Formes modulaires modulo p

Philémon Varnet

23 Octobre 2025

Table des matières

1 Formes modulaires sur $\mathbb{C}$

1.1 Rappels et notations

- On a posé
$$\Delta(q) := q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$
- Si $k \geq 4$, la k-ième *série d'Eisenstein*
$$G_k(q) = -\frac{B_k}{2k} + \sum_{n\geq 1}\sigma_{k-1}(n)q^n$$
est une forme modulaire de poids k où B_k est le k-ième nombre Bernouilli. La k-ième *série d'Eisenstein normalisée* est alors
$$E_k(q) := -\frac{2k}{B_k}G_k(q) = 1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)q^n$$
- Si $k \in \mathbb{Z}$, $M_k(\mathbb{C})$ désigne le $\mathbb{C}$-espace vectoriel des formes modulaires de poids k. L'anneau des formes modulaires est alors
$$M(\mathbb{C}) := \sum_{k\in\mathbb{Z}} M_k(\mathbb{C})$$
vu comme sous-anneau de $\mathbb{C}[[q]]$. On note aussi, si A est un sous-anneau de $\mathbb{C}$ et $k \in \mathbb{Z}$, $M_k(A)$ le A-module des formes modulaires de poids k défini par
$$M_k(A) := M_k(\mathbb{C}) \cap A[[q]]$$

L'anneau des formes modulaires sur A est donc naturellement

$$M(A) := \sum_{k\in\mathbb{Z}} M_k(A)$$

et c'est un sous-anneau de $A[[q]]$.

- Si p est un nombre premier, on note $\mathcal{O}$ l'ensemble des rationnels p-entiers, i.e. l'ensemble des $q \in \mathbb{Q}$ tels que $\nu_p(q) \geq 0$. C'est un sous-anneau de $\mathbb{Q}$.
- On a vu dans l'exposé d'Antoine que pour tout $k \in \mathbb{Z}$, $M_k(\mathbb{C})$ est engendré, en tant que $\mathbb{C}$-ev, par les $E_4^r E_6^r$ où $(r,s) \in \mathbb{N}^2$, $4r+6s = k$ et que

$$\dim M_k(\mathbb{C}) = \begin{cases} \lfloor k/12 \rfloor \text{ si } k \equiv 2 \pmod{12} \\ \lfloor k/12 \rfloor + 1 \text{ sinon} \end{cases}$$

On rappelle que

$$E_4 = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n = 1 + 240q + 2160q^2 + 6720q^3 + \dots$$
$$E_6 = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n = 1 - 504q - 16632q^2 - 122976q^3 - \dots$$

et on a la relation

$$\Delta = \frac{E_4^3 - E_6^2}{1728}$$

On note également

$$E_2 = 1 - 24\sum_{n\geq 1}\sigma_1(n)q^n = 1 - 24q - 72q^2 - 96q^3 - \dots$$

qui n'est pas une forme modulaire.

1.2 Structure

Proposition 1.1. *La somme définissant $M(\mathbb{C})$ est directe : on a en fait*

$$M(\mathbb{C}) = \bigoplus_{k\in\mathbb{Z}} M_k(\mathbb{C})$$

Démonstration. Soit $N \geq 1$, $f_1, \dots, f_N$ des formes modulaires de poids $k_1, \dots, k_N \geq 0$ distincts telles que

$$\sum_{i=1}^{N} f_i = 0$$

Soit $z \in \mathcal{H}$. Alors pour tout $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$0 = \sum_{i=1}^{N} f_i(gz) = \sum_{i=1}^{N} (cz+d)^{k_i} f_i(z)$$

En prenant par exemple $g = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$ pour $k \in \mathbb{Z}$, on a que le polynôme $P = \sum_{i=1}^{N} f_i(z) X^{k_i}$ s'annule sur l'ensemble infini $\{kz+1 \mid k \in \mathbb{Z}\}$ donc est nul ; ainsi $f_i(z) = 0$ pour tout $1 \leq i \leq N$ et $z \in \mathcal{H}$, donc $f_i = 0$ pour tout $1 \leq i \leq N$. ∎

Corollaire 1.1. *On en déduit que si A est un sous-anneau de $\mathbb{C}$,*

$$M(A) = \bigoplus_{k\in\mathbb{Z}} M_k(A)$$

Lemme 1.1. *Soit A un anneau, $n \geq 1$ et $(f_i)_{i=0,\dots,n-1} \in A[[q]]^n$ tels que, pour tout $i = 0, \dots, n-1$, f_i de la forme $f_i(q) = q^i + a_{i+1}^{(i)} q^{i+1} + \dots = q^i(1 + r_i(q))$. Alors $(f_i)_{i=0,\dots,n-1}$ est libre sur A.*

Démonstration. En écrivant une relation de liaison $\sum_{i=0}^{n-1} \lambda_i f_i = 0$ où $\lambda_0, \dots, \lambda_{n-1} \in A$, on obtient, en regardant le coefficient constant, $\lambda_0 = 0$, puis $\lambda_1 = 0$ avec le coefficient en q, etc. et on a récursivement $\lambda_i = 0$ pour tout i. ■

Proposition 1.2. *Soit A un sous-anneau de $\mathbb{C}$, $k \geq 0$ et $d = \dim M_k(\mathbb{C})$. On fixe $r, s \geq 0$ tels que $0 \leq 4r + 6s \leq 14$ et $4r + 6s \equiv k \pmod{12}$. Alors la famille des $f_t = \Delta^t E_4^r E_6^{s+2(d-t-1)}$ où $t \in [\![0, d-1]\!]$ est une A-base de $M_k(A)$.*

