quad \det \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_p) = p^3 \pmod{11}.$$

On va démontrer le résultat suivant :

**Lemme.** La représentation  $\rho_{f_1, \mathcal{L}}$  est surjective.

Démonstration : Il résulte de (6) que l'on a

$$\det \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_2) = 8, \quad \det \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_5) = 4, \quad \det \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_7) = 2.$$

Par ailleurs, on déduit des formules (3), (4) et (5) les égalités

$$\mathrm{Tr} \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_2) = 7, \quad \mathrm{Tr} \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_5) = 5, \quad \mathrm{Tr} \rho_{f_1, \mathcal{L}}(\mathrm{Frob}_7) = 8.$$

On constate alors que les éléments  $\rho_{f_1, \mathcal{L}}(\text{Frob}_5)$ ,  $\rho_{f_1, \mathcal{L}}(\text{Frob}_2)$  et  $\rho_{f_1, \mathcal{L}}(\text{Frob}_7)$  vérifient respectivement les conditions 1, 2 et 3 de la proposition. L'image de  $\rho_{f_1, \mathcal{L}}$  contient donc  $\text{SL}_2(\mathbb{F}_{11})$ . Par ailleurs, le déterminant de  $\rho_{f_1, \mathcal{L}}$  est  $\chi^{23} = \chi^3$ , où  $\chi$  est le caractère cyclotomique donnant l'action de  $G_{\mathbb{Q}}$  sur les racines 11-ièmes de l'unité. Puisque tout élément de  $\mathbb{F}_{11}^*$  est un cube et que  $\chi$  est surjectif, la proposition entraîne le résultat.

Indépendamment de la proposition, il est facile de constater que  $\rho_{f_1, \mathcal{L}}$  est irréductible car le polynôme minimal de  $\rho_{f_1, \mathcal{L}}(\text{Frob}_2)$  est irréductible sur  $\mathbb{F}_{11}$ , de sorte que  $\rho_{f_1, \mathcal{L}}(\text{Frob}_2)$  n'est pas diagonalisable sur  $\mathbb{F}_{11}$ . Il n'en va pas de même pour la représentation  $\rho_{f_1, \mathcal{L}'}$  associée à  $\mathcal{L}'$ . On peut en effet démontrer que  $\rho_{f_1, \mathcal{L}'}$  est réductible et qu'elle est représentable sous la forme

$$\begin{pmatrix} \chi & 0 \\ 0 & \chi^2 \end{pmatrix}.$$

## Bibliographie

- [De] P. Deligne, Formes modulaires et représentations  $\ell$ -adiques, Séminaire Bourbaki **355** (1969), Lecture Notes **179** (1971), 139-172.
- [De-Se] P. Deligne et J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 507-530.
- [Go] R. Godement, Analyse mathématique IV, Springer 2003.
- [Ha-Wr] G. H. Hardy et E. M. Wright, An introduction to the Theory of Numbers, Fifth Edition, Oxford 1979.
- [Le] D. H. Lehmer, The Vanishing of Ramanujan's Function  $\tau(n)$ , *Duke Math. J.* **14** (1947), 429-433.
- [Ra] S. Ramanujan, Collected Papers.
- [Ri] K. Ribet, On  $\ell$ -Adic Representations Attached to Modular Forms, *Invent. Math.* **28** (1975), 245-275.
- [Sa] P. Samuel, Théorie algébrique des nombres, deuxième édition, Hermann, Paris 1971.
- [Se1] J.-P. Serre, Une interprétation des congruences relatives à la fonction  $\tau$  de Ramanujan, Séminaire Delange-Pisot-Poitou **14** (1967/68).
- [Se2] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.
- [Se3] J.-P. Serre, Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer), Séminaire Bourbaki **416** (1971/72).
- [Se4] J.-P. Serre, Valeurs propres des opérateurs de Hecke modulo  $\ell$ , *Astérisque* **24-25** (1975), 109-117.
- [Se5] J.-P. Serre, Sur la lacunarité des puissances de  $\eta$ , *Glasgow Math. J.* **27** (1985), 203-221.
- [Sw] H. P. F. Swinnerton-Dyer, On  $\ell$ -adic representations and congruences for coefficients of modular forms, dans Modular Functions of One Variable III, Lecture Notes **350** (1976), 1-55.
- [Wa] L. Washington, Introduction to Cyclotomic Fields, Springer GTM **83**, 1982.
- [Wi] J. R. Wilton, Congruence properties of Ramanujan's function  $\tau(n)$ , *Proc. London Math. Soc.* **31** (1930), 1-10.
- [Za] D. Zagier, Introduction to Modular Forms, From Number Theory to Physics, M. Waldschmidt, P. Moussa, J.-M. Luck, C. Itzykson (Editeurs), Springer-Verlag 1992.