Formes automorphes
et
réseaux unimodulaires pairs

Voisins de Kneser des réseaux de Niemeier

Gaëtan Chenevier[1] & Jean Lannes[2]

7 octobre 2016

1. Centre de Mathématiques Laurent Schwartz, École Polytechnique, 91128 Palaiseau Cedex, France (avant 10/2014). Université Paris-Sud, Département de mathématiques, Bâtiment 425, 91405 Orsay Cedex (à partir de 10/2014). Pendant la rédaction de ce mémoire, G. Chenevier a été financé par le C.N.R.S. , et il a reçu le soutien des projets ANR-10-BLAN 0114 et ANR-14-CE25.

2. Université Paris 7, UFR de Mathématiques, bâtiment Sophie Germain, avenue de France, 75013 Paris, France.

Préface

Les *formes automorphes* sont des fonctions définies sur des *groupes adéliques*, issues de l'analyse harmonique, dont la théorie constitue une vaste généralisation de celle des formes modulaires. La célèbre *conjecture de fonctorialité* de Langlands prédit des liens inattendus entre certaines formes automorphes associées à des groupes très différents. Des progrès récents établissent une partie de ces conjectures générales, et de leurs raffinements par Arthur, pour les groupes classiques. Si les démonstrations sont d'une complexité redoutable, les énoncés sont par contre fascinants par leur extrême beauté, leur vaste champs d'applications, et d'une certaine façon, par leur simplicité. Dans ce mémoire, nous nous proposons de réexaminer quelques problèmes d'origine classique de la théorie des nombres et des formes quadratiques sous l'angle de ces résultats récents.

Un cas particulier, dans lequel les conjectures de Langlands conservent néanmoins tout leur sel, tout en étant épurées des nombreuses difficultés présentes en général, est celui où l'on se restreint à étudier des formes automorphes *non ramifiées en tous les nombres premiers*. On parle aussi de formes de *niveau* 1. Lorsque l'on traite des formes modulaires classiques ou de Siegel, exemples historiques s'il en est de formes automorphes, cette hypothèse signifie que l'on considère seulement des formes modulaires pour les groupes $\mathrm{SL}_2(\mathbb{Z})$ ou $\mathrm{Sp}_{2g}(\mathbb{Z})$, et non pour les sous-groupes de congruences généraux.

L'intérêt du cas des formes automorphes de niveau 1 ne réside pas uniquement en les simplifications qu'il apporte, il est également très attractif pour l'arithméticien de par le mélange de rareté et d'élégance des exemples (que l'on songe là encore à la théorie des formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$). En outre, ces formes sont reliées, de manière parfois très directe, parfois beaucoup moins, et parfois seulement conjecturale, aux objets de la géométrie algébrique (variétés, champs) qui sont à la fois propres et lisses sur l'anneau $\mathbb{Z}$ des entiers, voire même aux *motifs* sur les rationnels ayant bonne réduction partout, objets aussi fascinants que mystérieux.

Dans ce travail, nous nous proposons d'étudier les conjectures d'Arthur et Langlands dans ce cadre des formes automorphes de niveau 1, de donner des formulations précises des énoncés résultants des travaux d'Arthur dans ce contexte, et d'illustrer ces derniers par des exemples plus spécifiques mais particulièrement piquants. Nous confronterons également les résultats d'Arthur à ceux issus de constructions plus classiques, celles de *séries thêta*, qui mettent à portée de main de nombreux exemples. Certaines de ces constructions se révèlent encore plus riches, comme nous l'avons d'écouvert, lorsqu'on

les combine avec le *principe de trialité*. Soulignons notre volonté de travailler avec des groupes si possible de grand rang, plus révélateurs de la richesse des phénomènes généraux, et de s'éloigner des exemples classiques fournis par les "petits" groupes comme GL_2, qui ont déjà fait l'objet d'une abondante littérature.

Nos illustrations porteront principalement sur la théorie des formes quadratiques sur $\mathbb{Z}$ qui sont non dégénérées et définies positives, autrement dit sur les réseaux euclidiens *(entiers et) pairs* dont le déterminant est 1 ou 2. Cette condition de déterminant signifie exactement que la quadrique projective associée est lisse sur $\mathbb{Z}$, auquel cas le groupe spécial orthogonal associé est lisse (et même réductif) sur $\mathbb{Z}$. Dans les dimensions (inférieures ou égales à 25) où ces objets sont classifiés, la question concrète qui va nous intéresser est la détermination, pour tout nombre premier p, du nombre de *p-voisinages* au sens de Kneser entre les classes de tels objets. Nous appellerons cette question comme le *problème des p-voisins*.

Le problème des p-voisins peut être abordé de manière très élémentaire : c'est le point de vue que nous adopterons dans l'introduction, puis dans l'organisation du mémoire, où il jouera un rôle de fil conducteur. Cela nous permettra en outre de commencer par exposer l'histoire riche et fascinante de ce sujet, et de mettre en évidence quelques énoncés simples mais frappants qui sont conséquences de nos résultats (cas de la dimension 16, détermination des graphes des p-voisins en dimension 24, résolution de la conjecture de Nebe-Venkov portant sur les combinaisons linéaires de séries thêta de genre supérieur des réseaux de Niemeier...). Toutefois, il paraît utile d'expliquer en amont notre motivation originelle qui était de tester les résultats d'Arthur dans un contexte à la fois concret et de grande dimension, et qui n'apparaîtra qu'au second plan dans l'introduction.

Dans la suite de cette préface, nous dégagerons la place du problème des p-voisins dans le paysage général des conjectures de Langlands, voire des motifs, et nous expliquerons le cheminement d'idées qui nous a conduit naturellement à ce problème. Cet éclaircissement (ou obscurcissement selon le point de vue !) permettra on l'espère d'intéresser des lecteurs moins sensibles aux attraits de la théorie des réseaux euclidiens. Il s'agira d'un passage en tous cas nécessaire pour comprendre les idées de sa résolution que nous proposerons, qui utilisera de manière cruciale les développements récents susmentionnés. Cette disproportion apparente entre la sophistication des méthodes utilisées et l'aspect élémentaire du problème des p-voisins est d'ailleurs l'un des charmes de ce dernier.

Le plan sera le suivant. Nous reviendrons d'abord de manière plus pré-

cise sur la notion de forme automorphe de niveau 1 (étudiée au chapitre IV du mémoire). Après avoir discuté de quelques exemples, nous présenterons brièvement les conjectures de Langlands, l'accent étant mis sur un énoncé que nous appellerons *conjecture d'Arthur-Langlands* (chapitres VI & VIII). Nous expliquerons comment Langlands et Arthur motivent cette conjecture au moyen d'un groupe hypothétique, le *groupe de Langlands de* $\mathbb{Z}$, que nous noterons $\mathrm{L}_{\mathbb{Z}}$. Lorsque l'on restreint les énoncés aux formes automorphes *algébriques*, on peut dans une large mesure susbtituer à $\mathrm{L}_{\mathbb{Z}}$ le groupe de Galois absolu de $\mathbb{Q}$. Il nous sera alors possible de fournir les éclaircissements promis ci-dessus, et également de laisser entrevoir quelques uns des problèmes restant à résoudre après avoir "mis dans la machine" les résultats d'Arthur.

Formes automorphes de niveau 1

Fixons un (schéma en) groupe algébrique linéaire G défini et *réductif* sur l'anneau $\mathbb{Z}$ des entiers. Ceci signifie que G est connexe, lisse sur $\mathbb{Z}$, et que sa réduction modulo p est réductive sur $\mathbb{Z}/p\mathbb{Z}$ pour tout nombre premier p. Les exemples les plus importants sont GL_n et les fameux groupes de Chevalley, ou leurs groupes isogènes comme PGL_n, mais d'autres exemples joueront un rôle important par la suite.

Le groupe adélique $G(\mathbb{A})$ est un groupe topologique localement compact de manière naturelle, produit *restreint* du groupe de Lie réel $G(\mathbb{R})$ et des groupes de Lie p-adiques $G(\mathbb{Q}_p)$ avec p parcourant tous les nombres premiers ; $G(\mathbb{Q})$ en est un sous-groupe discret. On note Z la composante neutre du centre de $G(\mathbb{R})$ (égale à 1 si G est semisimple). On dispose d'une mesure borélienne $G(\mathbb{A})$-invariante et finie sur l'espace homogène $G(\mathbb{Q})\backslash G(\mathbb{A})/Z$. Une question centrale est de décrire l'espace de Hilbert $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A})/Z)$ des *formes automorphes de carré intégrable de* G, vu comme représentation unitaire de $G(\mathbb{A})$ pour les translations à droite. Conformément à nos objectifs, nous nous limiterons à considérer le sous-espace

$$\mathcal{A}^2(G) = \mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A})/Z \cdot G(\widehat{\mathbb{Z}}))$$

des formes automorphes *de niveau* 1, qui n'est autre que le sous-espace des $G(\widehat{\mathbb{Z}})$-invariants de $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A})/Z)$. C'est un espace de Hilbert muni d'une représentation unitaire naturelle de $G(\mathbb{R})$ et, pour chaque premier p, de l'action de l'anneau de convolution

$$\mathrm{H}_p(G) = \mathbb{Z}[G(\mathbb{Z}_p)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p)],$$

dont les éléments sont les *opérateurs de Hecke* en p. Il s'agit de décrire $\mathcal{A}^2(G)$ muni de ces actions commutantes de $G(\mathbb{R})$ et de l'anneau commutatif $\mathrm{H}(G) := \bigotimes_p \mathrm{H}_p(G)$.

Notons $\Pi(G)$ l'ensemble des classes d'isomorphisme d'objets de la forme $\pi_\infty \otimes \pi_f$, avec π_∞ une représentation irréductible unitaire de $G(\mathbb{R})$ et π_f une représentation de dimension 1 de l'anneau $\mathrm{H}(G)$. Un tel π_f peut également être vu comme une collection de morphismes d'anneaux[1] $\pi_p : \mathrm{H}_p(G) \to \mathbb{C}$; on parle aussi de *système de valeurs propres des opérateurs de Hecke*. Notons de plus $\mathrm{m}(\pi)$ la *multiplicité* de π comme sous-représentation de $\mathcal{A}^2(G)$; elle est finie d'après Harish-Chandra. Une *représentation automorphe discrète* de G est un élément π de $\Pi(G)$ avec $\mathrm{m}(\pi) \neq 0$. Notons enfin $\Pi_{\mathrm{disc}}(G) \subset \Pi(G)$ le sous-ensemble de ces représentations. Pour des raisons générales, nous pouvons écrire

$$(1) \qquad \mathcal{A}^2(G) = \mathcal{A}^2_{\mathrm{disc}}(G) \overset{\perp}{\oplus} \mathcal{A}^2_{\mathrm{cont}}(G) \quad \text{avec} \quad \mathcal{A}^2_{\mathrm{disc}}(G) \simeq \overset{\perp}{\bigoplus_{\pi \in \Pi_{\mathrm{disc}}(G)}} \mathrm{m}(\pi)\ \pi.$$

L'espace $\mathcal{A}^2_{\mathrm{disc}}(G)$ contient le sous-espace $\mathcal{A}^2_{\mathrm{cusp}}(G)$ des formes *paraboliques*, dont la définition est une généralisation naturelle de celle de forme modulaire parabolique. On note $\Pi_{\mathrm{cusp}}(G) \subset \Pi_{\mathrm{disc}}(G)$ le sous-ensemble des éléments qui interviennent dans $\mathcal{A}^2_{\mathrm{cusp}}(G)$. La description des sous-ensembles $\Pi_{\mathrm{cusp}}(G) \subset \Pi_{\mathrm{disc}}(G)$ de $\Pi(G)$ est le coeur du problème. En effet, on sait depuis Langlands décrire la partie *continue* $\mathcal{A}^2_{\mathrm{cont}}(G)$ en terme des $\mathcal{A}^2_{\mathrm{cusp}}(L)$ où L parcourt les sous-groupes de Levi des sous-groupes paraboliques propres de G définis sur $\mathbb{Z}$. Nous ne nous intéresserons pas à $\mathcal{A}^2_{\mathrm{cont}}(G)$ dans ce mémoire.

Deux exemples

Les représentations π dans $\Pi_{\mathrm{disc}}(G)$ se manifestent concrètement de manière bien différente selon la nature de leur *composante archimédienne* π_∞. Si U est une représentation unitaire irréductible arbitraire de $G(\mathbb{R})$, et si l'on pose $\mathcal{A}_U(G) := \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}^2(G))$, on a

$$\mathcal{A}_U(G) = \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}^2_{\mathrm{disc}}(G)) \simeq \bigoplus_{\{\pi \,\in\, \Pi_{\mathrm{disc}}(G) \,|\, \pi_\infty \simeq U\}} \mathrm{m}(\pi)\ \pi_f$$

C'est un $\mathrm{H}(G)$-module de manière évidente, de dimension finie sur $\mathbb{C}$ d'après Harish-Chandra. La description de ces $\mathrm{H}(G)$-modules $\mathcal{A}_U(G)$ quand U parcourt le dual unitaire de $G(\mathbb{R})$ est équivalente à celle de $\Pi_{\mathrm{disc}}(G)$ tout entier.

1. Nous nous écartons ici de la tradition, selon laquelle π_p désigne plutôt la classe d'isomorphisme du sous $\mathbb{C}[G(\mathbb{Q}_p)]$-module (irréductible) de $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A})/Z)$ engendŕe par un élément non nul arbitraire de π. Cette différence n'est qu'apparente, car c'est une conséquence bien connue de la commutativité de $\mathrm{H}_p(G)$ que les deux définitions renferment exactement la même information.

En guise de point de repère, il paraît utile d'illustrer ces notions dans le cas particulier du groupe $G = \mathrm{PGL}_2$.[2] Si U est dans la *série discrète*, disons de plus bas poids l'entier (pair) $k > 0$, alors $\mathcal{A}_U(G)$ s'identifie de manière naturelle à l'espace des formes modulaires paraboliques de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ muni de l'action standard des opérateurs de Hecke sur ce dernier. Si $U := U_s$ est dans la *série principale ou complémentaire*, paramétrée de manière usuelle par un élément $s \in i\mathbb{R} \cup [0, 1[$, alors $\mathcal{A}_{U_s}(G)$ s'identifie au Hecke-module des *formes de Maass* paraboliques de valeur propre $\frac{1-s^2}{4}$ pour le Laplacien du demi-plan de Poincaré. Contrairement au cas précédent, ces espaces sont très mystérieux : Selberg a démontré[3] $\mathcal{A}_{U_s}(G) = 0$ pour $s > 0$, mais on ne connaît aucune valeur exacte de s telle que $\mathcal{A}_{U_s}(G)$ est non nul, ou s'il peut être de dimension > 1. Enfin, l'unique représentation unitaire restante de $\mathrm{PGL}_2(\mathbb{R})$ est, d'après Bargmann, la représentation triviale 1, et l'on a évidemment $\dim \mathcal{A}_1(G) = 1$ (considérer les fonctions constantes).

Discutons maintenant de l'exemple qui sera d'une très grande importance pour la suite. Soient $n \geq 1$ un entier et $\mathbb{R}^n$ l'espace euclidien standard de dimension n. Il se trouve que le groupe spécial orthogonal (compact) de $\mathbb{R}^n$ est de la forme $G(\mathbb{R})$ avec G réductif sur $\mathbb{Z}$ si, et seulement si, l'entier n est congru à -1, 0 ou $+1$ modulo 8. Décrivons un tel G sous l'hypothèse $n \equiv 0 \bmod 8$. Il est bien connu que dans ce cas $\mathbb{R}^n$ possède des *réseaux unimodulaires pairs*. Tout tel réseau L est naturellement muni d'une forme quadratique entière, définie positive et non-dégénérée sur $\mathbb{Z}$. Le (schéma en) groupe orthogonal associé O_L est lisse sur $\mathbb{Z}$, de composante neutre SO_L semisimple sur $\mathbb{Z}$, et de points réels $\mathrm{SO}(\mathbb{R}^n)$.

Nous noterons $\mathcal{L}_n$ l'ensemble des réseaux unimodulaires pairs de $\mathbb{R}^n$. Deux éléments quelconque de $\mathcal{L}_n$ sont dans le même *genre*, c'est-à-dire isométriques sur $\mathbb{Z}_p$ pour tout premier p (et donc également sur les rationnels, d'après Hasse et Minkowski). Cela entraîne d'une part que l'espace $\mathcal{A}^2(\mathrm{SO}_L)$ dépend de manière inessentielle du choix de L. Pour fixer les idées, nous nous bornerons dans le mémoire à considérer $\mathrm{SO}_n := \mathrm{SO}_{\mathrm{E}_n}$, où E_n désigne le réseau unimodulaire pair *standard* engendré par $\frac{1}{2}(1, \ldots, 1)$ et les n-uples d'entiers $(x_1, \ldots, x_n)$ tels que $\sum_i x_i$ est pair. Une seconde conséquence est que l'on dispose d'une identification naturelle

$$\mathcal{L}_n \xrightarrow{\sim} \mathrm{SO}_n(\mathbb{Q})\backslash \mathrm{SO}_n(\mathbb{A})/\mathrm{SO}_n(\widehat{\mathbb{Z}})$$

compatibles aux actions évidentes de part et d'autre de $\mathrm{SO}_n(\mathbb{R})$. Si 1 désigne la représentation triviale de $G(\mathbb{R})$, et si $\widetilde{\mathrm{X}}_n = \mathrm{SO}(\mathbb{R}^n)\backslash\mathcal{L}_n$ désigne l'ensemble

2. Suivant nos définitions, on a un isomorphisme canonique $\mathcal{A}^2(\mathrm{PGL}_n) \xrightarrow{\sim} \mathcal{A}^2(\mathrm{GL}_n)$.

3. C'est l'analogue archimédien de la conjecture de Ramanujan, encore ouvert pour les sous-groupes de congruences généraux.

fini des classes d'isométrie directe d'éléments de $\mathcal{L}_n$, on a donc des isomorphismes naturels

$$\mathcal{A}_1(\mathrm{SO}_n) \simeq \{f : \widetilde{\mathrm{X}}_n \to \mathbb{C}\} \simeq \bigoplus_{\{\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n) \,|\, \pi_\infty \simeq 1\}} \mathrm{m}(\pi)\ \pi_f.$$

L'espace vectoriel $\mathbb{C}[\widetilde{\mathrm{X}}_n]$, dual de $\mathcal{A}_1(\mathrm{SO}_n)$, est donc un $\mathrm{H}(\mathrm{SO}_n)$-module de manière naturelle. Par exemple, c'est un exercice de voir que l'endomorphisme de $\mathbb{C}[\widetilde{\mathrm{X}}_n]$, associant à la classe d'un réseau la somme des classes de ses p-voisins, est induit par un élément de $\mathrm{H}_p(\mathrm{SO}_n)$ que nous noterons T_p. La determination de cet endomorphisme est exactement le problème considéré au début de l'introduction.[4] Ajoutons que les espaces $\mathcal{A}_U(\mathrm{SO}_n)$, avec U arbitraire (mais nécessairement de dimension finie), ont des interprétations analogues en termes de fonctions $\mathrm{SO}_n(\mathbb{R})$-équivariantes $\mathcal{L}_n \to U^*$; de nombreux espaces de ce type joueront également un rôle dans ce mémoire.