Démonstration. L'expression de $\dim_{\mathbb{C}} M_k(\mathbb{C})$ donne qu'on a $k + 12 = 12d + 4r + 6s$. On en déduit que f_t est bien dans $M_k(A)$ pour tout $t \in [\![0, d-1]\!]$.
La famille des f_t est libre sur A : comme Δ^t de la forme $q^t + q^{t+1}(\dots)$, $E_4(0) = 1$ et $E_6(0) = 1$, c'est vrai par le Lemme 1.1.
C'est donc une base sur $\mathbb{C}$. Si $f \in M_k(A)$ qu'on écrit $f = \sum_{t=0}^{d-1} \lambda_t f_t$ où les λ_t sont dans $\mathbb{C}$, avec $[f]_j$ le j-ième coefficient de f dans son q-développement,

$$[f]_j = \lambda_t + \lambda_{t+1}[f_{t+1}]_j + \dots + \lambda_{d-1}[f_{d-1}]_j$$

pour $j \in [\![0, d-1]\!]$. On obtient un système triangulaire qui donne $\lambda_t \in A$ pour tout $t \in [\![0, d-1]\!]$, ce qui conclut. ■

Corollaire 1.2. *Si A est un sous-anneau de $\mathbb{C}$, on a*

$$M(A) = A[E_4, E_6, \Delta]$$

De plus, si 6 est inversible dans A,

$$M(A) = A[E_4, E_6]$$

Démonstration. La première partie de l'énoncé découle immédiatement de la Proposition 1.2 et de la définition de $M(A)$. La seconde partie s'en déduit aisément car dans le cas où $6 \in \mathcal{A}^\times$, comme $1728 = 12^3 \in A^\times$,

$$\Delta = \frac{E_4^3 - E_6^2}{1728} \in A[E_2, E_4]$$

■

Ce dernier résultat signifie que pour tout sous-anneau A de $\mathbb{C}$ dans lequel 6 est inversible, le morphisme

$$\begin{array}{ccc} A[Q,R] & \xrightarrow{\varphi_A} & M(A) \\ Q & \longmapsto & E_4 \\ R & \longmapsto & E_6 \end{array}$$

est surjectif (où Q et R sont des indéterminées). On a même mieux :

Corollaire 1.3. *Si A est un sous-anneau de $\mathbb{C}$ tel que $6 \in A^\times$ alors φ_A est un isomorphisme.*

Démonstration. C'est une conséquence immédiate de la Proposition 1.1 : si $P \in \ker \varphi_A$ et $i, j \geq 0$, avec $k = 4u + 6j$, la projection de $\varphi_A(P)$ sur $M_k(A)$ est nulle donc le coefficient en $Q^i R^j$ de P est nul puisque la famille des $E_2^r E_4^s$ où $4r + 6s = k$ est libre (sur $\mathbb{C}$ donc) sur A. ■

Définition 1.1. Soit A un anneau, $u, v \in \mathbb{N}^*$ et $k \geq 0$. On dit que $P \in A[X, Y]$ est (u, v)-*homogène de degré* k si P s'écrit comme combinaison linéaire à coefficient dans A de monômes de la forme $X^r Y^s$ où $ur + vs = k$. On dira simplement que P est homogène lorsque u et v sont donnés clairement par le contexte.
De manière générale, tout polynôme $P \in A[X, Y]$ s'écrit comme somme de polynômes homogènes, et son degré, noté $d(P)$, est le degré maximal des polynômes homogènes non nuls apparaissant dans cette somme (et vaut par convention $-\infty$ s'il est nul). On vérifie facilement que d satisfait les mêmes propriétés que le degré usuel, à savoir $d(PQ) = d(P) + d(Q)$ ainsi que $d(P + Q) \leq \max(d(P), d(Q))$ pour $P, Q \in A[X, Y]$.

On vient de voir que si A est un sous-anneau de $\mathbb{C}$ dans lequel 6 est inversible, les éléments de $M_k(A)$ sont les polynômes $(4, 6)$-homogènes en E_4 et E_6.

2 L'anneau des formes modulaires modulo p

2.1 Réduction modulo p

On fixe dans la suite un nombre premier p.

Etant donnée une série formelle

$$f(q) = \sum_{n=0}^{+\infty} a_n q^n \in \mathbb{Q}[[q]]$$

on dit que f est *p-entière* si ses coefficients $(a_n)_{n\geq 0}$ sont p-entiers ; leur ensemble est noté, sans surprise, $\mathcal{O}[[q]]$. Le morphisme d'anneaux $\mathcal{O} \twoheadrightarrow \mathbb{F}_p$ s'étend naturellement aux séries formelles en un morphisme d'anneaux $\mathcal{O}[[q]] \twoheadrightarrow \mathbb{F}_p[[q]]$ via réduction modulo p coefficient par coefficient. L'image de $f(q) \in \mathcal{O}[[q]]$ par ce morphisme est alors noté

$$\overline{f}(q) = \sum_{n=0}^{+\infty} \overline{a_n} q^n \in \mathbb{F}_p[[q]]$$

On pourra écrire indifféremment $\overline{f} = \overline{g}$ et $f \equiv g \pmod{p}$ pour $g, f \in \mathcal{O}[[q]]$.

