ÉTUDE DE CERTAINES FORMES MODULAIRES DE SIEGEL DE GENRE 2

SALIM TAYOU

Mémoire de master 2
encadré par Gaëtan Chenevier

Table des matières

Date: 20 décembre 2016.

1. Introduction

On s'intéresse dans ce mémoire à l'étude des formes modulaires classiques et des formes modulaires de Siegel. L'étude des formes modulaires remonte aux travaux de Klein sur les courbes elliptiques à la fin du dix-neuvième siècle. L'un des premiers exemples de formes modulaires est la fonction Δ de Jacobi

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n,$$

où $q = e^{2i\pi z}$. Les propriétés mystérieuses des coefficients $\tau(n)$ attira plusieurs grands mathématiciens à investir ce domaine. C'est ainsi que Ramanujan conjectura que $\tau(mn) = \tau(m)\tau(n)$ dès que m et n sont premiers entre eux, $\tau(p^{k+1}) = \tau(p^k)\tau(p) - p\tau(p^{k-1})$ pour p premier ou encore que $|\tau(p)| \leq 2p^{\frac{11}{2}}$ pour tout nombre premier p. La démonstration des deux premières propriétés est due à Hecke qui eut l'idée de faire agir une algèbre d'endomorphisme sur l'espace des formes modulaires, connue maintenant sous le nom d'algèbre de Hecke. Quant à la seconde propriété, elle fut démontrée par Deligne en plusieurs étapes, d'abord en se ramenant aux conjectures de Weil, puis en démontrant les conjectures de Weil.
L'étude des formes modulaires de Siegel fut initiée, comme son nom l'indique, par Siegel. Il s'agit cette fois de considérer des fonctions définies sur le demi espace de Siegel $\mathcal{H}_g$ pour g entier naturel non nul. On sait associer, dans un sens qui sera clair plus tard, à ces formes modulaires des représentations galoisiennes ℓ-adiques, pour ℓ nombre premier. Le résultat principal de ce mémoire sera de démontrer que ces représentations sont irréductibles et de donner la forme de leurs

images, pour $g = 2$ et pour ℓ assez grand avec une borne calculable explicitement.
Je tiens à remercier Gaëtan Chenevier pour ses nombreuses explications et le temps précieux qu'il m'a accordé. Je tiens à remercier également Quentin Guignard pour les corrections qu'il a apportées à ce document.

2. Formes modulaires classiques

2.1. **Introduction.** Nous introduisons dans cette partie les objets de base de la théorie des formes modulaires classiques, à savoir le demi-plan de Poincaré et les sous groupes discrets de $\mathrm{Sl}_2(\mathbb{Z})$. Nous nous inspirerons de l'exposition donnée dans [15] et [5]. On se place dans le demi plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C}/z = x + iy, y > 0\}$
Le groupe spécial linéaire $\mathrm{SL}(2, \mathbb{R})$ agit sur $\mathcal{H}$ via :

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathcal{H} \to \mathcal{H}, \qquad z \mapsto \gamma z = \quad \frac{az + b}{cz + d}$$

Il est facile de voir que l'action est bien définie à partir de l'identité

$$Im(\gamma z) = \frac{Im(z)}{|cz + d|^2}$$

et qu'elle est transitive.

On s'intéressera plus particulièrement à la restriction de cette action à des sous groupes discrets de $\mathrm{SL}(2, \mathbb{R})$.
On fixe un entier naturel N non nul. On définit :

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}), a \equiv d \equiv 1 \pmod{N};\ b \equiv c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}), a \equiv d \equiv 1 \pmod{N}; c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}), c \equiv 0 \pmod{N} \right\}.$$

Ce sont tous des sous-groupes de $\mathrm{SL}(2, \mathbb{Z})$. Le quotient $\Gamma_0(N)/\Gamma_1(N)$ s'identifie à $(\mathbb{Z}/N\mathbb{Z})^\times$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$. On peut vérifier qu'ils sont d'indice fini dans $SL(2, \mathbb{Z})$ et on a les formules suivantes :

$$[\mathrm{SL}(2, \mathbb{Z}) : \Gamma_0(N)] = N \prod_{p/N} (1 + \frac{1}{p}),$$

$$[\mathrm{SL}(2, \mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p/N} (1 + \frac{1}{p}),$$

où p parcourt l'ensemble des nombres premiers. Notons Γ un des sous-groupes $\Gamma(N)$, $\Gamma_1(N)$ ou $\Gamma_0(N)$. Le quotient de $\mathcal{H}$ par l'action de Γ peut être muni d'une structure de surface de Riemann pour laquelle l'application de passage au quotient $\pi : \mathcal{H} \to \Gamma\backslash\mathcal{H}$ est holomorphe. On notera alors $Y(N) := \Gamma(N)\backslash\mathcal{H}$, $Y_1(N) := \Gamma_1(N)\backslash\mathcal{H}$, $Y_0(N) := \Gamma_0(N)\backslash\mathcal{H}$. On peut compactifier ces surfaces en rajoutant un nombre fini de points (voir [5], chapitre 2) pour obtenir des surfaces de Riemann compactes notées respectivement $X(N)$, $X_1(N)$, $X_0(N)$.
Le groupe Γ agit à droite sur l'ensemble des fonctions f définies sur $\mathcal{H}$ à valeurs dans $\mathbb{C}$ via :

$$f[\gamma]_k(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

avec $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ et $k \in \mathbb{N}$.

Définition 2.1. *Soit k un entier naturel. On appelle forme modulaire de poids k et de niveau Γ une fonction $f : \mathcal{H} \to \mathbb{C}$ qui vérifie :*

(1) f est holomorphe sur $\mathcal{H}$

(2) $f[\gamma]_k(z) = f(z)$ pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

(3) Pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f[\gamma]_k$ vérifie $f[\gamma]_k(z+N) = f[\gamma]_k(z)$ pour tout z dans $\mathcal{H}$, donc admet un développement en série de Fourier de la forme $f[\gamma]_k(z) = \sum_{n=-\infty}^{n=\infty} a_n q_N^n$ avec $q_N = \exp\frac{2i\pi z}{N}$. On requiert alors que $a_n = 0$ pour $n < 0$.

Elle est dite parabolique, si de plus dans tous les développements précédents, $a_0 = 0$.

On notera $M_k(\Gamma)$ l'espace vectoriel sur $\mathbb{C}$ des formes modulaires de poids k et de niveau Γ. Son sous-espace vectoriel des formes paraboliques est noté $S_k(\Gamma)$. Notons également $M(\Gamma) := \bigoplus_{k\geq 0} M_k(\Gamma)$ l'algèbre graduée sur $\mathbb{C}$ des formes modulaires de niveau Γ et $S(\Gamma) := \bigoplus_{k\geq 0} S_k(\Gamma)$ son idéal des formes paraboliques.
Les espaces $M_k(\Gamma)$ et $S_k(\Gamma)$ sont de dimension finie (voir [5], chapitre 3). Comme $\Gamma_1(N)$ est distingué dans $\Gamma_0(N)$, il agit naturellement sur $S_k(\Gamma_1(N))$. Cette action se factorise par le quotient $\Gamma_0(N)/\Gamma_1(N) = (\mathbb{Z}/N\mathbb{Z})^\times$. On notera alors $\langle d\rangle$ l'action d'un élément d dans $(\mathbb{Z}/N\mathbb{Z})^\times$, dit opérateur de diamant . L'espace $S_k(\Gamma_1(N))$ se décompose alors sous la forme

$$S_k(\Gamma_1(N)) = \bigoplus_{\epsilon:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} S_k(N,\epsilon)$$

où ϵ parcourt l'ensemble des caractères de $(\mathbb{Z}/N\mathbb{Z})^\times$ et

$$S_k(N,\epsilon) = \{f \in S_k(\Gamma_1(N)), \langle d\rangle\, f = \epsilon(d)f, \quad \forall d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Remarquons que $S_k(N,1) = S_k(\Gamma_1(N))^{\Gamma_0(N)}$.

Exemple 2.2. *On définit les séries d'Eisenstein :*

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}\setminus(m,n)\neq(0,0)} \frac{1}{(cz+d)^k}; \quad (k>2, z\in\mathcal{H}).$$

Ce sont des formes modulaires de poids k et de niveau $\Gamma(1)$.
Leur q-développement est donné par (voir [15]) :

$$G_k(z) = 2\zeta(k) + 2\frac{2\pi i^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n = 2\zeta(k)E_k(z)$$

où $\sigma_{k-1}(n) = \sum_{d\setminus n} d^{k-1}$ et $E_k = 1 + \frac{2\pi i^k}{\zeta(k)(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$. On peut montrer que la $\mathbb{C}$-algèbre $M_k(\Gamma(1))$ est égale à $\mathbb{C}[E_4, E_6]$.
On définit la fonction Δ par :

$$\Delta(z) = \frac{1}{12^3}(E_4^3 - E_6^2) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

C'est l'unique forme parabolique de poids 12 de niveau $\Gamma(1)$ et normalisée (c'est-à-dire $\tau(1)=1$).

2.2. **Opérateurs de Hecke.** Nous introduisons dans ce paragraphe une algèbre d'opérateurs, dite algèbre de Hecke, qui agit sur l'espace des formes modulaires paraboliques, et dont les éléments sont normaux pour un produit scalaire hermitien, dit de Petersson. La commutativité de l'algèbre de Hecke assure l'existence d'une base formée de valeurs propres. Nous ne donnerons ici que des rappels. Pour plus de détails, nous renvoyons au chapitre 5 du livre de Diamond et Shurman [5].
Soient N un entier naturel non nul et p un nombre premier. Pour $f \in M_k(\Gamma_1(N))$, on rappelle que l'action de l'opérateur de Hecke T_p sur f est donnée par :

(1) $T_p f = \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right)$ si $p \mid N$.

(2) $T_p f = \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) + p^{k-1} < p > f(pz)$ si $p \nmid N$.

Si $f \in S_k(\Gamma_1(N))$ a pour développement $\sum_n a_n(f)q^n$, alors :

$$(T_p f)(z) = \sum_n a_{np}(f)q^n + 1_N(p)p^{k-1}\sum_n a_n(\langle p\rangle\, f)q^{np}$$

où 1_N est la caractère trivial modulo N. On étend ensuite l'opérateur diamant à $\mathbb{Z}$ tout entier de la manière suivante : si n est un entier premier à N alors $\langle n\rangle$ est l'opérateur donné par la classe de n modulo

N. Sinon, $\langle n\rangle$ est l'opérateur nul.
Ensuite, on pose :

— $T_1 = 1$;
— $T_{mn} = T_m \circ T_n$ si $(m,n) = 1$;
— $T_{p^r} = T_p \circ T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}$ pour $r \geq 2$, et p premier.

Ils commutent entre eux sur $S_k(\Gamma_1(N))$ et satisfont l'identité formelle

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{(p,N)=1} (1 - T_p p^{-s} + \langle p\rangle p^{k-1} p^{-2s})^{-1} \prod_{p\backslash N} (1 - T_p p^{-s})^{-1}.$$

On peut munir $S_k(\Gamma_1(N))$ d'un produit scalaire hermitien, dit produit scalaire de Petersson (voir [5]), pour lequel les opérateurs T_n et $\langle n\rangle$, avec $(n,N) = 1$, sont normaux, donc simultanément diagonalisables.

Une forme parabolique $f = \sum_n a_n q^n$ propre pour tous les opérateurs de Hecke est dite normalisée si elle vérifie en plus $a_1 = 1$. Dans ce cas, on a $T_n(f) = a_n f$, pour tout entier $n \geq 1$. On note $\mathbb{Q}(f)$ le corps engendré par les $(a_n)_{n\in\mathbb{Q}}$. Alors $\mathbb{Q}(f)$ est une extension finie de $\mathbb{Q}$ (voir [5]).

On définit la série L de Dirichlet d'une forme parabolique par l'expression suivante

$$L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s}.$$

Proposition 2.3 ([5], Chap.5)**.** *Si $f \in M_k(\Gamma_1(N))$ est parabolique alors $L(s,f)$ converge absolument pour tout s tel que $Re(s) > \frac{k}{2} + 1$. De plus, si $f \in M_k(N,\epsilon)$, alors f est une forme propre normalisée si et seulement si $L(s,f)$ admet un développement en produit eulérien sous la forme*

$$L(s,f) = \prod_p \left(1 - a_p p^{-s} + \epsilon(p) p^{k-1-2s}\right)^{-1}.$$

2.3. **Représentations galoisiennes.** Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Pour tout nombre premier p, on fixe des clôtures algébriques $\overline{\mathbb{Q}_p}$ et $\overline{\mathbb{F}_p}$ du corps des nombres p-adiques $\mathbb{Q}_p$ et du corps fini $\mathbb{F}_p$ respectivement. Le choix d'un plongement $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ définit un plongement de $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ dans $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Ainsi, vu comme sous-groupe de $G_{\mathbb{Q}}$, $G_{\mathbb{Q}_p}$ s'appelle groupe de décomposition en p et il est bien défini à conjugaison près. On a

$$\overline{\mathbb{Q}_p} \supset \mathbb{Q}_p^{mr} \supset \mathbb{Q}_p^{nr} \supset \mathbb{Q}_p$$

où on note $\mathbb{Q}_p^{nr} = \mathbb{Q}_p(\xi_m, (m,p) = 1)$ la sous-extension maximale non ramifiée sur $\mathbb{Q}_p$, et $\mathbb{Q}_p^{mr}$ la sous-extension maximale modérément ramifiée sur $\mathbb{Q}_p$. On note $\mathrm{I}_p := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{nr})$, appelé groupe d'inertie en p, et $\mathrm{I}_p^s = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{mr})$ appelé le groupe d'inertie sauvage en p, c'est

un pro-p groupe. Le quotient $\mathrm{I}_p/\mathrm{I}_p^s$ est un groupe profini commutatif d'ordre premier à p, appelé groupe d'inertie modéré. Le quotient $G_{\mathbb{Q}_p}/\mathrm{I}_p$ s'identifie canoniquement à $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. L'élément de $G_{\mathbb{F}_p}$ défini par $a \mapsto a^p$ engendre topologiquement $G_{\mathbb{F}_p}$ et s'appelle morphisme de Frobenius. Sa pré-image dans $G_{\mathbb{Q}_p}$ est définie modulo I_p et s'appelle substitution de Frobenius en p, notée $Frob_p$.
Soient ℓ un nombre premier, L une extension finie de $\mathbb{Q}_\ell$ et V un espace vectoriel de dimension finie sur L. Une représentation continue $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ est appelée représentation ℓ-adique de $G_{\mathbb{Q}}$. Si $\dim_L(V) = n$, alors $\mathrm{GL}(V)$ est isomorphe en tant que groupe topologique à $\mathrm{GL}_n(L)$. Une représentation ℓ-adique est dite non-ramifiée en p si $\mathrm{I}_p \subset Ker(\rho)$. Dans ce cas $\rho(Frob_p)$ est bien défini.

Définition 2.4. *Soient $f = \sum_n a_n q^n \in S_k(N, \epsilon)$ une forme propre normalisée et $\mathbb{Q}(f) \to E$ un plongement dans une extension finie de $\mathbb{Q}_\ell$. Une représentation ℓ-adique V de dimension 2 sur E est dite associée à f si, pour tout nombre premier p qui ne divise pas $N\ell$, V est non ramifiée en p et*

$$\det(1 - XFrob_p : V) = 1 - a_p(f)X + \epsilon(p)p^{k-2}X^2.$$

On a alors le théorème suivant :

Théorème 2.5 ([15])**.** *Soient $N \geq 1$ et $k \geq 2$ des entiers et $\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^\times$ un caractère. Soient $f \in S_k(N, \epsilon)$ une forme propre normalisée et λ une place de $\mathbb{Q}(f)$ au dessus de ℓ. Alors il existe une représentation ℓ-adique $V_{f,\lambda}$ définie sur $\mathbb{Q}(f)_\lambda$ associée à f.*

Remarque 2.6.

Étant donné une forme modulaire comme dans le théorème, on sait donc qu'il existe une représentation continue $\rho : G_{\mathbb{Q}} \to GL(V)$ associée à cette forme modulaire, où V est espace vectoriel de dimension 2 sur une extension finie F de $\mathbb{Q}_\ell$. On peut trouver un réseau L de V stable par ρ. En effet, partant de n'importe quel réseau L, la représentation étant continue, l'ensemble $\{g \in G_{\mathbb{Q}}, g.L = L\}$ est un sous-groupe ouvert de $G_{\mathbb{Q}}$ donc d'indice fini. On prend alors le réseau engendré par les $g.L$, pour $g \in G_{\mathbb{Q}}$. On considère ensuite le quotient $L/\pi L$, où π est une uniformisante de l'anneau de valuation de F. C'est une représentation de $G_{\mathbb{Q}}$ de dimension 2 telle que que pour tout nombre premier p ne divisant pas $N\ell$, on a $\det(1 - XFrob_p) = 1 - \widetilde{a_p(f)}X + \widetilde{\epsilon(p)}p^{k-2}X^2$, où $\widetilde{x}$ signifie la réduction d'un élément entier x de F modulo π. Réciproquement, étant donné une représentation continue de dimension 2 sur $\overline{\mathbb{F}_\ell}$, une question intéressante serait de savoir quand est ce qu'elle est la réduction d'une représentation galoisienne associée à une forme

modulaire. On dira dans ce cas que la représentation est modulaire. L'objectif du paragraphe suivant est de donner une condition suffisante de modularité.

3. Conjecture de Serre

Soient p un nombre premier et $\overline{\mathbb{F}}_p$ une clôture algébrique du corps fini $\mathbb{F}_p$. On se donne un morphisme continu $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ où V est un espace vectoriel de dimension 2 sur $\overline{\mathbb{F}}_p$. Considérons un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}$. On note alors c l'élément de $G_{\mathbb{Q}}$ donné par la conjugaison complexe. On dira que la représentation ρ est impaire si $\det(\rho(c)) = -1$. Remarquons que cela est indépendant du plongement choisi de $\overline{\mathbb{Q}}$ dans $\mathbb{C}$, car on ne change c qu'à conjugaison près. On a introduit la notion de modularité dans la remarque qui suit le théorème 2.5. Serre a conjecturé dans [19] le résultat suivant : :

Théorème 3.1 (Conjecture de Serre-Version faible)**.** *Si ρ est irréductible et impaire alors ρ est modulaire.*

En fait, Serre donne encore plus de détails sur la forme modulaire de laquelle proviendrait la représentation en précisant son niveau, son poids et son caractère. La recette proposée par Serre est la suivante :

3.1. **Niveau de la représentation.** il est donné par le conducteur d'Artin de la représentation. De façon plus précise, soit ℓ un nombre premier, avec $\ell \neq p$. Choisissons une extension à $\overline{\mathbb{Q}}$ de la valuation ℓ-adique sur $\mathbb{Q}$. Considérons alors la suite des groupes de ramifications (voir [17], Partie 2, chap.4)

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset \cdots ,$$

où G_0 est le groupe d'inertie en ℓ. On pose alors

$$n(l, \rho) = \sum_{i=0}^{\infty} \frac{\dim V/V^{G_i}}{[G_0 : G_i]}.$$

C'est un entier positif, égal à 0 si et seulement si la représentation est non ramifiée en ℓ, et $n(l, \rho) = \dim V/V_0$ si, et seulement si, la représentation est modérément ramifiée en ℓ. Le conducteur de ρ est donné par

$$N(\rho) = \prod_{l \neq p} l^{n(l,\rho)}.$$

3.2. **Caractère de la représentation.** Le caractère associé à la représentation est défini de la manière suivante : le déterminant $\det\rho : G_{\mathbb{Q}} \to {\overline{\mathbb{F}}_p}^{\times}$ est un morphisme de groupes, d'image un sous-groupe cyclique fini de ${\overline{\mathbb{F}}_p}^{\times}$, d'ordre premier à p.

Le conducteur de $\det\rho$ divise pN. Il induit donc d'après le théorème de Kronecker-Weber, un homomorphisme de $(\mathbb{Z}/pN\mathbb{Z})^{\times}$ dans ${\overline{\mathbb{F}}_p}^{\times}$, ou, de manière équivalente, un couple d'homomorphismes

$$\phi : (\mathbb{Z}/p\mathbb{Z})^{\times} \to {\overline{\mathbb{F}}_p}^{\times}$$

et

$$\epsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to {\overline{\mathbb{F}}_p}^{\times}$$

ce qui définit le caractère ϵ.
Avant de définir le poids de la représentation, faisons un petit intermède sur les caractères fondamentaux. On pourra aussi consulter à profit la partie préliminaires de l'article [18] de Serre.