Le principe de fonctorialité de Langlands

Décrivons de manière un peu grossière les conjectures générales de Langlands dans le cas des formes de niveau 1. Un point de départ est la notion, introduite par Langlands, de groupe *dual*. Si G est réductif sur $\mathbb{Z}$, son dual au sens de Langlands est simplement "le" groupe algébrique linéaire et réductif sur $\mathbb{C}$, noté $\widehat{G}$, dont la *donnée radicielle basée* est *duale* (ou *inverse*) à celle de $G_{\mathbb{C}}$:

$G_{\mathbb{C}}$	GL_n	PGL_n	Sp_{2g}	PGSp_{2g}	SO_{2n+1}	SO_{2n}	PGSO_{2n}
$\widehat{G}$	GL_n	SL_n	SO_{2g+1}	Spin_{2g+1}	Sp_{2n}	SO_{2n}	Spin_{2n}

Ce groupe permet d'abord à Langlands de *paramétrer* les éléments de $\Pi(G)$. Il observe que l'*isomorphisme de Satake* fournit une bijection canonique, pour chaque nombre premier p, entre l'ensemble des morphismes d'anneaux $\mathrm{H}_p(G) \to \mathbb{C}$ et celui des classes de conjugaison semisimples dans $\widehat{G}(\mathbb{C})$. De même, il interprête le *caractère infinitésimal* (au sens d'Harish-Chandra) d'une représentation unitaire de $G(\mathbb{R})$ comme une classe de conjugaison semisimple dans l'algèbre de Lie de $\widehat{G}$. Au final, à chaque élément π de $\Pi(G)$ est associé une collection de classes de conjugaisons

$$\mathrm{c}(\pi) = (\mathrm{c}_\infty(\pi), \mathrm{c}_2(\pi), \mathrm{c}_3(\pi), \cdots)$$

4. En fait, nous considèrerons surtout le problème analogue, quoique légèrement plus simple, dans lequel SO_n est remplacé par $\mathrm{O}_n = \mathrm{O}_{\mathrm{E}_n}$, dont le seul défaut est de ne pas tout à fait s'insérer dans les conventions adoptées ici, car O_n n'est pas connexe, mais cette nuance est un détail à ce stade.

qui détermine entièrement les π_p pour tout p premier, ainsi que le caractère infinitésimal de π_∞, ce qui laisse un nombre fini de possibilités pour π_∞. Ces paramétrisations, rappelées au chapitre VI, ont des aspects très concrets. Par exemple, nous verrons que pour π dans $\Pi(\mathrm{SO}_n)$ on la relation :

$$\pi_p(\mathrm{T}_p) \;=\; p^{\frac{n}{2}-1}\,\mathrm{trace}\,\mathrm{c}_p(\pi). \tag{2}$$

Soient G et G' deux groupes réductifs sur $\mathbb{Z}$ et un morphisme de groupes algébriques $r : \widehat{G} \to \widehat{G'}$. Le *principe de fonctorialité* de Langlands prédit, pour chaque *constituant* π dans $\mathcal{A}^2(G)$, l'existence d'un constituant π' de $\mathcal{A}^2(G')$ qui lui *correspond*, au sens où l'on a l'égalité de classes de conjugaison $r(\mathrm{c}_v(\pi)) = \mathrm{c}_v(\pi')$ pour tout v dans l'ensemble $\mathrm{V} := \{\infty, 2, 3, 5, \ldots\}$ des places de $\mathbb{Q}$. Il s'agit d'un principe, plutôt que d'une conjecture, car ainsi formulé il n'est pas tout à fait exact, et ceci même si l'on donne un sens convenable au terme "constituant". Nous nous proposons dans ce qui suit de préciser ce principe de fonctorialité dans le cas particulier important $G' = \mathrm{GL}_n$, auquel cas r n'est rien d'autre qu'une représentation du groupe algébrique $\widehat{G}$. C'est cet énoncé que nous appellerons la conjecture d'Arthur-Langlands.

Le groupe de Langlands de $\mathbb{Z}$

Langlands a observé que la formulation de ses conjectures devient lumineuse si l'on suppose l'existence d'un certain groupe [5] $\mathrm{L}_\mathbb{Z}$, dont les représentations dans $\widehat{G}$ paramètrent les représentations automorphes de G en un sens à préciser. On peut penser ici à ce groupe comme étant une extension du groupe de Galois absolu de $\mathbb{Z}$ (... trivial d'après Minkowski !). Pour les besoins de cette préface, il nous suffira d'admettre que $\mathrm{L}_\mathbb{Z}$ est un groupe topologique compact (donc limite inverse de groupes de Lie compacts) soumis aux axiomes notés (L1), (L2) et (L3) que nous allons introduire ci-dessous.

(L1) $\mathrm{L}_\mathbb{Z}$ *est muni, pour tout nombre premier p, d'une classe de conjugaison* $\mathrm{Frob}_p \subset \mathrm{L}_\mathbb{Z}$*, et sa pro-algèbre de Lie complexifiée, d'une classe de conjugaison semisimple* Frob_∞.

Soit G réductif sur $\mathbb{Z}$. Suivant Arthur et Langlands, notons $\Psi(G)$ l'ensemble des classes de $\widehat{G}(\mathbb{C})$-conjugaison de morphismes de groupes

$$\psi : \mathrm{L}_\mathbb{Z} \times \mathrm{SL}_2(\mathbb{C}) \longrightarrow \widehat{G}(\mathbb{C}) \tag{3}$$

5. Pour être tout à fait honnêtes, précisons que Langlands définit plutôt un groupe s'appliquant à toutes les formes automorphes, plutôt qu'à celles de niveau 1, dont notre $\mathrm{L}_\mathbb{Z}$ ne serait qu'un quotient [Lan79, §2]. De plus, comme Arthur [Art89, §8], nous adoptons le point de vue de Kottwitz [Kot84, §12] consistant à voir le groupe de Langlands comme un groupe topologique plutôt qu'un groupe pro-algébrique comme le fait Langlands.

supposés continus, et algébriques sur le facteur $\mathrm{SL}_2(\mathbb{C})$. Un tel ψ est dit *discret* si le centralisateur C_ψ de $\mathrm{Im}\ \psi$ dans $\widehat{G}(\mathbb{C})$ est fini modulo le centre $\mathrm{Z}(\widehat{G})$ de ce dernier. Par exemple, si G est GL_n, auquel cas on a également $\widehat{G} = \mathrm{GL}_n$ et ψ n'est rien d'autre qu'une représentation de dimension n de $\mathrm{L}_\mathbb{Z} \times \mathrm{SL}_2(\mathbb{C})$, alors ψ est discret si, et seulement si, c'est une représentation irréductible. On note $\Psi_{\mathrm{disc}}(G) \subset \Psi(G)$ le sous-ensemble des classes de morphismes discrets.

Parallèllement à ce qui a été fait pour $\Pi(G)$, Arthur et Langlands associent à chaque ψ dans $\Psi(G)$ une collection de classes de conjugaison $\mathrm{c}(\psi) = (\mathrm{c}_v(\psi))_{v\in\mathrm{V}}$ définie par $\mathrm{c}_\infty(\psi) = \psi(\mathrm{Frob}_\infty, \mathrm{e}_\infty)$ et $\mathrm{c}_p(\psi) = \psi(\mathrm{Frob}_p, \mathrm{e}_p)$, où les e_v sont respectivement les éléments de $\mathfrak{sl}_2(\mathbb{C})$ pour $v = \infty$, et $\mathrm{SL}_2(\mathbb{C})$ pour $v = p$, définis par

$$\mathrm{e}_\infty = \begin{bmatrix} -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \quad \text{et} \quad \mathrm{e}_p = \begin{bmatrix} p^{-\frac{1}{2}} & 0 \\ 0 & p^{\frac{1}{2}} \end{bmatrix}.$$

(L2) *Pour tout entier $n \geq 1$, il existe une unique bijection*

$$\pi \mapsto \psi_\pi, \qquad \Pi_{\mathrm{disc}}(\mathrm{GL}_n) \xrightarrow{\sim} \Psi_{\mathrm{disc}}(\mathrm{GL}_n),$$

vérifiant $\mathrm{c}(\pi) = \mathrm{c}(\psi_\pi)$ pour tout $\pi \in \Pi_{\mathrm{disc}}(\mathrm{GL}_n)$. De plus, ψ_π est trivial sur $\mathrm{SL}_2(\mathbb{C})$ si, et seulement si, on a $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$.

Cet axiome, et la compacité de $\mathrm{L}_\mathbb{Z}$, contiennent la *conjecture de Ramanujan généralisée*. On en déduit aussi $|\mathrm{L}_\mathbb{Z}^{\mathrm{ab}}| = \dim \mathcal{A}(\mathrm{GL}_1) = 1$. Nous montrerons au chapitre IX que (L2) entraîne également que $\mathrm{L}_\mathbb{Z}$ est connexe.

(L3) *Pour tout G réductif sur $\mathbb{Z}$, il existe une décomposition*

$$\mathcal{A}_{\mathrm{disc}}(G) \ = \ \bigoplus^{\perp}_{\psi\in\Psi_{\mathrm{disc}}(G)} \mathcal{A}_\psi(G),$$

stable par $G(\mathbb{R})$ et $\mathrm{H}(G)$, et vérifiant la propriété suivante : si $\pi \in \Pi(G)$ intervient dans $\mathcal{A}_\psi(G)$ alors on a $\mathrm{c}(\pi) = \mathrm{c}(\psi)$.

On doit à Arthur l'idée que le défaut de validité de la conjecture de Ramanujan puisse être entièrement expliqué par la présence du $\mathrm{SL}_2(\mathbb{C})$ dans la définition de $\Psi(G)$ (Formule (3)).

Arthur et Langlands renforcent l'axiome (L3) par une réciproque de la propriété ci-dessus, appelée *formule de multiplicité*, dont la formulation nécessite toutefois l'introduction d'ingrédients plus techniques. Disons simplement qu'elle prend la forme suivante. Si $\psi \in \Psi_{\mathrm{disc}}(G)$ et $\pi \in \Pi(G)$ vérifient

$\mathrm{c}(\pi) = \mathrm{c}(\psi)$, alors la multiplicité de π dans $\mathcal{A}_\psi(G)$ est donnée par le produit scalaire entre deux caractères "explicites"[6] du groupe fini $\mathrm{C}_\psi/\mathrm{Z}(\widehat{G})$.

La conjecture d'Arthur-Langlands

Revenons à notre objectif d'énoncer la conjecture d'Arthur-Langlands à laquelle nous avons fait allusion plus haut. On suppose d'abord l'existence de $\mathrm{L}_\mathbb{Z}$ satisfaisant (L1), (L2) et (L3). Soient G réductif sur $\mathbb{Z}$, π dans $\Pi_{\mathrm{disc}}(G)$ et $r : \widehat{G} \to \mathrm{GL}_n$ une représentation. Soit $\psi \in \Psi_{\mathrm{disc}}(G)$ tel que π intervient dans $\mathcal{A}_\psi(G)$, il en existe d'après (L3). La décomposition en irréductibles de la représentation $r \circ \psi$ du groupe produit $\mathrm{L}_\mathbb{Z} \times \mathrm{SL}_2(\mathbb{C})$ s'écrit sous la forme $\oplus_i r_i \otimes \mathrm{Sym}^{d_i-1}\mathbb{C}^2$ pour certaines représentations irréductibles r_i de dimension n_i de $\mathrm{L}_\mathbb{Z}$, et certains entiers $d_i \geq 1$. D'après (L2), on a $r_i \simeq \psi_{\pi_i}$ pour un unique $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{GL}_{n_i})$. En particulier, pour tout $v \in \mathrm{V}$, on a l'identité entre classes de conjugaison

$$r(\mathrm{c}_v(\pi)) = \bigoplus_i \mathrm{c}_v(\pi_i) \otimes \mathrm{Sym}^{d_i-1}(e_v) \tag{4}$$

(le lecteur n'aura pas de mal à déchiffrer le sens du terme de droite de cette égalité).

Ainsi, si l'on a π dans $\Pi_{\mathrm{disc}}(G)$ et une représentation $r : \widehat{G} \to \mathrm{GL}_n$, on conjecture l'existence d'une décomposition $n = \sum_i n_i d_i$ et de représentations $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{GL}_{n_i})$, uniques à permutation près des indices i, vérifiant l'égalité (4) : c'est la forme exacte de la conjecture d'Arthur-Langlands que nous avions promise. Observons que sa formulation ne fait pas intervenir $\mathrm{L}_\mathbb{Z}$, que l'on peut donc au final oublier.

Dans son travail déjà mentionné, Arthur a démontré les cas particuliers suivants de cette conjecture : $G_\mathbb{Q}$ est soit le groupe symplectique Sp_{2g} d'un espace symplectique sur $\mathbb{Q}$ de dimension $2g$, soit le groupe spécial orthogonal d'un espace quadratique de dimension $2n$ (resp. $2n+1$) sur $\mathbb{Q}$ possédant un sous-espace isotrope de dimension n, $\pi \in \Pi_{\mathrm{disc}}(G)$ est quelconque, et r est la représentation naturelle de $\widehat{G}$, appelée *représentation standard*, de dimension respective $2g+1$, $2n$ et $2n$. Pour de tels groupes, Arthur démontre aussi une

6. La définition de ces deux caractères est très délicate. L'un est un morphisme de groupes $\mathrm{C}_\psi/\mathrm{Z}(\widehat{G}) \to \mathbb{C}^\times$ défini par Arthur [Art89, p. 55] au moyen de *facteurs* ε de certaines fonctions L associées à ψ. L'autre caractère dépend de la définition d'un sous-ensemble fini de représentations unitaires de $G(\mathbb{R})$ associé à ψ, noté $\Pi_\infty(\psi)$, appelé maintenant *paquet d'Arthur* [Art89, §4]. Ce caractère est non nul si, et seulement si, π_∞ est dans $\Pi_\infty(\psi)$. Dans le cas particulier important $\mathrm{C}_\psi = \mathrm{Z}(\widehat{G})$, on constate que la multiplicité de π dans $\mathcal{A}_\psi(G)$ est non nulle si, et seulement si, on a $\pi_\infty \in \Pi_\infty(\psi)$.

version de la formule de multiplicité à laquelle nous avons fait allusion dans la discussion de l'axiome (L3). Nous énoncerons des formes plus précises des résultats d'Arthur dans le chapitre VIII du mémoire. Soulignons en revanche que nous ne dirons rien des démonstrations d'Arthur, qui dépassent de très loin le cadre de ce travail.

Représentations galoisiennes et motifs

Le groupe $\mathrm{L}_{\mathbb{Z}}$ est soumis à bien d'autre conjectures. Une des plus tentante est qu'il satisfait à la *propriété de Sato-Tate* : les Frob_p sont équirépartis dans l'ensemble des classes de conjugaison de $\mathrm{L}_{\mathbb{Z}}$, muni de sa mesure de probabilité invariante.[7] Nous discutons plutôt dans ce paragraphe des liens conjecturés entre $\mathrm{L}_{\mathbb{Z}}$, motifs et représentations galoisiennes.

Ces liens ne concerneront que le quotient de $\mathrm{L}_{\mathbb{Z}}$ dont les représentations irréductibles paramètrent, au sens de l'axiome (L2), les représentations π dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$ qui sont *algébriques*. Cet adjectif signifie ici que, si l'on note λ_i les valeurs propres de la classe de conjugaison $\mathrm{c}_\infty(\pi) \subset \mathrm{M}_n(\mathbb{C})$, on a $\lambda_i - \lambda_j \in \mathbb{Z}$ pour tous i, j. On note alors $\mathrm{w}(\pi)$ le maximum des différences $\lambda_i - \lambda_j$, que l'on appelle le *poids motivique* de π.

Notons $\overline{\mathbb{Q}} \subset \mathbb{C}$ le sous-corps des nombres algébriques. Fixons ℓ un nombre premier, $\overline{\mathbb{Q}}_\ell$ une clôture algébrique du corps des nombres ℓ-adiques, et $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$ un plongement. Suite aux travaux de nombreux mathématiciens (dont Clozel, Deligne, Fontaine, Grothendieck, Langlands, Mazur, Serre, Shimura, Taniyama, Tate, Weil ...) on conjecture l'existence d'une bijection naturelle $\pi \mapsto \rho_{\pi,\iota}$ entre l'ensemble des π algébriques dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$, et l'ensemble des classes d'isomorphismes de représentations irréductibles et continues $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ supposées *non ramifiées* en tout premier $p \neq \ell$, *cristalline en* ℓ au sens de Fontaine, et de plus petit *poids de Hodge-Tate* 0. On demande que cette bijection satisfasse à l'égalité suivante[8]

$$\det(t - \rho_{\pi,\iota}(\mathrm{Frob}_p)) = \iota(\det(t - p^{\mathrm{w}(\pi)/2}\mathrm{c}_p(\pi)))$$

pour tout premier $p \neq \ell$, ce qui la caractérise uniquement.

Cet énoncé constitue manifestement un analogue "algébrique" de l'axiome (L2). De nombreux résultats partiels, mais difficiles et importants, en sont connus. Suivant Fontaine et Mazur, on s'attend à ce que les représentations

7. Étant donné la connexité de $\mathrm{L}_{\mathbb{Z}}$, il ne serait pas difficile de voir que cette propriété entraîne la conjecture de Sato-Tate usuelle pour les formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$.

8. Cette égalité n'a de sens que parce que l'on conjecture également que le polynôme caractéristique $\det(t - \mathrm{c}_p(\pi))$ est à coefficients dans $\overline{\mathbb{Q}}$ si π est algébrique.

galoisiennes mises en jeu soient exactement celles intervenant dans les réalisations ℓ-adiques des motifs purs sur $\mathbb{Q}$ ayant *bonne réduction partout.*

Conclusion

Soient G réductif sur $\mathbb{Z}$ et r une représentation de $\widehat{G}$. Comme nous l'avons vu, la conjecture d'Arthur-Langlands prédit que pour tout π dans $\Pi_{\mathrm{disc}}(G)$ la collection de classes de conjugaison $r(\mathrm{c}(\pi))$ s'exprime en un sens précis en terme de *briques de bases* qui sont des éléments π_i de $\Pi_{\mathrm{cusp}}(\mathrm{GL}_{n_i})$, et des entiers d_i, vérifiant $\dim r = \sum_i n_i d_i$. Des questions qui se posent naturellement sont : supposons $\pi \in \Pi_{\mathrm{disc}}(G)$ donnée, par exemple telle que π_f intervienne concrètement dans un certain $\mathcal{A}_U(G)$, peut-on déterminer les π_i et les d_i associés ? est-il plus facile de déterminer ces derniers que π elle-même ?

Un premier obstacle qui se présente si l'on cherche à illustrer ces questions est de pouvoir disposer d'exemples de groupes G et de représentations unitaires irréductibles U de $G(\mathbb{R})$ pour lesquels on sache déterminer si $\mathcal{A}_U(G)$ est non nul, voire sa dimension. Lorsque U est dans la série discrète, c'est un problème accessible mais notoirement difficile : quand $G = \mathrm{Sp}_{2g}$ cela contient par exemple la question de déterminer la dimension des espaces de formes modulaires paraboliques de Siegel pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, un problème classique qui n'a été résolu que très récemment par Taïbi en genre $3 \leq g \leq 7$. Si U n'est pas dans la série discrète, il paraît sans espoir de d'obtenir une formule pour $\dim \mathcal{A}_U(G)$, comme le montre l'exemple $\mathrm{G} = \mathrm{PGL}_2$.

Le cas particulier $G(\mathbb{R})$ compact, auquel cas toutes ses représentations sont dans la série discrète, se distingue par le fait que la question de déterminer $\dim \mathcal{A}_U(G)$ est sensiblement plus élémentaire. Nous en étudierons de nombreux exemples avec $G = \mathrm{SO}_n$. Le cas $G = \mathrm{SO}_{24}$ est particulièrement intéressant de ce point de vue, car c'est l'un des groupes de plus grand rang pour lequel on sache déterminer $\dim \mathcal{A}_U(G)$ pour au moins *une* représentation U (et avec $\mathcal{A}_U(G) \neq 0$). En effet, on a $\dim \mathcal{A}_1(G) = |\widetilde{\mathrm{X}}_{24}|$ et ce cardinal vaut 25 car le réseau de Leech est le seul parmi les 24 réseaux de Niemeier qui n'admette pas d'isométrie indirecte. On ne peut que se poser la question suivante :

Question 0. Soient r la représentation standard de $\widehat{\mathrm{SO}_{24}}$ et π dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ avec $\pi_\infty = 1$; peut-on déterminer la collection des representations π_i et des entiers d_i qui correspond à π et r suivant la conjecture d'Arthur-Langlands ? [9]

9. Observons incidemment que les résultats d'Arthur ne s'appliquent pas directement ici car SO_n n'est pas (quasi-)déployé sur $\mathbb{Q}$. Nous vérifierons toutefois que la conjecture d'Arthur-Langlands est bien vérifiée lorsque π et r sont comme dans l'énoncé de la Question 0, en nous ramenant aux résultats d'Arthur pour Sp_{2g} par des arguments de séries thêta.

C'est la question à l'origine de ce travail. Les formules (4) et (2) montrent qu'une réponse positive à cette question donne des informations décisives sur le problème des p-voisins en dimension 24.