On note alors

$$M_k(\mathbb{F}_p) := \overline{M_k(\mathcal{O})} = \left\{\overline{f} \mid f \in M_k(\mathcal{O})\right\}$$

la réduction de $M_k(\mathcal{O})$ modulo p, ainsi que

$$M(\mathbb{F}_p) := \overline{M(\mathcal{O})} = \sum_{k\in\mathbb{Z}} M_k(\mathbb{F}_p)$$

la réduction de $M(\mathcal{O})$ modulo p, sous-anneau de $\mathbb{F}_p[[q]]$: c'est *l'anneau des formes modulaires modulo p*. L'objet de la suite de cet exposé est de déterminer la structure de $M(\mathbb{F}_p)$.

$$\begin{array}{ccc} \mathcal{O}[Q,R] & \xrightarrow{\pi} & \mathbb{F}_p[Q,R] \\ \downarrow{\scriptstyle \varphi_{\mathcal{O}}} & & \downarrow{\scriptstyle \varphi_{\mathbb{F}_p}} \\ M(\mathcal{O}) & \xrightarrow{\pi} & M(\mathbb{F}_p) \end{array}$$

2.2 Premières observations

Proposition 2.1. *Soit $k \in \mathbb{Z}$. On a $\dim_{\mathbb{C}} M_k(\mathbb{C}) = \dim_{\mathbb{F}_p} M_k(\mathbb{F}_p)$.*

Démonstration. L'image de la famille des $f_t \in M_k(\mathcal{O}), t \in [\![0, d-1]\!]$ définie en Proposition 1.2 par le morphisme de réduction modulo p engendre $M_k(\mathbb{F}_p)$ par surjectivité. Elle est aussi libre par le Lemme 1.1. ■

Ainsi, d'un point de vue linéaire, on ne distingue pas $M_k(\mathbb{C})$ et $M_k(\mathbb{F}_p)$ si $k \in \mathbb{Z}$. Néanmoins, vont apparaître des différences essentielles entre les anneaux $M(\mathbb{C})$ et $M(\mathbb{F}_p)$.

Proposition 2.2. *On a :*

- $E_{p-1} \in M_{p-1}(\mathcal{O})$ *et* $E_{p-1} \equiv 1 \pmod{p}$ *;*
- *Si* $p \geq 5$, $E_{p+1} \in M_{p+1}(\mathcal{O})$ *et* $E_{p+1} \equiv E_2 \pmod{p}$.

Démonstration. On a vu les résultats suivants dans l'exposé d'Alexis :

Théorème (Von Staudt–Clausen). *Si $k \geq 1$,*

$$B_{2k} + \sum_{\substack{p \text{ premier} \\ p-1 \mid 2k}} \frac{1}{p} \in \mathbb{Z}$$

Théorème (Congruences de Kummer). *Si $k, \ell \geq 1$ sont tels que $k \equiv \ell \not\equiv 0 \pmod{p-1}$, alors*

$$\frac{B_k}{k} \equiv \frac{B_\ell}{\ell} \pmod{p}$$

On déduit du théorème de Clausen-Von Staudt $pB_{p-1} \equiv -1 \pmod{p}$ donc $E_{p-1} \in M_{p-1}(\mathcal{O})$ et $\frac{p-1}{B_{p-1}}\sigma_{p-1}(n) \equiv 0 \pmod{p}$ pour tout $n \geq 1$, d'où $E_{p-1} \equiv 1 \pmod{p}$. Similairement, si $p \geq 5$, par les congruences de Kummer, comme $p+1 \equiv 2 \not\equiv 0 \pmod{p-1}$,

$$\frac{B_{p+1}}{p+1} \equiv \frac{B_2}{2} \equiv \frac{1}{12} \pmod{p}$$

donc $E_{p+1} \in M_{p+1}(\mathcal{O})$. En outre, pour tout $n \geq 1$, par petit Fermat,

$$\sigma_p(n) = \sum_{d|n} d^p \equiv \sum_{d|n} d = \sigma_1(n) \pmod{p}$$

d'où

$$E_{p+1} = 1 - \frac{2p}{B_{p+1}} \sum_{n\geq 1} \sigma_p(n) q^n \equiv 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n = E_2 \pmod{p}$$

■

En particulier, E_2 est une forme modulaire modulo p pour tout $p \geq 5$!

Corollaire 2.1. *Si $k \in \mathbb{Z}$, on a $M_k(\mathbb{F}_p) \subseteq M_{k+p-1}(\mathbb{F}_p)$.*

Démonstration. On a $E_{p-1}M_k(\mathcal{O}) \subseteq M_{k+p-1}(\mathcal{O})$, d'où le résultat en réduisant modulo p et en utilisant $E_{p-1} \equiv 1 \pmod{p}$. ■

Ainsi, la somme $M(\mathbb{F}_p) = \sum_{k\in\mathbb{Z}} M_k(\mathbb{F}_p)$ est ici loin d'être directe et il y a plein de recouvrement. On va voir que l'obstruction donnée par le corollaire est en quelque sorte "la seule".

3 Structure de $M(\mathbb{F}_p)$

3.1 Cas $p = 2$ et $p = 3$

Lorsque $p = 2$ ou $p = 3$, p divise 240 et 504. On voit donc que $\overline{E}_4 = \overline{E}_6 = 1$ et ainsi $\overline{M} = \mathbb{F}_p[\overline{\Delta}]$. Dans les deux cas, cet anneau est isomorphe à $\mathbb{F}_p[X]$: la famille des $\overline{\Delta}^i$ où $i \geq 0$ est libre par le Lemme 1.1.

Dans la suite, on se place dans le cas $p \geq 5$.