3.3. **Caractères fondamentaux.** On se donne un nombre premier p, et on fixe une clôture algébrique $\overline{\mathbb{Q}_p}$ du corps des nombres p-adiques $\mathbb{Q}_p$ et $\overline{\mathbb{F}_p}$ du corps fini $\mathbb{F}_p$. On fixe un isomorphisme $\sigma : \mathbb{Z}_p^{nr}/p\mathbb{Z}_p^{nr} \to \overline{\mathbb{F}_p}$, où $\mathbb{Z}_p^{nr}$ désigne l'anneau des entiers de $\mathbb{Q}_p^{nr}$. Le groupe d'inertie en p est $\mathrm{I}_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{nr})$.

Si $N > 0$, on notera x_N une racine (p^N-1)-ième de p dans $\overline{\mathbb{Q}_p}$ On définit alors le caractère fondamental de niveau N par la composée

$$\psi_N : \mathrm{I}_p \to \mu_{p^N-1} \to \overline{\mathbb{F}_p}$$

donnée par

$$\tau \mapsto \frac{\tau(x_N)}{x_N} \mapsto \sigma\left(\frac{\tau(x_N)}{x_N}\right).$$

Ceci est indépendant du choix de x_N car I_p agit trivialement sur les racines (p^N-1)-ième l'unité dans $\overline{\mathbb{Q}_p}$. L'image de ψ_N est alors le groupe multiplicatif de l'unique sous-corps de $\overline{\mathbb{F}_p}$ de cardinal p^N.

Lemme 3.2. *ψ_1 est le caractère cyclotomique modulo p restreint à I_p. Si M divise N alors $\psi_M = {\psi_N}^{\frac{p^N-1}{p^M-1}}$.*

Démonstration. Notons ξ_p une racine p-ième de l'unité et $K = {\mathbb{Q}_p}^{nr}(\xi_p)$ alors $p = (1-\xi_p)^{p-1}.u$ avec $u = \prod_{a\in(\mathbb{Z}/p\mathbb{Z})^{\times}} \frac{1-\xi_p^a}{1-\xi_p}$. Remarquons que u est une unité de O_K car il est dans O_K et son inverse aussi. Par ailleurs, pour $\sigma \in \mathrm{I}_p$, on a par définition du caractère cyclotomique χ_p, $\sigma(\xi_p) = {\xi_p}^{\chi_p(\sigma)}$. On va construire une racine $(p-1)$-ième de u dans K. Considérons le polynôme $P(X) = X^{p-1}-u$. Sa réduction modulo l'idéal

maximal de O_K est un polynôme séparable dans $\overline{\mathbb{F}_p}$ donc il est scindé dans une extension finie de $\mathbb{F}_p$, disons $\mathbb{F}_{p^r}$ pour $r \geq 1$. Soit L le corps des fractions de $W(\mathbb{F}_{p^r})$, l'anneau des vecteurs de Witt à coefficients dans $\mathbb{F}_{p^r}$. L est donc une extension finie non ramifiée de $\mathbb{Q}_p$ de corps résiduel $\mathbb{F}_{p^r}$. Alors P est scindé dans le corps résiduel de $L(\xi_p)$, qui est une extension finie de $\mathbb{Q}_p$, donc par le lemme de Hensel, il existe v dans $L(\xi_p) \subset K$ qui soit racine de P, donc racine $(p-1)$-éme de u et qui soit de réduction égale à une racine de P dans $\mathbb{F}_{p^r}$. En particulier, $\sigma(v)$ est congru à v modulo l'idéal maximal de K. Ainsi, $(1-\xi_p)v$ est une racine $(p-1)$-ième de p. D'où :

$$\begin{aligned}\psi_1(\sigma) = \frac{\sigma(v)}{v}\frac{1-\xi_p^{\chi_p(\sigma)}}{1-\xi_p} &= \frac{\sigma(v)}{v}\left(\sum_{t=0}^{\chi_p(\sigma)-1}\xi_p^t\right)\\ &\equiv \frac{v}{v}\left(\sum_{t=0}^{\chi_p(\sigma)-1}1\right) \pmod{\ell}\\ &\equiv \chi_p(\sigma) \pmod{\ell}.\end{aligned}$$

Pour le deuxième point, il suffit de remarquer que $x_N^{\frac{p^N-1}{p^M-1}}$ est une racine (p^M-1)-ième de ℓ. □

3.4. **Poids de la représentation.** Soit ρ_p la restriction de ρ à $D_p := G_{\mathbb{Q}_p}$, le groupe de décomposition en p. Rappelons que I_p désigne le sous-groupe d'inertie en p. Alors l'action de I_p est donnée dans une base convenable sous l'une des formes suivantes [19] :

(1) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$;

(2) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}\psi_2^{\alpha+p\beta} & 0\\ 0 & \psi_2^{\beta+p\alpha}\end{pmatrix}$, avec $0 \leq \alpha < \beta \leq p-1$;

(3) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}\chi_p^{\alpha} & 0\\ 0 & \chi_p^{\beta}\end{pmatrix}$, avec $0 \leq \alpha \leq \beta \leq p-2$ et $(\alpha,\beta) \neq (0,0)$.

(4) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}\chi_p^{\beta} & *\\ 0 & \chi_p^{\alpha}\end{pmatrix}$, avec $0 \leq \alpha \leq p-2$ et $1 \leq \beta \leq p-1$ et $\beta \neq \alpha+1$;

(5) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}\chi_p^{\alpha+1} & *\\ 0 & \chi_p^{\alpha}\end{pmatrix}$, avec $0 \leq \alpha \leq p-2$, l'action de I_p n'étant pas semi simple et peu ramifiée;

(6) $\rho_{|\mathrm{I}_p} = \begin{pmatrix}\chi_p^{\alpha+1} & *\\ 0 & \chi_p^{\alpha}\end{pmatrix}$, avec $0 \leq \alpha \leq p-2$, l'action de I_p n'étant pas semi simple et très ramifiée;

Les poids correspondants sont respectivement :

(1) $k(\rho) = p$;
(2) $k(\rho) = 1 + p\alpha + \beta$;
(3) $k(\rho) = 1 + p\alpha + \beta$;
(4) $k(\rho) = 1 + p\inf(\alpha, \beta) + \sup(\beta, \alpha)$;
(5) $k(\rho) = 1 + p\alpha + (\alpha + 1)$;
(6) $k(\rho) = 1 + p\alpha + (\alpha + 1) + p - 1 = (\alpha + 1)(p + 1)$ si $p \neq 2$, $k(\rho) = 4$ si $p = 2$;

Dans les cas (5) et (6), le groupe d'inertie sauvage agit non trivialement. Il y a alors deux types possibles de ramification sauvage : peu ramifié et très ramifié. On les définit comme suit : le groupe $\rho_p(\mathrm{I}_p)$ définit une extension finie K totalement ramifiée de $\mathbb{Q}_p^{nr}$, alors que le groupe d'inertie sauvage $\rho_p(\mathrm{I}_p^s)$ définit la plus grande extension modérément ramifiée de $\mathbb{Q}_p^{nr}$ dans K, notée K_{mr}. On montre alors (voir [19]) que

$$K = K_{mr}(x_1^{\frac{1}{p}}, ..., x_m^{\frac{1}{p}}), \quad \text{où} \quad p^m = [K : K_{mr}],$$

les x_i étant des éléments de $\mathbb{Q}_p^{nr\times}/\mathbb{Q}_p^{nr\times p}$. Si v_p est la valuation de $\mathbb{Q}_p^{nr}$, normalisée par $v_p(p) = 1$, nous dirons que l'extension K (ou la représentation ρ_p) est peu ramifiée si

$$v_p(x_i) \equiv 0 \pmod{p}, \quad \text{pour} \quad i = 1, ..., m.$$

Dans le cas contraire, nous dirons que K et ρ_p sont très ramifiées.

Théorème 3.3 (Conjecture de Serre - Version forte)**.** *Soit ρ une représentation de de $G_{\mathbb{Q}}$ dimension 2 sur $\overline{\mathbb{F}_p}$. On suppose que ρ est irréductible et impaire. Alors ρ provient d'une forme modulaire de poids $k(\rho)$, de niveau $N(\rho)$ et de caractère $\epsilon(\rho)$.*

La conjecture de Serre a été démontrée par Chandrashekhar Khare et Jean-Pierre Wintenberger (voir [11]).

4. Un peu de théorie de Hodge p-adique

On parlera dans ce paragraphe des principaux résultats de la théorie de Hodge p-adique dont on aura besoin dans ce mémoire. On se contentera dans la plupart des cas de citer des résultats sans démonstrations en renvoyant à la référence appropriée.
Le but de la théorie de Hodge p-adique est de comprendre et de classifier les représentations p-adiques du groupe de décomposition D_p de $G_{\mathbb{Q}}$ au dessus d'un nombre premier p. Ce groupe s'identifie naturellement à $G_{\mathbb{Q}_p}$, le groupe de Galois absolu de $\mathbb{Q}_p$. La théorie fut initiée par Tate et son élève Sen, puis ensuite développée par Fontaine, Breuil, Colmez... .

4.1. **Représentations p-adiques.** Soit k un corps parfait de caractéristique p. On note $F = W(k)[\frac{1}{p}]$ le corps des fractions de l'anneau des vecteurs de Witt de k. Soit K/F une extension totalement ramifiée, et soit $C = \widehat{\overline{K}}$ une complétion d'une clôture algébrique de K. Dans le cas où k se plonge dans $\overline{\mathbb{F}_p}$, on notera $C = \mathbb{C}_p$, le corps des nombres complexes p-adiques. On se placera sous cette hypothèse dorénavant. On rappelle que $\mathbb{C}_p$ est algébriquement clos. Si k est une extension finie de $\mathbb{F}_p$ alors K est une extension finie de $\mathbb{Q}_p$ et F en est l'extension maximale non ramifiée.
Pour n entier naturel, soit $\mu_n(\overline{K}) = \{x \in \overline{K}, x^n = 1\}$. On fixe une fois pour toute un système compatible de racines primitives p^n-ème de l'unité $(\epsilon_n)_{n\in\mathbb{N}}$ avec $\epsilon_0 = 1$ et $\epsilon_n \in \mu_m(\overline{K})$ tel que $\epsilon_{n+1}^p = \epsilon_m$ et $\mu_{p^\infty} = \cup_{n\in\mathbb{N}}\mu_{p^n}$. Soit $K_m = K(\epsilon_m)$, $K_\infty = \cup_{n\in\mathbb{N}}K_n$. Soit $G_K = \mathrm{Gal}(\overline{K}/K)$ et $\chi_p : G_K \to {\mathbb{Z}_p}^\times$ le caractère cyclotomique, i.e : $\sigma(\xi) = \xi^{\chi_p(\sigma)}$, $\sigma \in G_K$, $\xi \in \mu_{p^\infty}$. On alors $\mathrm{Ker}(\chi_p) = \mathrm{Gal}(\overline{K}/K_\infty)$ et $\Gamma_K = \mathrm{Gal}(K_\infty/K)$ s'injecte continument dans ${\mathbb{Z}_p}^\times$, c'est même un isomorphisme quand $K = \mathbb{Q}_p$. Une représentation p-adique de G_K est un $\mathbb{Q}_p$-espace vectoriel V de dimension finie d et muni d'une action linéaire continue de G_K. Les représentations p-adiques forment une catégorie abélienne, avec comme morphismes les applications $\mathbb{Q}_p$-linéaires G_K-invariantes. On la note $Rep_{\mathbb{Q}_p}(G_K)$.

Exemple 4.1. *Pour $r \in \mathbb{Z}$, on note $\mathbb{Q}_p(r) = \mathbb{Q}_p.e_r$ avec l'action de $G_{\mathbb{Q}_p}$ donnée par $\sigma.e_r = \chi_p(\sigma)^r e_r$. C'est la r-torsion de Tate de $\mathbb{Q}_p$. Un autre exemple est donné par le module de Tate d'une courbe elliptique E, $V = \mathbb{Q}_p \otimes T_pE$. C'est une représentation p-adique de dimension 2. Plus généralement, si on considère X une variété projective lisse sur K, alors la cohomologie étale de la variété $H^i_{et}(X_{\overline{K}}, \mathbb{Q}_p)$ est une représentation p-adique de $G_{\mathbb{Q}_p}$.*

Le dernier exemple est d'une importance capitale, le deuxième en étant juste un cas particulier, et c'est l'une des motivations de l'étude des représentations p-adiques.
L'une des méthodes d'étude des représentations p-adiques est celle développée par Fontaine. On définit d'abord un anneau de périodes B : c'est une algèbre topologique sur $\mathbb{Q}_p$ munie d'une action linéaire continue de G_K et des structures additionnelles compatibles avec l'action de G_K, de telle manière à ce que le B^{G_K}-module $D_B(V) = (B \otimes_{\mathbb{Q}_p} V)^{G_K}$, qui hérite de ces structures, soit un invariant intéressant de V. L'action de G_K sur $B\otimes_{\mathbb{Q}_p}V$ est ici l'action diagonale. Pour que cette construction marche, il faudrait en plus supposer que B est G_K-régulier, c'est-à-dire

que B^{G_K} est un corps.
Soit V une représentation p-adique de G_K.

Définition 4.2. *La représentation V est dite B-admissible si $V \otimes_{\mathbb{Q}_p} B$ est une B-représentation triviale de G_K, i.e isomorphe à B^n pour un certain entier n.*

L'action de G_K sur $V \otimes_{\mathbb{Q}_p} B$ est semi-linéaire, car G_K agit non trivialement sur B en général. On va donner une autre caractérisation des représentations B-admissibles, si B est un anneau de période G_K-régulier. Tout d'abord, on dispose de l'application naturelle

$$\alpha_V : D_B(V) \otimes_K B \to V \otimes_{\mathbb{Q}_p} B, v \otimes \lambda \mapsto \lambda v$$

.

Théorème 4.3 ([8, 2])**.** *L'application α_V est injective, et on équivalence entre les propriétés suivantes :*

(1) La représentation V est B-admissible ;

(2) Le morphisme α_V est un isomorphisme ;

(3) On a l'égalité $\dim_{B^{G_K}} D_B(V) = \dim_{\mathbb{Q}_p} V$

Il en résulte notamment du théorème que l'on a toujours

$$\dim_{B^{G_K}} D_B(V) \leq \dim_{\mathbb{Q}_p} V.$$

Dans ce qui suit, les représentations que l'on va définir correspondent à des choix particuliers d'anneaux de périodes.

4.2. **Représentations de Hodge-Tate.** Soit H un sous-groupe fermé de G_K. Une des propriétés importantes de $\mathbb{C}_p$ est que l'on sait décrire $\mathbb{C}_p^H$, le sous-corps des éléments de $\mathbb{C}_p$ invariants par l'action de H. On a clairement $\overline{K}^H \subset \mathbb{C}_p^H$. Comme $\mathbb{C}_p^H$ est complet, le complété de $\overline{K}^H$, noté $\widehat{\overline{K}^H}$, est inclus dans $\mathbb{C}_p^H$.

Théorème 4.4 (Le théorème d'Ax-Sen-Tate)**.** *Soit H un sous-groupe fermé de G_K. On a alors l'égalité $\mathbb{C}_p^H = \widehat{\overline{K}^H}$.*

On définit l'anneau de Hodge-Tate $B_{HT} = \mathbb{C}_p[T, T^{-1}] = \bigoplus_{i\in\mathbb{Z}} \mathbb{C}_p(i)$, avec $\mathbb{C}_p(i) = \mathbb{C}_p T^i$, et on fait agir G_K sur T^i par χ_p^i, pour $i \in \mathbb{Z}$, χ_p étant le caractère cyclotomique. On a donc $B_{HT}^{G_K} = K$, et par conséquent, B_{HT} est G_K-régulier. Si V est une représentation p-adique, on notera $D_{HT}(V) = (B_{HT} \otimes_{\mathbb{Q}_p} V)^{G_K}$.

Définition 4.5 (Représentations de Hodge-Tate)**.** *Soit V une représentation p-adique continue de G_K. On dit que V est de Hodge-Tate, si V est B_{HT}-admissible.*

Du fait que chaque composante $\mathbb{C}_p(i)$ est G_K-stable, on a $D_{HT}(V) = \bigoplus_{i\in\mathbb{Z}}(\mathbb{C}_p(i)\otimes_{\mathbb{Q}_p} V)^{G_K}$. Donc si V est de Hodge-Tate, il n'existe qu'un nombre fini de i tel que $(\mathbb{C}_p(i)\otimes_{\mathbb{Q}_p} V)^{G_K}$ soit non nul, et si on les compte avec une multiplicité égale à $\dim_K (\mathbb{C}_p(i)\otimes_{\mathbb{Q}_p} V)^{G_K}$, on obtient exactement n entiers. On les appelle les poids de Hodge-Tate de V.

4.3. **Représentations de de Rham.** On définit

$$\widetilde{E}^+ = \varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p} = \{(x_0, x_1, ...), (x_{i+1})^p = x_i\}.$$

On peut munir cet ensemble d'une structure d'anneau : pour deux éléments $x = (x^{(i)})$ et $y = (y^{(i)})$ de $\widetilde{E}^+$, l'addition est définie par $(x+y)_i = \lim_{j\to\infty}\left(x_{(i+j)} + y_{(i+j)}\right)^{p^j}$ et la multiplication par $(xy)_{(i)} = x_{(i)}y_{(i)}$. Ces deux lois font de $\widetilde{E}^+$ un anneau local parfait de caractéristique p. Soit $\epsilon = (\epsilon_n)$ l'élément de $\widetilde{E}^+$ correspondant au système compatible des racines primitives p^n-ième de l'unité déjà introduit. Alors $\mathbb{F}_p((\epsilon-1)) \subset \widetilde{E} = \widetilde{E}^+[(\epsilon-1)^{-1}]$. En fait, $\widetilde{E}$ est un corps et c'est la complétion de la clôture algébrique de $\mathbb{F}_p((\epsilon-1))$.
On définit une valuation sur $\widetilde{E}$ par $v_{\widetilde{E}}(x) = v_p(x_0)$. L'anneau de la valuation n'est rien d'autre que $\widetilde{E}^+$. On a une application naturelle θ de $\widetilde{E}^+$ vers $\mathcal{O}_{\mathbb{C}_p}/p$ définie en envoyant $x = (x_i)$ vers la classe de x_0 modulo p, qui est un morphisme d'anneaux. Soit $\widetilde{A}^+ = W(\widetilde{E}^+)$ l'anneau des vecteurs de Witt sur $\widetilde{E}^+$. On définit :

$$\widetilde{B}^+ = \widetilde{A}^+[\frac{1}{p}] = \{\sum_{k>>_\infty} p^k[x_k], \quad x_k \in \widetilde{E}^+\},$$

où $[x] \in \widetilde{A}^+$ désigne le relèvement de Teichmüller d'un élément $x \in \widetilde{E}^+$. L'application θ s'étend alors en un morphisme surjectif $\widetilde{B}^+ \to \mathbb{C}_p$ qui envoie $\sum p^k[x_k]$ vers $\sum p^k[(x_k)_0]$. Soit $[\epsilon_1] = [(\epsilon_1, ...)]$, de telle manière à ce que $\epsilon_1^p = \epsilon$, et soit $\omega = \frac{([\epsilon]-1)}{([\epsilon_1]-1)}$. Alors $\theta(\omega) = 1 + \epsilon_1 + ... + \epsilon_1^{p-1} = 0$. En fait, le noyau de θ est l'idéal engendré par ω ([2]). On définit l'anneau $B_{dR}{}^+ = \varprojlim_n \widetilde{B}^+/ker(\theta)^n$. Tout élément de $B_{dR}{}^+$ s'écrit alors sous la forme $\sum_{n=0}^{+\infty} x_n w^n$. C'est naturellement une F-algèbre. Comme $\theta(1-[\epsilon]) = 0$, la série

$$-\sum_{n=1}^{+\infty} \frac{(1-[\epsilon])^n}{n}$$

converge vers un élément de $B_{dR}{}^+$ noté t.

On définit alors $B_{dR} = B_{dR}{}^+[\frac{1}{t}]$. C'est un corps muni d'une filtration définie, pour $i \in \mathbb{Z}$, par $\mathrm{Fil}^i B_{dR} = t^i B_{dR}{}^+$. Il est aussi muni d'une

action de G_K. On peut montrer ([8]) que $B_{dR}^{G_K} = K$, ce qui en fait un corps G_K régulier.