Avant d'en dire plus sur la question 0, ajoutons que les π_i qui y apparaissent ne sont pas quelconques, mais algébriques. En fait, plus généralement, si G est réductif sur $\mathbb{Z}$ et si π est dans $\Pi_{\mathrm{disc}}(G)$ avec π_∞ dans la série discrète, alors les valeurs propres de $\mathrm{c}_\infty(\pi)$ dans la représentation adjointe de $\mathrm{Lie}\,\widehat{G}$ sont dans $\mathbb{Z}$ (Harish-Chandra) ; il en résulte que si r est une représentation arbitraire de $\widehat{G}$, alors les représentations π_i associés à π et r par la conjecture d'Arthur-Langlands sont nécessairement algébriques. Ainsi, ces π ont des liens avec motifs et représentations galoisiennes, ce qui les rend d'autant plus intéressants. Ces liens sont profonds. Nous verrons notamment que la formule de multiplicité d'Arthur suggère que si π dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_{8k})$ est algébrique, isomorphe à sa *duale*, et si les valeurs propres de $\mathrm{c}(\pi_\infty)$ sont tous distinctes, alors il existe π' dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{8k})$ vérifiant $r(\mathrm{c}(\pi')) = \mathrm{c}(\pi)$. Ces relations inattendues entre représentations galoisiennes et réseaux unimodulaires pairs montre bien l'intérêt d'étudier les $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ pour l'arithméticien.

Revenons à la question 0. L'obstacle qui se présente immédiatement est que, du moins au moment où nous avions débuté ce travail, très peu de résultats étaient connus sur $\Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$ avec $n > 2$, et ce même si l'on se restreint aux représentations algébriques.[10] Par exemple, s'il existait une représentation π dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ vérifiant $\pi_\infty = 1$, telle que l'une des π_i associée soit dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_{n_i})$ avec n_i grand, alors il est très probable que nous ne pourrions jamais rien dire d'intéressant à son sujet, ainsi donc que sur le problème des p-voisins. Observons que l'on a toujours $n_i \leq 24$, mais aussi $\mathrm{w}(\pi_i) \leq 22$, par inspection de $\mathrm{c}_\infty(\pi)$.

Un de nos résultats principaux sera la démonstration d'une classification des représentations π dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$, avec $n \geq 1$ arbitraire, qui sont algébriques et de poids motivique $\mathrm{w}(\pi) \leq 22$. Nous verrons qu'il n'existe que 11 telles représentations, et qu'elles interviennent toutes (en tant que π_i) dans la réponse à la question 0. On a de plus $n \leq 4$ dans tous les cas, exactement quatre d'entre elles étant dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_4)$. Ces quatre représentations, qui *proviennent* de formes de Siegel de genre 2 à valeurs vectorielles, joueront un grand rôle dans ce mémoire.

L'énoncé de classification ci-dessus est de portée plus vaste : G étant arbi-

10. La situation a bien changée depuis grâce aux travaux [CR12] et [Tai14], qui bien que parus avant le présent travail ont en fait été entièrement motivés par ce dernier. Des questions importantes subsistent toutefois, par exemple on ne connaît pas le nombre des π dans $\Pi_{\mathrm{cusp}}(\mathrm{GL}_3)$ algébriques ayant une composante archimédienne π_∞ donnée.

traire, la conjecture d'Arthur-Langlands suggère que toute représentation π dans $\Pi_{\mathrm{disc}}(G)$ telle que π_∞ est dans la série discrète avec $\mathrm{c}_\infty(\pi)$ assez "petit" est *fabriquée* à partir des 11 représentations en question. Nous verrons par exemple comment utiliser cette approche pour déterminer la dimension de l'espace des formes modulaires paraboliques de Siegel pour $\mathrm{Sp}_{2g}(\mathbb{Z})$ de poids ≤ 12, en genre $g \geq 1$ quelconque.

Il paraît raisonnable de terminer ici cette préface, et de laisser au lecteur le plaisir de se plonger dans l'introduction proprement dite du mémoire.

Remerciements

Les auteurs tiennent à remercier le Centre de Mathématiques de l'École Polytechnique, dont les structures ont permis la collaboration improbable entre un arithméticien et un topologue amateurs de formes quadratiques. Ils remercient également chaleureusement Colette Moeglin, David Renard et Olivier Taïbi pour des discussions utiles à ce travail, ainsi que Richard Borcherds et Thomas Mégarbané pour leurs remarques. Enfin, les auteurs remercient respectivement Valeria et Martine pour leur soutien tout au long de ce projet qui a parfois paru sans fin.

Table des matières

I Introduction **1**

I.1 Réseaux unimodulaires pairs 1
I.2 Voisins à la Kneser 3
I.3 Séries thêta et formes modulaires de Siegel 6
I.4 Formes automorphes des groupes classiques 10
I.5 Représentations automorphes algébriques de petit poids . 14
I.6 Démonstration des théorèmes D et E 16
I.7 Quelques applications 17

II Algèbre bilinéaire et quadratique **20**

II.1 Généralités sur les formes bilinéaires et quadratiques . . . 20
II.2 Sur les b-modules et q-modules sur $\mathbb{Z}$ 30
II.3 Systèmes de racines et réseaux unimodulaires pairs 36

III Voisins à la Kneser **49**

III.1 Variations sur la notion de voisins à la Kneser 49
III.2 Sur les opérateurs de Hecke associés à la notion de voisinage 60
III.3 Exemples 62
III.4 Sur les d-voisinages entre un réseau de Niemeier avec racines et le réseau de Leech 67

IV Formes automorphes et opérateurs de Hecke **98**

IV.1 Réseaux et ensembles de classes des $\mathbb{Z}$-groupes 98
IV.2 Correspondances de Hecke 105
IV.3 Formes automorphes d'un $\mathbb{Z}$-groupe 117
IV.4 Formes automorphes pour O_n 122
IV.5 Formes modulaires de Siegel 128

V Séries thêta et réseaux unimodulaires pairs 135
V.1 Séries thêta de Siegel 135
V.2 Séries thêta de $E_8 \oplus E_8$ et E_{16} 137
V.3 Séries thêta des réseaux de Niemeier 140
V.4 Une construction alternative de $I_4(\Delta)$ par trialité 143
V.5 Appendice : un exemple simple de relation d'Eichler . . . 156

VI Paramétrisation de Langlands 159
VI.1 Rappels et notations sur les k-groupes réductifs 159
VI.2 Paramétrisation de Satake 166
VI.3 L'isomorphisme de Harish-Chandra 176
VI.4 La conjecture d'Arthur-Langlands 183

VII Quelques cas de la conjecture d'Arthur-Langlands 193
VII.1 Retour sur les relations d'Eichler 193
VII.2 $\Pi_{\mathrm{disc}}(O_8)$ et trialité 197
VII.3 Quelques conséquences des travaux d'Ikeda et Böcherer . 202
VII.4 Une table des premiers éléments de $\Pi_{\mathrm{disc}}(SO_8)$ 204
VII.5 $M_{\text{dét}}(O_{24})$ 206

VIII La classification d'Arthur pour les $\mathbb{Z}$-groupes classiques 208
VIII.1 Paramètres standards pour les groupes classiques 208
VIII.2 Représentations autoduales de PGL_n 210
VIII.3 La formule de multiplicité d'Arthur 222
VIII.4 Séries discrètes 229
VIII.5 Formules de multiplicité explicites : un formulaire 253
VIII.6 Compatibilité à la correspondance thêta 263
VIII.7 Compatibilité à la fonction L de Böcherer 266

IX Démonstration des théorèmes principaux 272
IX.1 Les formes modulaires de genre 2 de Tsushima 272
IX.2 $\Pi_{\mathrm{disc}}(SO_{24})$ et la conjecture de Nebe-Venkov 285
IX.3 Représentations algébriques de poids motivique ≤ 22 . . 294
IX.4 Démonstration du théorème E 326
IX.5 Formes de Siegel de poids ≤ 12 328

IX.6 Vers une nouvelle démonstration de l'égalité $|X_{24}| = 24$. 345
IX.7 Quelques éléments de $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ pour $n = 15, 17$ et 23 . . 346

X Applications 349
X.1 24 représentations galoisiennes ℓ-adiques 349
X.2 Retour sur les p-voisins des réseaux de Niemeier 353
X.3 Détermination des $\tau_{j,k}(q)$ pour de petites valeurs de q . . 359
X.4 Congruences à la Harder 375

A Le réseau de Barnes-Wall et les séries thêta de Siegel des réseaux unimodulaires pairs de dimension 16 **407**

B Formes quadratiques et voisins en dimension impaire 411

C Tables 437

D Bibliographie 444

I. Introduction

1. Réseaux unimodulaires pairs

Fixons un entier $n \geq 1$ et considérons l'espace euclidien $\mathbb{R}^n$ muni de son produit scalaire standard $(x_i) \cdot (y_i) = \sum_i x_i y_i$. Un réseau unimodulaire pair de rang n est un réseau $L \subset \mathbb{R}^n$ de covolume 1 tel que $x \cdot x$ est pair pour tout x dans L. L'ensemble $\mathcal{L}_n$ de ces réseaux est muni d'une action du groupe orthogonal euclidien $\mathrm{O}(\mathbb{R}^n)$, et nous notons

$$\mathrm{X}_n \ := \ \mathrm{O}(\mathbb{R}^n) \backslash \mathcal{L}_n$$

l'ensemble des classes d'isométrie de réseaux unimodulaires pairs de rang n. À chaque L dans $\mathcal{L}_n$, on peut associer une forme quadratique

$$\mathrm{q}_L : L \to \mathbb{Z}, \ \ x \mapsto \frac{x \cdot x}{2},$$

dont la forme bilinéaire sous-jacente $x \cdot y$ est de déterminant 1. L'application $L \mapsto \mathrm{q}_L$ induit alors une bijection entre X_n et l'ensemble des classes d'isomorphisme de formes quadratiques de rang n, définies positives, et de déterminant 1, sur l'anneau des entiers $\mathbb{Z}$.

Il est bien connu que l'ensemble X_n est fini, et qu'il est non vide si, et seulement si, on a $n \equiv 0 \bmod 8$. Un exemple standard d'élément de $\mathcal{L}_n$ est

$$\mathrm{E}_n \ := \ \mathrm{D}_n + \mathbb{Z}e$$

où $\mathrm{D}_n = \{(x_i) \in \mathbb{Z}^n, \sum_i x_i \equiv 0 \bmod 2\}$, $e = \frac{1}{2}(1, 1, \ldots, 1)$, et $n \equiv 0 \bmod 8$. Expliquons cette notation. À tout élément L de $\mathcal{L}_n$ est associé un système de racines (de type ADE)

$$\mathrm{R}(L) \ := \ \{x \in L, x \cdot x = 2\},$$

de rang $\leq n$. Le système de racines $\mathrm{R}(\mathrm{E}_8)$ est alors de type $\mathbf{E}_8$ et engendre $\mathbb{Z}$-linéairement E_8. Pour $n > 8$, $\mathrm{R}(\mathrm{E}_n)$ est de type $\mathbf{D}_n$ et engendre D_n.

L'ensemble X_n n'a été déterminé qu'en dimension $n \leq 24$. Mordell et Witt ont respectivement démontré

$$\mathrm{X}_8 = \{\mathrm{E}_8\} \text{ et } \mathrm{X}_{16} = \{\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8\}.$$

Les deux réseaux E_{16} et $\mathrm{E}_8 \oplus \mathrm{E}_8$ joueront un grand rôle dans ce mémoire. Ils sont à la fois faciles et difficiles à distinguer : leurs systèmes de racines sont différents, mais ils représentent chaque entier exactement le même nombre de fois. Cette dernière propriété, fameuse, conduit par exemple aux tores isospectraux de Milnor.

Les éléments de X_{24} ont été classifiés par Niemeier [Ni73], qui a notamment démontré $|\mathrm{X}_{24}| = 24$. Avant d'en dire plus sur ces derniers, mentionnons que pour $n \geq 32$ la formule de masse Minkowski-Siegel-Smith montre que la taille de X_n explose. Par exemple, on a $|\mathrm{X}_{32}| > 8 \cdot 10^6$ [Ser70] ; il y a même plus d'un milliard d'éléments dans X_{32} d'après King [Kin03].

Le plus fameux des réseaux de Niemeier (on appelle ainsi les éléments de $\mathcal{L}_{24}$) est le réseau de Leech. À isométrie près, c'est le seul élément L de $\mathcal{L}_{24}$ tel que $\mathrm{R}(L) = \emptyset$ (Conway). Un fait remarquable est que si L est un réseau de Niemeier non isomorphe au réseau de Leech, alors $\mathrm{R}(L)$ est de rang 24 et tous ses constituants irréductibles ont même nombre de Coxeter ; une démonstration simple en a été donnée par Venkov [Ven80]. Le miracle est alors que $L \mapsto \mathrm{R}(L)$ induit une bijection entre $\mathrm{X}_{24} - \{\text{Leech}\}$ et l'ensemble des classes d'isomorphisme de systèmes de racines R de rang 24 dont les constituants irréductibles sont de type ADE et tous de même nombre de Coxeter $\mathrm{h}(R)$. La démonstration est une vérification fastidieuse, au cas par cas.

R	$\mathbf{D}_{24}$	$\mathbf{D}_{16}\mathbf{E}_8$	$3\mathbf{E}_8$	$\mathbf{A}_{24}$	$2\mathbf{D}_{12}$	$\mathbf{A}_{17}\,\mathbf{E}_7$	$\mathbf{D}_{10}\,2\mathbf{E}_7$	$\mathbf{A}_{15}\,\mathbf{D}_9$
h(R)	46	30	30	25	22	18	18	16
R	$3\mathbf{D}_8$	$2\mathbf{A}_{12}$	$\mathbf{A}_{11}\,\mathbf{D}_7\,\mathbf{E}_6$	$4\mathbf{E}_6$	$2\mathbf{A}_9\mathbf{D}_6$	$4\mathbf{D}_6$	$3\mathbf{A}_8$	$2\mathbf{A}_7\,2\mathbf{D}_5$
h(R)	14	13	12	12	10	10	9	8
R	$4\mathbf{A}_6$	$4\mathbf{A}_5\,\mathbf{D}_4$	$6\mathbf{D}_4$	$6\mathbf{A}_4$	$8\mathbf{A}_3$	$12\mathbf{A}_2$	$24\mathbf{A}_1$	
h(R)	7	6	6	5	4	3	2	

Table I.1 – Les 23 systèmes de racines équi-Coxeter de type ADE et de rang 24

Les résultats mentionnés dans ce paragraphe sont exposés dans le chapitre II. Il s'agit pour l'essentiel d'un chapitre de rappels. Nous développons d'abord des prérequis d'algèbre bilinéaire et quadratique. Ils sont nécessaires à la compréhension des constructions de formes quadratiques auxquelles nous

avons fait allusion ci-dessus, et d'autres dont nous aurons besoin au cours du mémoire. En particulier, nous rappelons la théorie de Venkov et réexpliquons la construction de certains des réseaux de Niemeier. Nous en profitons également pour faire quelques rappels sur les (schémas en) groupes classiques sur $\mathbb{Z}$, qui seront utilisés dans la suite du mémoire. L'appendice B contient notamment une variante des résultats du chapitre II : nous y étudions les réseaux pairs de $\mathbb{R}^n$ de déterminant 2, et plus généralement la théorie des formes quadratiques sur $\mathbb{Z}$ (de dimension impaire) correspondante.

2. Voisins à la Kneser

Soit p un nombre premier. La notion de p-voisins a été introduite par M. Kneser, elle peut être vue comme un procédé de construction de réseaux à partir de réseaux connus. Dans le chapitre III, nous étudions plusieurs variations de cette notion et nous en donnons de nombreux exemples.

Suivant Kneser, deux réseaux L, M dans $\mathcal{L}_n$ sont dits *p-voisins* si $L \cap M$ est d'indice p dans L (et donc dans M). Il est aisé de fabriquer tous les p-voisins d'un réseau L appartenant à $\mathcal{L}_n$ donné. En effet, à chaque droite isotrope ℓ de $L \otimes \mathbb{F}_p$, disons engendrée par un élément x de L vérifiant $\mathrm{q}_L(x) \equiv 0 \bmod p^2$, on peut associer le réseau unimodulaire pair

$$\mathrm{vois}_p(L; \ell) := H + \mathbb{Z}\,\frac{x}{p},$$

avec $H = \{y \in L, x \cdot y \equiv 0 \bmod p\}$ (ce réseau ne dépend pas du choix de x). L'application $\ell \mapsto \mathrm{vois}_p(L; \ell)$ induit une bijection entre $\mathrm{C}_L(\mathbb{F}_p)$ et l'ensemble des p-voisins de L, où C_L désigne la quadrique projective (et lisse) sur $\mathbb{Z}$ définie par $\mathrm{q}_L = 0$. Cette quadrique étant hyperbolique sur $\mathbb{F}_p$ pour tout premier p, le nombre de p-voisins de L est exactement $|\mathrm{C}_L(\mathbb{F}_p)| = 1 + p + p^2 + \cdots + p^{n-2} + p^{\frac{n}{2}-1}$, une quantité que l'on note $\mathrm{c}_n(p)$.

Par exemple, considérons l'élément $\rho = (0, 1, 2, \ldots, 23)$ de E_{24}. Il engendre une droite isotrope dans $\mathrm{E}_{24} \otimes \mathbb{F}_{47}$ car $\sum_{i=1}^{23} i^2 \equiv 0 \bmod 47$. Il n'est pas très difficile de vérifier que $\mathrm{vois}_{47}(\mathrm{E}_{24}; \rho)$ ne possède pas de racine, d'où une isométrie

$$\mathrm{vois}_{47}(\mathrm{E}_{24}; \rho) \simeq \mathrm{Leech}.$$

Cette construction particulièrement simple du réseau de Leech est attribuée à Thompson dans [CS99], et nous y reviendrons plus loin. Elle illustre le slogan affirmant que de nombreuses constructions de réseaux sont des cas particuliers de constructions de voisins.

Revenant au cadre général, on dispose pour tout L dans $\mathcal{L}_n$ d'une partition de la quadrique $\mathrm{C}_L(\mathbb{F}_p)$ donnée par la classe d'isométrie du p-voisin

associé. Un des objets de ce mémoire est d'étudier cette partition en dimension $n \leq 24$. Par exemple, peut-on déterminer le nombre $\mathrm{N}_p(L, M)$ de p-voisins de L isométriques à un $M \in \mathcal{L}_n$ donné ? Le premier cas intéressant est bien entendu celui de la dimension $n = 16$. Il sera commode, pour formuler le résultat, d'introduire l'opérateur linéaire $\mathrm{T}_p : \mathbb{Z}[\mathrm{X}_n] \to \mathbb{Z}[\mathrm{X}_n]$ défini par $\mathrm{T}_p\,[L] = \sum [M]$, la somme portant sur les p-voisins M de L.

Théorème A. *Dans la base* $\mathrm{E}_8 \oplus \mathrm{E}_8,\ \mathrm{E}_{16}$ *la matrice de* T_p *est*

$$\mathrm{c}_{16}(p) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (1 + p + p^2 + p^3)\, \frac{1 + p^{11} - \tau(p)}{691} \begin{bmatrix} -405 & 286 \\ 405 & -286 \end{bmatrix},$$

où τ *est la fonction de Ramanujan, définie par* $q \prod_{m \geq 1} (1 - q^m)^{24} = \sum_{n \geq 1} \tau(n) q^n$.

Par exemple, on a la formule $\mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8,\ \mathrm{E}_{16}) = \frac{405}{691}(1 + p^{11} - \tau(p))\frac{p^4-1}{p-1}$. Ce théorème était sans doute connu des spécialistes, mais nous n'en avons pas trouvé de trace sous cette forme dans la littérature. Nous en donnerons plusieurs démonstrations, sur lesquelles nous reviendrons plus loin. D'après la théorie des formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$ et des séries thêta, la présence de $\tau(n)$ dans les questions de réseaux paraît de prime abord assez classique. Par exemple, si l'on pose $\mathrm{r}_L(n) = |\{x \in L, x \cdot x = 2n\}|$, on montre facilement $\mathrm{r}_{\mathrm{Leech}}(p) = \frac{65520}{691}(1 + p^{11} - \tau(p))$ pour tout premier p, une formule d'apparence similaire à celle du théorème. Néanmoins, l'apparition de $\tau(p)\frac{p^4-1}{p-1}$ dans le problème de comptage de p-voisins évoqué plus haut est sensiblement plus subtile ; elle s'avèrera équivalente à un cas non trivial de fonctorialité d'Arthur-Langlands. [1]

Notre théorème principal est un énoncé du même type que le théorème A mais concernant les réseaux de Niemeier. Il est possible d'en donner un énoncé dans le style du théorème précédent, qui est toutefois très indigeste. Chose remarquable, il fait intervenir les formes modulaires paraboliques pour $\mathrm{SL}_2(\mathbb{Z})$ de poids $k \leq 22$ ainsi que 4 formes modulaires de Siegel pour $\mathrm{Sp}_4(\mathbb{Z})$ à valeurs vectorielles. Les formules explicites contiennent de si gros coefficients rationnels qu'il est tout à fait étonnant à première vue que $\mathrm{N}_p(L, M)$ soit un nombre entier ! Nous énoncerons une version plus conceptuelle (et équivalente) de notre résultat au §I.4 (Théorème E). Expliquons en revanche dès à présent certaines conséquences concernant les réseaux de Niemeier d'une analyse de nos formules.