3.2 Opérateur de dérivation ∂

Définition 3.1. Si A est un anneau commutatif, on appelle *dérivation* un morphisme de groupe $D : (A, +) \to (A, +)$ vérifiant aussi la règle de Leibniz : pour tout $f, g \in A$,

$$D(fg) = fD(g) + gD(f)$$

Remarquons que

$$D(1) = D(1 \cdot 1) = D(1) + D(1)$$

ce qui donne $D(1) = 0$. De manière générale, posons $C_D := \ker D$. C'est un sous-anneau de A, appelé *sous-anneau des constantes* de A : c'est un sous-groupe de A, on vient de voir que $1 \in C_D$ et si $a, b \in C_D$,

$$D(a \cdot b) = aD(b) + bD(b) = 0 + 0 = 0$$

donc $a \cdot b \in C_D$.
La dérivation D est C_D-linéaire : on a, pour tout $c \in C_D$ et $a \in A$,

$$D(ca) = cD(a) + aD(c) = cD(a)$$

Elle est donc B-linéaire pour tout sous-anneau B de C_D.
On a vu dans les exposés précédents l'opérateur sur $\mathbb{C}[[q]]$ donné par $\theta = q\dfrac{d}{dq}$. C'est une dérivation sur $\mathbb{C}[[q]]$ qui est $\mathbb{C}$-linéaire ($\mathbb{C}$ est le sous-anneau des constantes de θ). Notons que l'on a $\dfrac{\partial}{\partial z}e^{2i\pi z} = 2i\pi e^{2i\pi z}$, donc pour f une fonction faiblement modulaire (en identifiant f de variable z et $\tilde{f}$ telle que $\tilde{f}(q) = f$ où $q = e^{2i\pi z}$),

$$\frac{\partial f}{\partial z} = \frac{\partial f}{\partial q}\frac{\partial q}{\partial z} = 2i\pi q\frac{\partial f}{\partial q} = 2i\pi\theta(f)$$

On définit maintenant, si $k \in \mathbb{Z}$ et $f \in M_k(\mathbb{C})$,

$$\partial f := 12\theta f - kE_2 f$$

Proposition 3.1. *On a les propriétés suivantes sur ∂ :*

- *Si A est un sous-anneau de $\mathbb{C}$, $f \in M_k(A)$, $\partial f \in M_{k+2}(A)$;*
- *On a $12\theta E_2 - E_2^2 = -E_4$;*
- *∂ vérifie $\partial E_4 = -4E_6$ et $\partial E_6 = -6E_4^2$*

Démonstration.

- Soit A un sous-anneau de $\mathbb{C}$, $f \in M_k(A)$. Partons de l'égalité $f(-1/z) = z^k f(z)$, que l'on dérive logarithmiquement :

$$\frac{1}{z^2}\frac{f'(-1/z)}{f(-1/z)} = \frac{k}{z} + \frac{f'(z)}{f(z)} \tag{1}$$

  En particulier, pour $f = \Delta$, de poids 12 :

$$\frac{1}{z^2}\frac{\Delta'(-1/z)}{\Delta(-1/z)} = \frac{12}{z} + \frac{\Delta'(z)}{\Delta(z)}$$

  Mais on a vu dans l'exposé introductif l'identité :

$$\frac{\Delta'}{\Delta}(z) = \frac{1}{2i\pi q}\frac{\theta(\Delta)}{\Delta} = \frac{1}{2i\pi}E_2$$

  d'où l'équation fonctionnelle de E_2 :

$$\frac{1}{z^2}2i\pi E_2(-1/z) = \frac{12}{z} + 2i\pi E_2(z) \tag{2}$$

  et $12 \cdot (1) - k \cdot (2)$ permet d'éliminer le terme en $1/z$, et en posant $F(z) = 12\dfrac{f'(z)}{f(z)} - 2i\pi kE_2(z)$ on obtient :

$$\frac{1}{z^2}F(-1/z) = F(z)$$

  Puis en posant $G(z) = F(z)f(z) = 2i\pi\partial(f)$,

$$\frac{1}{z^2}\frac{G(-1/z)}{f(-1/z)} = \frac{G(z)}{f(z)}$$

  soit

$$G(-1/z) = z^2 f(-1/z)\frac{G(z)}{f(z)} = z^{k+2}G(z)$$

  d'où G donc ∂f est modulaire de poids $k+2$. Par ailleurs, on voit sur la formule définissant ∂f que son q-développement est bien à coefficients dans A.

- C'est très semblable, en dérivant (2).
- ∂E_4 est donc une forme modulaire de poids 6, donc colinéaire à E_6 ; on obtient $\partial E_4 = -4E_6$ en regardant le coefficient constant. On procède de même pour ∂E_6.

■

Proposition 3.2. *On étend par linéarité la définition de ∂ à $M(\mathbb{C})$. Alors pour tout sous-anneau A de $\mathbb{C}$, ∂ définit une dérivation A-linéaire sur $M(A)$.*

Démonstration. Il est clair que c'est un endomorphisme de groupe de $M(A)$. Soit $f \in M_k(A), g \in M_\ell(A)$. On a :

$$\begin{aligned} f\partial g + g\partial f &= f(12\theta g - \ell E_2 g) + g(12\theta f - kE_2 f) \\ &= 12(f\theta g + g\theta f) - (k+\ell)E_2 fg \\ &= 12\theta(fg) - (k+\ell)E_2 fg = \partial(fg) \end{aligned}$$

Par bilinéarité de $(f,g) \mapsto \partial(fg)$, le résultat tient aussi pour $f, g \in M(A)$. ■

Le résultat suivant permet alors d'identifier ∂.