Définition 4.6 (Représentations de de Rham)**.** *Soit V une représentation p-adique continue de G_K. On dit que V est de de Rham, si elle est B_{dR}-admissible.*

Rappelons que cela veut dire que, étant donné une représentation p-adique V, $\dim_K D_{dR}(V) = \dim_{\mathbb{Q}_p} V$, où l'on a noté

$$D_{dR}(V) = B_{dR} \otimes_{\mathbb{Q}_p} V^{G_K}.$$

C'est un espace vectoriel filtré sur K, la filtration étant $\mathrm{Fil}^i D_{dR}(V) = \mathrm{Fil}^i B_{dR} \otimes_{\mathbb{Q}_p} V^{G_K}$ pour $i \in \mathbb{Z}$. On peut aussi montrer ([8]) que l'action d'un élément $g \in \mathrm{G}_K$ sur t est simplement la multiplication par le caractère cyclotomique $\chi_p(g)$, ce qui fait que le i-ème gradué de la filtration $\mathrm{Gr}^i B_{dR} = \mathrm{Fil}^i B_{dR}/\mathrm{Fil}^{i+1} B_{dR}$ est isomorphe à $\mathbb{C}_p(i)$ comme G_K-modules. On en déduit que $\mathrm{Gr} B_{dR} = \bigoplus_{i\in\mathbb{Z}} \mathrm{Gr}^i B_{dR}$ est isomorphe à $\bigoplus \mathbb{C}_p(i)$ comme G_K-modules. D'où l'isomorphisme $\mathrm{Gr} B_{dR} \cong B_{HT}$.

Proposition 4.7. *Soit V une représentation p-adique. Si V est B_{dR}-admissible alors elle est B_{HT}-admissible.*

Démonstration. On a la suite exacte

$$0 \to \mathrm{Fil}^{i+1} B_{dR} \to \mathrm{Fil}^i B_{dR} \to \mathbb{C}_p(i) \to 0,$$

Ce qui donne

$$0 \to \mathrm{Fil}^{i+1} B_{dR} \otimes_{\mathbb{Q}_p} V \to \mathrm{Fil}^i B_{dR} \otimes_{\mathbb{Q}_p} V \to \mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V \to 0,$$

en prend alors les G_K-invariants

$$0 \to \mathrm{Fil}^{i+1} B_{dR} \otimes_{\mathbb{Q}_p} V^{G_K} \to \mathrm{Fil}^i B_{dR} \otimes_{\mathbb{Q}_p} V^{G_K} \to \mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V^{G_K}.$$

On obtient une injection

$$GrD_{dR}(V) = \bigoplus_{i\in\mathbb{Z}} \mathrm{Gr}^i D_{dR}(V) \hookrightarrow \bigoplus_{i\in\mathbb{Z}} \mathbb{C}_p(i) \otimes_{\mathbb{Q}_p} V^{G_K} = D_{HT}(V).$$

Il s'ensuit que si V est de de Rham, alors

$$\dim_{\mathbb{Q}_p}(V) = \dim_K(\mathrm{Gr} D_{dR}(V)) \leq \dim_K D_{HT}(V) \leq \dim_{\mathbb{Q}_p}(V).$$

Il a donc égalité et V est alors de Hodge-Tate. □

4.4. **Représentations cristallines.** On a construit dans le paragraphe précédent l'anneau B_{dR}^+ et on avait vu que tout élément de cet anneau s'écrit sous forme $\sum_{n\geq 0} x_n\omega^n$, où $x_n \in \widetilde{B}^+$. On définit

$$B_{cris}^+ = \{x \in B_{dR}^+, \quad x = \sum_{n\geq 0} x_n \frac{\omega^n}{n!}, \quad x_n \to 0 \quad \text{dans} \quad \widetilde{B}^+\}.$$

On définit $B_{cris} = B_{cris}^+[\frac{1}{t}]$. Ce n'est pas un corps ($\omega - p$ est dans B_{cris} mais pas son inverse) ; on peut montrer que $B_{cris}^{G_K} = F$, l'extension maximale non ramifiée de K. Il existe une extension naturelle continue du Frobenius à B_{cris} qui commute avec l'action de G_K et qu'on note ϕ.

Définition 4.8 (Représentations Cristallines)**.** *Soit V une représentation p-adique. On dit que V est cristalline si elle est B_{cris}-admissible.*

On note $D_{cris}(V) = (B_{cris} \otimes_{\mathbb{Q}_p} V)^{G_K}$. C'est un F-espace vectoriel, muni d'une application σ-semi-linéaire $\phi : D_{cris}(V) \to D_{cris}(V)$ (σ étant le relèvement du Frobenius à F) tel que $D_{cris}(V)_K = D_{cris}(V) \otimes_F K$ est muni d'une filtration $(\mathrm{Fil}^i(D_{cris}(V)_K))_{i\in\mathbb{Z}}$ exhaustive ($\cup_{i\in\mathbb{Z}}\mathrm{Fil}^i(D_{cris}(V)_K) = D_{cris}(V)_K$) et séparée $\cap_{i\in\mathbb{Z}}\mathrm{Fil}^i(D_{cris}(V)) = \{0\}$. C'est ce qu'on appelle un ϕ-module filtré. L'endomorphisme ϕ est appelé Frobenius. Un morphisme entre deux ϕ-modules filtrés D et D' est une application F-linéaire $f : D \to D'$ compatibles aux Frobenius $f \circ \phi = \phi' \circ f$, et tel que $f_K : D_K \to D'_K$ soit compatible aux filtrations ($f_K(\mathrm{Fil}^i D_K) \subset \mathrm{Fil}^i D'_K, \forall i \in \mathbb{Z}$). Un sous-$\phi$-module filtré D' de D est un ϕ-module filtré tel que l'inclusion de D' dans D soit un morphisme de ϕ-modules. On note MF_K^ϕ la catégorie formée par les ϕ-modules filtrés.

4.5. **Admissibilité des modules filtrés.** Soit D un ϕ-module filtré. Il est donc muni d'un Frobenius et on dispose d'une filtration sur D_K. Ces deux aspects n'ont aucune raison d'avoir une compatibilité entre eux. Or, dans le cas des ϕ-modules qui proviennent des représentations cristallines, ces deux attributs sont compatibles en un sens que nous allons préciser. On associe à D deux entiers : l'entier de Hodge et l'entier de Newton.

4.5.1. *Entier de Hodge.* Pour $i \in \mathbb{Z}$, on note

$$\mathrm{Gr}^i D_K = \mathrm{Fil}^i(D)/\mathrm{Fil}^{i+1}(D_{cris}(V))$$

et on définit

$$t_H D = \sum_{i\in\mathbb{Z}} i \dim_K(\mathrm{Gr}^i D_K).$$

Cet entier s'appelle le nombre de Hodge de D et ne dépend que de la filtration.

4.5.2. *Entier de Newton.* On fixe une base de D sur F. Soit A la matrice de ϕ dans cette base. Le déterminant de A dépend du choix de la base, par contre sa valuation n'en dépend pas. On pose $t_N(D) = v_p(det(A))$. C'est le nombre de Newton de D. Il ne dépend que du Frobenius de D.

Définition 4.9.
— *On dit qu'un dit ϕ-module filtré D est faiblement admissible s'il est de dimension finie, de Frobenius bijectif, $t_H(D) = t_N(D)$ et pour tout sous-ϕ-module filtré D' de D, $t_H(D') \leq t_N(D')$.*
— *On dit qu'un module D est admissible s'il existe une représentation cristalline p-adique V tel que $D_{cris}(V) = D$.*

Théorème 4.10 ([8, 7])**.** *Le foncteur D_{cris} est une équivalence de catégories entre la catégorie $Rep^{cris}_{G_{\mathbb{Q}_p}}$ des représentations cristallines de dimension finie de $G_{\mathbb{Q}_p}$ et la catégorie des ϕ-modules filtrés faiblement admissibles.*

4.6. **Poids de Serre d'une représentation.** Soit V une $\overline{\mathbb{F}_\ell}$-représentation continue de dimension finie d de $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$. On définit les poids modérés de Serre de la représentation comme suit : c'est un d-uplet d'entiers dans $[0, \ell-1]$ où $d = \dim V$ vérifiant les conditions suivantes : si V est une extension de V_1 par V_2, on définit les poids modérés de V comme la réunion des poids modérés de V_1 et de V_2. Si V est irréductible, alors la restriction de V à I_ℓ est somme directe de d caractères de la forme

$$\psi_d{}^{n\ell^t}, \quad t = 0, 1..., d-1,$$

où $n < \ell^d - 1$ qui n'est pas divisible par aucun $\frac{\ell^d-1}{\ell^r-1}$ pour $r < d$, et ψ_d est le caractère fondamental de niveau d. Les poids de V sont alors par définition les chiffres de l'entier n dans son écriture en base ℓ. Autrement dit, si $n = a_0 + a_1\ell + ... + a_{d-1}\ell^{d-1}$, ce sont les entiers a_0, a_1...,a_{d-1} comptés avec multiplicités. Soit maintenant V une représentation cristalline de $G_{\mathbb{Q}_\ell}$ de dimension d. Alors V admet un réseau W stable par l'action de $G_{\mathbb{Q}_\ell}$, et donc $W/\ell W$ est une représentation de $G_{\mathbb{Q}_\ell}$ sur le corps fini $\mathbb{F}_\ell$. Les poids de Serre de cette représentation sont alors donnés par le théorème suivant, dû à Fontaine et Lafaille.

Théorème 4.11 ([**?**])**.** *Soient V une représentation cristalline de $G_{\mathbb{Q}_\ell}$ de dimension d sur $\mathbb{Q}_\ell$ et W un réseau stable. Soient $\lambda_1 \leq ...\lambda_d$ les poids de Hodge-Tate de V. On suppose que $\lambda_d < \ell - 1$. Alors les $(\lambda_i)_{0\leq i\leq d}$ sont exactement les poids de Serre de la représentation $W/\ell W$.*

5. Sous-groupes maximaux du groupe symplectique

L'objectif de cette partie est de classifier les sous-groupes maximaux du groupe des similitudes d'une forme bilinéaire alternée sur un espace vectoriel de dimension 4 sur un corps fini. Dans un premier temps, on rappellera des résultats généraux sur les groupes symplectiques ainsi que quelques résultats spécifiques à la dimension 4 qui nous permettront de déduire un isomorphisme exceptionnel. On passera ensuite à la classification proprement dite. Nous en donnerons plusieurs formulations.

5.1. **Quelques rappels sur les groupes symplectiques.** On fixe k un corps de caractéristique différente de 2. Soit V un espace vectoriel de dimension $2n$ sur k, muni d'une forme bilinéaire alternée non dégénérée A. C'est un élément de $\bigwedge^2 V^*$. On définit le groupe des similitudes symplectiques de A comme suit :

$$\mathrm{GSp}(A) := \{g \in \mathrm{GL}(V), \exists \eta(g) \in k^\times, \forall x, y \in V, A(g(x), g(y)) = \eta(g)A(x, y)\}.$$

Le scalaire $\eta(g)$ s'appelle facteur de similitude de g et l'application $\eta : \mathrm{GSp}(A) \to k^\times$ est un morphisme de groupe, de noyau le groupe $\mathrm{Sp}(A)$, le groupe symplectique associé à A, et on a la suite exacte courte :

$$1 \to \mathrm{Sp}(A) \to \mathrm{GSp}(A) \xrightarrow{\eta} k^\times \to 1.$$

Si on se place dans une base convenable, la matrice de A peut être mise sous forme $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ et on note alors

$$\mathrm{GSp}_{2n}(k) := \mathrm{GSp}(A), \quad \mathrm{Sp}_{2n}(k) := \mathrm{Sp}(A)$$

et on a donc :

$$\mathrm{GSp}_{2n}(k) = \{M \in \mathrm{M}_{2n}(k), \exists \eta(M) \in k^\times : M^t J M = \eta(M) J\}.$$

On note $\mathrm{PGSp}(A)$ le quotient du groupe $\mathrm{GSp}(A)$ par son centre formé des homothéties. De même, $\mathrm{PSp}(A)$ est le quotient de $\mathrm{Sp}(A)$ par $\{\pm Id_V\}$, où Id_V désigne l'application identité de V. On a alors la suite exacte :

$$1 \to \mathrm{PSp}(A) \to \mathrm{PGSp}(A) \xrightarrow{\eta} k^\times / {k^\times}^2 \to 1.$$

5.2. **Quelques résultats spécifiques à la dimension 4.**

5.2.1. *Construction d'une forme quadratique sur $\bigwedge^2 V$.* On suppose maintenant que $n = 2$. On dispose alors d'une application bilinéaire :

$$b : \overset{2}{\bigwedge} V \times \overset{2}{\bigwedge} V \to \overset{4}{\bigwedge} V$$

induite par l'application multilinéaire alternée

$$\begin{aligned} V \times V \times V \times V &\to \bigwedge^4 V \\ (u, v, w, z) &\mapsto u \wedge v \wedge w \wedge z \end{aligned}$$

L'application b est symétrique car les tenseurs d'ordre 2 commutent. Elle est non dégénérée. Ceci peut se voir simplement en écrivant sa matrice dans une base de tenseurs purs donnés par une base de V. Si on fixe une base (e_0, e_1, e_2, e_3) de V, alors l'application

$$k \to \bigwedge^4 V, \alpha \mapsto \alpha e_0 \wedge e_1 \wedge e_2 \wedge e_3$$

est un isomorphisme. Via cet isomorphisme, on peut voir b comme une forme bilinéaire symétrique non dégénérée, canonique à un scalaire non-nul près, car un changement de base de V ne modifie b qu'à un scalaire non nul près. La matrice de b dans la base $(e_i \wedge e_j)_{i<j}$ est diagonale par blocs, avec des $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sur la diagonale. En particulier, b admet un espace totalement isotrope de dimension 3. On notera q la forme quadratique associée à b, définie par $q(x) = b(x, x)$ pour tout $x \in \bigwedge^2 V$. Pour tout u, v dans V, $q(u \wedge v) = 0$. L'ensemble des tenseurs purs est donc inclus dans le cône isotrope de q. Notons $\mathcal{K}$ ce cône isotrope.

Lemme 5.1. *Le cône isotrope $\mathcal{K}$ de q est formé des tenseurs purs.*

Démonstration. Choisissons une base (e_0, e_1, e_2, e_3) de V et soit a un vecteur isotrope pour q. On écrit $a = \sum_{i<j} a_{ij} e_i \wedge e_j$, alors $a \wedge a = (a_{01}a_{23} - a_{02}a_{13} + a_{03}a_{12}) e_0 \wedge e_1 \wedge e_2 \wedge e_3$ et donc $a_{01}a_{23} - a_{02}a_{13} + a_{03}a_{12}$ est égal à 0. Si $a_{23} \neq 0$, on peut écrire $a = (a_{03}e_0 + a_{13}e_1 + a_{23}e_2) \wedge (e_3 - \frac{a_{12}}{a_{23}} e_1 - \frac{a_{02}}{a_{23}} e_0)$. Sinon, si $a_{02} = a_{03} = 0$ alors $a = (a_{01}e_0 - a_{12}e_2 - a_{13}e_3) \wedge (e_1)$ et si ce n'est pas le cas, alors on peut supposer par exemple que $a_{03} \neq 0$ auquel cas $a = (a_{03}e_0 + a_{13}e_1 + a_{23}e_2) \wedge (\frac{a_{02}}{a_{03}} e_2 + e_3)$. □

5.2.2. *Lien avec la forme symplectique.* Pour clarifier les idées, on va fixer une base (e_0, e_1, e_2, e_3) de V dans laquelle la matrice de A est J. Cela ne nuit nullement à la généralité de la situation mais simplifiera les démonstrations et certains énoncés. La forme b est donc un accouplement non dégénéré, et induit un isomorphisme entre $\bigwedge^2 V$ et $\bigwedge^2 V^*$. Notons $\widetilde{A}$ l'élément de $\bigwedge^2 V$ qui correspond à la forme symplectique A via cet isomorphisme.

Lemme 5.2. *Le vecteur $\widetilde{A}$ est non isotrope pour b.*

Démonstration. En effet, comme la matrice de A dans la base (e_0, e_1, e_2, e_3) est J, on a alors $A = e_0^* \wedge e_3^* + e_1^* \wedge e_2^*$. Par suite, $\widetilde{A} = e_0 \wedge e_3 + e_1 \wedge e_2$. D'où $\widetilde{A} \wedge \widetilde{A} \neq 0$ □

Il découle de ce lemme que la restriction de la forme b à $H := \widetilde{A}^{\perp}$ est non dégénérée. Notons b_H cette restriction. Remarquons que b_H admet un espace totalement isotrope de dimension 2, car l'intersection de H et d'un espace totalement isotrope de b est de dimension au moins 2. Il est exactement de dimension 2 car la forme b_H est non dégénérée. La matrice de b_H peut donc être mise dans une base convenable sous la forme

$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & a \end{pmatrix}, \quad \text{où} \quad a \in \mathbb{F}_q^{\times}.$$

Le groupe linéaire de V agit de manière naturelle sur $\bigwedge^2 V$. Tout élément de $\mathrm{GL}(V)$ est une similitude pour b, c'est-dire un élément de $\mathrm{GO}(b)$. De plus, le facteur de similitude d'un élément $g \in \mathrm{GL}(V)$ pour la forme b est le déterminant de g. En effet, cela découle de l'égalité, valable pour u, v, w, z des éléments de V :

$$\wedge^4 g(u \wedge v \wedge w \wedge z) = \det(g) u \wedge v \wedge w \wedge z.$$

Le sous-groupe $\mathrm{GSp}(A)$ agit, par définition, de manière scalaire sur A, et par suite sur $\widetilde{A}$ aussi. Il stabilise donc $H = \widetilde{A}^{\perp}$. On obtient un morphisme naturel $\iota : \mathrm{GSp}(A) \to \mathrm{GO}(b_H)$. Soit $\widetilde{\mathrm{GO}}(b_H)$ le sous-groupe de $\mathrm{GO}(b_H)$ constitué des éléments qui ont un facteur de similitude qui est carré parfait. Alors l'image de $\mathrm{GSp}(A)$ par le morphisme ι est incluse dans $\widetilde{\mathrm{GO}}(b_H)$. En effet, cela découle du lemme suivant :

Lemme 5.3. *Soit $g \in \mathrm{GSp}(A)$. Alors $\det(g) = \eta(g)^2$.*

Démonstration. Soit α une racine carré de $\eta(g)$ dans un extension finie L de k. On a alors $\frac{1}{\alpha} g \in \mathrm{Sp}(A_L)$, A_L étant la forme symplectique obtenue par extension des scalaires à L. Or, $\mathrm{Sp}(A_L) \subset \mathrm{SL}(V \otimes_k L)$, donc $\det(\frac{1}{\alpha} g) = 1$. Ce qui implique $\det(g) = \alpha^4 = \eta(g)^2$.

□

Comme toute homothétie de H est de facteur de similitude carré parfait, le centre de $\widetilde{\mathrm{GO}}(b_H)$ est constitué de toutes les homothéties. Notons $\widetilde{\mathrm{PGO}}(b_H)$ et $\mathrm{PO}(b_H)$ les quotients de $\widetilde{\mathrm{GO}}(b_H)$ et $\mathrm{O}(b_H)$ par leurs centres respectifs. Alors le morphisme naturel $\mathrm{PO}(b_H) \to \widetilde{\mathrm{PGO}}(b_H)$ est un isomorphisme. L'injectivité est claire. Pour la surjectivité, tout

élément g de $\widetilde{\mathrm{GO}}(b_H)$ a un facteur de similitude de la forme α^2, avec $\alpha \in k^\times$ donc $\alpha^{-1}g$ appartient à $\mathrm{O}(b_H)$. Mais, $\alpha^{-1}g$ et g ont la même image dans $\widetilde{\mathrm{PGO}}(b_H)$.
Finalement, on récupère un morphisme $\mathrm{GSp}(A) \to \mathrm{PO}(b_H)$. Le noyau de ce morphisme est formé des éléments qui stabilisent les points de $\bigwedge^2 V$, donc les plans de V, par suite les intersections de plans, donc les droites. Par conséquent, le noyau est formé des matrices scalaires. D'où un morphisme injectif $\mathrm{PGSp}(A) \to \mathrm{PO}(b_H)$.

5.3. **Isomorphisme entre** $\mathrm{PGSp}(A)$ **et** $\mathrm{PO}(b_H)$**.** On se propose dans cette partie de montrer que le morphisme $\mathrm{PGSp}(A) \to \mathrm{PO}(b_H)$ est un isomorphisme lorsque le corps k est fini. On sait qu'il est injectif, il reste à montrer la surjectivité. Pour ce faire, on va montrer qu'ils ont les même cardinaux. Faisons quelques rappels qui nous seront utiles pour la suite.

5.3.1. *Théorème de Witt.* On donne ici une version adaptée à notre situation du théorème de Witt. Pour plus de détails, on pourra consulter [14].

Théorème 5.4 (Théorème de Witt)**.** *Soient (E, b), (E', b') deux espaces vectoriels munis de formes bilinéaires (symétriques ou alternées). On suppose que (E, b) et (E', b') sont isométriques. Soient F un sous espace de E et $u : F \to E'$ une isométrie. Alors u admet un prolongement $v : E \to E'$ qui est encore une isométrie.*

5.3.2. *Classification des plans quadratiques.* Un plan quadratique est un espace vectoriel de dimension 2 sur k, muni d'une forme bilinéaire symétrique. Soit (P, b_P) un plan quadratique.