1. La comparaison du théorème A et de la formule pour $\mathrm{r}_{\mathrm{Leech}}(p)$ donnée ci-dessus conduit d'ailleurs à la relation "purement quadratique" suivante, que nous ne savons pas démontrer directement : $\mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16}) = \frac{9}{1456} \cdot \mathrm{r}_{\mathrm{Leech}}(p) \cdot \frac{p^4-1}{p-1}$.

Considérons le graphe $\mathrm{K}_n(p)$ d'ensemble de sommets X_n, où les classes de deux réseaux non isomorphes L et M sont reliées par une arête si, et seulement si, on a $\mathrm{N}_p(L, M) \neq 0$. Kneser a démontré que $\mathrm{K}_n(p)$ est connexe, quels que soient n et p, comme conséquence de son célèbre théorème d'approximation forte. Ce joli énoncé montre que l'on peut théoriquement reconstruire X_n à partir du réseau E_n et d'un nombre premier. Ce fut d'ailleurs utile à Niemeier pour comprendre X_{24} par 2-voisinages.

Le graphe $\mathrm{K}_{16}(p)$ est le graphe connexe à deux sommets, d'après Kneser. C'est bien sûr compatible avec l'estimation $|\tau(p)| < 2p^{\frac{11}{2}}$ (Deligne-Ramanujan) et la formule pour $\mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16})$ donnée par le théorème A. Par contre, le graphe $\mathrm{K}_{24}(2)$, déterminé par Borcherds [CS99], n'est pas du tout trivial. Il est de diamètre 5 et cette page Wikipedia http://en.wikipedia.org/wiki/Niemeier_lattice en donne une jolie représentation, aussi due à Borcherds. Nos résultats permettent par exemple de déterminer $\mathrm{K}_{24}(p)$ pour tout nombre premier p (§X.2). [2]

Théorème B. *(i) Soit L un réseau de Niemeier avec racines. Alors L est un p-voisin du réseau de Leech si, et seulement si, $p \geq \mathrm{h}(\mathrm{R}(L))$.*

(ii) Le graphe $\mathrm{K}_{24}(p)$ est complet si, et seulement si, $p \geq 47$.

Faisons quelques remarques sur cet énoncé. Le point (i) concerne les constructions du réseau de Leech comme p-voisin d'un réseau de Niemeier avec racines. Par exemple, on observe sur le graphe de Borcherds $\mathrm{K}_{24}(2)$ que Leech est à distance 5 de E_{24} et qu'il n'est relié qu'au réseau de système de racines $24\mathbf{A}_1$, le réseau de Niemeier avec racines le plus délicat à construire (il nécessite le code de Golay, §II.3). Cette dernière propriété est en fait assez simple à comprendre : si le réseau de Leech est un 2-voisin du réseau de Niemeier L (avec racines), alors il existe un sous-groupe d'indice 2 de L qui ne contient pas de racine. En particulier, $\mathrm{R}(L)$ a la propriété que la somme de deux racines n'est jamais une racine, de sorte que ses constituants irréductibles sont de rang 1, *i.e.* $\mathrm{R}(L) = 24\mathbf{A}_1$. Parmi ceux de la table I.1, ce système de racines est aussi le seul dont le nombre de Coxeter est 2, en accord avec le (i).

La partie la plus élémentaire du théorème B, démontrée au §III.4 et généralisant l'observation ci-dessus, consiste à vérifier que l'on a $p \geq \mathrm{h}(\mathrm{R}(L))$ si Leech est p-voisin de L. C'est un analogue formel d'un résultat de Kostant [Kos59] affirmant que l'ordre minimal d'un élément régulier d'ordre fini dans un groupe de Lie compact connexe adjoint coïncide avec le nombre de

2. Une liste de ces graphes est disponible à l'adresse http://gaetan.chenevier.perso.math.cnrs.fr/niemeier/niemeier.html.

Coxeter de son système de racines. En revanche, la démonstration des autres assertions nécessite l'utilisation du théorème E ainsi qu'un ensemble d'inégalités de type Ramanujan, elle ne sera complétée qu'au chapitre X (§X.2 et §X.3).

Dans le chapitre III, nous étudions également les cas limites de l'assertion (i) du théorème ci-dessus (de manière directe, *i.e.* sans faire usage du théorème E). Nous procédons pour cela à une analyse détaillée des éléments c de $\mathrm{C_L}(\mathbb{F}_p)$ vérifiant $\mathrm{vois}_p(L;c) \simeq$ Leech, L étant un réseau de Niemeier de système de racines $R = \mathrm{R}(L)$ non vide. Il est nécessaire à la pertinence des énoncés d'étudier plus généralement les d-voisins de L, où $d \geq 1$ est un entier non nécessairement premier (§III.1). Nous démontrons que si ρ est un vecteur de Weyl de R, et si $h = \mathrm{h}(R)$, on a des isométries (Théorème III.4.2.10)

$$\mathrm{vois}_h(L;\rho) \simeq \mathrm{vois}_{h+1}(L;\rho) \simeq \text{Leech}. \tag{2.1}$$

Cela a un sens car on a $\rho \in L$ (Borcherds) et $\mathrm{q}_L(\rho) = h(h+1)$ (Venkov). Cet énoncé contient par exemple l'observation de Thompson susmentionnée. En fait, ces 23 (ou 46) constructions du réseau de Leech ne sont autres que les fameuses *holy constructions* de Conway et Sloane [CS82]. Nous donnons cependant une nouvelle démonstration des isométries (2.1) par des méthodes de voisins, et montrons les identités

$$\mathrm{N}_h(L, \text{Leech}) = \frac{|W|}{\varphi(h)g} \quad \text{et} \quad \mathrm{N}_{h+1}(L, \text{Leech}) = \frac{|W|}{h+1}, \tag{2.2}$$

où W désigne le groupe de Weyl de R, et g^2 son indice de connexion au sens de Bourbaki. Nous terminons par une étude de $\mathrm{vois}_2(L;\rho)$ inspirée de résultats de Borcherds (Figure III.1).

3. Séries thêta et formes modulaires de Siegel

Revenons à la question de déterminer l'opérateur T_p sur $\mathbb{Z}[\mathrm{X}_n]$. Quelques observations simples s'imposent : les T_p commutent et sont auto-adjoints sur $\mathbb{R}[\mathrm{X}_n]$ pour un produit scalaire adéquat [NV01] (§III.2). Il s'agit donc d'en déterminer une base de vecteurs propres communs ainsi que les collections de valeurs propres des T_p associées. La seule droite propre évidente, engendrée par $\sum_{L \in \mathrm{X}_n} \frac{[L]}{|\mathrm{O}(L)|}$, est de valeur propre $\mathrm{c}_n(p)$ sous T_p.

Ainsi que nous l'avons entrevu dans la préface, nous sommes en fait en présence d'un problème déguisé de théorie spectrale des formes automorphes. En effet, si $G = \mathrm{O}_n$ désigne le (schéma en) groupe orthogonal sur $\mathbb{Z}$ défini

par la forme quadratique $\mathrm{q}_{\mathrm{E}_n}$, et $\mathbb{A}$ l'anneau des adèles de $\mathbb{Q}$, des arguments de théorie du genre conduisent à un isomorphisme de $G(\mathbb{R})$-ensembles $\mathcal{L}_n \simeq G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$ (§II.2, §IV.1). Il s'ensuit que le dual de $\mathbb{R}[\mathrm{X}_n]$ s'identifie à l'espace des fonctions à valeurs réelles sur $G(\mathbb{Q})\backslash G(\mathbb{A})$ qui sont invariantes à droite par $G(\mathbb{R}) \times G(\widehat{\mathbb{Z}})$. Dans cette description, l'opérateur T_p est induit par un élément particulier de l'anneau $\mathrm{H}(G)$ des opérateurs de Hecke de G.

Ces observations tout à fait classiques sont rappelées dans le chapitre IV du mémoire. Bien que nous nous intéressons principalement aux formes automorphes du $\mathbb{Z}$-groupe O_n, nos énoncés et démonstrations en feront intervenir diverses déclinaisons (formes automorphes pour SO_n, PGO_n et PGSO_n), ainsi que des formes modulaires pour $\mathrm{SL}_2(\mathbb{Z})$, des formes modulaires de Siegel à valeurs vectorielles pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, et même, par le biais des résultats d'Arthur, des formes automorphes pour PGL_n. Il sera donc nécessaire d'adopter dès le départ un point de vue suffisamment général englobant tous ces objets (§IV.3). Le lecteur trouvera aux §IV.1 et §IV.2 un exposé élémentaire sur les opérateurs de Hecke. L'accent est mis sur les exemples fournis par les groupes classiques et leurs variantes (Hecke, Satake, Shimura), ils donnent plus de largeur de vue sur les p-voisins et leurs généralisations. Les §IV.4 et §IV.5 sont consacrés à des rappels sur les formes automorphes pour O_n et les formes modulaires de Siegel. Soulignons que la rédaction de ce chapitre s'adresse au non-spécialiste, et prétend à peu d'originalité.

Une approche pour étudier le $\mathrm{H}(\mathrm{O}_n)$-module $\mathbb{Z}[\mathrm{X}_n]$ consiste à examiner les séries thêta de Siegel de tout genre $g \geq 1$ des éléments de $\mathcal{L}_n$. Pour tout $n \equiv 0 \bmod 8$ et $g \geq 1$, elles fournissent une application linéaire

$$\vartheta_g : \mathbb{C}[\mathrm{X}_n] \to \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z})),\ [L] \mapsto \vartheta_g(L),$$

où $\mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ désigne l'espace des formes modulaires de Siegel de poids $k \in \mathbb{Z}$ pour le groupe $\mathrm{Sp}_{2g}(\mathbb{Z})$ (§V.1). La pertinence de cette application pour notre problème vient des relations de commutation d'Eichler généralisées ; elles montrent que ϑ_g entrelace chaque élément de $\mathrm{H}(\mathrm{O}_n)$ avec un certain élément "explicite" de $\mathrm{H}(\mathrm{Sp}_{2g})$ (Eichler, Freitag, Yoshida, Andrianov, §V.1). L'application ϑ_g est trivialement injective pour $g \geq n$. La question de déterminer la structure du $\mathrm{H}(\mathrm{Sp}_{2g})$-module $\mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est en revanche notoirement difficile, et ce d'autant plus que g est grand. Néanmoins, nous développerons au chapitre IX une stratégie permettant de résoudre des nouveaux cas de cette question, qui repose entre autres sur les résultats récents d'Arthur [Art13].

L'application ϑ_g a fait l'objet de nombreux travaux. Son noyau, qui décroît quand g grandit, décrit les relations linéaires entre les séries thêta de genre

g des éléments de $\mathcal{L}_n$, et la détermination de son image est un exemple du célèbre *problème de la base* d'Eichler. Précisément, ϑ_g induit une application injective

$$\operatorname{Ker}\vartheta_{g-1}/\operatorname{Ker}\vartheta_g \longrightarrow \mathrm{S}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z})) \tag{3.1}$$

où $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) \subset \mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ désigne le sous-espace des formes paraboliques (voir le §V.1 ou la note de bas de page ci-dessous pour la convention sur ϑ_0), et il s'agit de savoir si elle est surjective. Un résultat important de Böcherer [Boc89] donne une condition nécessaire et suffisante pour qu'une forme propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$ soit dans son image en termes de l'annulation en un certain entier d'une fonction L associée (§VII.2).

Cas de la dimension $n = 16$.

Le cas de la dimension 16 est l'objet d'une histoire fameuse, rappelée au §V.2. En effet, un résultat classique de Witt et Igusa assure que l'on a

$$\vartheta_g(\mathrm{E}_8 \oplus \mathrm{E}_8) = \vartheta_g(\mathrm{E}_{16}) \ \text{ si } \ g \leq 3. \tag{3.2}$$

Ces identités remarquables affirment que $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16} représentent toutes les formes quadratiques entières positives de rang ≤ 3 exactement le même nombre de fois. L'annulation bien connue $\mathrm{S}_8(\mathrm{SL}_2(\mathbb{Z})) = 0$ traite le cas $g = 1$ (et conduit aux tores isospectraux de Milnor déjà mentionnés). En particulier [3], "le" vecteur propre non trivial de $\mathbb{Z}[\mathrm{X}_{16}]$ est $[\mathrm{E}_{16}]-[\mathrm{E}_8\oplus\mathrm{E}_8]$. La difficulté en genres 2 et 3 est que l'annulation de $\mathrm{S}_8(\mathrm{Sp}_{2g}(\mathbb{Z}))$, bien que toujours vraie, est plus délicate à démontrer. Dans l'appendice A, nous exposons une autre démonstration ingénieuse des identités (3.2) due à Kneser, qui ne repose pas sur de telles annulations.

La forme $J = \vartheta_4(\mathrm{E}_8 \oplus \mathrm{E}_8) - \vartheta_4(\mathrm{E}_{16})$, qui n'est autre que la fameuse *forme de Schottky*, est en revanche non nulle. D'après Poor et Yuen [PY96], on sait même qu'elle engendre $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. Le théorème A résulte alors de la résolution par Ikeda [Ike01] de la conjecture de Duke-Imamoğlu [BK00]. En effet, appliquée à la forme modulaire Δ dans $\mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, cette dernière assure l'existence d'une forme modulaire de Siegel non nulle dans $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ qui est propre pour les opérateurs de Hecke dans $\mathrm{H}(\mathrm{Sp}_8)$, de valeurs propres explicitement déterminées par les $\tau(p)$. La démonstration d'Ikeda est difficile ; une des contributions de ce mémoire est d'avoir donné une autre démonstration de son théorème, très différente, dans le cas particulier ci-dessus.

3. Cette assertion peut se démontrer de manière beaucoup plus directe. En effet, si ϑ_0 désigne l'application linéaire $\mathbb{C}[\mathrm{X}_n] \to \mathbb{C}$ envoyant sur 1 la classe de tout élément de $\mathcal{L}_n$, on constate que l'on a $\vartheta_0 \circ \mathrm{T}_p = \mathrm{c}_n(p)\,\vartheta_0$, de sorte que $\operatorname{Ker}\vartheta_0$ est stable par T_p.

Le résultat important est le suivant. Pour toute fonction $f : \mathcal{L}_n \to \mathbb{C}$, on définit $\mathrm{T}_p(f) : \mathcal{L}_n \to \mathbb{C}$ en posant pour tout $L \in \mathcal{L}_n$, $\mathrm{T}_p(f)(L) = \sum_M f(M)$, la somme portant sur les p-voisins de L. Si $1 \leq g \leq n/2$, on note $\mathrm{H}_{d,g}(\mathbb{R}^n)$ l'espace des polynômes $(\mathbb{R}^n)^g \to \mathbb{C}$ qui sont harmoniques pour le laplacien euclidien de $(\mathbb{R}^n)^g$, et qui satisfont $P \circ \gamma = (\text{dét}\gamma)^d\, P$ pour tout $\gamma \in \mathrm{GL}_g(\mathbb{C})$ (§V.4). C'est une représentation linéaire de $\mathrm{O}(\mathbb{R}^n)$ de manière naturelle.

Théorème C. *Soient $q + \sum_{n\geq 2} a_n q^n$ une forme modulaire de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ propre pour les opérateurs de Hecke, et $d = \frac{k}{2} - 2$. Il existe une fonction $f : \mathcal{L}_8 \to \mathbb{C}$ telle que :*

(i) pour tout nombre premier p, on a $\mathrm{T}_p(f) = p^{-d}\, \frac{p^4-1}{p-1}\, a_p\, f$,

(ii) f engendre sous $\mathrm{O}(\mathbb{R}^8)$ une représentation isomorphe à $\mathrm{H}_{d,4}(\mathbb{R}^8)$.

Le §V.4 est principalement consacré à la démonstration d'un cas particulier de ce théorème dans le cas $k = 12$, qui conduit à une démonstration complète et relativement élémentaire du théorème A. Le cas général ci-dessus sera démontré et précisé au §VII.2.

Donnons une idée de la démonstration. Nous commençons par réaliser la forme modulaire de départ comme série thêta $\sum_{x\in \mathrm{E}_8} P(x)\, q^{\frac{x\cdot x}{2}}$ où $P : \mathbb{R}^8 \to \mathbb{C}$ est un polynôme harmonique bien choisi. Dans le cas de Δ, "l'invariant" harmonique de degré 8 de $\mathrm{W}(\mathbf{E}_8)$ convient, et en général on invoque un résultat de Waldspurger [Wal79]. Cette construction définit un sous-espace des fonctions $\mathcal{L}_8 \to \mathbb{C}$ qui sont propres pour les opérateurs de Hecke dans $\mathrm{H}(\mathrm{O}_8)$, de valeurs propres reliées aux a_p par les relations d'Eichler, et qui engendrent une représentation isomorphe à $\mathrm{H}_{8,1}(\mathbb{R}^8)$ sous l'action de $\mathrm{O}(\mathbb{R}^8)$. L'idée principale consiste à leur appliquer à la source un automorphisme d'ordre 3 de $\mathcal{L}_8$ issu de la trialité. Cet automorphisme est construit à partir d'une structure d'octonions de Coxeter sur E_8 et de l'identité $\mathcal{L}_8 \simeq G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$ avec $G = \mathrm{PGSO}_8$. Les fonctions obtenues conviennent : nous renvoyons au §V.4 pour les démonstrations.

La condition (ii) de l'énoncé assure que la fonction f donne naissance à une série thêta de Siegel de genre 4 (à coefficients "pluriharmoniques"). Quand elle est non nulle, cette série thêta est un substitut du relèvement d'Ikeda de genre 4 de la forme modulaire de départ. On vérifie cette non-annulation quand $k = 12$; on déduit aisément le théorème A.

Mentionnons enfin que nous démontrerons plus tard (Théorème IX.5.10) l'annulation $\mathrm{S}_8(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ pour tout $g \neq 4$. Quand $g = 5, 6$ elle avait déjà été obtenue par Poor et Yuen [PY07]. Par conséquent, l'application $\vartheta_g : \mathbb{C}[\mathrm{X}_{16}] \to \mathrm{M}_8(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est surjective pour tout genre $g \geq 1$.

Cas de la dimension 24

Ce cas a fait l'objet de travaux remarquables d'Erokhin [Ero79], Borcherds-Freitag-Weissauer [BFW98] et Nebe-Venkov [NV01] (§V.3). Erokhin a montré $\operatorname{Ker}\vartheta_{12} = 0$, et les trois auteurs de [BFW98] ont prouvé que $\operatorname{Ker}\vartheta_{11}$ est de dimension 1. Une étude fine de toute la filtration de $\mathbb{Z}[\mathrm{X}_{24}]$ par les $\operatorname{Ker}\vartheta_g$ a été entreprise par Nebe et Venkov *loc. cit.* Leur point de départ est une explicitation de l'opérateur T_2 sur $\mathbb{Z}[\mathrm{X}_{24}]$ qu'ils déduisent de résultats de Borcherds (§III.3.3) ; cet opérateur étant à valeurs propres distinctes et entières, ils obtiennent une base de $\mathbb{Q}[\mathrm{X}_{24}]$ constituée de vecteurs propres des T_p dans $\mathbb{Q}[\mathrm{X}_{24}]$. Ils proposent également une conjecture pour la dimension de l'image de l'application (3.1) pour tout entier $1 \leq g \leq 12$, dont ils démontrent des cas particuliers. Nous établissons leur conjecture et montrons que le problème de la base d'Eichler admet une réponse positive en dimension $n = 24$, pour tout genre $1 \leq g \leq 23$ (Théorème IX.5.2 et Corollaire IX.5.7) :

Théorème D. *L'application* $\vartheta_g : \mathbb{C}[\mathrm{X}_{24}] \to \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *est surjective, et induit un isomorphisme* $\operatorname{Ker}\vartheta_{g-1}/\operatorname{Ker}\vartheta_g \xrightarrow{\sim} \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$*, pour tout entier* $g \leq 23$*. La dimension de* $\mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *pour* $g \neq 24$ *est donnée par la table :*

g	1	2	3	4	5	6	7	8	9	10	11	12	> 12
$\dim \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$	1	1	1	2	2	3	3	4	2	2	1	1	0

Nous donnerons une idée de la démonstration au §6, le point le plus délicat étant la première assertion. Il résulte du théorème une description complète de la filtration des $\operatorname{Ker}\vartheta_g$ sur $\mathbb{Z}[\mathrm{X}_{24}]$. Mentionnons que le problème de la base d'Eichler admet une réponse négative en dimension $n = 32$ et genre $g = 14$, comme nous l'observons au corollaire VII.3.5.