Proposition 3.3. *Soit A un anneau commutatif et $P, Q \in A[X,Y]$. Il existe une unique dérivation D sur $A[X,Y]$ qui est A-linéaire telle que $D(X) = P$ et $D(Y) = Q$.*

Démonstration. Soit D une dérivation sur $A[X,Y]$ telle que $D(X) = P, D(Y) = Q$. Soit $i, j \geq 0$. On a $D(X^iY^j) = iX^{i-1}Y^jD(X) + X^ijY^{j-1}D(Y) = \dfrac{\partial X^iY^j}{\partial X}P + \dfrac{\partial X^iY^j}{\partial Y}Q$ d'où par linéarité, pour tout $U \in A[X,Y]$:

$$D(U) = \frac{\partial U}{\partial X}P + \frac{\partial U}{\partial Y}Q$$

Réciproquement, on vérifie que la formule précédente définit bien une dérivation sur $A[X,Y]$ ce qui conclut. ■

Soit A un sous-anneau de $\mathbb{C}$ avec 6 inversible. Soit ∂^* la dérivation définie sur $A[Q,R]$ par $\partial^*Q = -4R, \partial^*R = -6Q^2$. Comme $M(A) \simeq A[Q,R]$, on a $\partial F(E_4,E_6) = \partial^* F(E_4,E_6)$ pour tout $F \in A[Q,R]$ et on pourra identifier ∂ et ∂^*.
En considérant $A = \mathcal{O}$ et la réduction modulo p, on a aussi que le diagramme suivant commute.

$$\begin{array}{ccccc} \mathcal{O}[Q,R] & \xrightarrow{\pi} & \mathbb{F}_p[Q,R] & \xrightarrow{\partial} & \mathbb{F}_p[Q,R] \\ \downarrow{\scriptstyle \varphi_{\mathcal{O}}} & & \downarrow{\scriptstyle \varphi_{\mathbb{F}_p}} & & \downarrow \\ M(\mathcal{O}) & \xrightarrow{\pi} & M(\mathbb{F}_p) & \xrightarrow{\partial} & M(\mathbb{F}_p) \end{array}$$

3.3 Le polynôme $A(Q,R)$

On fixe dans toute la suite $A \in \mathcal{O}[Q,R]$ l'unique polynôme tel que $A(E_4,E_6) = E_{p-1}$.

Proposition 3.4. *On a $\partial^2\overline{A} = -Q\overline{A}$.*

Démonstration. Par Proposition 2.2,

$$\partial\overline{A}(E_4,E_6) = 12\theta(1) - (p-1)\overline{PA}(\overline{E}_4,\overline{E}_6) = \overline{E}_2 = \overline{E}_{p+1}$$

Posons $B \in \mathcal{O}[Q,R]$ tel que $B(E_4,E_6) = E_{p+1}$. Alors $(\partial A - B)(E_4,E_6) \in M_{p+1}(\mathcal{O})$ est dans le noyau du morphisme de groupe

$$M_{p+1}(\mathcal{O}) \xrightarrow{\pi_{p+1}} M_{p+1}(\mathbb{F}_p)$$

qui vaut $pM_{p+1}(\mathcal{O})$ (pour le constater, il suffit de décomposer un élément de $\ker \pi_{p+1}$ dans la base des $E_4^r E_6^s$ avec $4r+6s=p+1$). On en déduit $(\partial A - B)(E_4, E_6) \in pM(\mathcal{O})$ d'où $\partial A - B \in p\mathcal{O}[Q,R]$ puis $\partial \overline{A} = \overline{B}$. On a de même, en utilisant $12\theta E_2 - E_2^2 = -E_4$, que $\partial \overline{B} = -Q\overline{A}$ ce qui conclut. ■

Lemme 3.1. *Le polynôme $\overline{A}$ est sans facteur carré.*

Démonstration.