Définition 5.5. *On dit que P est :*

(1) parabolique si la forme b_P est de rang 1 ;
(2) hyperbolique si b_P est non dégénérée et admet au moins un vecteur isotrope ;
(3) elliptique si b_P est non dégénérée et n'admet pas de vecteurs isotropes ;

Remarque 5.6.

Si b_P est non dégénérée, il est équivalent de dire que P est hyperbolique ou que l'opposé du discriminant de b_P est un carré parfait dans k. Il est aussi équivalent de dire que P est elliptique ou que l'opposé du discriminant de b_P n'est pas un carré parfait. On rappelle que le discriminant est la classe modulo les carrés de $k^\times$ du déterminant de la matrice de b_P dans n'importe quelle base de P.

5.3.3. *Calcul des cardinaux de* $\mathrm{PGSp}(A)$ *et* $\mathrm{PO}(b_H)$. On suppose dorénavant que le corps k est fini de cardinal q.

Proposition 5.7. *(1)* $\mathrm{PGSp}(A)$ *est de cardinal* $q^4(q^4-1)(q^2-1)$ *;*
(2) $\mathrm{PO}(b_H)$ *est de cardinal* $q^4(q^4-1)(q^2-1)$ *;*

La démonstration de cette proposition passe par plusieurs lemmes intermédiaires. Tout d'abord, le groupe $\mathrm{GSp}(A)$ agit transitivement sur les plans hyperboliques de V, comme on peut le voir par le théorème de Witt. Soit P un plan hyperbolique et G_P son stabilisateur dans $\mathrm{GSp}(A)$. Alors l'indice de G_P dans $\mathrm{GSp}(A)$ est égal au nombre de plans hyperboliques de V. Or, un plan hyperbolique est engendré par deux vecteurs u, v tel que $u \wedge v \wedge \widetilde{A} \neq 0$, i.e $u \wedge v \notin H$. Réciproquement, si on se donne un vecteur de $\bigwedge^2 V$ isotrope pour b et qui ne soit pas dans H, on peut l'écrire sous forme $u \wedge v$, avec u, v des vecteurs de V qui vérifient $u \wedge v \wedge \widetilde{A} \neq 0$. Le couple (u, v) engendre alors un plan hyperbolique de V. Deux vecteurs isotropes de $\bigwedge^2 V$ donnent le même plan hyperbolique si, et seulement si, ils sont colinéaires. On déduit que le nombre de plans hyperboliques est égal au nombre de droites de $\bigwedge^2 V$ isotropes, non orthogonales à $\widetilde{A}$.

Lemme 5.8. *(1) L'ensemble des vecteurs isotropes de* $\bigwedge^2 V$ *est de cardinal* $q^5 + q^3 - q^2 - 1$ *;*
(2) L'ensemble des vecteurs isotropes de H *est de cardinal* $q^4 - 1$ *;*

Démonstration. (1) La matrice de b peut être écrite dans une base convenable sous la forme

$$\begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}.$$

Il suffit donc de calculer le nombre de solutions non nulles de l'équation $x_0x_1 + x_2x_3 + x_4x_5 = 0$.
(2) De même, la matrice de b_H peut être mise sous forme

$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & a \end{pmatrix}, \quad \text{où} \quad a \in k^\times.$$

On calcule ensuite le nombre de solutions de l'équation $x_0x_1 + x_2x_3 + ax_4^2 = 0$. □

Il découle de ce lemme que le nombre de droites de $\bigwedge^2 V$ isotropes non orthogonales à $\widetilde{A}$ est $q^2(q^2+1)$.
Soit A_P la restriction de la forme A à P. Le morphisme de restriction $r : G_P \to \mathrm{GSp}(A_P) = \mathrm{GL}(P)$ est surjectif par le théorème de Witt. Le noyau de ce morphisme est constitué des éléments qui agissent trivialement sur P. Il résulte de la décomposition orthogonale $V = P \oplus P^\perp$, que ce noyau est égal à $\mathrm{Sp}(A_{P^\perp}) = \mathrm{SL}(P^\perp)$. On a donc

$$\begin{aligned} \#\mathrm{GSp}(A) &= \#G_p.[\mathrm{GSp}(A) : G_P] \\ &= \#\mathrm{GL}(P).\#\mathrm{SL}(P^\perp).[\mathrm{GSp}(A) : G_P] \\ &= (q^2-1)(q^2-q)(q)(q^2-1)q^2(q^2+1) \end{aligned}$$

Enfin,

$$\#\mathrm{PGSp}(A) = \frac{\#\mathrm{GSp}(A)}{q-1} = q^4(q^4-1)(q^2-1).$$

Passons au calcul du cardinal du groupe $\mathrm{O}(b_H)$. L'idée est de calculer le nombre de plans hyperboliques de H pour ensuite se ramener à des groupes orthogonaux plus petits. Soit $\mathcal{P}_{hyp}$ l'ensemble des plans hyperboliques de H.

Lemme 5.9. *$\mathcal{P}_{hyp}$ est de cardinal $\frac{q^3(q^2+1)(q+1)}{2}$.*

Démonstration. L'application suivante

$$\mathcal{F} = \{(u,v) \in H^2, b(u,u) = b(v,v) = 0, b(u,v) = 1\} \to \mathcal{P}_{hyp},$$

définie en associant à un couple (u,v) la plan qu'ils engendrent, est de fibres de cardinal constant égal à $2(q-1)$. Reste à calculer le cardinal de $\mathcal{F}$. Par le lemme 5.8, il y a q^4-1 vecteurs isotropes dans H. On se donne un vecteur u isotrope. Comme b est non dégénérée, il existe au moins un élément v de H tel que $b(u,v) = 1$. L'ensemble E de tels éléments est un espace affine de cardinal q^4. Il est la réunion disjointe des sous-ensembles $D_w := \{w + \lambda u, \lambda \in k\}$, où w parcourt un ensemble Θ de cardinal fini. Ce sont tout simplement les classes de la relation d'équivalence définie sur E par

$$v \sim w \Leftrightarrow \exists \lambda \in k : v - w = \lambda u.$$

Chaque ensemble D_w est de cardinal q et contient exactement un vecteur isotrope. Il y a donc exactement q^3 vecteurs isotropes dans E. Il s'ensuit que $\mathcal{F}$ est de cardinal $q^3(q^4-1)$. D'où

$$\#\mathcal{P}_{hyp} = \frac{q^3(q^4-1)}{2(q^2-1)} = \frac{q^3(q^2+1)(q+1)}{2}.$$

□

Soit P un plan hyperbolique. On note G_P son stabilisateur dans $\mathrm{O}(b_H)$. Le théorème de Witt nous dit que l'action de $\mathrm{O}(b_H)$ sur $\mathcal{P}_{hyp}$ est transitive. Donc, G_P est d'indice $\frac{q^3(q^2+1)(q+1)}{2}$ dans $\mathrm{O}(b_H)$. Par ailleurs, G_P est isomorphe à $\mathrm{O}(b_P)\times\mathrm{O}(b_{P^\perp})$. Un calcul direct montre que $\mathrm{O}(b_P)$ est de cardinal $2(q-1)$. Le calcul du cardinal de $\mathrm{O}(b_{P^\perp})$ se fait en procédant de même : on compte le nombre de plans hyperboliques et on calcule le cardinal du stabilisateur d'un plan hyperbolique. On trouve $\#(\mathrm{O}(b_{P^\perp})) = 2q(q^2-1)$.

Au final

$$\#(\mathrm{O}(b_H)) = \frac{q^3(q^2+1)(q+1)}{2}.2(q-1).2q(q^2-1) = 2q^4(q^4-1)(q^2-1).$$

Corollaire 5.10. *On suppose que le corps k est fini. Alors le morphisme* $\mathrm{PGSp}(A) \to \mathrm{PO}(b_H)$ *est un isomorphisme.*

Démonstration. Il est injectif et on a égalité des cardinaux. □

5.4. **Sous-groupes maximaux du groupe projectif symplectique.** Rappelons les notations du paragraphe précédent : k est un corps fini, V est un espace vectoriel de dimension 4 sur k muni d'une forme bilinéaire alternée non dégénérée A. On supposera, à chaque fois que cela est nécessaire, que V est muni d'une base (e_0, e_1, e_2, e_3) dans laquelle la matrice de A est J. Le but ultime de ce qui suit est de classifier les sous-groupes maximaux de $\mathrm{PGSp}(A) = \mathrm{PGSp}_4(k)$. On commence d'abord par $\mathrm{PSp}(A) = \mathrm{PSp}_4(k)$. On suppose que $k = \mathbb{F}_q$ avec q une puissance d'un nombre premier ℓ.

5.4.1. *Première formulation.* Mitchell a classifié dans [13] les sous-groupes maximaux de $\mathrm{PSp}_4(\mathbb{F}_q)$. Elle est reprise par King dans [12], page 8 sous la forme qui va suivre. Les définitions des objets évoqués sont expliqués après le théorème.

Théorème 5.11. *Soit $\ell > 3$ un nombre premier et $q = l^r$, $r \geq 1$. Soit G un sous-groupe maximal de* $\mathrm{PSp}_4(\mathbb{F}_q)$. *Alors G a l'une des formes suivantes :*

1. *Stabilisateur d'une droite de V, d'indice q^3+q^2+q+1 ;*
2. *Stabilisateur d'une congruence parabolique, d'indice q^3+q^2+q+1 ;*
3. *Stabilisateur d'une congruence hyperbolique, d'indice $\frac{q^2(q^2+1)}{2}$;*
4. *Stabilisateur d'une congruence elliptique, d'indice $\frac{q^2(q^2-1)}{2}$;*
5. *Stabilisateur d'une quadrique, d'indice $\frac{q^3(q^2+1)(q+1)}{2}$;*
6. *Stabilisateur d'une quadrique, d'indice $\frac{q^3(q^2+1)(q-1)}{2}$;*

(7) *Stabilisateur d'une cubique tordue de* $\mathrm{P}(V)$*, d'indice* $q^3(q^4-1)$ *(pour* $q>7$*) ;*

(8) *Groupe contenant* $E_{16}=(\mathbb{Z}/2\mathbb{Z})^4$*, avec* $G/E_{16}=\mathcal{A}_5$ *ou* $\mathcal{S}_5$ *;*

(9) *Groupe isomorphe à* $\mathcal{A}_6, \mathcal{S}_6$ *ou* $\mathcal{A}_7$ *;*

(10) *Groupe conjugué sous* $\mathrm{PSp}(4,\mathbb{F}_q)$ *à* $\mathrm{PSp}(4,\mathbb{F}_{l^k})$*, avec* $\frac{r}{k}$ *un nombre premier impair ;*

(11) *Groupe conjugué sous* $\mathrm{PGSp}(4,\mathbb{F}_q)$ *à* $\mathrm{PSp}(4,\mathbb{F}_{l^k})$*, avec* $\frac{r}{k}=2$ *;*

De plus, les cas (8) *et* (9) *ne peuvent arriver que si* $r=1$*.*

5.4.2. *Explication des termes du théorème.* Si W est un espace vectoriel de dimension finie, on note $\mathrm{P}(W)$ l'espace projectif associé. On dispose de l'application naturelle de Plücker $(\mathrm{P}(V)\times\mathrm{P}(V))\backslash\Delta \to \mathrm{P}(\bigwedge^2 V)$, où Δ désigne la diagonale de $\mathrm{P}(V)\times\mathrm{P}(V)$. Un élément de $(\mathrm{P}(V)\times\mathrm{P}(V))\backslash\Delta$ détermine une droite de $\mathrm{P}(V)$, ou de manière équivalente, un plan de V. La forme bilinéaire b n'est pas très bien définie sur $\mathrm{P}(\bigwedge^2 V)\times\mathrm{P}(\bigwedge^2 V)$. Par contre, on peut toujours parler d'orthogonalité et d'isotropie. Deux droites de $\mathrm{P}(V)$ s'intersectent si, et seulement si, leurs images dans $\mathrm{P}(\bigwedge^2 V)$ sont orthogonales. Les vecteurs isotropes de $\mathrm{P}(\bigwedge^2 V)$ sont exactement les droites de $\mathrm{P}(V)$. Ainsi, le cône isotrope de b fournit une paramétrisation des droites de $\mathrm{P}(V)$. Ce n'est qu'une simple reformulation des résultats dans le cas affine.
Une congruence parabolique est l'ensemble des droites de $\mathrm{P}(V)$ qui intersectent une droite Q fixe de $\mathrm{P}(V)$ telle que l'image de Q dans $\bigwedge^2 V$ est orthogonale à $\widetilde{A}$.
Soit R un point de $\mathrm{P}(\bigwedge^2 V)$ non isotrope pour b. Il correspond à une droite (R) de $\bigwedge^2 V$. On suppose que la restriction de b au plan engendré par $\widetilde{A}$ et (R) est non dégénérée. Supposons que la droite projective $(\widetilde{A}R)$ intersecte $\mathcal{K}$ en deux points, disons R_1 et R_2, qui correspondent alors à deux droites D_1 et D_2 de $\mathrm{P}(V)$. D_1 et D_2 ne s'intersectent pas, sinon la restriction de b au plan engendré par $\widetilde{A}$ et R serait dégénéré.
Une congruence hyperbolique est l'ensemble des droites de $\mathrm{P}(V)$ qui sont d'images dans $\mathrm{P}(\bigwedge^2 V)$ orthogonales à la droite projective $(\widetilde{A}R)$, ou de manière équivalente, c'est l'ensemble des droites de $\mathrm{P}(V)$ qui intersectent les droites D_1 et D_2. Si l'intersection de $(\widetilde{A}R)$ et $\mathcal{K}$ est vide, une congruence elliptique est alors l'ensemble des droites de $\mathrm{P}(V)$ qui sont d'images dans $\mathrm{P}(\bigwedge^2 V)$ orthogonales à la droite projective $(\widetilde{A}R)$.
Soit D une droite de $\mathrm{P}(H)$, où $H=\widetilde{A}^{\perp}$. Elle correspond à un plan $\widetilde{D}$ de $\bigwedge^2 V$. On suppose $b_{|\widetilde{D}}$ est non dégénérée. Une quadrique de $\mathrm{P}(V)$ est l'ensemble des droites de $\mathrm{P}(V)$ qui sont d'images dans $\mathrm{P}(\bigwedge^2 V)$ orthogonales à la droite projective D. Selon que la droite D intersecte $\mathcal{K}$

en deux ou aucun point, on obtient les situations (5) et (6) du théorème qui correspondent respectivement à la situation où le plan $\widetilde{D}$ est hyperbolique et elliptique.

On suppose $\ell > 3$. Soit W un espace vectoriel de dimension 2 sur $\mathbb{F}_q$. Une cubique tordue est donnée par l'image du plongement de Veronese

$$\begin{array}{rcl} \mathrm{P}(W) & \to & \mathrm{P}(S^3W) \\ x & \mapsto & x^3 \end{array}$$

où S^3W est la puissance symétrique troisième de W. Notons $\mathcal{C}$ cette image. Hirschfeld montre dans [10], page 228, que le stabilisateur de $\mathcal{C}$ dans $\mathrm{PGL}(S^3W)$ est $\mathrm{PGL}(W)$ qui agit naturellement sur $\mathrm{P}(S^3W)$. Les valeurs propres de tels éléments sont donc de la forme $\{\lambda^3, \lambda^2\mu, \lambda\mu^2, \mu^3\}$. On retiendra donc qu'ils sont de quotients successifs constants.
Pour voir ce groupe comme un sous-groupe d'un groupe général symplectique, on choisit une base (x, y) de W et on définit l'application suivante :

$$\begin{array}{rcl} \psi : W^3 \times W^3 & \to & \mathbb{F}_q \\ (x_1, x_2, x_3, y_1, y_2, y_3) & \mapsto & \dfrac{1}{6} \displaystyle\sum_{\sigma \in \mathcal{S}_3} \prod_{i=1}^{3} \det(x_i, y_{\sigma(i)}) \end{array}$$

ψ est indépendante du choix de la base de W à un scalaire non nul près. Elle est symétrique en les trois premières et trois dernières coordonnées, donc se factorise à travers $S^3W \times S^3W$. L'application obtenue, qu'on note $\widetilde{\psi}$, est bilinéaire alternée. Elle est non dégénérée car sa matrice dans la base $(x^3, 3x^2y, 3xy^2, y^3)$ de S^3W est

$$\begin{pmatrix} & & & -1 \\ & & 1 & \\ & -1 & & \\ 1 & & & \end{pmatrix}.$$

Par ailleurs, d'après l'expression de W, pour tout $f \in \mathrm{GL}(W)$

$$\psi(f(x_1), f(x_2), f(x_3), f(y_1), f(y_2), f(y_3),) = \det(f)^3 \psi(x_1, x_2, x_3, y_1, y_2, y_3).$$

On en déduit l'inclusion $\mathrm{GL}(W) \hookrightarrow \mathrm{GSp}(\widetilde{\psi})$. Le facteur de similitude d'un élément f de $\mathrm{GL}(W)$ est $\det(f)^3$. L'image dans $\mathrm{PSp}(\widetilde{\psi})$ de l'intersection de $\mathrm{GL}(W)$ avec $\mathrm{Sp}(\widetilde{\psi})$ est le sous-groupe cherché.

Dans toutes les configurations qu'on vient définir, un stabilisateur est un sous-groupe de $\mathrm{PSp}_4(\mathbb{F}_q)$ qui préserve globalement la configuration considérée.

5.4.3. *Deuxième formulation.* On va maintenant reformuler les cas (2) à (6) du théorème 5.11 en termes plus exploitables. La situation est la suivante : on dispose d'un groupe G qui stabilise l'ensemble des tenseurs purs de l'orthogonal d'un plan P de $\bigwedge^2 V$. On voudrait alors voir que c'est équivalent au fait de stabiliser P tout court. C'est le but de ce qui suit.

Lemme 5.12. *Soit un P un plan de $\bigwedge^2 V$, i.e un sous espace vectoriel de dimension 2. Alors $P^\perp \cap \mathcal{K}$ engendre $P^\perp$.*

Démonstration. La restriction de la forme b à P est soit nulle, soit de rang 1 soit de rang 2.

(1) Dans le cas où le rang est nul, il est facile de voir, en vertu du lemme 5.1, que le plan P peut être engendré par deux tenseurs purs qui ont un élément en commun et qu'on peut donc en écrire une base sous la forme $(u \wedge v, u \wedge w)$ avec (u, v, w, z) base de V. On peut vérifier que $(u \wedge v, u \wedge w, u \wedge z, v \wedge w)$ est une base de $P^\perp$. Il s'ensuit donc que $P^\perp \cap \mathcal{K}$ engendre $P^\perp$.

(2) Dans le cas où le rang de la restriction de b à P est 1, P admet une base (a, d) tel que la matrice de q soit $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, de manière équivalente a est un tenseur pur, $d \wedge d \neq 0$ et $d \wedge a = 0$. On peut alors trouver une base (u, v, w, z) de V tel que $a = u \wedge v$, $d = u \wedge w + v \wedge z$. On peut vérifier que la famille $(u \wedge v, u \wedge z, v \wedge w, (u - v) \wedge (w + z))$ est une base de $P^\perp$.

(3) Le cas où le rang est 2 se scinde en deux sous-cas : dans le premier, q admet une base formée de vecteurs isotropes notée $(u_0 \wedge u_1, u_2 \wedge u_3)$ avec $u_0 \wedge u_1 \wedge u_2 \wedge u_3 \neq 0$. La famille (u_0, u_1, u_2, u_3) forme une base de V et on peut vérifier que $(u_0 \wedge u_2, u_0 \wedge u_3, u_1 \wedge u_2, u_1 \wedge u_3)$ est une base de $P^\perp$. La deuxième et dernière possibilité est que q soit anisotrope et se représente par la matrice $\begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix}$ avec ν non carré parfait dans $\mathbb{F}_q$, on se place alors dans une extension quadratique de $\mathbb{F}_q$ et on se ramène au cas hyperbolique.

□

Corollaire 5.13. *Soient P un plan de $\bigwedge^2 V$ et g un élément de $\mathrm{GL}(V)$ tel que $g(P^\perp \cap \mathcal{K}) \subset P^\perp \cap \mathcal{K}$. Alors $g(P) \subset P$.*

Démonstration. Comme $P^\perp$ est engendré par ses vecteurs isotropes, g stabilise $P^\perp$ et par suite P aussi car g est une similitudes pour b. □

On peut maintenant reformuler le théorème 5.11.