4. Formes automorphes des groupes classiques

Les formes modulaires de Siegel, ainsi que les espaces de formes automorphes pour O_n, peuvent être étudiés à l'aide des travaux récents d'Arthur [Art13]. La formulation même des énoncés nécessite cependant des rappels préliminaires sur le point de vue de Langlands sur la théorie des formes automorphes [Lan70] [Bor77] que nous avons regroupés dans le chapitre VI. Les grandes lignes de ce point de vue ont déjà été dégagées dans la préface. Nous en reprenons ici brièvement quelques aspects.

Soit G un schéma en groupes semi-simple [4] sur $\mathbb{Z}$. On note $\Pi_{\mathrm{disc}}(G)$ l'ensemble des sous-représentations topologiquement irréductibles de l'espace des fonctions de carré intégrable sur $G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$ pour les actions naturelles de $G(\mathbb{R})$ et de l'anneau $\mathrm{H}(G)$ des opérateurs de Hecke de G (§IV.3). L'isomorphisme de Satake associe à tout $\pi \in \Pi_{\mathrm{disc}}(G)$ et tout premier p une classe de conjugaison semi-simple $\mathrm{c}_p(\pi)$ dans $\widehat{G}(\mathbb{C})$, où $\widehat{G}$ désigne le groupe semi-simple complexe dual de Langlands de $G_{\mathbb{C}}$ (§VI.1, §VI.2). Ce point de vue éclairant sur les valeurs propres des opérateurs de Hecke, dû à Langlands, est explicité au §VI.2.8 dans le cas des groupes classiques et des opérateurs d'intêret pour ce mémoire, en suivant l'exposé de Gross [Gro98]. De même, nous rappelons comment l'isomorphisme d'Harish-Chandra associe au caractère infinitésimal de la composante archimédienne π_∞ de π une classe de conjugaison semi-simple $\mathrm{c}_\infty(\pi)$ dans l'algèbre de Lie de $\widehat{G}$ (§VI.3).

Comme nous l'avons déjà expliqué dans la préface, une conjecture centrale et structurante, initialement due à Langlands et précisée par Arthur [Art89], est que ces collections de classes de conjugaison s'expriment toutes en terme des données similaires relatives aux $\Pi_{\mathrm{disc}}(\mathrm{PGL}_m)$ pour $m \geq 1$. Cette conjecture est discutée au §VI.4.4. Donnons ici une seconde manière de l'énoncer, à l'aide de fonctions L, qui est particulièrement directe. Fixons $\pi \in \Pi_{\mathrm{disc}}(G)$ et $r : \widehat{G}(\mathbb{C}) \to \mathrm{SL}_n(\mathbb{C})$ une représentation algébrique. On dispose alors suivant Langlands d'un produit eulérien

$$\mathrm{L}(s, \pi, r) = \prod_p \mathrm{dét}(1 - p^{-s}\, r(\mathrm{c}_p(\pi)))^{-1},$$

qui est absolument convergent pour tout nombre complexe s de partie réelle assez grande. Quand G est le $\mathbb{Z}$-groupe PGL_m, et que r est la représentation tautologique de $\widehat{G} = \mathrm{SL}_m$, on pose simplement $\mathrm{L}(s, \pi) = \mathrm{L}(s, \pi, r)$. La conjecture d'Arthur-Langlands pour le couple (π, r) prédit l'existence d'un entier $k \geq 1$, et pour $i = 1, \ldots, k$ d'une représentation[5] $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ et d'un entier $d_i \geq 1$, tels que l'on ait l'égalité

$$\mathrm{L}(s, \pi, r) = \prod_{i=1}^{k} \prod_{j=0}^{d_i - 1} \mathrm{L}(s + j - \frac{d_i - 1}{2}, \pi_i). \tag{4.1}$$

4. La discussion qui suit ne s'y applique pas verbatim à certains $\mathbb{Z}$-groupes naturels ici, comme O_n ou PGO_n, qui sont non connexes. Nous précisons dans le texte les modifications à apporter afin de les englober, mais nous ignorerons ce détail dans cette introduction.

5. On note traditionnellement $\Pi_{\mathrm{cusp}}(G) \subset \Pi_{\mathrm{disc}}(G)$ le sous-ensemble des représentations intervenant dans le sous-espace des formes automorphes paraboliques [GGPS66] (§IV.3).

De manière légèrement abusive, la collection des classes de conjugaison $r(\mathrm{c}_v(\pi))$ sera appelée *paramètre de Langlands* du couple (π, r) ; elle sera notée $\psi(\pi, r)$. Lorsque l'égalité (4.1) est vérifiée, elle sera notée symboliquement [6]

$$\psi(\pi, r) = \oplus_{i=1}^{k} \pi_i[d_i].$$

Si G est un $\mathbb{Z}$-*groupe classique* (§VI.4.7, §VIII.1), alors $\widehat{G}$ est un groupe classique complexe et vient avec une représentation tautologique appelée *représentation standard*, notée St. Un résultat important démontré par Arthur [Art13] est que la conjecture ci-dessus est vraie si l'on suppose que G est soit Sp_{2g}, soit un $\mathbb{Z}$-groupe spécial orthogonal déployé, et si $r = \mathrm{St}$.

Au chapitre VII, nous illustrons ces théories en donnant de nombreux exemples de cas particuliers de la conjecture d'Arthur-Langlands, concernant les formes automorphes pour SO_n ou les formes de Siegel pour $\mathrm{Sp}_{2g}(\mathbb{Z})$. Ils ne reposent pas sur les travaux d'Arthur, mais sur des constructions plus classiques de séries thêta. Nous rappelons le point de vue de Rallis sur les relations d'Eichler (§VII.1) ainsi que des résultats importants de Böcherer et d'Ikeda. Nous démontrons le théorème C et donnons d'autres applications de la trialité à la construction de certains éléments de $\Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ (§VII.2). Un ingrédient des démonstrations est un léger raffinement de l'identité de Rallis à la paire $(\mathrm{PGO}_n, \mathrm{PGSp}_{2g})$ (§VII.1.4). Au final, notre analyse recouvre suffisamment de constructions pour permettre par exemple de déterminer $\psi(\pi, \mathrm{St})$ pour 13 des 16 "premières" représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ (§VII.4).

Nous pouvons maintenant énoncer l'analogue pour X_{24} du théorème A ; nous renvoyons au §X.1 pour une formulation de ce théorème en terme de représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dans l'esprit de l'annonce [CL11]. Nous devons au préalable introduire quelques notations supplémentaires :

– La représentation Δ_w, pour $w \in \{11, 15, 17, 19, 21\}$, désignera l'élément de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ engendré par la droite $\mathrm{S}_{w+1}(\mathrm{SL}_2(\mathbb{Z}))$ des formes modulaires paraboliques de poids $w+1$ pour $\mathrm{SL}_2(\mathbb{Z})$.

– La représentation $\mathrm{Sym}^2\Delta_w$ est le carré symétrique de Gelbart-Jacquet de Δ_w [GJ78]. C'est l'unique élément de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_3)$ vérifiant l'identité $\mathrm{c}_v(\mathrm{Sym}^2\Delta_w) = \mathrm{Sym}^2\,\mathrm{c}_v(\Delta_w)$ pour toute place v de $\mathbb{Q}$.

– Si (w, v) est l'un des 4 couples $(19, 7)$, $(21, 5)$, $(21, 9)$ ou $(21, 13)$, la représentation $\Delta_{w,v}$ est un certain élément de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_4)$ défini et étudié au §IX.1. Son caractère infinitésimal $\mathrm{c}_\infty(\Delta_{w,v})$, qui est par définition la classe

6. Au sens strict, notre notation inclus l'identité naturelle correspondante sur les caractères infinitésimaux (§VI.4.4). De plus, le facteur $\pi_i[d_i]$ sera simplement noté $[d_i]$ (resp. π_i) lorsque $n_i = 1$ (resp. $d_i = 1$). Ces conventions sont utilisées dans la table I.2.

de conjugaison d'un élément semi-simple dans $\mathrm{M}_4(\mathbb{C})$, a pour valeurs propres [7] $\pm\frac{w}{2}$ et $\pm\frac{v}{2}$; nous verrons même plus loin que cette propriété caractérise $\Delta_{w,v}$ uniquement.

Théorème E. *Les paramètres $\psi(\pi, \mathrm{St})$ des 24 représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ engendrées par les fonctions $\mathrm{X}_{24} \to \mathbb{C}$ propres pour $\mathrm{H}(\mathrm{O}_{24})$ sont :*

$[23] \oplus [1]$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4] \oplus \Delta_{11}[2] \oplus [9]$
$\mathrm{Sym}^2\Delta_{11} \oplus [21]$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{15}[6] \oplus [9]$
$\Delta_{21}[2] \oplus [1] \oplus [19]$	$\Delta_{15}[8] \oplus [1] \oplus [7]$
$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus [17]$	$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [7]$
$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus [1] \oplus [15]$	$\Delta_{19}[4] \oplus \Delta_{11}[4] \oplus [1] \oplus [7]$
$\Delta_{19}[4] \oplus [1] \oplus [15]$	$\Delta_{21,9}[2] \oplus \Delta_{15}[4] \oplus [1] \oplus [7]$
$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus [13]$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{11}[6] \oplus [5]$
$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4] \oplus [13]$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [5]$
$\Delta_{17}[6] \oplus [1] \oplus [11]$	$\Delta_{21}[2] \oplus \Delta_{11}[8] \oplus [1] \oplus [3]$
$\Delta_{21}[2] \oplus \Delta_{15}[4] \oplus [1] \oplus [11]$	$\Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [3]$
$\Delta_{21,13}[2] \oplus \Delta_{17}[2] \oplus [1] \oplus [11]$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10] \oplus [1]$
$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [9]$	$\Delta_{11}[12]$

TABLE I.2 – Les paramètres standards des $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telles que $\pi_\infty = 1$.

Soulignons que dans un travail remarquable [IKE06], Ikeda était parvenu à déterminer 20 des 24 paramètres ci-dessus, à savoir ceux ne contenant pas les représentations $\Delta_{w,v}$.

Étant donné l'importance du rôle joué par les $\Delta_{w,v}$ dans ce mémoire, il s'impose d'indiquer brièvement leur origine. Soit (j, k) l'un des 4 couples $(6, 8), (4, 10), (8, 8)$ ou $(12, 6)$. Une formule de dimension due à R. Tsushima [TSU83] montre que l'espace des formes modulaires de Siegel pour $\mathrm{Sp}_4(\mathbb{Z})$ qui sont paraboliques et à coefficients dans $\mathrm{Sym}^j \otimes \text{dét}^k$ est de dimension 1. Nous en donnons un générateur concret par une construction de série thêta à coefficients "pluriharmoniques" basée sur le réseau E_8. Si $\pi_{j,k}$ désigne l'élément de $\Pi_{\mathrm{cusp}}(\mathrm{PGSp}_4)$ engendré par cette forme propre, on a alors la relation $\psi(\pi_{j,k}, \mathrm{St}) = \Delta_{w,v}$ avec $(w, v) = (2j + k - 3, j + 1)$. Remarquons que

7. De même, $\mathrm{c}_\infty(\Delta_w)$ a pour valeurs propres $\pm\frac{w}{2}$.

PGSp_4 est isomorphe au $\mathbb{Z}$-groupe classique déployé $\mathrm{SO}_{3,2}$, de groupe dual le groupe complexe Sp_4, de sorte que la théorie d'Arthur s'applique à $(\pi_{j,k}, \mathrm{St})$.

Le théorème E sera démontré au §X.4.3, par une méthode que nous décrirons au §I.6. Néanmoins, nous en donnerons d'abord deux autres démonstrations *conditionnelles* aux §X.2.10 et §X.2.11. Ces démonstrations, obtenues en appliquant la *formule de multiplicité* d'Arthur [Art13], seront à terme les plus naturelles, mais elles dépendent actuellement de certains énoncés précisant ceux d'Arthur, qui bien qu'attendus ne sont pas encore disponibles.

Au chapitre VIII, nous revenons donc sur les résultats généraux d'Arthur [Art13], que nous spécifions au cas des groupes classiques G sur $\mathbb{Z}$ et de leurs formes automorphes "non ramifiées partout" ; une telle analyse a déjà été menée à bien dans [CR12, §3], que nous reprenons et complétons. L'essentiel du chapitre est consacré à l'explicitation de la fameuse formule de multiplicité sus-mentionnée. Il s'agit d'une condition nécessaire et suffisante pour qu'une collection donnée de (π_i, d_i) "provienne" d'un $\pi \in \Pi_{\mathrm{disc}}(G)$, au sens où $\psi(\pi, \mathrm{St}) = \oplus_{i=1}^{k} \pi_i[d_i]$, tout en ayant une composante π_∞ prescrite (§VIII.3). Nous nous limitons au cas où π_∞ est une série discrète de $G(\mathbb{R})$ et expliquons de manière concrète la paramétrisation de ces dernières par Shelstad (§VIII.4). C'est cette paramétrisation qui intervient dans la formule d'Arthur. La version de cette formule que nous donnons n'est à présent démontrée que si G est déployé sur $\mathbb{Z}$ et si tous les entiers d_i sont égaux à 1. Nous la discutons cependant en général, en précisant les conjectures desquelles divers cas particuliers dépendent (§VIII.4.21), car elle éclaire grandement les constructions particulières étudiées tout au long de ce mémoire. Dans le cas $G = \mathrm{SO}_n$ ou des formes de Siegel pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, des formulaires concrets sont dégagés au §VIII.5. Nous vérifions par exemple qu'ils sont compatibles aux résultats du chapitre VII et aux résultats de Böcherer sur l'image de l'application (3.1) (§VIII.6). Comme promis, nous montrons enfin au §IX.2 que ces formules conduisent à une démonstration conditionnelle simple, bien qu'assez miraculeuse, du théorème E.

5. Représentations automorphes algébriques de petit poids

Soit $m \geq 1$ un entier. Nous disons qu'une représentation $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$ est *algébrique* si les valeurs propres de $\mathrm{c}_\infty(\pi)$ sont dans $\frac{1}{2}\mathbb{Z}$ et de différences deux à deux dans $\mathbb{Z}$ (§VIII.2.6). La plus grande des différences entre deux valeurs propres de $\mathrm{c}_\infty(\pi)$ est alors appellée *poids motivique* de π ; c'est un

entier ≥ 0 noté $\mathrm{w}(\pi)$. Ainsi que nous l'avons vu dans la préface [8], ces représentations algébriques ont un intérêt propre, car ce sont précisément celles qui sont reliées aux représentations ℓ-adiques "géométriques" du groupe de Galois absolu de $\mathbb{Q}$, par le yoga de Fontaine-Mazur et Langlands (§VIII.2.16). Leur intérêt dans les questions qui nous préoccupent ici réside plutôt dans l'observation suivante.

Soient G un $\mathbb{Z}$-groupe semi-simple, $\pi \in \Pi_{\mathrm{disc}}(G)$ telle que π_∞ a même caractère infinitésimal qu'une représentation algébrique V de dimension finie de $G(\mathbb{C})$, et $r : \widehat{G} \to \mathrm{SL}_n(\mathbb{C})$ une représentation algébrique. Supposons $\psi(\pi, r) = \oplus_{i=1}^k \pi_i[d_i]$ suivant Arthur et Langlands. Les représentations π_i sont alors algébriques, de poids motivique borné en fonction des plus hauts poids de V et r (§VIII.2). Par exemple, si $G = \mathrm{Sp}_{2g}$ et si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ est engendrée par une forme modulaire de Siegel propre de poids k pour $\mathrm{Sp}_{2g}(\mathbb{Z})$ (avec disons $k > g$, mais cette condition peut être affaiblie), on peut écrire $\psi(\pi, \mathrm{St}) = \oplus_{i=1}^k \pi_i[d_i]$ d'après Arthur, et les π_i sont algébriques de poids motivique $\leq 2k - 2$. Un ingrédient important de nos démonstrations est alors l'énoncé de classification suivant, d'intérêt indépendant, démontré au §IX.3.

Théorème F. *Soient $n \geq 1$ et $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ algébrique de poids motivique ≤ 22. Alors π appartient à la liste des 11 représentations suivantes :*

$$1,\ \Delta_{11},\ \Delta_{15},\ \Delta_{17},\ \Delta_{19},\ \Delta_{19,7},\ \Delta_{21},\ \Delta_{21,5},\ \Delta_{21,9},\ \Delta_{21,13},\ \mathrm{Sym}^2\Delta_{11}.$$

En poids motivique < 11, ce théorème affirme que l'on a $n = 1$ et que π est la représentation triviale, un résultat était déjà connu de Mestre et Serre (au langage près, voir [Mes86, §III, Remarque 1]). Dans ce cas très particulier, il fournit entre autres une explication "automorphe" du théorème classique de Minkowski affirmant que tout corps de nombres distinct de $\mathbb{Q}$ est ramifié en au moins un nombre premier (cas $\mathrm{w}(\pi) = 0$), ou encore de la conjecture de Shaffarevic, démontrée indépendamment par Abrashkin et Fontaine, selon laquelle il n'y a pas de variété abélienne sur $\mathbb{Z}$ (cas $\mathrm{w}(\pi) = 1$). À notre connaissance, l'énoncé du théorème F est déjà nouveau dans le cas particulier $\mathrm{w}(\pi) = 11$. Soulignons que l'on n'y fait pas d'hypothèse sur l'entier n, et qu'il entraîne $n \leq 4$.

Notre démonstration de ce théorème, dans le prolongement des travaux de Stark, Odlyzko et Serre sur les minorations des discriminants de corps de nombres, repose sur un analogue dans le cadre des fonctions L automorphes

8. La définition d'algébricité donnée dans la préface, d'apparence plus restrictive, est en fait équivalente à celle ci-dessus : voir la remarque VIII.2.14. Le poids motivique $\mathrm{w}(\pi)$ est aussi le double de la plus grande valeur propre de $\mathrm{c}_\infty(\pi)$.

des *formules explicites* de Riemann et Weil en théorie des nombres premiers. Cet analogue a été développé par Mestre [Mes86], puis appliqué par Fermigier aux fonctions $\mathrm{L}(s,\pi)$ pour $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ [Fer96]. Nous l'appliquons plus généralement à la fonction L "de Rankin-Selberg" d'une paire arbitraire $\{\pi,\pi'\}$ de représentations automorphes cuspidales algébriques de PGL_n et $\mathrm{PGL}_{n'}$ (Jacquet, Piatetski-Shapiro, Shalika).

Dans le cas particulier où π' est la duale de π, cette méthode avait déjà porté ses fruits dans un travail de Miller [Mil02] ; cependant notre étude comprend quelques nouveautés qui méritent d'être signalées. Tout d'abord, nous avons découvert que certaines formes bilinéaires symétriques, qui sont définies sur l'anneau de Grothendieck K_∞ du groupe de Weil de $\mathbb{R}$ et à valeurs réelles, et qui interviennent de manière naturelle dans l'écriture des formules explicites, sont définies positives sur des sous-groupes assez gros de K_∞. C'est cet énoncé qui est responsable de la finitude de la liste apparaissant dans le théorème F. De plus, nous établissons des critères simples, portant par exemple uniquement sur π_∞ et π'_∞, interdisant l'existence simultanée de π et de π'. Nous renvoyons au §IX.3 pour des énoncés précis.