- Commençons par montrer que les facteurs irréductibles de $\overline{A}$ dans $\overline{\mathbb{F}}_p$ sont de la forme Q, R ou $R^2 - cQ^3$ où $c \in \overline{\mathbb{F}}_p^\times$. Ces derniers sont bien irréductibles dans $\overline{\mathbb{F}}_p[Q,R]$, car une factorisation non triviale donnerait un facteur de degré 1 (via les degrés) $aR+bQ$ où $(a,b) \neq (0,0)$, et si par exemple $b \neq 0$, $aR+bQ$ diviserait $R^2 - c(-a/b)R^3$ ce qui est impossible compte-tenu du degré en Q.
  Posons $Q = x^4$ et $R = y^6$ où x, y sont dans la clôture algébrique de $\overline{\mathbb{F}}_p(Q,R)$. Alors, $P(x,y) := \overline{A}(x^4, y^6)$ est homogène au sens usuel, de degré $p-1$, en x, y : si $\lambda \in \overline{\mathbb{F}}_p$,
  $$\overline{A}(\lambda^4 x^4, \lambda^6 y^6) = \lambda^{p-1}\overline{A}(x^4, y^6) = \lambda^{p-1}P(x,y)$$
  Ainsi, en factorisant $P(1,X)$ dans $\overline{\mathbb{F}}_p$,
  $$P(x,y) = x^{p-1}P(1,y/x) = \alpha x^{p-1}(y/x)^v \prod_{i=1}^{r}(y/x - c_i) = \alpha x^u y^v \prod_{i=1}^{r}(y - c_i x)$$
  où $u+v+r = p-1$ et $\alpha, c_i \in \overline{\mathbb{F}}_p^\times$. On note $S = \{c_i \mid i = 1, \dots, r\}$, μ_{12} le sous-groupe de $\overline{\mathbb{F}}_p^\times$ des racines 12-ième de l'unité, cyclique d'ordre 12 car $p \nmid 12$. Notons que si $\lambda \in \mu_{12}$,
  $$P(1, \lambda X) = \overline{A}(1, \lambda^6 X^6) = \overline{A}(1, \pm X^6) = (\pm 1)^{p-1}\overline{A}(\pm 1, X^6) = P(\pm 1, X) = \overline{A}(1, X^6) = P(1,X)$$
  Ainsi, l'action de μ_{12} sur $\overline{\mathbb{F}}_p^\times$ par multiplication se restreint à S et celle-ci est libre. Maintenant, si $s \in S$, son orbite O_s est de cardinal $|\mu_{12}| = 12$ et
  $$\prod_{t \in O_s}(X - t) = \prod_{\lambda \in \mu_{12}}(X - \lambda r) = \prod_{i=0}^{11}(X - \zeta^i r) = X^{12} - \zeta^{12} r^{12} = X^{12} - r^{12}$$
  où ζ est un générateur de μ_{12}. On a donc
  $$\prod_{i=1}^{r}(y - c_i x) = \prod_{j=1}^{h}(y^{12} - r_j^{12} x^{12}) = \prod_{j=1}^{h}(R^2 - r_j^{12} Q^3)$$
  où les r_j sont des représentants des orbites qui partitionnent S, où $r = 12h$. En écrivant ainsi
  $$\overline{A}(Q,R) = \alpha x^u y^v \prod_{j=1}^{h}(R^2 - r_j^{12} Q^3)$$
  En prenant les degrés en x et en y, on obtient que $4 \mid u$ et $6 \mid v$, d'où finalement
  $$\overline{A}(Q,R) = Q^{u'} R^{v'} \prod_{j=1}^{h}(R^2 - r_j^{12} Q^3)$$
  où $u' = u/4$ et $v' = v/6$.
- Soit alors $k \geq 1$ la valuation d'un facteur irréductible F de A. Supposons par l'absurde $k > 1$. Si F est de la forme $R^2 - cQ^3$ où $c \neq 0$, et on ne peut pas avoir $c = 1$ car $\overline{E}_6^2 - \overline{E}_4^3 \in q\mathbb{F}_p[[q]]$. Comme $\partial(R^2 - cQ^3) = 12(c-1)Q^2 R$ est premier avec $R^2 - cQ^3$, en écrivant $\overline{A} = (R^2 - cQ^3)^k U$ où $R^2 - cQ^3 \nmid U$, la valuation de $R^2 - cQ^3$ dans
  $$\partial \overline{A} = \partial(R^2 - cQ^3)^k U + (R^2 - cQ^3)^k \partial U = 12(c-1)Q^2 R(R^2 - cQ^3)^{k-1} U + (R^2 - cQ^3)^k \partial U$$
  est nécessairement $k-1$. De même, celle de $\partial^2 \overline{A}$ est $k-2$, absurde. Si $F = Q$, $\partial F = -4R$ est premier avec F, le même argument s'applique. De même pour $F = R$.

■

Lemme 3.2. *On pose $k = \overline{\mathbb{F}}_p$. Soit $P \in k[X,Y]$, (u,v)-homogène de degré $p-1$ et sans facteur carré. Alors $P \pm 1$ est irréductible dans $k[X,Y]$.*

Démonstration. On prend $P \in k[X,Y]$ qui est (u,v)-homogène de degré $p-1$ et on montre que si $P+1$ n'est pas irréductible, alors P a un facteur carré (le cas de $P-1$ s'en déduit en considérant $-P$).
On considère l'action de $k^\times$ sur $k[X,Y]$ donnée par :

$$\lambda \cdot P(X,Y) = P(\lambda^u X, \lambda^v Y) \qquad \forall \lambda \in k^\times, P \in k[X,Y]$$

Plusieurs remarques :

1. Si $L \in k[X,Y]$ est homogène de degré n, alors pour tout $\lambda \in k^\times$, $\lambda \cdot L = \lambda^n L$. En effet, si $i,j \geq 0$ vérifient $ui + vj = n$ et $\lambda \in k^\times$,
$$\lambda \cdot X^i Y^j = (\lambda^u X)^i (\lambda^v Y)^j = \lambda^{p-1} X^i = X^i Y^j$$
et on conclut par k-linéarité de l'action.
2. Si $L \in k[X,Y]$, on note $H(L)$ la partie homogène de degré maximal de L. Alors pour tout $\lambda \in k^\times$, $H(\lambda \cdot L) = \lambda^n H(L)$, où n est le degré de $H(L)$. Ceci découle du point précédent et du fait que cette action préserve le degré en X et Y (au sens usuel) des monômes.
3. Soit $L, S \in k[X,Y]$. On a $H(LS) = H(L)H(S)$.
Pour le montrer, on écrit $L = H(L) + L'$, $S = H(S) + S'$, et développer le produit donne $LS = H(L)H(S) + H(L)S' + H(S)L' + L'S'$. Comme $H(L)H(S)$ est homogène de degré $n+m$ où $n = d(H(L)), m = d(H(S))$, que le degré de $H(L)S' + H(S)L' + L'S'$ est $< n+m$, on on a bien le résultat.
4. Soit μ_{p-1} le sous-groupe de $k^\times$ des racines $(p-1)$-ième de l'unité, cyclique d'ordre $p-1$; soit aussi A l'ensemble des facteurs irréductibles de $P+1$. Alors A est fixé par μ_{p-1} : si $\lambda \in \mu_{p-1}$, $\lambda \cdot A = A$.
Ceci provient du fait que $P+1$ est fixé par μ_{p-1} d'après le point 1 (si $\lambda \in \mu_{p-1}$, $\lambda \cdot (P+1) = \lambda \cdot P + \lambda \cdot 1 = \lambda^{p-1} P + 1 = P + 1$). Ainsi, si $\lambda \in \mu_{p-1}$ et Q est un facteur irréductible de $P+1 = QS$, $\lambda \cdot (P+1) = (\lambda \cdot Q)(\lambda \cdot S)$ donc $\lambda \cdot Q$ divise aussi P et est irréductible (car de même si U divise $\lambda \cdot Q$, $\lambda^{-1} \cdot U$ divise Q donc U est un diviseur trivial).
5. Soit $Q_1 \in A$ quelconque. Alors l'orbite de Q_1 sous l'action de μ_{p-1} est non triviale. On aurait en effet, dans le cas contraire, pour ζ générateur de μ_{p-1}, $\zeta \cdot Q_1 = Q_1$ donc $H(\zeta \cdot Q_1) = \zeta^n H(Q_1) = H(Q_1)$ d'où $n \mid p-1$. Or, $1 \leq n = d(H(Q_1)) \leq d(Q_1) < p-1$ car $P+1$ est supposé non irréductible, c'est absurde. On note $Q_2 = \zeta \cdot Q_1 \neq Q_1$, qui est dans A par le point 4.