Théorème 5.14. *Soit $\ell > 3$ un nombre premier et $q = l^r$, $r \geq 1$. Soit G un sous-groupe maximal de $\mathrm{PSp}_4(\mathbb{F}_q)$. Alors G a l'une des formes suivantes :*

1. *Stabilisateur d'une droite de V, d'indice $q^3 + q^2 + q + 1$;*
2. *Stabilisateur d'un plan parabolique engendré par $\widetilde{A}$ et par un vecteur isotrope de H. Il est d'indice $q^3 + q^2 + q + 1$;*
3. *Stabilisateur d'un plan hyperbolique contenant $\widetilde{A}$. Il est d'indice $\frac{q^2(q^2+1)}{2}$;*
4. *Stabilisateur d'un plan elliptique contenant $\widetilde{A}$. Il est d'indice $\frac{q^2(q^2+1)}{2}$;*
5. *Stabilisateur d'un plan hyperbolique contenu dans H. Il est d'indice $\frac{q^3(q^2+1)(q+1)}{2}$;*
6. *Stabilisateur d'un plan elliptique contenu dans H. Il est d'indice $\frac{q^3(q^2+1)(q-1)}{2}$;*
7. *Stabilisateur d'une cubique tordue de $\mathrm{P}(V)$, d'indice $q^3(q^4-1)$ (pour $q > 7$) ;*
8. *Groupe contenant $E_{16} = (\mathbb{Z}/2\mathbb{Z})^4$, avec $G/E_{16} = \mathcal{A}_5$ ou $\mathcal{S}_5$;*
9. *Groupe isomorphe à $\mathcal{A}_6, \mathcal{S}_6$ ou $\mathcal{A}_7$;*
10. *Groupe conjugué sous $\mathrm{PSp}(4, \mathbb{F}_q)$ à $\mathrm{PSp}(4, \mathbb{F}_{l^k})$, avec $\frac{r}{k}$ un nombre premier impair ;*
11. *Groupe conjugué sous $\mathrm{PGSp}(4, \mathbb{F}_q)$ à $\mathrm{PSp}(4, \mathbb{F}_{l^k})$, avec $\frac{r}{k} = 2$;*

De plus, les cas (8) *et* (9) *ne peuvent arriver que si $r = 1$.*

5.5. **Calculs des indices.** L'objectif de cette partie est de calculer les indices des cas (1) à (6) du théorème 5.14. On admettra plusieurs faits sur les groupes classiques, démontrés dans le livre de Dieudonné [14].

On rappelle que la flèche $\iota : \mathrm{PGSp}(A) \to \mathrm{PO}(b_H)$ est un isomorphisme. Soit $\mathrm{SO}(b_H)$ le sous-groupe de $\mathrm{O}(b_H)$ constitué des matrices de déterminant 1. La flèche $\mathrm{SO}(b_H) \to \mathrm{PO}(b_H)$ est injective, donc un isomorphisme par égalité des cardinaux. On a donc un isomorphisme $\mathrm{PGSp}(A) \to \mathrm{SO}(b_H)$. Le sous-groupe $\mathrm{PSp}(A)$ est d'indice 2 dans $\mathrm{PGSp}(A)$. Comme $\mathrm{PSp}(A)$ est simple, c'est le groupe dérivé de $\mathrm{PGSp}(A)$. De l'autre côté, le groupe dérivé $\mathrm{D}(\mathrm{SO}(b_H))$ de $\mathrm{SO}(b_H)$ est d'indice 2 et engendré par les carrés (voir [14]). La flèche ι se restreint donc en un isomorphisme $\mathrm{PSp}(A) \to \mathrm{D}(\mathrm{SO}(b_H))$.

Le quotient $\mathrm{SO}(b_H)/\mathrm{D}(\mathrm{SO}(b_H))$ peut être décrit explicitement. Pour ce faire, on aura besoin d'introduire la norme spinorielle.

Proposition 5.15 (Norme spinorielle [16], page 334)**.** *Il existe une application*

$$\theta : \mathrm{O}(b_H) \to \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2},$$

appelée norme spinorielle, qui vérifie :

(1) θ est un morphisme de groupes ;

(2) Pour tout vecteur non isotrope x de H, si τ_x est la réflexion par rapport à x, alors

$$\theta(\tau_x) = q(x).$$

La norme spinorielle induit une application $\theta : \mathrm{SO}(b_H) \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$. On admet pour le moment qu'elle reste surjective. Le noyau contient le sous-groupe engendré par les carrés, il est donc égal à $\mathrm{D}(\mathrm{SO}(b_H))$. Ainsi, le calcul des indices se fera en deux étapes : étant donné un sous-groupe maximal G de $\mathrm{PSp}(A)$, on construit un sous-groupe G' de $\mathrm{PGSp}(A)$ tel que G soit d'indice 2 dans G'. On exhibera pour cela un élément de G' de norme spinorielle non triviale, et cela démontrera au passage que l'application θ reste surjective sur $\mathrm{SO}(b_H)$. On calcule ensuite l'indice de G' dans $\mathrm{PGSp}(A)$. Les résultats de ces calculs nous permettront dans la partie suivante d'établir la liste des sous-groupes maximaux de $\mathrm{PGSp}(A)$.

5.5.1. *Stabilisateur d'une droite.* Soit G un sous-groupe de $\mathrm{PSp}_4(\mathbb{F}_q)$ qui stabilise une droite de V. Comme toute droite de V est isotrope, le théorème de Witt nous dit que l'action de $\mathrm{PSp}_4(\mathbb{F}_q)$ est transitive sur les droites de V. L'indice de G dans $\mathrm{PSp}_4(\mathbb{F}_q)$ est donc égal au nombre de droites de V.

5.5.2. *Stabilisateur d'un plan parabolique.* Soit G est un sous-groupe de $\mathrm{PSp}_4(\mathbb{F}_q)$ qui stabilise un plan P parabolique de $\bigwedge^2 V$. Soit G' le sous-groupe de $\mathrm{PGSp}_4(\mathbb{F}_q)$ qui stabilise P. P est engendré par $\widetilde{A}$ et un vecteur isotrope w appartenant à H. Comme G' stabilise H et P, il stabilise leur intersection qui est la droite engendrée par w. Il s'identifie en fait au stabilisateur de cette droite dans $PO(b_H)$. Or, on sait par le théorème de Witt que l'action du groupe $PO(b_H)$ est transitive sur les droites isotropes.

Il s'ensuit donc que l'indice de G' dans $\mathrm{PSp}_4(\mathbb{F}_q)$ est le nombre de droites isotropes de H, qui est égal à q^3+q^2+q+1 par le lemme 5.8. Il reste maintenant à voir que G est d'indice 2 dans G'. Il suffit d'exhiber un élément dans $\mathrm{SO}(b_H)$ qui soit de norme spinorielle non-triviale et qui soit dans G'. Soit c un élément de ${\mathbb{F}_q}^\times$ qui n'est pas un carré parfait.

On peut trouver une décomposition $H = P_1 \oplus P_2 \oplus \mathbb{F}_q.x$ telle que P_1 et P_2 soient des plans hyperboliques, de base hyperboliques (w, w') et (z, z') respectivement, et x est un vecteur non isotrope. Soit f l'élément

de $\mathrm{GL}(H)$ défini relativement à cette décomposition par la matrice

$$\begin{pmatrix} 1 & 0 & & & \\ 0 & 1 & & & \\ & & 0 & -\frac{q(x)}{c} & \\ 0 & & \frac{c}{q(x)} & 0 & \\ & & & & -1 \end{pmatrix}.$$

C'est bien un élément de $\mathrm{SO}(b_H)$, et on a $f = \tau_y \circ \tau_x$, où $y = z + \frac{c}{q(x)} z'$. D'où $\theta(f) = q(y)q(x) = c$.

5.5.3. *Stabilisateur d'un plan hyperbolique et elliptique : cas (3) et (4).* Soit G un sous-groupe de $\mathrm{PSp}(A)$ qui stabilise un plan P, contenant $\widetilde{A}$ et telle que la restriction de b à P soit non dégénérée. Notons toujours G' le sous-groupe de $\mathrm{PGSp}(A)$ qui stabilise P. Soit R un élément de P tel que la matrice de b dans la base $(\widetilde{A}, R)$ soit diagonale. En particulier, le droite engendrée par R, notée (R) par la suite, est l'intersection de P et H. Elle est donc stable par l'action de G'. En fait, un élément de $\mathrm{PGSp}(A)$ qui stabilise (R) stabilise clairement le plan P. Donc G' est exactement le stabilisateur de (R) dans $\mathrm{PO}(b_H)$. Il est donc d'indice égal au cardinal de l'orbite de (R) sous l'action de $\mathrm{PO}(b_H)$.

Soit $\epsilon : {\mathbb{F}_q}^\times \to {\mathbb{F}_q}^\times / {\mathbb{F}_q}^{\times 2}$. C'est un morphisme de groupes, surjectif, d'image de cardinal 2 et de noyau constitué des carrés de ${\mathbb{F}_q}^\times$. Notons c un élément de ${\mathbb{F}_q}^\times$ qui n'est pas un carré parfait. Le groupe ${\mathbb{F}_q}^\times / {\mathbb{F}_q}^{\times 2}$ est isomorphe à $\{-1, 1\}$. L'image par cet isomorphisme de $\epsilon(d)$, pour d dans $\mathbb{F}_q^\times$ est le symbole de Legendre de d. On le note $\left(\frac{d}{q}\right)$.

Pour toute droite non isotrope D de $\bigwedge^2 V$, la quantité $\epsilon(q(D))$ est bien définie, où $q(D)$ est la valeur de q en n'importe quel générateur de la droite D. En effet, changer de générateur de D revient à multiplier par un scalaire non nul, ce qui multiplie la valeur de q par un carré. Or, ϵ est trivial sur les carrés.

On suppose toujours que la matrice de b_H est

$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & a \end{pmatrix}.$$

La matrice de b dans la décomposition $H \oplus \mathbb{F}_q\widetilde{A}$ est donc

$$\begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & a & 0 \\ & & & & 0 & q(\widetilde{A}) \end{pmatrix}.$$

Le discriminant de b est alors $\epsilon(aq(\widetilde{A}))$. Par ailleurs, on sait qu'il vaut $\epsilon(-1)$.

L'orbite de (R) sous l'action de $PO_5(\mathbb{F}_q)$ sur l'ensemble des droites de H est constituée des droites qui ont même image par $\epsilon \circ q$. Cela résulte du théorème de Witt.
On a, pour $x \in H$

$$q(x) = q(R) \Leftrightarrow x_0x_1 + x_2x_3 + ax_4^2 = q(R).$$

Le nombre de solutions de cette équation est $q^2(q^2 + \left(\frac{q(R)a^{-1}}{q}\right))$. Comme deux solutions opposées déterminent la même droite, le cardinal de $\{D \in \mathrm{P}(H), \epsilon(q(D)) = 1\}$ est donc

$$\frac{q^2(q^2 + \left(\frac{q(R)a^{-1}}{q}\right))}{2}.$$

Si P est hyperbolique, l'opposé du discriminant de la restriction de b à P est un carré parfait. Dit autrement, $\epsilon(q(R)) = \epsilon(-q(\widetilde{A}))$. Mais on sait que $\epsilon(-q(\widetilde{A})) = \epsilon(a)$. Il s'ensuit que $q(R)a^{-1}$ est un carré parfait. Donc, $\left(\frac{q(R)a^{-1}}{q}\right) = 1$. L'indice est donc $\frac{q^2(q^2+1)}{2}$.
Si P est elliptique, l'opposé du discriminant de la restriction de b à P n'est pas un carré parfait. On alors $\epsilon(cq(R)) = \epsilon(-q(\widetilde{A}))$. Donc $q(R)a^{-1}$ n'est pas un carré parfait. D'où l'indice est $\frac{q^2(q^2-1)}{2}$.

La dernière étape est de montrer que G est d'indice 2 dans G'. Pour cela, on complète R en une base (R, R_1, R_2, R_3) de H telle que b_H ait pour matrice dans cette base

$$\begin{pmatrix} q(R) & & & & \\ 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ & & & 1 & \\ & & & & t \end{pmatrix}, \quad \text{où} \quad t \in \mathbb{F}_q^\times.$$

Soit alors f l'automorphisme linéaire de H défini relativement à cette base par la matrice

$$\begin{pmatrix} -1 & & & & \\ & 0 & -\frac{q(R)}{c} & & \\ & -\frac{c}{q(R)} & 0 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}.$$

C'est bien un élément de $\mathrm{SO}(b_H)$, et on a $f = \tau_y \circ \tau_R$, où $y = R_1 + \frac{c}{q(R)} R_2$. D'où $\theta(f) = q(R).(\frac{c}{q(R)}) = c$.

5.5.4. *Stabilisateur d'un plan hyperbolique et elliptique : cas (5) et (6).* Soit G un sous-groupe de $\mathrm{PSp}(A)$ qui stabilise un plan P non dégénéré inclus dans H. Notons toujours G' le sous-groupe de $\mathrm{PGSp}(A)$ qui stabilise P. Il est d'indice égal au cardinal de l'orbite de P sous l'action de $\mathrm{PGSp}(A) = \mathrm{SO}(b_H)$.

Soit $\mathcal{P}$ l'ensemble des plans de H sur lesquels la restriction de b est non dégénérée. L'action de $PO(b_H)$ sur $\mathcal{P}$ a deux orbites : l'une est formée des plans hyperboliques, l'autre est formée des plans elliptiques. Cela résulte du théorème de Witt.

Le nombre de plans hyperboliques est donné par le lemme 5.9.

Lemme 5.16. *Le nombre de plans elliptiques dans $\mathcal{P}$ est $\frac{q^3(q^2+1)(q-1)}{2}$.*

Démonstration. On procède de manière différente. On sait que le nombre cherché est l'indice du stabilisateur d'un plan elliptique P dans $\mathrm{O}(b_H)$. Soit G_P ce stabilisateur. Il est isomorphe à $\mathrm{O}(b_P) \times \mathrm{O}(b_{P^\perp})$. Par un calcul direct, $\mathrm{O}(b_P)$ est de cardinal $2(q+1)$. Le cardinal de $\mathrm{O}(b_{P^\perp})$ a déjà été calculé dans la preuve du lemme 5.9. Il vaut $2q(q^2-1)$. D'où l'indice vaut

$$\frac{2q^4(q^4-1)(q^2-1)}{2(q+1)(2q(q^2-1))} = \frac{q^3(q^2+1)(q-1)}{2}.$$

□

Enfin, l'indice de G dans G' se calcule de manière similaire : on peut trouver une décomposition $H = P \oplus P' \oplus \mathbb{F}_q.x$ et une base $(y_i)_{1 \leq i \leq 5}$ adaptée à cette décomposition telle que P' soit un plan hyperbolique et la matrice de b_H dans cette base soit

$$\begin{pmatrix} 1 & & & & \\ 0 & d & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & d' \end{pmatrix}, \quad \text{où} \quad d, d' \in \mathbb{F}_q^{\times}.$$

Soit alors f l'automorphisme linéaire de H défini relativement à cette base par la matrice

$$\begin{pmatrix} -1 & & & & \\ & 1 & & & \\ & & 0 & -c^{-1} & \\ & & -c & 0 & \\ & & & & 1 \end{pmatrix}.$$

C'est bien un élément de $\mathrm{SO}(b_H)$, et on a $f = \tau_y \circ \tau_{y_1}$, où $y = y_3 + cy_4$. D'où $\theta(f) = q(y_1).q(y) = c$.

5.5.5. *Stabilisateur d'une cubique tordue.* Soit G un sous-groupe de $\mathrm{PSp}(A)$ qui stabilise une cubique tordue de $\mathrm{P}(V)$. D'après la partie 5.4.2, c'est l'intersection d'un sous-groupe G' avec $\mathrm{PSp}(A)$. Le groupe G' provient de l'action du groupe linéaire d'un espace vectoriel W de dimension 2 sur S^3W. Le facteur de similitude d'un élément $f \in \mathrm{GL}(W)$ est $\det(f)^3$. Le morphisme $\eta : \mathrm{pGSp}(A) \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ est donc non trivial sur G', de noyau G. D'où G est d'indice 2 dans G'.

5.6. **Sous-groupes maximaux du groupe projectif des similitudes symplectiques.** On détermine dans cette partie les sous-groupes maximaux de $\mathrm{PGSp}(A)$. Le travail a été essentiellement fait dans la partie précédente sur le calcul des indices des cas (1) à (7). En effet, on a montré que dans les cas (1) à (7), un groupe maximal G de $\mathrm{PSp}(A)$ est l'intersection d'un sous-groupe G' de $\mathrm{PGSp}(A)$ et de $\mathrm{PSp}(A)$ tel que G est d'indice 2 dans G'.

Lemme 5.17. *Soit G' un sous-groupe de* $\mathrm{PGSp}(A)$*. On suppose que $G := G' \cap \mathrm{PSp}(A)$ est maximal dans* $\mathrm{PSp}(A)$ *et d'indice* 2 *dans G'. Alors G' est un sous-groupe maximal de* $\mathrm{PGSp}(A)$*.*

Démonstration. En effet, si $G' \subset H \subsetneq \mathrm{PGSp}(A)$ alors $G \subset H \cap \mathrm{PSp}(A)$ donc $H \cap \mathrm{PSp}(A) = G$ ou $H \cap \mathrm{PSp}(A) = \mathrm{PSp}(A)$.
Si $H \cap \mathrm{PSp}(A) = \mathrm{PSp}(A)$, alors $H = \mathrm{PSp}(A)$, et dans ce cas $G' = \mathrm{PSp}(A)$, mais alors G ne peut pas être d'indice 2 dans G'.
Sinon, on alors $H \cap \mathrm{PSp}(A) = G$. Soit τ un élément de $H\backslash\mathrm{PSp}(A)$, alors $H = G \sqcup \tau G$. Il s'ensuit que $[H : G] = 2$. Or, $[H : G] = [H : G'][G' : G] = 2[H : G']$. Par suite, $G' = H$. □

On a donc la nouvelle liste suivante :

Théorème 5.18. *Soient $\ell > 3$ un nombre premier et $q = l^r$, $r \geq 1$. Soit G un sous-groupe maximal de* $\mathrm{PGSp}_4(\mathbb{F}_q)$*. Alors G a l'une des formes suivantes :*

(1) Stabilisateur d'une droite de V, d'indice $q^3 + q^2 + q + 1$;

(2) *Stabilisateur d'un plan parabolique engendré par $\widetilde{A}$ et par un vecteur isotrope de $B^{\perp}$. Il est d'indice q^3+q^2+q+1 ;*
(3) *Stabilisateur d'un plan hyperbolique contenant $\widetilde{A}$. Il est d'indice $\frac{q^2(q^2+1)}{2}$;*
(4) *Stabilisateur d'un plan elliptique contenant $\widetilde{A}$. Il est d'indice $\frac{q^2(q^2+1)}{2}$;*
(5) *Stabilisateur d'un plan hyperbolique contenu dans H. Il est d'indice $\frac{q^3(q^2+1)(q+1)}{2}$;*
(6) *Stabilisateur d'un plan anisotrope contenu dans H. Il est d'indice $\frac{q^3(q^2+1)(q-1)}{2}$;*
(7) *Stabilisateur d'une cubique tordue de $\mathrm{P}(V)$, d'indice $q^3(q^4-1)$ $(q>7)$;*
(8) *Groupe contenant un sous-groupe H d'indice 2, tel que H contienne $E_{16}=(\mathbb{Z}/2\mathbb{Z})^4$, $H/E_{16}=\mathcal{A}_5$ ou $\mathcal{S}_5$;*
(9) *Groupe contenant un sous-groupe H d'indice 2 isomorphe à $\mathcal{A}_6, \mathcal{S}_6$ ou $\mathcal{A}_7$;*
(10) *Groupe conjugué sous $\mathrm{PSp}_4(\mathbb{F}_q)$ à $\mathrm{PGSp}_4(\mathbb{F}_{l^k})$, avec $\frac{r}{k}$ un nombre premier impair ou égal à 1 ;*
(11) *Groupe conjugué sous $\mathrm{PGSp}_4(\mathbb{F}_q)$ à $\mathrm{PSp}_4(\mathbb{F}_{l^k})$, avec $\frac{r}{k}=2$;*

De plus, les cas (8) *et* (9) *ne peuvent arriver que si $r=1$.*

6. Formes modulaires de Siegel

Nous allons nous intéresser dans ce qui suit aux formes modulaires de Siegel. Nous suivrons de près l'article de Van der Geer dans [21] aulequel nous renvoyons pour certaines démonstrations.