6. Démonstration des théorèmes D et E

Donnons les grandes lignes de la démonstration du théorème E (§IX.4.3). Soit $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que π_∞ est la représentation triviale. Les résultats d'Erokhin et Borcherds-Freitag-Weissauer rappelés au §I.3 montrent que π admet un "ϑ-correspondant" dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$, engendré par une forme de Siegel de poids 12 et de genre $g \leq 11$ (§VII.1), à l'exception près d'un π déjà déterminé par Ikeda [Ike01] et vérifiant $\psi(\pi,\mathrm{St}) = \Delta_{11}[12]$. Le théorème d'Arthur appliqué à ce ϑ-correspondant, et le point de vue de Rallis sur les relations d'Eichler, entraînent que le couple (π,St) vérifie la conjecture d'Arthur-Langlands. Une étude combinatoire simple reposant uniquement sur le théorème F montre qu'il y a au plus 24 possibilités pour $\psi(\pi,\mathrm{St})$ (celles de la table I.2). Mais il y a également au moins 24 possibilités pour $\psi(\pi,\mathrm{St})$, car d'après Nebe et Venkov l'opérateur T_2 admet des valeurs propres distinctes sur $\mathbb{C}[\mathrm{X}_{24}]$, ce qui termine la démonstration.

Cette méthode permet d'étudier plus généralement les représentations dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ engendrées par une forme modulaire de Siegel de poids $k \leq 12$ pour le groupe $\mathrm{Sp}_{2g}(\mathbb{Z})$ (§IX.5). Le théorème D est le fruit de cette étude dans le cas particulier $k = 12$. On trouve en tout 23 formes modulaires de Siegel pour $\mathrm{Sp}_{2g}(\mathbb{Z})$ qui sont propres pour $\mathrm{H}(\mathrm{Sp}_{2g})$, de poids 12, et de genre $g \leq 23$, dont nous décrivons au passage les paramètres standards

(Table C.1). Dans le cas des formes de poids $k \leq 11$, nous démontrons le théorème suivant, généralisant des résultats de [DI98] et [PY07] (Théorème IX.5.10).

Théorème G. *Soient $g \geq 1$ et $k \in \mathbb{Z}$.*

(i) Si $k \leq 10$ alors $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$, à moins que (k, g) ne soit parmi

$$(8,4), \quad (10,2), \quad (10,4), \quad (10,6), \quad (10,8),$$

auquel cas $\dim \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 1$. Les paramètres standards des 5 éléments de $\Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ engendrés par ces espaces sont respectivement

$$\Delta_{11}[4]\oplus[1], \quad \Delta_{17}[2]\oplus[1], \quad \Delta_{15}[4]\oplus[1], \quad \Delta_{17}[2]\oplus\Delta_{11}[4]\oplus[1] \quad \text{et} \quad \Delta_{11}[8]\oplus[1].$$

(ii) Si $k = 11$ alors $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$, sauf peut-être si $g = 6$.

Indiquons quelques difficultés dans les démonstrations des théorèmes D et G qui n'apparaissent pas dans celle du théorème E. Soit π un élément de $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ engendré par une forme modulaire de Siegel de poids $k \leq 12$ et de genre $g < 12 + k$. Le théorème F permet de montrer qu'il n'y a qu'une liste finie explicite de possibilités pour $\psi(\pi, \mathrm{St})$. En revanche, contrairement à la situation du théorème E, certains éléments de cette liste ne devraient pas intervenir, comme le montre une inspection de la formule de multiplicité. Nous contournons l'utilisation de cette formule par un recours à des résultats de Böcherer [Boc89] et d'Ikeda [Ike01, Ike13], ainsi qu'à un ensemble de constructions de séries thêta. L'annulation de $\mathrm{S}_{11}(\mathrm{Sp}_{12}(\mathbb{Z}))$ est attendue, mais nous ne pouvons la démontrer inconditionellement. Les cas $g \geq k$ sont plus délicats (nous ne savons même pas comment expliciter la formule de multiplicité d'Arthur dans ce cas). Nous les excluons de manière *ad hoc* en utilisant les travaux de S. Mizumoto [Miz91] sur les pôles de la fonction $\mathrm{L}(s, \pi, \mathrm{St})$ (§VIII.7).

7. Quelques applications

D'après le théorème E, la question initiale de déterminer les $\mathrm{N}_p(L, M)$ pour L, M dans X_{24} et p premier devient équivalente à celle de déterminer les valeurs propres des opérateurs de Hecke agissant sur les 4 formes modulaires de Siegel à valeurs vectorielles pour $\mathrm{Sp}_4(\mathbb{Z})$ mentionnées au §4. Nous exposons au §X.3 une méthode que nous avons découverte pour y parvenir, utilisant l'analyse des p-voisins du réseau de Leech effectuée au §III.4.

Soit (j,k) l'un des 4 couples considérés au §I.4, c'est-à-dire $(6,8)$, $(4,10)$, $(8,8)$ ou $(12,6)$. Notons (w,v) le couple $(2j+k-3, j+1)$ correspondant. Si q est un entier de la forme p^k avec p premier et k entier ≥ 1, nous posons

$$\tau_{j,k}(q) \;=\; q^{\frac{w}{2}} \text{ trace } \mathrm{c}_p(\Delta_{w,v})^k,$$

c'est un nombre complexe qui est en fait dans $\mathbb{Z}$.

Théorème H. *Soit (j,k) l'un des 4 couples $(6,8),(4,10),(8,8)$ ou $(12,6)$. Les entiers $\tau_{j,k}(p)$ avec p premier ≤ 113, et $\tau_{j,k}(p^2)$ avec p premier ≤ 29, sont respectivement donnés par les tables C.3 et C.4.*

Ces résultats confirment et étendent des calculs antérieurs de Faber et van der Geer [FvdG04] [vdG08, §25], par des méthodes très différentes. Au final, nous disposons donc de la valeur exacte de $\mathrm{N}_p(L,M)$ pour tout L,M dans X_{24} et tout nombre premier $p \leq 113$.

Le théorème F montre que la question du calcul des $\tau_{j,k}(q)$ est peut-être moins futile qu'elle ne le paraît. En effet, compte tenu des conjectures de Langlands, ce théorème suggère une classification parallèle, encore à démontrer du côté ℓ-adique, des motifs purs et effectifs sur $\mathbb{Q}$, ayant bonne réduction partout, et de poids motivique ≤ 22. Par exemple, il impose une contrainte conjecturale remarquable sur la fonction zêta de Hasse-Weil du champs de Deligne-Mumford $\overline{\mathcal{M}_{g,n}}$ classifiant les courbes stables de genre g munies de n points marqués, avec $g \geq 2$, $n \geq 0$ et $3g-3+n \leq 22$: elle devrait s'exprimer uniquement en termes des coefficients des formes modulaires paraboliques normalisées de poids ≤ 22 pour $\mathrm{SL}_2(\mathbb{Z})$ et des $\tau_{j,k}(q)$. Cela confirme certains résultats (resp. conjectures) de Bergström, Faber et van der Geer [FvdG04, Fab13, BFG14] lorsque $g=2$ (resp. $g=3$).

Nous donnons au §X.4 des applications du théorème E aux congruences satisfaites par les entiers $\tau_{j,k}(p)$ avec p premier. Ces congruences sont obtenues par une étude des vecteurs propres de T_2 dans la base naturelle de $\mathbb{Z}[\mathrm{X}_{24}]$ et par des arguments de représentations galoisiennes. Entre autres, nous démontrons la congruence conjecturée par Harder dans [Har08].

Théorème I. (Conjecture de Harder) *Pour tout premier p on a la congruence*

$$\tau_{4,10}(p) \equiv \tau_{22}(p) + p^{13} + p^8 \bmod 41,$$

où $\tau_{22}(p)$ désigne le p-ième coefficient de la forme modulaire parabolique normalisée de poids 22 pour le groupe $\mathrm{SL}_2(\mathbb{Z})$.

Revenons enfin sur la démonstration du théorème E esquissée au §6. Elle utilise l'égalité $|X_{24}| = 24$, conséquence de la classification de Niemeier. Cependant, nous expliquons au §IX.6 comment la combinaison des idées ci-dessus et des formules de multiplicité d'Arthur (incluant les conjectures 4.22 et 4.25 formulées au §VIII) permet en retour de se passer de cette égalité, et même de la redémontrer "sans aucun calcul de réseaux euclidiens". Mieux, nous retrouvons non seulement qu'il existe exactement 24 réseaux de Niemeier à isométries près, mais également qu'un seul d'entre eux ne possède pas d'isométrie de déterminant -1.

Est-il raisonnable d'espérer pouvoir estimer finement le cardinal de X_{32} par une telle méthode ? La question reste entière, mais l'exemple de la dimension 24 montre que cette approche, chère au premier auteur, est moins farfelue qu'elle n'en a l'air. Un ingrédient nécessaire à ce projet est la connaissance des représentations algébriques (disons "autoduales, régulières") dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ dont le poids motivique est ≤ 30 : des progrès dans cette direction ont été récemment obtenus dans [CR12] et [Tai14].

*

* *

Pour conclure cette introduction, disons un mot sur l'utilisation dans ce mémoire des résultats récents d'Arthur. Ces derniers reposent sur un ensemble impressionnant de travaux difficiles, certaines démonstrations étant encore toutes fraîches (voir [Art13], [MW14, Wal14] et la discussion du §VIII.1). C'est pourquoi il nous a semblé utile d'indiquer, par une étoile*, dans le corps du mémoire, les énoncés dépendant des résultats du livre [Art13]. Dans cette introduction, cela concerne les démonstrations des théorèmes B, D, E, F [9], G, H et I. En revanche, précisons que contrairement aux annonces que nous avions faites initialement dans [CL11] et [Che13], nos démonstrations ne reposent plus sur les résultats annoncés par Arthur *loc. cit.* dans son dernier chapitre sur les formes intérieures, ni sur les propriétés conjecturales des paquets d'Arthur du type de ceux étudiés par Adams et Johnson.

9. En ce qui concerne le théorème F, nous en démontrons en fait une variante quasiment aussi forte sans aucun recours à la théorie d'Arthur : voir le théorème IX.3.2.

II. Algèbre bilinéaire et quadratique

1. Généralités sur les formes bilinéaires et quadratiques

Soit A un anneau commutatif unitaire.

Nous appellerons b-*module* sur A, un A-module projectif de type fini L muni d'une forme bilinéaire symétrique non dégénérée, c'est-à-dire telle que l'homomorphisme induit $L \to \mathrm{Hom}_A(L, A)$ est un isomorphisme ; quand A sera un corps nous remplacerons évidemment "b-module" par "b-*espace vectoriel*". Le plus souvent la forme bilinéaire symétrique $L \times L \to A$ sera notée $(x, y) \mapsto x.y$. Dans ce mémoire les anneaux A auxquels nous aurons affaire seront des anneaux principaux ou des corps si bien que nous aurions pu remplacer dans la définition ci-dessus "A-module projectif de type fini" par "A-module libre de dimension finie".

Soit S une matrice symétrique de taille (n, n) à coefficients dans A, la notation $\langle S \rangle$ désignera le A-module A^n muni de la forme bilinéaire dont la matrice dans la base canonique est S ; il est clair que $\langle S \rangle$ est un b-module si et seulement si l'on a $\text{dét}\, S \in A^\times$. Si S est une matrice diagonale de coefficients diagonaux $a_1, a_2, \ldots, a_n$ alors $\langle S \rangle$ sera plutôt notée $\langle a_1, a_2, \ldots, a_n \rangle$.

Nous supposons maintenant que A est un anneau de Dedekind ; on note K son corps des fractions. (En fait, étant donné les anneaux que nous avons en tête, à savoir $\mathbb{Z}$ et $\mathbb{Z}_p$, nous pourrions remplacer "anneau de Dedekind" par "anneau principal".)

Soit V un K-espace vectoriel de dimension finie. On appelle *réseau* de V (par rapport à A) un sous-A-module L de V, qui engendre V comme K-espace vectoriel et qui est de type fini sur A ; un tel L est un A-module projectif dont le rang est égal à $\dim_K V$.

Soit V un b-espace vectoriel sur K. Soit L un réseau de V. Le sous-A-module de V formé des éléments y tels que $x.y$ appartient à A pour tout x dans L est un réseau de V que l'on appelle le *dual* de L et que l'on note $L^\sharp$.

Nous dirons que le réseau L est *entier* si $x.y$ appartient à A pour tous x et y dans L, en d'autres termes si l'on a $L \subset L^\sharp$.

Soit L un réseau entier de V. Considérons le quotient $L^\sharp/L$:
– Le A-module $L^\sharp/L$ est de torsion et de type fini.
– La forme bilinéaire symétrique dont V est muni induit sur $L^\sharp/L$ une "forme" bilinéaire symétrique non dégénérée à valeurs dans K/A. Ici "non dégénérée" signifie que l'homomorphisme, induit par la forme en question, $L^\sharp/L \to \mathrm{Hom}_A(L^\sharp/L, K/A)$ est un isomorphisme.

Nous appelons ce type d'objet un e-*module* sur A. Un e-module sur A est donc un A-module de torsion et de type fini muni d'une forme bilinéaire symétrique non dégénérée à valeurs dans K/A (*forme d'enlacement*). Nous appelons *résidu* de L le e-module $L^\sharp/L$. La considération du quotient $L^\sharp/L$ est bien sûr fort ancienne, mais notre terminologie n'est pas classique, par exemple $L^\sharp/L$ est appelé "dual quotient group" ou "glue group" dans [CS99] et "conoyau de L" dans [BLLV74] ; nous le noterons souvent $\mathrm{rés}\, L$.

Dans la mesure du possible nous étendrons aux e-modules les notations et la terminologie utilisées pour les modules munis d'une forme bilinéaire symétrique à valeurs dans A. Voici quelques exemples. Soit C un e-module :

– la forme bilinéaire symétrique $C \times C \to K/A$ sera le plus souvent notée $(x, y) \mapsto x.y$;

– nous dirons qu'un sous-module I de C est *isotrope* si l'on a $x.y = 0$ pour tous éléments x et y de I, autrement dit si l'on a $I \subset I^\perp$, $I^\perp$ désignant l'orthogonal de I ;

– nous dirons qu'un sous-module I de C est un *lagrangien* si l'on a $I = I^\perp$.

Nous appellerons $\widetilde{\mathrm{b}}$-*module* sur A (qui est toujours supposé de Dedekind) un A-module projectif de type fini L muni d'une forme bilinéaire symétrique telle que l'homomorphisme induit $L \to \mathrm{Hom}_A(L, A)$ est injectif (ou, ce qui revient au même, telle que la forme bilinéaire induite sur $K \otimes_A L$ est non dégénérée). Un réseau entier d'un b-espace vectoriel sur K est le type même d'un tel objet. Réciproquement tout $\widetilde{\mathrm{b}}$-module L sur A peut être vu comme un réseau entier du b-espace vectoriel $K \otimes_A L$. Un $\widetilde{\mathrm{b}}$-module L possède donc un résidu $\mathrm{rés}\, L$ qui est un e-module ; le A-module sous-jacent à $\mathrm{rés}\, L$ s'identifie au conoyau de l'injection $L \hookrightarrow \mathrm{Hom}_A(L, A)$.

En remplaçant, dans les définitions précédentes, formes bilinéaires symétriques par formes bilinéaire alternées, on obtient, *mutatis mutandis*, les définitions respectives de a-*module*, ae-*module*, $\widetilde{\mathrm{a}}$-*module* et *résidu* d'un $\widetilde{\mathrm{a}}$-module. Par exemple, un ae-module sur A est un A-module de torsion et de type fini

C muni d'une forme bilinéaire alternée $C \times C \to K/A$ telle que l'homomorphisme induit $C \to \mathrm{Hom}_A(C, K/A)$ est un isomorphisme. On observera qu'un a-module sur A est toujours de rang pair et qu'il en est de même pour un $\widetilde{\mathrm{a}}$-module si A est de Dedekind.

Rappelons qu'une application $f : M \to N$ entre deux A-modules est dite *quadratique* si elle vérifie les deux propriétés suivantes :
– on a $f(ax) = a^2 f(x)$ pour tout a dans A et tout x dans M ;
– l'application $M \times M \to N, (x, y) \mapsto f(x + y) - f(x) - f(y)$ est bilinéaire.
Dans le cas $N = A$, on dit que f est une forme quadratique sur M.

On obtient, *mutatis mutandis*, les définitions respectives de q-*module*, qe-*module* et $\widetilde{\mathrm{q}}$-*module*, en remplaçant dans les définitions précédentes formes bilinéaires symétriques par formes quadratiques. Par exemple un q-module sur A est un A-module projectif de type fini L muni d'une forme quadratique $\mathrm{q} : L \to A$ telle que la forme bilinéaire symétrique (dite *associée*)

$$L \times L \to A \qquad , \qquad (x, y) \ \mapsto \ \mathrm{q}(x + y) - \mathrm{q}(x) - \mathrm{q}(y)$$

est non dégénérée. Un qe-module sur A est un A-module de torsion et de type fini muni d'une forme quadratique non dégénérée à valeurs dans K/A (*forme quadratique d'enlacement*) ; le *résidu* d'un $\widetilde{\mathrm{q}}$-module est maintenant un qe-module. Un sous-module I d'un qe-module est *isotrope* si l'on a $\mathrm{q}(I) = 0$ (condition qui implique $I \subset I^{\perp}$) ; c'est un *lagrangien* si l'on a $\mathrm{q}(I) = 0$ en plus de la condition $I = I^{\perp}$. Un réseau L d'un q-espace vectoriel est *entier* si $\mathrm{q}(x)$ appartient à A pour tout x dans L (condition qui implique que $x.y$ appartient à A pour tous x et y dans L).

Si 2 n'est pas diviseur de zéro alors un q-module sur A n'est rien d'autre qu'un b-module *pair* c'est-à-dire un b-module L tel que $x.x$ est divisible par 2 pour tout x dans L : dans ce cas la forme quadratique est déterminée par l'égalité $x.x = 2\mathrm{q}(x)$. Si 2 est inversible dans A alors les notions de q-module et b-module coïncident ; on se souviendra cependant de ce que formes quadratiques et formes bilinéaires symétriques associées sont reliées par l'égalité précédente.

La proposition suivante est évidente... ce qui ne l'empêche pas d'être très utile.

Proposition 1.1. *Soient V un* b-*espace vectoriel (resp.* a-*espace vectoriel, resp.* q-*espace vectoriel) sur K et L un réseau entier de V. Soit $\gamma : L^{\sharp} \to \mathrm{rés}\, L$ l'homomorphisme de passage au quotient.*

(a) *Soit I un sous-module de* $\mathrm{rés}\, L$ *alors les deux conditions suivantes sont équivalentes :*
(i) le sous-module I est isotrope ;
(ii) le réseau $\gamma^{-1}(I)$ est entier.

(b) *L'application $I \mapsto \gamma^{-1}(I)$ est une bijection croissante de l'ensemble des sous-modules isotropes de* $\mathrm{rés}\, L$ *sur l'ensemble des réseaux entiers de V contenant L (et donc contenus dans $L^\sharp$).*

(c) *Soit I un sous-module isotrope de* $\mathrm{rés}\, L$*, alors la forme bilinéaire symétrique $I^\perp/I \times I^\perp/I \to K/A$ (resp. la forme bilinéaire alternée $I^\perp/I \times I^\perp/I \to K/A$, resp. la forme quadratique $I^\perp/I \to K/A$), induite par celle dont* $\mathrm{rés}\, L$ *est muni, fait de $I^\perp/I$ un* e*-module (resp.* ae*-module, resp.* qe*-module) qui s'identifie au résidu du réseau entier $\gamma^{-1}(I)$.*

Foncteurs hyperboliques

Soit A un anneau commutatif unitaire. Soit L un A-module projectif de type fini ; $\mathrm{Hom}_A(L, A)$ est encore un A-module projectif de type fini que l'on note L^* (et que l'on appelle le *dual* de L). L'application

$$L \oplus L^* \to A \qquad , \qquad (x, \xi) \mapsto \langle x, \xi \rangle$$

est une forme quadratique non dégénérée qui fait du A-module projectif de type fini $L \oplus L^*$ un q-module. Ce q-module est noté $\mathrm{H}(L)$ et appelé le q-module *hyperbolique* sur L.