Ecrivons alors $P + 1 = cQ_1 Q_2 \cdots Q_r$ en produit de facteurs irréductibles, où $c \in k^\times$. Alors par les points 3 puis 2 :

$$P = H(P+1) = cH(Q_1)H(Q_2)\cdots H(Q_r) = c\zeta^n H(Q_1)^2 \cdots H(Q_r)$$

ce qui montre que P a un facteur carré et conclut. ■

Corollaire 3.1. *Le polynôme $\overline{A} - 1$ est irréductible dans $\mathbb{F}_p[Q,R]$.*

Démonstration. C'est une application directe du Lemme 3.2 et du Lemme 3.1 avec $P = \overline{A}$ et $(u,v) = (4,6)$. ■

3.4 Théorème de structure de Swinnerton-Dyer

Soit $\mathfrak{a}$ le noyau du morphisme $\mathbb{F}_p[Q,R] \twoheadrightarrow M(\mathbb{F}_p)$. On a le résultat de structure très fort suivant :

Théorème 3.1 (Swinnerton-Dyer)**.** *L'idéal $\mathfrak{a}$ est principal engendré par $\overline{A} - 1$. Ainsi,*

$$M(\mathbb{F}_p) \simeq \mathbb{F}_p[Q,R]/(\overline{A} - 1)$$

Démonstration. On sait déjà que $\overline{A} - 1 \in \mathfrak{a}$, car on a vu en Proposition 2.2 que $A(E_4, E_6) - 1 \equiv E_{p-1} - 1 \equiv 0 \pmod p$. L'idéal $\mathfrak{a}$ est premier, puisque $\mathbb{F}_p[Q,R]/\mathfrak{a} \simeq M(\mathbb{F}_p)$ est un anneau intègre (c'est un sous-anneau des séries formelles sur $\mathbb{F}_p$, qui est intègre). De plus, par le Corollaire 3.1, $\overline{A} - 1$ est irréductible dans $\mathbb{F}_p[Q,R]$. Par le Lemme 3.3, ou bien $\mathfrak{a} = (\overline{A} - 1)$, ou bien $\mathbb{F}_p[Q,R]/\mathfrak{a} \simeq M(\mathbb{F}_p)$ est de $\mathbb{F}_p$-dimension finie. Mais ce second cas est impossible, car $M(\mathbb{F}_p)$ contient les sous-espaces $M_k(\mathbb{F}_p)$ qui sont de $\mathbb{F}_p$-dimension arbitrairement grande d'après la Proposition 2.1. Ceci achève la preuve du théorème. ■

Lemme 3.3. *Soit k un corps, $\mathfrak{p}$ un idéal premier de $k[X,Y]$ et $f \in \mathfrak{p}$ irréductible dans $k[X,Y]$. L'une des assertions suivantes est vérifiée :*

- *ou bien $\mathfrak{p} = (f)$;*
- *ou bien $k[X,Y]/\mathfrak{p}$ est de k-dimension finie.*

Démonstration. Supposons $(f) \subsetneq \mathfrak{p}$. Soit alors $h \in \mathfrak{p} \setminus (f)$. En décomposant h en produit d'éléments irréductibles et en utilisant le fait que $\mathfrak{p}$ est premier, $\mathfrak{p}$ contient un irréductible g différent de f. Le lemme qui suit nous donne alors $k[X,Y]/(f,g)$ est de k-dimension finie, et comme cet espace se projette linéairement sur $k[X,Y]/\mathfrak{p}$, on a le résultat voulu. ■

Lemme 3.4. *Soit k un corps et $f, g \in k[X,Y]$ premiers entre eux. Alors (f,g) est de codimension finie dans $k[X,Y]$.*

Démonstration. Montrons dans un premier temps que f, g sont premiers entre eux en tant qu'éléments de $K[Y]$ où $A = k[X]$ et $K = k(X) = \operatorname{Frac} A$.
Soit $h \in K[Y]$ un diviseur commun à f et g; on écrit $f = hf^*$ et $g = hg^*$ où $f^*, g^* \in K[Y]$. En regardant le contenu de Gauss de ces égalités : $c(f) = c(h)c(f^*)$ et $c(g) = c(h)c(g^*)$ d'où

$$f = c(f)\frac{h}{c(h)}\frac{f^*}{c(f^*)} \quad \text{et} \quad g = c(g)\frac{h}{c(h)}\frac{f^*}{c(f^*)}$$

Or, par définition du contenu, les polynômes $\dfrac{h}{c(h)}$, $\dfrac{f}{c(f)}$ et $\dfrac{g}{c(g)}$ sont dans $A[Y]$ donc $\dfrac{h}{c(h)}$ est un diviseur commun de f et g dans $A[Y] = k[X,Y]$ donc est une constante ce qui donne h constant.