6.1. **Groupe modulaire de Siegel.** Soit g un entier naturel non nul. On rappelle que le groupe symplectique est le groupe d'isométries de la forme bilinéaire alternée non dégénérée de $\mathbb{R}^{2g}$ donnée dans la base canonique par la matrice $J=\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. Sous forme matricielle, il est donné par

$$\mathrm{Sp}_{2g}(\mathbb{R})=\{M\in \mathrm{GL}_{2n}(\mathbb{R}), M^tJM=J\}.$$

Si on écrit ses éléments par blocs $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, a,b,c,d sont dans $\mathrm{M}(g,\mathbb{R})$ et doivent satisfaire

$$ab^t=ba^t$$
$$cd^t=dc^t$$
$$ad^t-bc^t=1_g$$

ou de manière équivalente :

$$\begin{aligned} c^t a &= a^t c \\ d^t b &= b^t d \\ d^t a - b^t c &= 1_g. \end{aligned}$$

Le groupe modulaire de Siegel de degré g est le sous-groupe discret $\mathrm{Sp}_{2g}(\mathbb{Z})$ de $\mathbb{R}^{2g}$, noté aussi Γ_g. L'analogue du demi-plan de Poincaré sera ce qu'on appelle le demi-espace de Siegel, il est défini par

$$\mathcal{H}_g = \{z \in M_g(\mathbb{C}), z^t = z, Im(z) > 0\},$$

c'est l'espace des matrices symétriques complexes de partie imaginaire définie positive.

Un élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe $\mathrm{Sp}_{2g}(\mathbb{R})$ agit sur $\mathcal{H}$ via :

$$z \mapsto (az + b)(cz + d)^{-1}.$$

L'action est bien définie (voir [21]) et se restreint en une action du groupe Γ_g. L'action de $\mathrm{Sp}_{2g}(\mathbb{R})$ est transitive et le stabilisateur du point $i1_g$ est le groupe unitaire

$$U(g) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{R}), a.a^t + b.b^t = 1_g \right\}.$$

L'action du sous-groupe discret Γ_g est propre et discontinue au sens où tout point z de $\mathcal{H}_g$ admet un voisinage ouvert U tel que l'ensemble $\{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})/\gamma(U) \cap U \neq \emptyset\}$ soit fini. Il est alors naturel de chercher un domaine fondamental de cette action. Il s'avère que, contrairement à la dimension 1, le domaine, construit par Siegel, est un peu plus compliqué et donné par les conditions suivantes :

(1) $|\det(cz + d)| \geq 1$ pour tout $(a, b, c, d) \in \Gamma_g$;

(2) La matrice $y = Im(z)$ est réduite au sens de Minkowski ;

(3) La matrice $x = Re(z)$ vérifie $|x_{ij}| \leq \frac{1}{2}$.

La deuxième condition veut dire que y vérifie les deux conditions $h^t y h \leq y_{kk}$ pour $k \in \{1, ..., g\}$ et pour tout vecteur primitif h de $\mathbb{Z}^g$, et $y_{k,k+1} \geq 0$ pour tout entier k tel que $0 \leq k \leq g$. Même lorsque $g = 2$, le bord reste assez compliqué à décrire (voir [21]).

6.2. **Formes de Siegel.** On commence d'abord par généraliser le facteur d'holomorphie "$(cz + d)^j$". Pour ce faire, considérons une représentation algébrique $\rho : \mathrm{GL}(g, \mathbb{C}) \to \mathrm{GL}(V)$ avec V espace vectoriel de dimension finie sur $\mathbb{C}$.

Définition 6.1. *On appelle forme modulaire de Siegel de poids ρ toute fonction $f : \mathcal{H}_g \to V$ holomorphe qui vérifie :*

$$f(\gamma.z) = \rho(cz + d)f(z)$$

pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ *et* $z \in \mathcal{H}_g$.
Pour $g = 1$, on requiert en plus que f vérifie les conditions de la définition 2.1.

La condition d'holomorphie aux bords lorsque $g > 1$ est automatique comme on le verra plus tard par le principe de Koecher.
On notera $M_\rho = M_\rho(\Gamma_g)$ l'espace vectoriel sur $\mathbb{C}$ des formes modulaires de poids ρ. On montre (Cf. [21]) que cet espace est de dimension finie. Remarquons que si $\rho = \rho_1 \oplus \rho_2$ est somme directe de deux représentations, alors $M_\rho = M_{\rho_1} \bigoplus M_{\rho_2}$. On peut donc se restreindre aux représentations irréductibles de $\mathrm{GL}(g, \mathbb{C})$, qu'on sait classifier via leurs poids [3].
Posons $M(\Gamma_g) := \bigoplus_{\rho \text{ irré.}} M_\rho(\Gamma_g)$. Pour $g = 1$, on a vu que cette somme directe admet une structure d'anneau gradué de type fini sur $\mathbb{C}$. Pour $g = 2$, on peut encore munir $M(\Gamma_g)$ d'une structure d'anneau gradué. Il s'agit d'abord de voir que les représentations irréductibles de $\mathrm{GL}(2, \mathbb{C})$ sont les représentations $\rho_{j,k}$ associées à $Sym^j(W) \otimes \det(W)^k$, où W est la représentation naturelle de $\mathrm{GL}(2, \mathbb{C})$. Elles correspondent aux représentations de plus haut poids $(\lambda_1, \lambda_2) = (j + k, k)$. En regardant alors $Sym^j(W)$ comme l'espace des polynômes de degré j en deux variables, on a des applications naturelles $Sym^{j_1}(W) \otimes Sym^{j_2}(W) \to Sym^{j_1+j_2}(W)$ et $\det(W)^{k_1} \otimes \det(W)^{k_2}$, ce qui définit la multiplication $M_{(j_1,k_1)} \otimes M_{(j_2,k_2)} \to M_{(j_1+j_2,k_1+k_2)}$, où l'on a noté $M_{(j,k)} = M_{\rho_{j,k}}(\Gamma_2)$. On montrera que cet anneau n'est pas type fini. Pour $g \geq 3$, il est encore possible de munir $M(\Gamma_g)$ d'une structure d'anneau gradué, nous référons à [23] pour plus de détails.

En prenant pour ρ la puissance k-iéme du déterminant, on retrouve la définition suivante, un peu plus habituelle des formes modulaires.

Définition 6.2. *Une forme modulaire de Siegel classique de poids k et degré g est une fonction holomorphe $f : \mathcal{H}_g \to \mathbb{C}$ telle que :*

$$f(\gamma(z)) = \det(cz + d)^k f(z)$$

avec $\gamma = (a, b, c, d) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ *et* $z \in \mathcal{H}_g$. *Si $g = 1$, on requiert de plus la condition d'holomorphie à l'infini comme dans la définition 2.1.*

On désignera par $M_k = M_k(\Gamma_g)$ l'espace vectoriel complexe des formes modulaires classiques de poids k.

6.3. **Développement en série de Fourier.** Les formes de Siegel admettent un développement en série de Fourier analogue à celui des formes modulaires classiques.

Définition 6.3. *Une matrice symétrique $n \in \mathrm{GL}(g, \mathbb{Q})$ est dite demi entière si $2n$ est une matrice à coefficients entiers et dont tous les coefficients diagonaux sont paires.*

Une matrice demi entière définit une forme linéaire à coefficients entiers sur $\mathcal{H}_g$ via la formule

$$Tr(nz) = \sum_{i=1}^{g} n_{ii} z_{ii} + 2 \sum_{1 \leq i < j \leq g} n_{ij} z_{ij}$$

avec $z = (z_{ij})_{1 \leq i \leq j \leq g} \in \mathcal{H}_g$. Écrivons $z = x + iy$ pour $z \in \mathcal{H}_g$, x étant la partie réelle et y la partie imaginaire. De même que dans le cas $g = 1$, une fonction $f : \mathcal{H}_g \to \mathbb{C}$ qui est périodique au sens où $f(z + s) = f(z)$ pour toute matrice symétrique à coefficients entiers s, admet un développement en série de Fourier

$$f(z) = \sum_{n \text{ demi entière}} a(n) e^{2i\pi Tr(nz)}$$

avec les coefficients $a(n)$ donnés par

$$a(n) = \int_{z \in D} f(z) e^{-2i\pi Tr(nz)} dx$$

où $D = \{z = x + iy, \forall i \leq j x_{ij} \in [\frac{-1}{2}, \frac{1}{2}]\}$. La série est uniformément convergente sur les compacts. On suppose maintenant que f est une forme de Siegel de poids ρ, comme f est invariante par $\begin{pmatrix} 1_g & s \\ 0 & 1_g \end{pmatrix}$ pour toute matrice s de taille g à coefficients entiers, on a alors de même un développement en série de Fourier

$$f(z) = \sum_{n \text{ demi entière}} a(n) e^{2i\pi Tr(nz)}$$

où les $a(n)$ sont cette fois des vecteurs, donnés par la même formule qu'en haut.

Lemme 6.4. *(1) Pour tout $u \in \mathrm{GL}(g, \mathbb{Z})$, et toute matrice n demi entière, on $a(u^t n u) = \rho(u^t) a(n)$.*

(2) Une forme modulaire de Siegel classique de poids k avec $gk \equiv 1 \pmod 2$ est identiquement nulle.

Démonstration. Pour le premier point, il suffit d'écrire

$$\begin{aligned} a(u^t n u) &= \int_{x \pmod 1} f(z) e^{-2i\pi Tr(u^t n u z)} dx \\ &= \rho(u^t) \int_{x \pmod 1} f(uzu^t) e^{-2i\pi Tr(nuzu^t)} dx \\ &= \rho(u^t) a(n). \end{aligned}$$

Pour le deuxième point, si on prend $u = -1_g$, on obtient pour toute matrice demi entière : $a(n) = \det(-1_g)^k a(n) = (-1)^{gk} a(n)$ ce qui permet de conclure. □

Théorème 6.5. *Soit $f \in M_\rho(\Gamma_g)$. Alors f est bornée sur tout sous-ensemble de $\mathcal{H}_g$ de la forme $\{z \in \mathcal{H}_g, Im(z) > c.1_g\}$ avec c symétrique définie positive.*

Démonstration. Le résultat pour $g = 1$ découle de la condition dans la définition. On suppose donc $g \geq 2$ et écrivons $f = \sum_n a(n) e^{2\pi i Tr(nz)} \in M_\rho(\Gamma_g)$. Par convergence absolue en $z = i1_g$, il existe une constante $M > 0$ telle que pour tout n on ait $|a(n)| \leq M e^{2\pi Tr(n)}$. Si n n'est pas positive, il existe alors un vecteur x à coordonnées entières primitives tel que $x^t n x < 0$. Par ailleurs, il existe une matrice $u \in \mathrm{GL}(g, \mathbb{Z})$ telle que x en soit le premier vecteur colonne. Quitte à considérer $a(u^t n u) = \rho(u^t) a(n)$, on peut donc supposer que le coefficient $n_{11} < 0$. Pour $m \in \mathbb{Z}$, posons $v = \begin{pmatrix} 1 & m & 0 \\ 0 & 1 & \\ 0 & 0 & 1_{g-2} \end{pmatrix} \in \mathrm{GL}(g, \mathbb{Z})$; il vient alors

$$|a(n)| \leq |\rho(v^t)^{-1}||a(v^t n v)| \leq M e^{2\pi Tr(v^t n v)} |\rho(v^t)^{-1}|.$$

Mais, $Tr(v^t n v) = Tr(n) + n_{11} m^2 + 2 n_{12} m$ qui tend vers $-\infty$ quand m tend vers $+\infty$, et $|\rho(v^t)^{-1}|$ est polynomiale en m, il s'ensuit que $a(n) = 0$. On peut donc écrire $f = \sum_{n \geq 0} a(n) e^{2\pi i Tr(nz)}$ et on peut alors majorer par la valeur en $ci.1_g$ de f, i.e $\sum_{n \geq 0} |a(n)| e^{-2\pi Tr(cn)}$ uniformément en z.

□

Au cours de la preuve précédente, on a montré le théorème suivant, dit principe de Koecher.

Théorème 6.6 (Principe de Koecher)**.** *Soit $f = \sum_n a(n) q^n \in M_\rho(\Gamma_g)$ avec $q^n = e^{2\pi i Tr(nz)}$ une forme modulaire de poids ρ. Alors $a(n) = 0$ si la matrice demi entière n n'est pas positive.*

Corollaire 6.7. *Une forme modulaire classique de poids négatif est identiquement nulle.*

Démonstration. Soit $f \in M_k(\Gamma_g)$ avec k un entier négatif. La fonction $h = \det(y)^{\frac{k}{2}}|f(z)|$ est invariante sous Γ_g. On peut prendre un domaine fondamental $\mathcal{D}$ qui soit contenu dans un ensemble de la forme $\{z = x + iy \in \mathcal{H}_g, Tr(x^2) < \frac{1}{c}, y > c.1_g\}$ pour un c réel strictement positif convenable. Il vient donc que pour k négatif, la quantité $\det(y)^{\frac{k}{2}}$ est bornée sur $\mathcal{D}$, et par le principe de Koecher, f est bornée sur $\{z \in \mathcal{H}_g : \det y \geq c\}$. Il s'ensuit que h est bornée sur $\mathcal{H}_g$, disons $h \leq c'$ et

$$a(n)e^{2\pi Trny} = \int_{xmod1} f(z)e^{-2i\pi Trnx}dx$$

on obtient alors

$$|a(n)|e^{2\pi Trny} \leq \sup_{xmod1} |f(x+iy)| \leq c' \det y^{-\frac{k}{2}}$$

Si on fait $y \to 0$ alors pour $k < 0$, on voit que $a(n) \to 0$ pour tout $n \geq 0$. □

6.4. **Opérateur de Siegel.** On a vu qu'une forme modulaire de Siegel de genre g, de poids ρ est bornée sur tout ensemble de la forme $\{z \in \mathcal{H}_g, Im(z) > c.1_g\}$, ce qui justifie la définition suivante :

Définition 6.8. *On définit l'opérateur* Φ *sur* $M_\rho(\Gamma_g)$ *par la formule suivante :*

$$\Phi f = \lim_{t \to +\infty} f \begin{pmatrix} z' & 0 \\ 0 & it \end{pmatrix} \text{ avec } z' \in \mathcal{H}_{g-1}, t \in \mathbb{R}_{>0}.$$

Au niveau du développement en série de Fourier, si on écrit $f(z) = \sum_{n \geq 0} a(n)e^{2\pi i Tr(nz)}$ alors $(\Phi f)(z') = \sum_{n' \geq 0} a(n')e^{2i\pi Tr(n'z')}$. L'opérateur de Siegel définit une application linéaire de $M_\rho(\Gamma_g)$ vers $M_{\rho'}(\Gamma_{g-1})$, où $\rho' = \rho_{|\mathrm{GL}_{g-1}}$ (voir [4] page 116).

Définition 6.9. *Une forme modulaire* $f \in M_\rho(\Gamma_g)$ *sera dite parabolique si* $\Phi f = 0$. *On notera* $S_\rho(\Gamma_g)$ *le sous espace des formes paraboliques.*

Il est facile de voir que f est une forme parabolique si, et seulement si, pour toute matrice n positive demi entière dont la coordonnée (g, g) est nulle, le coefficient $a(n)$ est nul. Comme toute matrice qui admet un vecteur isotrope s'écrit dans une base avec une coordonnée (g, g) nulle et en utilisant la relation $a(u^t nu) = \rho(u^t)a(n)$, on voit que c'est équivalent à $a(n) = 0$ pour toute matrice n qui n'est pas définie.

Lemme 6.10. [1] *Soient* $j > 0$ *et* $k > 4$. *L'application* $\Phi : M_{j,k}(\Gamma_2) \to S_{j+k}(\Gamma_1)$ *est surjective.*

Par application successive de l'opérateur de Siegel, on obtient des formes de Siegel dans $M_\rho(\Gamma_r)$ pour $r \leq g$, Soient maintenant f_1 et

f_2 deux formes modulaires de poids ρ dont l'une est parabolique. On définit le produit scalaire de Petersson par la formule

$$(f_1, f_2) = \int_F (\rho(Im(z))f_1(z), f_2(z))dz$$

avec $dz = \det(y)^{-(g+1)} \prod_{i\leq j} dx_{ij}dy_{ij}$ qui est une mesure invariante sur $\mathcal{H}_g$. Ici, F est un domaine fondamental pour l'action de Γ_g sur $\mathbb{H}_g$, et $(,)$ est un produit scalaire hermitien sur V.

6.5. **Algèbre de Hecke.** Les opérateurs de Hecke sont, sans nul doute, parmi les ingrédients essentiels de la théorie des formes modulaires classiques. Il parait donc raisonnable d'en construire une généralisation en genre $g > 1$. Pour plus de détails, on pourra consulter [21], paragraphe 16, ou [4], chapitre 4 pour un traitement plus complet. On pose $G := \mathrm{GSp}_{2g}(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_{2g}(\mathbb{Q}), \gamma^t J\gamma = \eta(\gamma)J, \eta(\gamma) \in \mathbb{Q}^\times\}$ et $G^+ = \{\gamma \in G, \eta(\gamma) > 0\}$. On définit l'algèbre de Hecke abstraite $H(\Gamma_g, G)$ comme les combinaisons linéaires formelles à coefficients rationnels des doubles classes $[\Gamma_g\gamma\Gamma_g]$ avec γ élément de G^+. Le groupe Γ_g agit à gauche sur une double classe $[\Gamma_g\gamma\Gamma_g]$ et on peut donc l'écrire comme union disjointe de représentants $\Gamma_g\gamma\Gamma_g = \cup_i\Gamma_g\beta_i$. Cette union est finie en vertu du lemme suivant.

Lemme 6.11. *Soit m un entier naturel. L'ensemble $\mathrm{O}_g(m) = \{\gamma \in \mathrm{M}_{2g}(\mathbb{Z}), \gamma^t J\gamma = mJ\}$ peut être écrit comme réunion finie disjointe de classes à droite. Toute classe à droite admet un représentant de la forme $(a, b; 0, d)$ avec $a^t d = m1_g$ et a triangulaire.*

On déduit donc qu'à toute double classe on peut associer une combinaison linéaire formelle de classes à droite. Notons $\mathcal{L}$ l'espace vectoriel sur $\mathbb{Q}$ engendré par les doubles classes à droite, on a alors une application linéaire naturelle injective $H(\Gamma, G) \to \mathcal{L}$, dont l'image est formée par les éléments invariants sous l'action de Γ_g, l'action d'un élément γ de Γ_g étant donnée par $\Gamma_g\alpha \mapsto \Gamma_g\alpha\gamma$. On munit $H(\Gamma_g, G)$ d'une structure d'algèbre via la loi suivante :

$$[\Gamma_g\gamma\Gamma_g].[\Gamma_g\delta\Gamma_g] = \sum_{i,j} \Gamma\gamma_i\delta_j,$$

où $[\Gamma_g\gamma\Gamma_g] = \sum_i \Gamma_g\gamma_i$ et $[\Gamma_g\delta\Gamma_g] = \sum_j \Gamma_g\delta_j$.

Proposition 6.12. *Soit $\gamma \in G^+$ à coefficients entiers. Alors la double classe $\Gamma\gamma\Gamma$ admet un unique représentant de la forme*

$$\alpha = diag(a_1, ..., a_g, d_1, ..., d_g)$$

avec a_i, d_i des entiers strictement positifs vérifiant $a_i d_i = \eta(\gamma)$, pour tout i. De plus, a_g divise d_g et a_i divise a_{i+1}, pour $i = 1, ..., g-1$.

La proposition précédente montre qu'on peut prendre pour représentants des doubles classes les matrices diagonales. On a alors que $H(\Gamma_g, G)$ est commutative et on a un isomorphisme d'algèbres ([9])

$$H(\Gamma_g, G) = \otimes_p H_p,$$

où $H_p = H(\Gamma_g, G \cap \mathrm{GL}(2g, \mathbb{Z}[\frac{1}{p}]))$. H_p a un sous-anneau engendré par les matrices à coefficients entiers. On note H_p^0 cet anneau. On a alors $H_p = H_p^0[\frac{1}{T}]$, avec $T = \Gamma_g(p1_{2g})\Gamma_g$.

Théorème 6.13 ([9])**.** *L'algèbre de Hecke H_p^0 est engendrée par les éléments $T(p)$ donnés par $\Gamma_g \begin{pmatrix} 1_g & 0_g \\ 0_g & p1_g \end{pmatrix} \Gamma_g$ et les éléments $T_i(p^2)$ pour $i = 1, ..., g$ donnés par*

$$\Gamma_g \begin{pmatrix} 1_{g-i} & & & \\ & p1_i & & \\ & & p^2 1_{g-i} & \\ & & & p1_i \end{pmatrix} \Gamma_g$$

.

Pour $m \geq 1$ entier naturel, par le lemme 6.11, $O_g(m)$ est réunion finie de doubles classes, dont la somme définit un élément de $H(\Gamma_g, G)$, qu'on note $T(m)$.