La forme bilinéaire symétrique associée est l'application

$$((x, \xi), (y, \eta)) \mapsto \langle x, \eta \rangle + \langle y, \xi \rangle \qquad ;$$

$L \oplus L^*$ muni de cette forme est appelé le b-module *hyperbolique* sur L et est encore noté $\mathrm{H}(L)$.

Pareillement, $L \oplus L^*$ muni de la forme bilinéaire alternée

$$((x, \xi), (y, \eta)) \mapsto \langle x, \eta \rangle - \langle y, \xi \rangle$$

est un a-module sur A, appelé a-module *hyperbolique* sur L et toujours noté $\mathrm{H}(L)$.

Soit H un q-module (resp. a-module) sur A ; rappelons que dans ce contexte un lagrangien de H est un facteur direct L avec $L = L^\perp$ et $\mathrm{q}(L) = 0$ (resp. $L = L^\perp$).

Proposition 1.2. *Soient H un* q*-module (resp.* a*-module) et L un lagrangien ; alors l'inclusion de L dans H se prolonge en un isomorphisme de* q*-modules (resp.* a*-modules)* $\mathrm{H}(L) \simeq H$.

Démonstration. On démontre la "version quadratique" de l'énoncé ; nous suivons sans vergogne la démonstration de [BL08, Proposition 2.1.5] qui traite implicitement de la "version alternée". Soient $i : L \to H$ l'inclusion de L dans H et $p : H \to L^*$ l'homomorphisme (de A-modules) composé de l'isomorphisme $H \to H^*$ induit par la forme bilinéaire et de l'homomorphisme i^*. Puisque L est un lagrangien, la suite de A-modules

$$0 \longrightarrow L \xrightarrow{\ i\ } H \xrightarrow{\ p\ } L^* \longrightarrow 0$$

est exacte. Il s'agit de montrer qu'il existe une section A-linéaire $s : L^* \to H$ de p vérifiant $\mathrm{q}(s(\xi)) = 0$ pour tout ξ dans L^*. Soit Σ l'ensemble des sections A-linéaires de p. L'ensemble Σ n'est pas vide puisque L^* est projectif ; de plus Σ possède une structure canonique d'espace affine sous $\mathrm{Hom}_A(L^*, L)$ que l'on identifie avec le A-module des formes bilinéaires sur L^*, disons $\mathcal{B}_{L^*}$. Soient $\mathcal{Q}_{L^*}$ le A-module des formes quadratiques sur L^* et $\gamma : \Sigma \to \mathcal{Q}_{L^*}$ l'application qui associe à une section s la forme quadratique $\xi \mapsto \mathrm{q}(s(\xi))$; soit u un élément de $\mathrm{Hom}_A(L^*, L)$, on constate que l'on a :

$$\gamma(s + u) = \gamma(s) + \widetilde{\gamma}(u) \qquad ,$$

$\widetilde{\gamma}$ désignant l'application $\mathcal{B}_{L^*} \to \mathcal{Q}_{L^*}$ qui associe à une forme bilinéaire u la forme quadratique $\xi \mapsto u(\xi, \xi)$. Le fait que $\gamma^{-1}(0)$ n'est pas vide résulte maintenant du fait que $\widetilde{\gamma}$ est surjective. Ceci est clair si L^* est libre ; le cas général en découle en faisant intervenir un A-module M tel que la somme directe $L^* \oplus M$ est libre de dimension finie. □

Remarque. La considération du b-espace vectoriel $\langle \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \rangle$ sur $\mathbb{F}_2$ montre que l'énoncé analogue à 1.2 pour les b-modules n'est pas vérifié en général.

On dit qu'un q-module (resp. a-module) est *hyperbolique* s'il est isomorphe à un $\mathrm{H}(L)$ pour un certain A-module projectif de type fini L ; la proposition ci-dessus dit en particulier qu'un q-module est hyperbolique si et seulement s'il possède un lagrangien.

Soient maintenant A un anneau de Dedekind (de corps des fractions K) et I un A-module de torsion de type fini ; $\mathrm{Hom}_A(I, K/A)$ est encore un A-module de torsion de type fini que l'on note $I^\vee$ (et que l'on appelle le *dual* de I). L'application

$$I \oplus I^\vee \to K/A \qquad , \qquad (x, \xi) \mapsto \langle x, \xi \rangle$$

est une forme quadratique non dégénérée qui fait du A-module de torsion de type fini $I \oplus I^\vee$ un qe-module. Ce qe-module est noté $\mathrm{H}(I)$ et appelé le qe-module *hyperbolique* sur I.

Soit H un qe-module sur A ; rappelons que dans ce contexte un lagrangien de H est un sous-module I avec $I = I^\perp$ et $\mathrm{q}(I) = 0$. La démonstration de la proposition suivante est laissée au lecteur (on pourra comparer le point (b) avec le point (b) de [BL08, Proposition 2.1.5]).

Proposition-Définition 1.3. *Soit H un* qe*-module. Soient I et J deux lagrangiens de H ; on dit que I et J sont* transverses *(ou que J est* transverse à I*) si l'on a $I \cap J = 0$.*

(a) *Soient I et J deux lagrangiens transverses de H. Alors la forme d'enlacement de H induit un isomorphisme $J \cong I^\vee$ et l'homomorphisme composé*

$$\mathrm{H}(I) = I \oplus I^\vee \to I \oplus J \to H$$

est un isomorphisme de qe*-modules (la première flèche est la somme directe de l'identité de I et de l'inverse de l'isomorphisme $J \cong I^\vee$).*

(b) *Soient I un lagrangien de H et $\mathcal{T}_I$ l'ensemble (éventuellement vide) des lagrangiens transverses à I. Alors $\mathcal{T}_I$ possède une structure canonique d'espace affine sous le A-module $(\Lambda^2(I^\vee))^\vee$ (en clair le A-module constitué des applications bilinéaires alternées $I^\vee \times I^\vee \to K/A$).*

On dit qu'un qe-module est *hyperbolique* s'il est isomorphe à un $\mathrm{H}(I)$ pour un certain A-module de type fini I ; le point (a) de la proposition ci-dessus dit en particulier qu'un qe-module est hyperbolique si et seulement s'il possède deux lagrangiens transverses.

Produits tensoriels de formes

Soit A un anneau commutatif ; soient L_1 et L_2 deux b-modules sur A. L'homomorphisme de A-modules, $L_1 \otimes_A L_2 \to (L_1 \otimes_A L_2)^* \cong L_1^* \otimes_A L_2^*$, produit tensoriel des homomorphismes structurels $L_1 \to L_1^*$ et $L_2 \to L_2^*$ fait de $L_1 \otimes_A L_2$ un b-module que l'on appelle le *produit tensoriel* des b-modules L_1 et L_2. La forme bilinéaire symétrique de $L_1 \otimes_A L_2$ est caractérisée par le fait que l'on a $(x_1 \otimes_A x_2).(y_1 \otimes_A y_2) = (x_1.y_1)(x_2.y_2)$ pour tous x_1, y_1 dans L_1 et tous x_2, y_2 dans L_2.

Mutatis mutandis on définit :

– le produit tensoriel d'un b-module et d'un q-module qui est un q-module ;

– le produit tensoriel d'un b-module et d'un e-module qui est un e-module ;

– le produit tensoriel d'un b-module et d'un qe-module qui est un qe-module ;

– le produit tensoriel d'un q-module et d'un e-module qui est un qe-module.

Par exemple si L_1 est un b-module et L_2 est un q-module alors la forme quadratique de $L_1 \otimes_A L_2$ est caractérisée par le fait que l'on a $\mathrm{q}(x_1 \otimes_A x_2) = (x_1.x_1)\mathrm{q}(x_2)$ pour tout x_1 dans L_1 et tout x_2 dans L_2.

Discriminant d'un q-module de rang constant pair, déterminant de Dickson-Dieudonné

Soient A un anneau commutatif et L un q-module sur A de rang constant pair, disons non nul. Soit $\Delta(L)$ le centre de la partie paire, notée $\mathrm{C}^+(L)$, de l'algèbre de Clifford de L (voir par exemple [Ch97, Chap. III]).

– La A-algèbre commutative $\Delta(L)$ est un "revêtement double" de A, en clair une A-algèbre étale et un A-module projectif de rang 2 [SGA7, Exposé XII, Proposition 1.5] qu'il faut voir comme le *discriminant* de L. Dans le cas $L = \mathrm{H}(P)$, avec P un A-module projectif de rang constant, ce revêtement est trivial (et même trivialisé) : $\Delta(L) = A \times A$.

– Un automorphisme α du q-module L induit un automorphisme $\Delta(\alpha)$ de la A-algèbre $\Delta(L)$. Si l'on identifie le groupe des automorphismes de la A-algèbre $\Delta(L)$ avec $\mathbb{Z}/2(A)$, alors $\Delta(\alpha)$ s'identifie à un élément de $\mathbb{Z}/2(A)$ que l'on appelle le *déterminant de Dickson-Dieudonné* de α ; nous le notons $\widetilde{\text{dét}}\,\alpha$. Rappelons la définition du foncteur en groupes $A \mapsto \mathbb{Z}/2(A)$ qui apparaît subrepticement ci-dessus : $\mathbb{Z}/2(A)$ est l'ensemble des éléments x de A vérifiant $x^2 = x$ muni de la loi de groupe $(x, y) \mapsto x + y - 2xy$.

Ces deux points sont une "globalisation" sans surprises de résultats bien connus dans le cas où A est un corps. Le cas subtil est celui où A est un corps de caractéristique 2, voir [Di55][Bou81a, §9, Exc. 9].

Soit L un b-module sur A de rang constant n. Le *déterminant de* L est le b-module $\Lambda^n L$ ($\Lambda^n L$ est un A-module projectif de rang 1, il est muni de la forme bilinéaire symétrique induite par celle de L) ; nous le notons $\text{dét}\, L$. Dans le cas où L est libre, la classe d'isomorphisme de $\text{dét}\, L$ s'identifie à un élément de $A^\times/A^{\times 2}$. Cet élément est la classe dans $A^\times/A^{\times 2}$ du déterminant de la matrice de Gram $[e_i.e_j]$, pour n'importe quelle base $(e_1, e_2, \ldots, e_n)$ de L ; la classe en question est aussi souvent notée $\text{dét}\, L$.

Soit L un q-module sur A de rang constant pair, disons $2n$ avec $n \geq 1$. La relation entre le discriminant de L et le déterminant du b-module sous-jacent est donnée par l'énoncé 1.4 ci-dessous dont nous devons une démonstration à Pierre Deligne. Pour formuler cet énoncé, il nous faut introduire quelques notations. On note $\mathrm{D}(L)$ est le conoyau de l'unité $\eta : A \to \Delta(L)$. On constate que le A-module $\mathrm{D}(L)$ est projectif de rang 1 (ceci résulte par exemple d'un argument de descente fidèlement plate [SGA $4\frac{1}{2}$, I, Prop. 4.2] puisque l'on a $\Delta(L) \otimes_A \Delta(L)) \cong \Delta(L) \times \Delta(L))$ et qu'il est muni d'une forme bilinéaire symétrique non dégénérée canonique, disons θ, que l'on peut définir, par exemple, comme induite par la forme bilinéaire symétrique $\Delta(L) \times \Delta(L) \to A, (x, y) \mapsto \mathrm{tr}_{\Delta(L)/A}((x - \bar{x})y)$ ($\bar{x}$ désignant le "conjugué" de x) ; en d'autres termes, $\mathrm{D}(L)$ possède une structure naturelle de b-module sur A de rang 1. On note enfin $(-1)^n \operatorname{dét} L$ le b-module sur A de rang 1 obtenu en multipliant par $(-1)^n$ la forme bilinéaire symétrique dont $\operatorname{dét} L$ est munie. Voici l'énoncé promis :

Proposition 1.4. *Les deux* b*-modules sur A de rang* 1*,* $\mathrm{D}(L)$ *et* $(-1)^n \operatorname{dét} L$*, sont naturellement isomorphes.*

Groupes classiques

L'objet essentiel de cette dernière rubrique du paragraphe et de fixer les notations et la terminologie relatives aux groupes orthogonaux et symplectiques (et leurs diverses déclinaisons) qui seront utilisées dans ce mémoire.

Soit A un anneau commutatif unitaire.

– Soit L un A-module projectif de type fini. On note $\mathrm{GL}(L)$ le groupe des automorphismes de L. Le foncteur $R \mapsto \mathrm{GL}(R \otimes_A L)$, défini sur la catégorie des A-algèbres commutatives et à valeurs dans la catégorie des groupes, est un A-schéma en groupes que l'on note GL_L ; on observera que si le rang de L est 1, alors $\mathrm{GL}(L)$ et GL_L s'identifient respectivement au groupe $A^\times$ et au A-schéma en groupes $\mathbb{G}_\mathrm{m}$ (si G est un $\mathbb{Z}$-schéma en groupes on note encore G le A-schéma en groupes obtenu par changement de base). Si L est de rang constant, disons n, on note SL_L le noyau de l'homomorphisme "déterminant" $\operatorname{dét} : \mathrm{GL}_L \to \mathrm{GL}_{\Lambda^n L} = \mathbb{G}_\mathrm{m}$. On note PGL_L le A-schéma en groupes défini comme le foncteur qui associe à une A-algèbre commutative R le groupe des automorphismes de la R-algèbre $\mathrm{End}_R(R \otimes_A L)$; PGL_L peut être aussi vu comme le A-schéma en groupes quotient de GL_L par $\mathbb{G}_\mathrm{m}$. Evidemment, dans le cas $A = \mathbb{Z}$ et $L = A^n$, la notation $\mathrm{GL}_{\mathbb{Z}^n}$, $\mathrm{SL}_{\mathbb{Z}^n}$, $\mathrm{PGL}_{\mathbb{Z}^n}$, sera remplacée par la notation GL_n, SL_n, PGL_n.

– Soit L un q-module (resp. b-module) sur A, un endomorphisme α du A-module sous-jacent est dit *orthogonal* si l'on a $\mathrm{q}(\alpha(x)) = \mathrm{q}(x)$ pour tout x dans L (resp. $\alpha(x).\alpha(y) = x.y$ pour tous x et y dans L) ; les endomorphismes orthogonaux forment un groupe pour la composition (les endomorphismes orthogonaux sont donc en fait des automorphismes) que l'on appelle le *groupe orthogonal* de L et que l'on note $\mathrm{O}(L)$. Le foncteur $R \mapsto \mathrm{O}(R \otimes_A L)$, défini sur la catégorie des A-algèbres commutatives et à valeurs dans la catégorie des groupes, est un A-schéma en groupes que l'on note O_L.

En fait les formes quadratiques jouent dans notre mémoire un rôle plus important que les formes bilinéaires symétriques. Une des raisons de cette prééminence est l'énoncé ci-dessous (qui n'est pas vérifié, en toute généralité, pour les b-modules).

Proposition 1.5 *Pour tout* q*-module L sur un anneau commutatif A, le A-schéma en groupes O_L est lisse sur A.*

Démonstration. Puisque la propriété que l'on veut vérifier est locale pour la topologie de Zariski, on peut supposer que L est libre, disons $L = A^n$ pour un certain entier n, ce que nous faisons ci-après. La forme quadratique s'écrit

$$(x_1, x_2, \ldots, x_n) \mapsto \sum_{i,j} q_{i,j}\, x_i x_j \qquad ,$$

$[q_{i,j}] := Q$ désignant une matrice $n \times n$, définie à l'addition d'une matrice alternée près (une *matrice alternée* est une matrice antisymétrique avec des zéros sur la diagonale, on peut également définir une matrice alternée comme une antisymétrisée), et une matrice M, de taille $n \times n$, à coefficients dans une A-algèbre R, appartient à $\mathrm{O}_L(R) := \mathrm{O}(R \otimes_A L)$ si et seulement si la matrice ${}^{\mathrm{t}}MQM - Q$ est alternée. La proposition résulte de ce que les équations fournies par cette caractérisation ($\frac{n(n+1)}{2}$ polynômes en n^2 indéterminées à coefficients dans A) satisfont au critère jacobien de lissité. □

On suppose maintenant que L est de rang constant pair. L'application qui associe à un automorphisme orthogonal α d'un q-module L son déterminant de Dickson-Dieudonné $\widetilde{\text{dét}}\,\alpha$ (voir plus haut) induit un homomorphisme de A-schémas en groupes, disons $\widetilde{\text{dét}} : \mathrm{O}_L \to \mathbb{Z}/2$. La proposition 1.4 implique que cet homomorphisme relève l'homomorphisme $\text{dét} : \mathrm{O}_L \to \mu_2$, en clair que le diagramme suivant

$$\begin{tikzcd} & \mathbb{Z}/2 \arrow[d] \\ \mathrm{O}_L \arrow[ur, "\widetilde{\text{dét}}"] \arrow[r, "\text{dét}"] & \mu_2 \end{tikzcd}$$

est commutatif (rappelons la définition de l'homomorphisme vertical : soit R une A-algèbre commutative, $\mathbb{Z}/2(R)$ est l'ensemble des éléments x de R

vérifiant $x^2 = x$, muni de la loi de groupe $(x, y) \mapsto x+y-2xy$, et l'homomorphisme $\mathbb{Z}/2(R) \to \mu_2(R)$ envoie x sur $1-2x$). Pour se convaincre de cette implication, contempler le diagramme commutatif suivant

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\eta"] \arrow[d, "\mathrm{id}"] & \Delta(L) \arrow[r] \arrow[d, "\Delta(\alpha)"] & \Lambda^{2n}L \arrow[r] \arrow[d, "\Lambda^{2n}\alpha"] & 0 \\
0 \arrow[r] & A \arrow[r, "\eta"] & \Delta(L) \arrow[r] & \Lambda^{2n}L \arrow[r] & 0
\end{tikzcd}$$

dont les lignes sont exactes.

Le A-schéma en groupes SO_L est défini comme le noyau de $\widetilde{\text{dét}}$.

Soit L un q-module sur A. On note $\mathrm{GO}(L)$ le sous-groupe de $\mathrm{GL}(L) \times A^\times$ constitué des couples (α, ν) tels que l'on a $\mathrm{q}(\alpha(x)) = \nu \mathrm{q}(x)$ pour tout x dans L. Le A-schéma en groupes GO_L est défini comme précédemment. Cette définition fait apparaître GO_L comme un sous-groupe de $\mathrm{GL}_L \times \mathbb{G}_\mathrm{m}$; le lecteur se convaincra que la restriction de la projection $\mathrm{GL}_L \times \mathbb{G}_\mathrm{m} \to \mathrm{GL}_L$ à GO_L est une immersion fermée et donc que GO_L peut être aussi vu comme un sous-groupe fermé de GL_L. On note $\nu : \mathrm{GO}_L \to \mathbb{G}_\mathrm{m}$ l'homomorphisme restriction de la projection $\mathrm{GL}_L \times \mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m}$ à GO_L. Le groupe $\mathrm{GO}(L)$, introduit ci-dessus, s'appelle le groupe des *similitudes orthogonales* de L, l'élément ν de $A^\times$ s'appelle le *facteur de similitude* de α. On note PGO_L le A-schéma en groupes quotient $\mathrm{GO}_L/\mathbb{G}_\mathrm{m}$.

On suppose à nouveau que L est de rang $2n$. Soit (α, ν) un élément de $\mathrm{GO}(L)$; on constate que l'élément $\nu^{-n} \operatorname{dét} \alpha$ de $A^\times$, disons d, vérifie $d^2 = 1$. On note $\mathrm{d} : \mathrm{GO}(L) \to \mu_2(A)$ l'homomorphisme de groupes $(\alpha, \nu) \mapsto d$. On note encore $\mathrm{d} : \mathrm{GO}_L \to \mu_2$ l'homomorphisme de A-schémas en groupes associé ; on obervera que d prolonge l'homomorphisme $\text{dét} : \mathrm{O}_L \to \mu_2$. La proposition 1.4 implique, comme plus haut, que d se relève en un homomorphisme $\widetilde{\mathrm{d}} : \mathrm{GO}_L \to \mathbb{Z}/2$ qui prolonge l'homomorphisme $\widetilde{\text{dét}} : \mathrm{O}_L \to \mathbb{Z}/2$. Précisons un peu. On rappelle que l'on identifie le groupe des automorphismes de $\Delta(L)$ avec $\mathbb{Z}/2(A)$; $\widetilde{\mathrm{d}}(\alpha, \nu)$ correspond, *via* cette identification, à la composition

$$\Delta(L) \xrightarrow{\Delta(\alpha)} \Delta(\nu L) \xrightarrow{[\nu]} \Delta(L) \qquad ,$$

νL désignant le q-module obtenu en multipliant la forme quadratique de L par ν et $[\nu]$ désignant l'isomorphisme induit par l'isomorphisme $[\nu] : \mathrm{C}^+(\nu L) \to \mathrm{C}^+(L)$ introduit dans [SGA7, Exposé XII, §1.3]. Le A-schéma en groupes GSO_L est défini comme le noyau de $\widetilde{\mathrm{d}}$. On constate que $\widetilde{\mathrm{d}}$ induit par passage au quotient un homomorphisme $\mathrm{PGO}_L \to \mathbb{Z}/2$; le A-schéma en groupes PGSO_L est défini comme le noyau de cet homomorphisme induit. Alternativement, PGSO_L peut être défini comme le quotient $\mathrm{GSO}_L/\mathbb{G}_\mathrm{m}$.