On peut donc écrire $a^*f + b^*g = 1$ où $a^*, b^* \in K[Y]$, puis en multipliant par un multiple commun dans $A = k[X]$ les dénominateurs des coefficients de a^* et b^*, on obtient $af + bg = c$ où $a, b \in A[Y] = k[X,Y]$ et $c \in k[X]$ non nul. On obtient donc que $c \in (f,g)$, puis en échangeant X et Y, on a $c' \in k[Y]$ non nul tel que $c' \in (f,g)$. Ainsi, $\overline{X}$ et $\overline{Y}$ sont k-algébriques dans $k[X,Y]/(f,g)$ qui est par conséquent une extension de k engendrée par un nombre fini d'éléments algébriques, donc est de k-dimension finie. ■

3.5 Graduation

Définition 3.2. Soit G un groupe abélien, A un anneau. On dit que A est *gradué par G* si on dispose de sous-groupes $A_g \subseteq A$ pour $g \in G$ tels que $A_g A_h \subseteq A_{g+h}$ pour $g, h \in G$ et $A = \bigoplus_{g \in G} A_g$.

Par exemple, on a vu que si A est un sous-anneau de $\mathbb{C}$, $M(A)$ est un anneau gradué par $\mathbb{Z}$.

Si I est un idéal d'un anneau $A = \bigoplus_{g \in G} A_g$ gradué par G, on dit que I est *homogène* si $I = \bigoplus_{g \in G} (I \cap A_g)$ (ce qui signifie que pour tout $a \in I$, les composantes homogènes de a sont dans I).

Proposition 3.5. *Si I est homogène, alors A/I est gradué par G :*

$$A/I = \bigoplus_{g \in G} (A_g + I)/I$$

Démonstration. Il est clair que $A = \sum_{g \in G} (A_g + I)/I$. On a maintenant que cette somme est directe : si $\sum_{g \in G} \overline{b}_g = \overline{0}$ où les $b_g \in A_g + I$ sont presque tous nuls, on écrit $b_g = a_g + c_g$ où $a_g \in A_g$ et $c_g \in I$, et alors $\sum_{g \in G} a_g + \sum_{g \in G} c_g \in I$ soit $\sum_{g \in G} a_g \in I$, ce qui impose $a_g \in I$ pour tout I car I homogène. On a donc $\overline{b}_g = \overline{0}$ d'où le caractère directe de la somme.
Les $(A_g + I)/I$ pour $g \in G$ forment maintenant bien une graduation de A/I car si $g, h \in G$,

$$(A_g + I)(A_h + I) \subseteq A_g A_h + I \subseteq A_{g+h} + I$$

donc $(A_g + I)/I \cdot (A_h + I)/I \subseteq (A_{g+h} + I)/I$ qui conclut. ■

Corollaire 3.2. *L'anneau $M(\mathbb{F}_p)$ est gradué par $\mathbb{Z}/(p-1)\mathbb{Z}$: posons, pour tout $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$,*

$$M_\alpha(\mathbb{F}_p) := \bigcup_{k\in\alpha} M_k(\mathbb{F}_p)$$

qui est un $\mathbb{F}_p$-ev d'après le Corollaire 2.1. Alors

$$M(\mathbb{F}_p) = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} M_\alpha(\mathbb{F}_p)$$

On a donc une notion de poids des formes modulaires modulo p, où le poids est pris modulo $p-1$.

Démonstration. On a une graduation

$$\mathbb{F}_p[Q,R] = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} E_\alpha[Q,R]$$

où l'on a posé $E_\alpha[Q,R]$ l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{F}_p$ des monômes Q^rR^s où $4r+6s \in \alpha$ pour $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$.
L'idéal $(\overline{A}-1)$ est homogène : comme $\overline{A}-1$ est de degré $p-1$, $(\overline{A}-1)E_\alpha[Q,R] \subseteq E_\alpha[Q,R]$ pour tout $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$. Si $P \in (\overline{A}-1)$, on écrit $P = (\overline{A}-1)Q$ où $Q = \sum_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} Q_\alpha$, puis $P = \sum_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} (\overline{A}-1)Q_\alpha$. Comme $(\overline{A}-1)Q_\alpha \in E_\alpha[Q,R]$, les composantes homogènes de P sont dans $(\overline{A}-1)$.
Par la Proposition 3.5, on obtient une graduation

$$\mathbb{F}_p[Q,R]/(\overline{A}-1) = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} E_\alpha[Q,R]/(\overline{A}-1)E_\alpha[Q,R]$$

Et l'isomorphisme $\mathbb{F}_p[Q,R]/(\overline{A}-1) \simeq M(\mathbb{F}_p)$ envoie $E_\alpha[Q,R]/(\overline{A}-1)E_\alpha[Q,R]$ sur $M_\alpha(\mathbb{F}_p)$. ■