Exemple 6.14. *On retrouve l'opérateur $T(p)$ introduit précédemment pour $m = p$. Pour $m = p^2$, on a $T(p^2) = \sum_{i=0}^{g} T_i(p^2)$.*

On va maintenant faire agir l'algèbre de Hecke sur les formes modulaires de Siegel. Soient $\rho : \mathrm{GL}(g, \mathbb{C}) \to \mathrm{GL}(V)$ une représentation irréductible de plus haut poids $(\lambda_1, ..., \lambda_g)$, γ un élément de $\mathrm{GSp}_{2g}^+(\mathbb{Q})$. Pour une fonction $f : \mathcal{H}_g \to V$, on définit

$$f[\gamma]_\rho(z) = \rho(cz + d)^{-1} f(\gamma(z)),$$

où $\gamma = (a, b, c, d)$. On vérifie que cela définit une action à droite de $\mathrm{GSp}_{2g}^+(\mathbb{Q})$ sur l'ensemble des fonctions complexes sur $\mathcal{H}_g$. Une forme modulaire est donc tout simplement une fonction holomorphe invariante par cette action restreinte à Γ_g, du moins pour $g > 1$. Soit maintenant $\Gamma_g \gamma \Gamma_g$ une double classe, on définit alors

$$[\Gamma_g \gamma \Gamma_g] f = \sum_i f[\gamma_i]_\rho,$$

où $[\Gamma_g \gamma \Gamma_g] = \sum_i \Gamma_g \gamma_i$. Il est aisé de voir que c'est indépendant des choix des représentants des classes à droites, et que cela définit un endomorphisme linéaire de $M_\rho(\Gamma_g)$. Les opérateurs de Hecke $T(m)$, pour $m \in \mathbb{N}$ fixent $S_\rho(\Gamma_g)$ et sont normaux pour le produit scalaire de Petersson, donc sont simultanément diagonalisables en base orthonormée.

6.6. **Les formes modulaires en genre 2.** On s'intéressera désormais aux formes modulaires de Siegel de genre 2. On rappelle qu'on a défini une structure d'anneau sur $M(\Gamma_2) = \bigoplus_\rho M_\rho(\Gamma_2)$, où ρ parcourt l'ensemble des représentations irréductibles de $\mathrm{GL}(2,\mathbb{C})$. Chaque ρ est donnée par un couple (j,k) tel que $\rho = Sym^j(W) \otimes \det(W)^k$, W étant la représentation naturelle de $\mathrm{GL}(2,\mathbb{C})$. En termes de plus haut poids, c'est la représentation associée au poids (λ_1, λ_2) avec $(j,k) = (\lambda_1 - \lambda_2, \lambda_2)$. On peut donc écrire $M(\Gamma_2) = \bigoplus_{j,k\geq 0} M_{j,k}(\Gamma_2)$. Comme on l'avait déjà annoncé, cet anneau n'est pas de type de fini.

Lemme 6.15 (Grundh)**.** *L'anneau $M(\Gamma_2)$ n'est pas de type fini.*

Démonstration. En effet, supposons que ce soit le cas, et notons $f_n, n = 1, ..., r$ une famille de générateurs, de poids respectifs (j_n, k_n). Si h est une forme modulaire non nulle de poids (j,k), avec $j > max\{j_n, n = 1, ..., r\}$. Alors h est somme de produits des f_n. Dans chaque produit, il existe au moins deux f_n tels que $j_n > 0$. Comme ϕ est un morphisme d'anneaux, $\Phi(g)$ se trouve dans l'idéal engendré par Δ^2. Or, on sait par 6.10 que $\Phi : \mathcal{M}_{j,k}(\Gamma_2) \to S_{j+k}(\Gamma_1)$ est surjective pour $j > 0$ et $k > 4$. Soit g dans $S_{j+k}(\Gamma_1)$ qui soit dans l'idéal engendré par Δ mais pas dans celui engendré par Δ^2, avec $k > 4$ et $j > max\{j_n, n = 1, ..., r\}$. Soit h dans $\mathcal{M}_{j,k}(\Gamma_2)$ un antécédent de g par Φ. Alors $\Phi(h)$ n'est pas dans l'idéal engendré par Δ^2, ce qui fournit la contradiction cherchée. □

Théorème 6.16. *$M_{j,k}(\Gamma_2) = \{0\}$ si j est impair.*

Démonstration. Soit f une forme modulaire dans $M_{j,k}(\Gamma_2)$. On a donc $f(\gamma.z) = \det(cz+d)^k \rho_j(cz+d) f(z)$ pour tout $z \in \mathcal{H}_g$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z})$, ρ_j désignant la représentation dans le $Sym^j(\mathbb{C}^2)$. On applique cette relation avec $\gamma = -I_4$, il vient pour tout z dans $\mathcal{H}_g$, $f(z) = (-1)^j f(z)$. Comme j est impair, f est identiquement nulle.

□

Soit f $\in M_{j,k}(\Gamma_2)$, propre pour l'action de l'algèbre de Hecke, de système de valeurs propres $(\tau_f(n))_{n\in\mathbb{N}}$. On définit la fonction Zeta de Spin de f par

$$Z_f(s) = \xi(2s - j - 2k + 4) \sum_{m\geq 1} \frac{\tau_f(m)}{m^s}.$$

Théorème 6.17 ([21])**.** *Soit $f \in M_{j,k}(\Gamma_2)$, propre pour l'action de l'algèbre de Hecke. Alors*

$$Z_f(s) = \prod_p Q_p(p^{-s})^{-1},$$

avec

$$Q_p(X) = 1-\tau_f(p)X+(\tau_f(p)^2-\tau_f(p^2)-p^{j+2k-4})X^2-\tau_f(p)p^{j+2k-3}X^3+p^{2j+4k-6}X^4$$

6.7. **Représentations galoisiennes associées aux formes modulaires de Siegel.** Dans le cas des formes modulaires de Siegel, on démontre aussi l'existence des représentations galoisiennes qui leur sont associées. Nous ne détaillerons pas ce point dans ce mémoire. On admettra donc le théorème suivant.

Théorème 6.18. [4, 22] *Soit f une forme modulaire de Siegel parabolique de niveau Γ_2, de poids (j,k), et propre pour l'action des opérateurs de Hecke. Soit $\mathbb{Q}(f)$ le corps de nombre engendré par les valeurs propres a_n. Pour tout nombre premier ℓ et λ idéal premier de $\mathbb{Q}(f)$ au dessus de ℓ, il existe une représentation galoisienne continue (r_f, V) de dimension 4 sur $\overline{\mathbb{Q}(f)_\lambda}$ et une forme bilinéaire alternée non dégénérée b sur V telles que la représentation*

$$r_f : G_{\mathbb{Q}} \to \mathrm{GSp}(b)$$

est non ramifiée en dehors de ℓ et vérifie :

(1) Pour tout premier $p \neq \ell$: $\det(Id - Xr_f(Frob_p)) = Q_p(X)$.

(2) Si η est le facteur de similitude associé à b, alors $\eta \circ r_f = \chi_\ell^{j+2k-3}$.

Remarque 6.19.

La dimension de l'espace des formes paraboliques $S_{j,k}(\Gamma_2)$ est égale à 1, pour $(j,k) \in \{(6,8);(8,8);(4,10);(12,6)\}$ (voir [21]). La condition d'être propre pour les opérateurs de Hecke est donc automatiquement vérifiée. On notera dans ce cas $r_{j,k}$ la représentation galoisienne associée à l'unique forme parabolique normalisée de $S_{j,k}(\Gamma_2)$. Le polynôme Q_p a été introduit dans le théorème 6.17.

7. Étude des représentations galoisiennes associées aux formes modulaires de Siegel de genre 2

Soit ℓ un nombre premier. On a associé dans le paragraphe précédent à toute forme modulaire de Siegel f parabolique de niveau Γ_2, de poids (j,k), une représentation galoisienne ℓ-adique r_f définie sur une extension E finie de $\mathbb{Q}_\ell$. La représentation r_f admet un réseau stable L. Soit π une uniformisante de E. L'espace $L/\pi L$ est une représentation

galoisienne continue sur $\overline{\mathbb{F}_\ell}$. On la note $\overline{r_{f,\ell}}$. L'objectif de cette partie sera d'étudier l'irréductibilité et les images de ces représentations lorsque $(j,k) \in \{(6,8);(8,8);(4,10);\ (12,6)\}$. Rappelons que dans ce cas, il y a une unique forme parabolique normalisée, et on a noté $r_{j,k}$ la représentation galoisienne associée. On note $\overline{r_{j,k,\ell}}$ la représentation résiduelle.

7.1. **Étude de l'irréductibilité.** On va suivre une méthode analogue à celle utilisée dans [6] pour étudier l'irréductibilité des $\overline{r_{j,k,l}}$ pour $(j,k) \in \{(6,8);(8,8);(4,10);(12,6)\}$. Pour ces formes modulaires, Chenevier et Lannes montrent ([4], Chapitre 9, Paragraphe 6) que les représentations $\overline{r_{j,k,l}}$ sont définies sur $\mathbb{F}_\ell$. La proposition suivante décrit l'action de l'inertie en ℓ.

Proposition 7.1 ([4])**.** *La représentation $\overline{r_{j,k,l}}$ restreinte à $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ est la réduction modulo ℓ d'une représentation cristalline dont les poids de Hodge-Tate sont $0, k-2, j+k-1, j+2k-3$. De plus, si $\ell > j+2k-2$, ce sont les poids de Serre modérés de cette restriction.*

Corollaire 7.2. *Soit $\ell > j+2k-2$. On suppose que la représentation $\overline{r_{j,k,\ell}}$ n'est pas irréductible. Alors la restriction de $\overline{r_{j,k,\ell}}$ au sous-groupe d'inertie I_ℓ agit de l'une des manières suivantes :*

$$\begin{pmatrix} 1 & * & * & * \\ 0 & \chi_\ell^{k-2} & * & * \\ 0 & 0 & \chi_\ell^{j+k-1} & * \\ 0 & 0 & 0 & \chi_\ell^{j+2k-3} \end{pmatrix}, \quad \begin{pmatrix} \psi_2^{j+2k-3} & * & * & * \\ 0 & \psi_2^{l(j+2k-3)} & * & * \\ 0 & 0 & \psi_2^{(k-2)+l(j+k-1)} & * \\ 0 & 0 & 0 & \psi_2^{j+k-1+l(k-1)} \end{pmatrix}$$

$$\begin{pmatrix} \psi_2^{j+2k-3} & * & * & * \\ 0 & \psi_2^{l(j+2k-3)} & * & * \\ 0 & 0 & \chi_\ell^{k-2} & * \\ 0 & 0 & 0 & \chi_\ell^{j+k-1} \end{pmatrix}, \quad \begin{pmatrix} 1 & * & * & * \\ 0 & \chi_\ell^{j+2k-3} & * & * \\ 0 & 0 & \psi_2^{(k-2)+l(j+k-1)} & * \\ 0 & 0 & 0 & \psi_2^{j+k-1+l(k-2)} \end{pmatrix}$$

Démonstration. Raisonnons sur la semi simplifiée V^{ss} de la représentation V. Par la proposition admise, on voit qu'il faut éliminer les cas où un caractère fondamental de niveau 3 ou 4 apparait. L'apparition d'un caractère de niveau 4 équivaut à dire que la représentation V^{ss} est irréductible. Cela équivaut à dire que dans la suite de Jordan-Hölder de V, il n'y a que deux termes, à savoir l'espace nul et V tout entier, ce qui équivaut à dire que V est irréductible, ce qui est exclu par hypothèse. L'apparition d'un caractère de niveau 3 se traduit par le fait que V^{ss} est somme de deux composantes irréductibles, la première de dimension 1, l'autre de dimension 3. L'action de I_ℓ est donc de la forme $\chi_\ell^{a_0} \oplus \bigoplus_{t=0}^{2} {\psi_3}^{n\ell^t}$ avec $\{a_0,a_1,a_2,a_3\} = \{0, k-2, j+k-1, j+2k-3\}$

et $n = a_1 + a_2 l + a_3 l^2$. Or, la représentation étant symplectique, on utilise l'argument général suivant sur les valeurs propres d'une similitude symplectique.

Lemme 7.3. *Soit $M \in \mathrm{GSp}_4(\overline{\mathbb{F}_\ell})$. L'ensemble $VP(M)$ des valeurs propres de M est invariant par l'application*

$$\phi : VP(M) \to VP(M), \alpha \mapsto \frac{\eta(M)}{\alpha}.$$

Admettons le lemme pour l'instant. On sait que $\eta \circ r_{j,k} = \chi_\ell^{j+2k-3}$. Donc par le lemme, l'inertie agit aussi via le caractère $\chi_\ell^{j+2k-3-a_0}$. La première possibilité est qu'il soit égal à $\chi_\ell^{a_0}$, ce qui implique que $\ell - 1$ divise $j+2+k-3-2a_0$. Mais ceci n'est pas vrai quelque soit la valeur de a_0 dans l'ensemble $\{0, k-2, j+k-1, j+2k-3\}$. La deuxième possibilité est que $\chi_\ell^{j+2k-3-a_0}$ soit égal à $\psi_3^{n\ell^t}$ pour un $t \in \{0,1,2,3\}$. Or, on sait que $\chi_\ell = \psi_3^{1+\ell+\ell^2}$, et que ψ_3 est d'ordre exactement $\ell^3 - 1$. On a donc

$$\begin{aligned} \chi_\ell^{j+2k-3-a_0} = \psi_3^{n\ell^t} &\Leftrightarrow \psi_3^{(j+2k-3-a_0)(1+\ell+\ell^2)} = \psi_3^{n\ell^t} \\ &\Leftrightarrow \ell^3 - 1 \backslash (j+2k-3-a_0)(1+\ell+\ell^2) - (\ell^t n) \end{aligned}$$

Ici on peut utiliser l'unicité de l'écriture en base ℓ, ce qui donne encore une fois $\ell - 1$ qui divise $j+2+k-3-2a_0$.
Il nous reste maintenant à prouver le lemme 7.3. Soit $M \in \mathrm{GSp}_4(\overline{\mathbb{F}_\ell})$. Soit α une valeur propre de M, alors

$$\begin{aligned} \det(M - \alpha I_4) = 0 &\Leftrightarrow \det(I_4 - \alpha M^{-1}) = 0 \\ &\Leftrightarrow \det(I_4 - \frac{\alpha}{\eta(M)} JMJ) = 0 \\ &\Leftrightarrow \det(M - \frac{\eta(M)}{\alpha} I_4) \end{aligned}$$

Ce qui conclut la preuve. □

Pour p nombre premier différent de ℓ, rappelons que le polynôme caractéristique de $\overline{r_{j,k,\ell}}(Frob_p)$ est :

$$P_{j,k,p}(X) = X^4 Q_p(\tfrac{1}{X})$$
$$= X^4 - \tau_{j,k}(p) X^3 + \tfrac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2} X^2 - \tau_{j,k}(p) p^{2k+j-3} X + p^{4k+2j-6}$$

ce qui définit $\tau_{j,k}(p)$ et $\tau_{j,k}(p^2)$. Le calcul de ces coefficients ont été effectués par Chenevier et Lannes dans [4]. Nous avons mis en annexe quelques valeurs qui nous seront utiles. Si la représentation $\overline{r_{j,k,\ell}}$ n'est pas irréductible, on est dans l'une des situations suivantes :

7.1.1. *Existence d'une droite ou d'un quotient de dimension 1 stable.* On suppose que $\overline{r_{j,k,\ell}}$ admet une droite stable ou un quotient de dimension 1 stable. Comme l'action est non ramifiée en dehors de ℓ, on conclut par 7.1 qu'elle donnée par χ_ℓ^i avec $i = 0, k-2, j+k-1$ ou $j+2k-3$. Il s'ensuit que $\chi_\ell^i(Frob_p)$ est racine du polynôme $P_{j,k,p}$ modulo ℓ. Or, on sait que les racines de $P_{j,k,p}$ sont stables par $\alpha \mapsto \frac{p^{j+2k-3}}{\alpha}$. On a donc soit $\chi_\ell^0(Frob_p)$ soit $\chi_\ell^{j+k-1}(Frob_p)$ est racine du polynôme $P_{j,k,p}$ modulo ℓ.
Dans le premier cas, on obtient la condition ℓ qui divise :

$$A_{j,k}(p) := \frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2} - \tau_{j,k}(p)(p^{2k+j-3}+1) + p^{4k+2j-6} + 1.$$

Dans le second cas, on doit avoir ℓ qui divise :

$$B_{j,k}(p) := p^{2k-4}(1+p^{2j+2}) - \tau_{j,k}(p)p^{k-2}(1+p^{j+1}) + \frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2}.$$

Le calcul explicite en quelques valeurs de p permet alors d'éliminer les valeurs ℓ pour lesquels cela pourrait être vrai. Le calcul est fait en annexe.

7.1.2. *Existence de deux composantes de dimension* 2 *reliées.* C'est le cas où après semi-simplification la représentation se décompose en deux représentations galoisiennes irréductibles :

$$\overline{r_{j,k,\ell}}^{ss} \cong \pi_1 \oplus \pi_2$$

tel que si α, β sont les racines du polynôme caractéristique de $\pi_1(Frob_p)$ alors $\frac{p^{2k+j-3}}{\alpha}, \frac{p^{2k+j-3}}{\beta}$ sont les racines de $\pi_2(Frob_p)$.
Deux cas sont alors à envisager :

— $\det(\pi_1) = \chi_\ell^{j+k-1} \qquad \det(\pi_2) = \chi_\ell^{j+3k-5}$.
— $\det(\pi_1) = \chi_\ell^{k-2} \qquad \det(\pi_2) = \chi_\ell^{2j+3k-4}$.

Dans le premier cas, le polynôme $P_{j,k,p}$ se factorise sous la forme :

$$P_{j,k,p}(X) = (X^2 - AX + p^{3k+j-5})(X^2 - \frac{A}{p^{k-2}} + p^{j+k-1})$$

En identifiant et en éliminant A, on voit que ℓ doit diviser :

$$C_{j,k}(p) := (\frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2} - p^{j+k-1} - p^{j+3k-5})(1+p^{k-2})^2 - p^{k-2}\tau_{j,k}(p)^2$$

Dans le second cas, on doit avoir une factorisation de la forme :

$$P_{j,k,p}(X) = (X^2 - AX + p^{3k+j-4})(X^2 - \frac{A}{p^{k-1}} + p^{k-2})$$

En identifiant et en éliminant A, on voit que ℓ doit diviser :

$$D_{j,k}(p) := (\frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2} - p^{k-2} - p^{j+3k-4})(1+p^{k-1})^2 - p^{k-1}\tau_{j,k}(p)^2$$

7.1.3. *Existence de deux composantes de dimension* 2 *non reliées.* Dans ce dernier cas, la semi-simplifiée est somme de deux représentations irréductibles $\overline{r_{j,k,l}}^{ss} \cong \pi_1 \oplus \pi_2$ avec $\det(\pi_1) = \det(\pi_2) = \chi_\ell^{j+2k-3}$. Alors $\pi_1|\mathrm{I}-l$ (resp.$\pi_2|\mathrm{I}-l$) est donnée par :

$$\begin{pmatrix} 1 & * \\ 0 & \chi_\ell^{j+2k-3} \end{pmatrix} ou \begin{pmatrix} \psi_2^{j+2k-3} & 0 \\ 0 & \psi_2^{l(j+2k-3)} \end{pmatrix}$$

respectivement :

$$\begin{pmatrix} \chi_\ell^{k-2} & * \\ 0 & \chi_\ell^{j+k-1} \end{pmatrix} ou \begin{pmatrix} \psi_2^{j+k-1+(k-2)l} & 0 \\ 0 & \psi_2^{k-2+(j+k-1)l} \end{pmatrix}$$

On utilise alors le théorème de Khare (Cf. [11]) : la représentation $\rho := \pi_2 \otimes \chi_\ell^{-k+2}$ est irréductible. Elle est impaire car son déterminant est χ_ℓ^{j+k-1} et $j+k-1$ est impair. Comme elle est non ramifiée hors de ℓ, le conducteur $N(\rho)$ est égal à 1. La restriction de ρ à I_l est donnée par l'une des deux possibilités :

$$\begin{pmatrix} 1 & * \\ 0 & \chi_\ell^{j+1} \end{pmatrix} ou \begin{pmatrix} \psi_2^{j+1} & 0 \\ 0 & \psi_2^{(j+1)l} \end{pmatrix}$$

Dans les deux cas, le poids $k(\rho)$ donné par la recette décrite dans le paragraphe 3.4 vaut $j+2$. Par le théorème 3.3, ρ est associée à une forme modulaire parabolique de niveau 1 et de poids $j+2$. Mais la seule forme parabolique de poids $j+2$ avec $j \in \{4,6,8,12\}$ et de niveau 1 est la forme nulle. Ce cas est donc exclu.

7.1.4. *Résultats des calculs explicites.* En utilisant les tables données dans [4], on calcule $A_{j,k}(p)$, $B_{j,k}(p)$, $C_{j,k}(p)$ et $D_{j,k}(p)$ pour certains premiers p. On retiendra le fait que les conditions de réductibilité précédemment étudiées imposent à ℓ de diviser les éléments de chaque ligne, dès que ℓ est supérieur à $j+2k-2$. On vient donc de démontrer le théorème suivant :

Théorème 7.4. *La représentation $\overline{r_{j,k,\ell}}$ est irréductible dans chacun des cas suivants :*

$$(j,k) = (6,8) \quad et \quad l \geq 23, \qquad (j,k) = (8,8) \quad et \quad l \geq 29$$

$$(j,k) = (12,6) \quad et \quad l \geq 23, \qquad (j,k) = (4,10) \quad et \quad l \geq 23, l \neq 41$$

7.2. **Étude de l'image.** Dans ce paragraphe, on va étudier les images possibles des représentations $r_{j,k}$ pour $(j,k) \in \{(6,6),(8,8),(12,6),(4,10)\}$ dans $\mathrm{GSp}_4(\mathbb{Z}_\ell)$. On va montrer, sous des hypothèses précises sur ℓ, que l'image est

$$\{M \in \mathrm{GSp}_4(\mathbb{Z}_\ell), \det(M) \in (\mathbb{Z}_\ell{}^\times)^{2j+4k-6}\}.$$

Notons pour simplifier ρ l'une des représentations précédentes. Dans un premier temps, on s'intéressera à l'image dans le groupe projectif $\mathrm{PGSp}_4(\mathbb{F}_\ell)$. On montrera que l'image contient $\mathrm{PSp}_4(\mathbb{F}_\ell)$. Un résultat de Serre permet alors de remonter à l'image dans $\mathrm{PGSp}_4(\mathbb{Z}_\ell)$.

7.2.1. *Calcul de l'image.* On commence par montrer que l'image de $\overline{\rho}$ dans $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ ne peut pas être contenue dans un sous-groupe maximal de la liste 5.18, du moins pour ℓ assez grand et tel que $\overline{\rho}$ soit irréductible. Notons G_ℓ l'image de $\overline{\rho}$ dans $\mathrm{GSp}_4(\mathbb{F}_\ell)$ et PG_ℓ l'image dans $\mathrm{PGSp}_4(\mathbb{F}_\ell)$. On suppose donc que c'est un sous-groupe strict de $\mathrm{PGSp}_4(\mathbb{F}_\ell)$. Par suite, G_ℓ est contenu dans l'un des sous-groupes maximaux de la liste 5.18.

7.2.2. *Stabilisateur d'une droite.* Ce cas n'est pas possible car on sait que la représentation est irréductible.

7.2.3. *Stabilisateur d'un plan parabolique.* Si G_ℓ stabilise un parabolique P, il stabilise alors l'unique droite isotrope D de P. La droite D correspond à un plan de V qui se trouve donc stable sous l'action de G_ℓ, ce qui contredit l'irréductibilité de la représentation.

7.2.4. *Stabilisateur d'un plan hyperbolique.* PG_ℓ est contenu dans le stabilisateur d'un plan P hyperbolique de $\bigwedge^2 V$. On voit alors que les éléments de PG_ℓ sont des similitudes pour b, donc sont soit de la forme $\begin{pmatrix} a & 0 \\ 0 & \frac{\alpha}{a} \end{pmatrix}$, soit de la forme $\begin{pmatrix} 0 & a \\ \frac{\alpha}{a} & 0 \end{pmatrix}$, avec α, a dans $\mathbb{F}_\ell^\times$. Les éléments de la première forme stabilisent les deux vecteurs isotropes de b, tandis que les deuxièmes les échangent. On construit ainsi un morphisme de groupe ϵ de PG_ℓ vers $\{\pm 1\}$, envoyant les éléments qui échangent les droites vers -1. Ce morphisme est surjectif, car sinon le groupe PG_ℓ stabilise deux plans de V, ce qui contredirait l'irréductibilité de son action sur V. L'idée ensuite est de remarquer que les éléments qui proviennent du groupe d'inertie en ℓ sont dans le noyau de ϵ. En fait, on remarque que les éléments qui échangent les deux droites ont un polynôme caractéristique de la forme $X^2 - \alpha$, donc ont des valeurs propres opposées. Or, on connait les valeurs propres des éléments du groupe d'inertie dans $\bigwedge^2 V$, ce sont les produits deux à deux des valeurs propres sur V, qui sont eux données par 7.2 : ce sont des caractères.

Remarquons que le groupe d'inertie sauvage en ℓ agit de manière unipotente et son image est un ℓ-Sylow, tandis le groupe d'inertie modéré en ℓ agit via un quotient fini, donc cyclique et engendre la partie diagonale. Soit donc σ un élément de I_p qui est un générateur de la partie diagonale de l'image de ρ. On a alors $\theta(\sigma) = -\eta(\sigma)$, avec $\theta = \psi_2^a$ et $\eta = \psi_2^b$, le couple (a, b) étant donné comme suit :

(1) $\{a,b\} \subset \{(l+1)(k-2), (l+1)(j+k-1), (l+1)(j+2k-3), (l+1)(j+3k-5), (l+1)(2j+3k-4)\}$

(2) $\{a,b\} \subset \{(l+1)(j+2k-3), k-2+l(j+k-1), l(k-2)+1(j+k-1), (l+2)(k-2)+(2l+1)(j+k-1), (2l+1)(k-2)+(l+2)(j+k-1)\}$

(3) $\{a,b\} \subset \{(l+1)(j+2k-3), (2l+1)(k-2)+j+k-1, (2l+1)(j+k-1)+k-2, (l+2)(k-2)+j+k-1, (l+2)(j+k-1)+k-2\}$

(4) $\{a,b\} \subset \{(l+1)(j+2k-3), 2(k-2)+(l+1)(j+k-1), (l+1)(k-2)+2(j+k-1), 2l(k-2)+(l+1)(j+k-1), (l+1)(k-2)+2l(j+k-1)\}$

Dans tous ces cas, $\psi_2^{a-b} = 1$, ce qui implique que dans chaque cas $\ell^2 - 1$ divise $a-b$. On obtient un ensemble fini de valeurs de ℓ qui vérifient ces conditions. Pour ℓ différent de ces valeurs, le morphisme ϵ est surjectif et définit une extension de degré de 2 de $\mathbb{Q}$ partout non ramifiée, ce qui n'est évidemment pas possible.

7.2.5. *Stabilisateur d'un plan elliptique.* Si PG_ℓ est contenu dans le stabilisateur d'un plan P elliptique de $\bigwedge^2 V$, on se ramène alors au cas précédent en se plaçant dans une extension quadratique de $\mathbb{F}_\ell$, $\overline{\rho}$ restant toujours irréductible dans cette extension.

7.2.6. *Stabilisateur d'une cubique.* Si PG_ℓ est le stabilisateur d'une cubique, on sait d'après la remarque qui suit 5.18 que tout élément f de PG_ℓ vérifie la propriété suivante : il existe une énumération des valeurs propres de f tel que les rapports successifs soient égaux. Pour $\ell > j + 2k - 2$ l'action de l'inertie est donnée par des matrices triangulaires comme dans 7.2. En particulier, on connait explicitement les valeurs propres des éléments du groupe d'inertie. Distinguons plusieurs cas :

(1) Les valeurs propres de l'action de l'inertie sont $\{1, \chi_\ell^{k-2}, \chi_\ell^{j+k-1}, \chi_\ell^{j+2k-3}\}$, on est alors dans l'un des cas suivants :

$$\chi_\ell^{(k-2)} = \chi_\ell^{(j+1)} \quad ; \quad \chi_\ell^{(k-2)} = \chi_\ell^{(-j-1)}$$
$$\chi_\ell^{(j+k-1)} = \chi_\ell^{(k-2)} \quad ; \quad \chi_\ell^{(j+k-1)} = \chi_\ell^{(-j-1)}$$

Ce qui implique que $\ell - 1$ divise $k - j - 3$, $k - 2 + j + 1$, $j + 1$ ou $2j + k$.

(2) Les valeurs propres de l'action de l'inertie sont $\{1,\chi_\ell^{j+2k-3}, \psi_2^{k-2+l(j+k-1)}, \psi_2^{l(k-2)+j+k-1}\}$. On a alors l'une des possibilités :

$$\begin{aligned} \psi_2^{(j+1)(l-1)+(l+1)(j+2k-3)} = 1 \quad &; \quad \psi_2^{(l+1)(j+2k-3)-(j+1)(l-1)} = 1 \\ \psi_2^{k-2+l(j+k-1)} = 1 \quad &; \quad \psi_2^{(l-2)(k-2)-(2l-1)(j+k-1)} = 1 \\ \psi_2^{(l-1)(j+2)} = 1 \quad &; \quad \psi_2^{(l+1)(j+2)} = 1. \end{aligned}$$

Cela implique que ℓ^2-1 divise l'un des exposants $(j+1)(l-1)+(l+1)(j+2k-3)$, $(l+1)(j+2k-3)-(j+1)(l-1)$, $k-2+l(j+k-1)$, $(l-2)(k-2)-(2l-1)(j+k-1)$, $(l-1)(j+2)$ ou $(l+1)(j+2)$.

(3) Les valeurs propres de l'action de l'inertie sont $\{\psi_2^{k-2+l(j+k-1)}, \psi_2^{l(k-2)+j+k-1}, \psi_2^{l(j+2k-3)}, \psi_2^{j+2k-3}\}$. On a alors

$$\begin{aligned} \psi_2^{2(l-1)(k-2)} = 1 \quad &; \quad \psi_2^{(l-1)(2l+3k-4)} = 1 \\ \psi_2^{2(l-1)(j+k-1)} = 1 & \end{aligned}$$

Ce qui implique ℓ^2-1 divise $2(l-1)(k-2)$, $(l-1)(2l+3k-4)$ ou $2(l-1)(j+k-1)$.

(4) Les valeurs propres de l'action de l'inertie sont $\{\psi_2^{l(j+2k-3)}, \psi_2^{j+2k-3}, \chi_\ell^{k-2}, \chi_\ell^{j+k-1}\}$. On alors

$$\begin{aligned} \psi_2^{(l-2)(j+k-1)+(2l-1)(k-2)} = 1 \quad &; \quad \psi_2^{(l-2)(k-2)+(2l-1)(j+k-1)} = 1 \\ \psi_2^{(l+1)(j+2k-3)} = 1 \quad &; \quad \psi_2^{(l+1)(k-2)} = 1 \\ \psi_2^{(2l+1)(l+1)} = 1 \quad &; \quad \psi_2^{(l+1)(j+1)} = 1 \end{aligned}$$

Cela implique de même que ℓ^2-1 divise $(l-2)(j+k-1)+(2l-1)(k-2)$, $(l-2)(k-2)+(2l-1)(j+k-1)$, $(l+1)(j+2k-3)2(l+1)(k-2)$ ou $(2l+1)(l+1)$, $(l+1)(j+1)$.

Dans tous les cas, ℓ ne peut prendre qu'un nombre fini de valeurs calculables explicitement.

7.2.7. *Cas restants.* Dans les cas 7 et 8, l'image est finie. Notons N son ordre, (égal à 1920, 3840, 360,720 ou 2520) alors tout élément de l'image de l'inertie est d'ordre divisant N, ce qui veut dire que les puissances N-ième des valeurs propres sont proportionnelles. On refait le même calcul que dans le paragraphe précédent. Les cas (10) et (11) impliquent que l'image peut être contenue dans $\mathrm{PSp}_4(\mathbb{F}_\ell)$. Cela entraîne que $\eta\circ\overline{\rho} = \chi_{j+2k-3}$ est à valeurs dans les carrés de $\mathbb{F}_\ell^\times$, ce qui n'est pas possible car χ_ℓ est surjectif et $j+2k-3$ est impair.

7.2.8. *L'image dans* $\mathrm{GSp}_4(\mathbb{Z}_l)$. On sait donc maintenant que l'image dans $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ est égale au groupe tout entier. Pour remonter à l'image dans $\mathrm{GSp}_4(\mathbb{F}_\ell)$, remarquons que le groupe dérivé $\mathrm{D}(G_\ell)$ de G_ℓ est contenu dans $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Comme ce dernier est simple, montrons que $\mathrm{D}(G_\ell)$ est distingué dans $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Soit $M \in \mathrm{Sp}_4(\mathbb{F}_\ell)$, on sait qu'il existe $\lambda \in \mathbb{F}_\ell$ tel que $\lambda M \in G_\ell$, d'où $MG_\ell M^{-1} = (\lambda M)G_\ell(\lambda M)^{-1} \subset G_\ell$. Ainsi, $\mathrm{Sp}_4(\mathbb{F}_\ell) \subset \mathrm{D}(G_\ell) \subset G_\ell$. Enfin, pour remonter à $\mathrm{GSp}_4(\mathbb{Z}_\ell)$, on aura besoin du lemme suivant :

Lemme 7.5 ([20])**.** *Soit K une extension finie de $\mathbb{Q}_\ell$ avec $\ell \geq 5$ et k le corps résiduel de O_K. Soit G un sous-groupe fermé de de $\mathrm{GSp}_4(O_K)$ tel que son image dans $\mathrm{GSp}_4(k)$ contienne $\mathrm{Sp}_4(k)$. Alors G contient $\mathrm{Sp}_4(\mathbb{F}_q)$.*

Grâce à ce lemme , on voit donc que $\rho(G_\mathbb{Q})$ contient $\mathrm{Sp}_4(\mathbb{Z}_\ell)$. Pour voir que l'image est bien ce qu'on avait annoncé au début, prenons M dans $\mathrm{GSp}_4(\mathbb{Z}_\ell)$ avec $\det(M) = a^{2j+4k-6}$ et $\eta(M) = a^{j+2k-3}$ où $a \in {\mathbb{Z}_\ell}^\times$. Par surjectivité du caractère cyclotomique, il existe $\sigma \in G_\mathbb{Q}$ tel que $\chi_\ell(\sigma) = a$. On donc $\det(M\rho(\sigma)^{-1}) = 1$. D'autre part, on sait que $\eta \circ \rho = {\chi_\ell}^{j+2k-3}$, η étant le facteur de similitude, donc $\eta(M\rho(\sigma)^{-1}) = 1$ et donc $M\rho(\sigma)^{-1}$ est dans $\mathrm{Sp}_4(\mathbb{Z}_\ell)$ qui est contenu dans l'image de ρ en vertu du lemme 7.5.

On a donc démontré le théorème suivant :

Théorème 7.6. *L'image de la représentation $r_{j,k}$ est*

$$\{M \in \mathrm{GSp}_4(\mathbb{Z}_\ell), \det(M) \in ({\mathbb{Z}_\ell}^\times)^{2j+4k-6}\}$$

pour ℓ en dehors d'un ensemble explicitement calculable.

8. Calculs explicites

q	$\tau_{(6,8)}(q)$	$\tau_{(8,8)}(q)$	$\tau_{(12,6)}(q)$	$\tau_{(4,10)}(q)$
2	0	1344	-240	1680
3	-2700	-6408	68040	55080
4	409600	348160	4276480	6700160
9	333371700	748312020	-8215290540	1854007380

Table 1. Quelques valeurs propres des opérateurs de Hecke en genre 2 [4]

p	2	3
$A_{6,8}(p)$	$3^3.5.37.137.197.2039$	$2.5.181.307.509.4776205843$
$B_{6,8}(p)$	$2^{12}.3^3.5.11$	$2.5.7.8167.4522201$
$C_{6,8}(p)$	$2^{28}.3^4.229^2$	$2^6.3^{12}.23.79.2749.52837.79939$
$D_{6,8}(p)$	$2^{12}.337^2.3121^2$	$2^4.3^{12}.13.59.71.13951114252717$

Table 2. Factorisations pour $(j,k) = (6,8)$

p	2	3
$A_{8,8}(p)$	$3^2.488358740729$	$2^{12}.11.13.43.67.64841599673$
$B_{8,8}(p)$	$2^{13}.3^2.5^2.13.43$	$2^{17}.3^8.5^2.11.13.67$
$C_{8,8}(p)$	$-2^{13}.3^2.17.23^3.37$	$-2^{13}.3^9.23^2.67.711097$
$D_{8,8}(p)$	$-2^6.3^3.5.7.29.61.41641$	$-2^9.3^6.5.41.1019.1404659131$

Table 3. Factorisations pour $(j,k) = (8,8)$

p	2	3
$A_{12,6}(p)$	$3^3.5.32581834951$	$2^{14}.5.11.121424757430201$
$B_{12,6}(p)$	$2^{13}.3^5.5.7.13.19$	$2^1 3.3^8.5.7.13$
$C_{12,6}(p)$	$-2^{14}.3^3.7.13.257$	$-2^{14}.3^9.7.13.107.1801$
$D_{12,6}(p)$	$-2^4.3^3.5.7.4985489$	$-2^8.3^4.5.13.41.193.14153287$

Table 4. Factorisations pour $(j,k) = (12,6)$

p	2	3
$A_{4,10}(p)$	$3^3.5^2.11.10861.54581$	$2^{11}.5^2.11.41.103.739.62253281$
$B_{4,10}(p)$	$2^{12}.3^2.5.11.41$	$2^1 1.3^1 2.5.11.41$
$C_{4,10}(p)$	$-2^{14}.3^4.11.67.36137$	$-2^{13}.3^{15}.11.17.173.2689$
$D_{4,10}(p)$	$-2^8.3^2.5^3.979560973$	$2^8.3^8.5^2.89.271.158663.496453$

TABLE 5. Factorisations pour $(j,k) = (4,10)$

RÉFÉRENCES

[1] T. ARAKAWA, *Dirichlet series corresponding to siegel's modular forms of degree n with level n*, Tohoku Math. J. (2), 42 (1990), pp. 261–286.

[2] L. BERGER, *An introduction to the theory of p-adic representations*, Geometric aspects of Dwork theory, 1 (2004), pp. 255–292.

[3] D. BUMP, *Lie Groups*, Graduate Texts in Mathematics, Springer, 2004.

[4] G. CHENEVIER AND J. LANNES, *Formes automorphes et voisins de Kneser des réseaux de Niemeier*, ArXiv e-prints, (2014).

[5] F. DIAMOND AND J. SHURMAN, *A First Course in Modular Forms*, Graduate Texts in Mathematics, Springer, 2005.

[6] L. V. DIEULEFAIT, *On the images of the Galois representations attached to genus 2 Siegel modular forms*, J. Reine Angew. Math., 553 (2002), pp. 183–200.

[7] L. FARGUES AND J.-M. FONTAINE, *Vector bundles and p-adic Galois representations*, in Fifth International Congress of Chinese Mathematicians. Part 1, 2, vol. 2 of AMS/IP Stud. Adv. Math., 51, pt. 1, Amer. Math. Soc., Providence, RI, 2012, pp. 77–113.

[8] J.-M. FONTAINE, *Arithmétique des représentations galoisiennes p-adiques*, Astérisque, (2004), pp. xi, 1–115. Cohomologies p-adiques et applications arithmétiques. III.

[9] E. FREITAG, *Siegelsche Modulfunktionen*, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 2013.

[10] J. HIRSCHFELD, *Finite Projective Spaces of Three Dimensions*, Oxford mathematical monographs, Clarendon Press, 1985.

[11] C. KHARE AND J.-P. WINTENBERGER, *Serre's modularity conjecture. I*, Invent. Math., 178 (2009), pp. 485–504.

[12] O. H. KING, *The subgroup structure of finite classical groups in terms of geometric configurations*, in Surveys in combinatorics 2005, vol. 327 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, pp. 29–56.

[13] H. H. MITCHELL, *The subgroups of the quaternary abelian linear group*, Transactions of the American Mathematical Society, 15 (1914), pp. 379–396.

[14] I. REINER, *Review : Jean dieudonné, la géométrie des groupes classiques*, Bull. Amer. Math. Soc., 62 (1956), pp. 417–420.

[15] T. SAITO, *Galois representations and modular forms*, preprint, (2006).

[16] W. SCHARLAU, *Quadratic and hermitian forms*, Grundlehren der mathematischen Wissenschaften, Springer, 1985.

[17] J. Serre, *Corps locaux*, Actualités scientifiques et industrielles, Hermann, 2004.

[18] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15 (1972), pp. 259–331.

[19] J.-P. Serre, *Corps locaux*, Hermann, 2004.

[20] J.-P. Serre, *Oeuvres, Collected papers. IV. 1985–1998*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013. Reprint of the 2000 edition [MR1730973].

[21] G. van der Geer, *Siegel Modular Forms*, The 1-2-3 of modular forms, (2008). Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad.

[22] R. Weissauer, *Four dimensional galois representations*, Preprint, (2000).

[23] M. H. Weissman, *Multiplying Modular Forms*, ArXiv Mathematics e-prints, (2006).