– Soit enfin L un a-module sur A. On note $\mathrm{Sp}(L)$ le groupe des automorphismes de cet a-module. Les A-schémas en groupes Sp_L, GSp_L, PGSp_L et l'homomorphisme $\nu : \mathrm{GSp}_L \to \mathbb{G}_\mathrm{m}$ sont définis *mutatis mutandis*. Si L est de rang constant, disons $2n$, la théorie du Pfaffien entraîne que l'homomorphisme dét : $\mathrm{GSp}_L \to \mathbb{G}_\mathrm{m}$ (induit par l'homomorphisme dét : $\mathrm{GL}_L \to \mathbb{G}_\mathrm{m}$) coïncide avec ν^n (relation qui implique en particulier que Sp_L est un sous-groupe de SL_L). Soit $n \geq 1$ un entier ; dans le cas où $A = \mathbb{Z}$ et où L est le a-module hyperbolique $\mathrm{H}(\mathbb{Z}^n)$, la notation $\mathrm{Sp}_{\mathrm{H}(\mathbb{Z}^n)}$, $\mathrm{GSp}_{\mathrm{H}(\mathbb{Z}^n)}$, $\mathrm{PGSp}_{\mathrm{H}(\mathbb{Z}^n)}$, sera remplacée par la notation Sp_{2n}, GSp_{2n}, PGSp_{2n}. On rappelle que Sp_2 s'identifie à SL_2.

Tous les A-schémas en groupes introduits ci-dessus sont affines et de présentation finie sur A ; pour abréger, de tels A-schémas en groupes seront appelés des *A-groupes*.

Une dernière remarque pour clore cette rubrique sur les groupes classiques : soit $\mathrm{P}G = G/\mathbb{G}_\mathrm{m}$ l'un des A-schémas en groupes "projectifs" que nous venons de définir ; au chapitre IV nous aurons seulement à considérer le groupe $\mathrm{P}G(A)$ pour des anneaux A avec $\mathrm{Pic}(A) = 0$ si bien que le monomorphisme canonique $G(A)/A^\times \to \mathrm{P}G(A)$ sera un isomorphisme.

2. Sur les b-modules et q-modules sur $\mathbb{Z}$

L'objet de ce paragraphe est de rappeler quelques points, très classiques, voir par exemple [Ser70, Chap. V][MH73, Chap. II], de la théorie des b-modules et q-modules sur $\mathbb{Z}$.

Pour organiser ces rappels, numérotés 1, 2 et 3 ci-après, il est commode de disposer du concept d'anneau de Witt, voir par exemple [MH73, Chap. I, §7]. Rappelons-en la définition. Soit A un anneau commutatif, l'ensemble des classes d'isomorphisme de b-modules sur A, disons $\mathcal{B}(A)$, est un monoïde commutatif pour la somme orthogonale, on note $\mathrm{W}(A)$ le monoïde quotient $\mathcal{B}(A)/\mathcal{N}(A)$, $\mathcal{N}(A)$ désignant le sous-monoïde engendré par les classes d'isomorphismes des b-modules neutres (un b-module est dit *neutre* s'il possède un *lagrangien*, c'est-à-dire un facteur direct qui est son propre orthogonal) ; le monoïde $\mathrm{W}(A)$ est un groupe et le produit tensoriel des b-modules en fait un anneau commutatif. Le groupe abélien $\mathrm{WQ}(A)$ est défini *mutatis mutandis* en termes de q-modules sur A, voir par exemple [MH73, App. 1] (rappelons que dans ce cas les q-modules neutres sont en fait hyperboliques, voir Proposition 1.2) ; $\mathrm{WQ}(A)$ est naturellement un $\mathrm{W}(A)$-module.

Venons-en maintenant au cas $A = \mathbb{Z}$.

1) Le premier des points auxquels nous faisions allusion plus haut, est la détermination de $\mathrm{W}(\mathbb{Z})$. Le résultat est le suivant : l'homomorphisme canonique $\mathrm{W}(\mathbb{Z}) \to \mathrm{W}(\mathbb{R})$ est un isomorphisme. Ceci peut être reformulé de deux façons :

– L'homomorphisme "signature", disons $\tau : \mathrm{W}(\mathbb{Z}) \to \mathbb{Z}$, est un isomorphisme. Précisons ce que l'on entend ici par *signature*. Soit E un b-espace vectoriel sur $\mathbb{R}$, un tel E est isomorphe à un b-espace vectoriel de la forme

$$\langle +1, +1, \ldots, +1, -1, -1, \ldots, -1 \rangle$$

et la signature de E, notée $\tau(E)$ ci-après, est la différence $n_+ - n_-$ entre le nombre de $+1$ et le nombre de -1 qui apparaissent ci-dessus. Il est clair que l'homomorphisme $\tau : \mathrm{W}(\mathbb{R}) \to \mathbb{Z}$ est un isomorphisme.

– L'homomorphisme "unité", disons $\eta : \mathbb{Z} \to \mathrm{W}(\mathbb{Z})$, est un isomorphisme. Pour une très jolie démonstration de ce résultat qui n'utilise pas le théorème de Hasse-Minkowski, voir [MH73, Chap. IV, §2].

Scholie 2.1. *Soient L_1 et L_2 deux* b*-modules sur $\mathbb{Z}$. Les deux conditions suivantes sont équivalentes :*
(i) les deux b*-espaces vectoriels sur $\mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} L_1$ et $\mathbb{Q} \otimes_{\mathbb{Z}} L_2$, sont isomorphes ;*
(ii) les deux b*-espaces vectoriels sur $\mathbb{R}$, $\mathbb{R} \otimes_{\mathbb{Z}} L_1$ et $\mathbb{R} \otimes_{\mathbb{Z}} L_2$, sont isomorphes.*

2) Le deuxième point concerne la théorie des "vecteurs de Wu". Soit L un b-module sur $\mathbb{Z}$; comme $\mathbb{F}_2 \otimes_{\mathbb{Z}} L$ est un b-espace vectoriel sur $\mathbb{F}_2$, il existe un élément u de L, bien défini modulo $2L$, tel que l'on a

$$x.x \equiv u.x \pmod 2$$

pour tout x dans L. Nous appelons u un *vecteur de Wu* (on rencontre aussi la terminologie "vecteur caractéristique", la terminologie "vecteur de Wu" fait référence aux classes définies dans la cohomologie modulo 2 des variétés compactes par Wen-Tsün Wu [Wu50]). On constate que la réduction modulo 8 de l'entier $u.u$ est indépendante du choix de u et que la correspondance $L \mapsto u.u$ induit un homomorphisme d'anneaux commutatifs unitaires, disons $\sigma : \mathrm{W}(\mathbb{Z}) \to \mathbb{Z}/8$. On observera que l'on peut ci-dessus remplacer $\mathbb{Z}$ par $\mathbb{Z}_2$ et que l'homomorphisme σ se factorise à travers $\mathrm{W}(\mathbb{Z}_2)$. Enfin, la réduction modulo 2 de σ se factorise par un homomorphisme $\mathrm{W}(\mathbb{F}_2) \to \mathbb{Z}/2$ qui coïncide avec l'isomorphisme "dimension modulo 2".

Compte tenu de ce que nous avons rappelé plus haut sur $\mathrm{W}(\mathbb{Z})$, σ s'identifie à la réduction modulo 8 de $\mathbb{Z}$ dans $\mathbb{Z}/8$.

Scholie 2.2. (a) *Soient L un* b*-module sur $\mathbb{Z}$ et u un vecteur de Wu de L. Alors on a la congruence*

$$\tau(L) \equiv u.u \pmod 8 \qquad .$$

(b) *La signature d'un* q*-module sur $\mathbb{Z}$ est divisible par* 8.

3) Le dernier point est plus technique. Soit L un b-module sur $\mathbb{Z}$ *impair*, c'est-à-dire non pair. Soit M le sous-module d'indice 2 de L constitué des vecteurs x vérifiant $x.x \equiv 0 \bmod 2$. L'application $M \to \mathbb{Z}, x \mapsto \frac{x.x}{2}$ fait de M un $\widetilde{\mathrm{q}}$-module dont on détermine le résidu ci-après.

On considère la suite exacte

$$0 \to L/M \to M^\sharp/M \to M^\sharp/L \to 0 \qquad .$$

Soient u un vecteur de Wu de L et v un élément de L avec $v.v \equiv 1 \bmod 2$ (ou encore $u.v \equiv 1 \bmod 2$) ; les quotients L/M et $M^\sharp/L$ sont des groupes cycliques d'ordre 2 respectivement engendrés par les classes de v et $\frac{u}{2}$ (L/M est en fait un lagrangien du e-module sous-jacent au qe-module $\operatorname{rés} M$ et $M^\sharp/L$ est canoniquement isomorphe au dual de ce lagrangien). La suite exacte ci-dessus est scindable si et seulement si u appartient à M c'est-à-dire si l'on a $u.u \equiv 0 \bmod 2$ ou encore, compte tenu de ce que nous avons rappelé dans le point 2, si la dimension de L est paire. On distingue donc deux cas, suivant la parité de cette dimension :

– Dans le cas $\dim L \equiv 1 \bmod 2$, $\operatorname{rés} M$ est isomorphe à $\mathbb{Z}/4$ et engendré par la classe de $\frac{u}{2}$; on a l'égalité dans $\mathbb{Q}/\mathbb{Z}$

$$\mathrm{q}(x\frac{u}{2}) = \frac{\tau(L)}{8}\, x^2$$

pour tout x dans $\mathbb{Z}$.

– Dans le cas $\dim L \equiv 0 \bmod 2$, $\operatorname{rés} M$ est isomorphe à $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ et engendré par les classes de $\frac{u}{2}$ et v ou encore les classes de $\frac{u}{2}$ et $\frac{u}{2} - v$; on a l'égalité dans $\mathbb{Q}/\mathbb{Z}$

$$\mathrm{q}(x\frac{u}{2} + y(\frac{u}{2} - v)) = \frac{\tau(L)}{8}\,(x^2 + y^2) + (\frac{\tau(L)}{4} + \frac{1}{2})\, xy$$

pour tous x et y dans $\mathbb{Z}$.

On voit par inspection que l'équation $\mathrm{q}(\iota) = 0$ avec $\iota \in \operatorname{rés} M - \{0\}$ n'a aucune solution pour $\tau(L) \not\equiv 0 \bmod 8$ et que pour $\tau(L) \equiv 0 \bmod 8$ elle en a exactement 2 à savoir $\frac{u}{2}$ et $\frac{u}{2} - v$. On a donc au bout du compte obtenu en particulier l'énoncé suivant :

Scholie 2.3. *Soient L un* b*-module sur $\mathbb{Z}$ impair et M le sous-module d'indice 2 de L constitué des vecteurs x vérifiant $x.x \equiv 0 \bmod 2$ (M est donc un $\widetilde{\mathrm{q}}$-module sur $\mathbb{Z}$). Les conditions suivantes sont équivalentes :*
(i) le qe*-module* $\operatorname{rés} M$ *est isomorphe à* $\mathrm{H}(\mathbb{Z}/2)$ *;*
(ii) la signature de L est divisible par 8.

Partition en deux classes des vecteurs de Wu

Soient L un b-module sur $\mathbb{Z}$ impair et M le sous-module d'indice 2 de L constitué des vecteurs x vérifiant $x.x \equiv 0 \bmod 2$.

Notons $\mathrm{Wu}(L)$ l'ensemble des vecteurs de Wu de L. L'action de L sur $\mathrm{Wu}(L)$ définie par $(u, x) \mapsto u+2x$ (u dans $\mathrm{Wu}(L)$ et x dans L) est libre et transitive. L'action, induite par restriction, de M sur $\mathrm{Wu}(L)$ a exactement deux orbites (celles de u et $u - 2v$, u désignant un vecteur de Wu arbitraire de L et v un élément de L avec $v.v \equiv 1 \bmod 2$) ; nous dirons que deux vecteurs de Wu dans la même orbite sont *équivalents*. Soient u_1 et u_2 deux vecteurs de Wu non équivalents ; on peut paraphraser la discussion qui précède le scholie 2.3 de la façon suivante :

– Les classes de $\frac{1}{2}u_1$ et $\frac{1}{2}u_2$ engendrent le groupe abélien $\operatorname{rés} M$.

– Si la dimension de L est impaire ces classes sont d'ordre 4 et opposées.

– Si la dimension de L est paire ces classes sont d'ordre 2 et constituent une base du $\mathbb{Z}/2$-espace vectoriel $\operatorname{rés} M$.

– On a les égalités suivantes dans $\mathbb{Q}/\mathbb{Z}$:

$$\mathrm{q}(\frac{u_1}{2}) = \frac{\tau(L)}{8} \quad , \quad \mathrm{q}(\frac{u_2}{2}) = \frac{\tau(L)}{8} \quad , \quad \mathrm{q}(\frac{u_1}{2} + \frac{u_2}{2}) = \frac{1 + \dim L}{2} \qquad ;$$

on observera que ces égalités déterminent dans les deux cas la forme quadratique d'enlacement $\mathrm{q} : \operatorname{rés} M \to \mathbb{Q}/\mathbb{Z}$.

Voici une illustration de ce qui précède. Soit n un entier naturel ; on considère la forme bilinéaire symétrique "euclidienne"

$$\mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z} \quad , \quad ((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)) \mapsto \sum_{i=1}^{n} x_i y_i \qquad .$$

Muni de cette forme, $\mathbb{Z}^n$ est un b-module sur $\mathbb{Z}$ impair que l'on note I_n. On note D_n le sous-module d'indice 2 de I_n constitué des vecteurs x vérifiant $x.x \equiv 0 \bmod 2$ ou encore $\sum_{i=1}^{n} x_i \equiv 0 \bmod 2$ (cette notation évoque sciemment la théorie des systèmes de racines, nous reviendrons sur ce thème au paragraphe 3). Soit $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ la base canonique de I_n ; on observe que

les vecteurs $u_1 := \varepsilon_1+\varepsilon_2+\ldots+\varepsilon_n$ et $u_2 := -\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_n$ sont des vecteurs de Wu pour I_n et que ces vecteurs sont non équivalents. Si n est divisible par 8 alors le qe-module $\operatorname{rés}\mathrm{D}_n$ peut être explicité de la façon suivante :

– comme $\mathbb{Z}$-module, $\operatorname{rés}\mathrm{D}_n$ est un $\mathbb{Z}/2$-espace vectoriel de dimension 2 dont les classes des vecteurs $\iota_1 := \frac{1}{2}u_1$ et $\iota_2 := \frac{1}{2}u_2$ constituent une base ;

– sa forme quadratique d'enlacement est déterminée par $\mathrm{q}(\iota_1) = 0$, $\mathrm{q}(\iota_2) = 0$ et $\iota_1.\iota_2 = \frac{1}{2}$.

Les points (b) et (c) de la proposition 1.1 montrent que le réseau de $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{I}_n$ engendré par D_n et $\frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)$ est un q-module sur $\mathbb{Z}$ que l'on note E_8 pour $n = 8$ et E_n ou D_n^+ pour $n \geq 16$ (et $n \equiv 0 \bmod 8$).

Scholie 2.4. *L'homomorphisme composé*

$$\mathrm{WQ}(\mathbb{Z}) \xrightarrow{\text{oubli}} \mathrm{W}(\mathbb{Z}) \xrightarrow{\tau} \mathbb{Z}$$

induit un isomorphisme (de $\mathrm{W}(\mathbb{Z})$*-modules) de* $\mathrm{WQ}(\mathbb{Z})$ *sur l'idéal* $8\mathbb{Z}$ *; le groupe* $\mathrm{WQ}(\mathbb{Z})$ *est infini cyclique engendré par la classe de* E_8*.*

Démonstration. Il suffit d'observer que l'oubli $\mathrm{WQ}(\mathbb{Z}) \to \mathrm{W}(\mathbb{Z})$ est injectif.

Genre d'un q-module sur $\mathbb{Z}$

Cet intertitre fait référence au point (b) de l'énoncé ci-dessous.

Scholie 2.5. *Soient* L *un* q*-module sur* $\mathbb{Z}$ *et* p *un nombre premier.*

(a) *Le* q*-espace vectoriel* $\mathbb{F}_p \otimes_{\mathbb{Z}} L$ *est hyperbolique.*

(b) *Le* q*-module* $\mathbb{Z}_p \otimes_{\mathbb{Z}} L$ *est hyperbolique.*

Démonstration. Le premier point implique le second ; en effet, deux q-modules L_1 et L_2 sur $\mathbb{Z}_p$ sont isomorphes si et seulement si les q-espaces vectoriels $\mathbb{F}_p \otimes_{\mathbb{Z}_p} L_1$ et $\mathbb{F}_p \otimes_{\mathbb{Z}_p} L_2$ le sont. Venons-en au point (a). Il suffit de montrer que l'homomorphisme naturel $\mathrm{WQ}(\mathbb{Z}) \to \mathrm{WQ}(\mathbb{F}_p)$ est trivial. Le cas p impair, facile, est laissé au lecteur. Pour $p = 2$, on peut invoquer les arguments suivants :

– L'invariant de Arf, disons $\mathrm{Arf} : \mathrm{WQ}(\mathbb{F}_2) \to \mathrm{H}^1_{\acute{e}t}(\mathbb{F}_2; \mathbb{Z}/2) \cong \mathbb{Z}/2$, est un isomorphisme.

– Le groupe $\mathrm{H}^1_{\acute{e}t}(\mathbb{Z}; \mathbb{Z}/2)$ est trivial.

L'argument ci-dessus peut être remplacé par l'argument ci-dessous, plus prosaïque :

– L'homomorphisme $\mathrm{WQ}(\mathbb{Z}) \to \mathrm{WQ}(\mathbb{F}_2)$ se factorise à travers $\mathrm{WQ}(\mathbb{Z}_2)$ et le déterminant d'un q-module L sur $\mathbb{Z}_2$ est égal à la classe dans $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$ de l'élément $(-1)^{\frac{\dim L}{2}}\,(-3)^{\mathrm{Arf}(\mathbb{F}_2\otimes_{\mathbb{Z}_2} L)}$ (pour se convaincre de cette égalité observer par exemple qu'un tel L se décompose en une somme orthogonale de q-modules de dimension 2, chacun muni d'une base (e, f) avec $e.f = 1$). $\square$

On peut alternativement déduire l'énoncé 2.5 de l'énoncé ci-dessous dont la démonstration est laissée au lecteur :

Proposition 2.6. *Soit p un nombre premier ; soient L_1 et L_2 deux* q*-modules sur $\mathbb{Z}_p$. Les conditions suivantes sont équivalentes :*
(i) L_1 et L_2 sont isomorphes ;
(ii) les deux q*-espaces vectoriels sur $\mathbb{F}_p$, $\mathbb{F}_p \otimes_{\mathbb{Z}} L_1$ et $\mathbb{F}_p \otimes_{\mathbb{Z}} L_2$, sont isomorphes ;*
(iii) L_1 et L_2 ont même dimension et même déterminant ;
(iv) les deux q*-espaces vectoriels sur $\mathbb{Q}_p$, $\mathbb{Q}_p \otimes_{\mathbb{Z}} L_1$ et $\mathbb{Q}_p \otimes_{\mathbb{Z}} L_2$, sont isomorphes ;*

En vue de futures références, nous ajoutons aux rappels précédents, les deux énoncés suivants qui sont des raffinements de l'énoncé 2.1.

Théorème 2.7. *Soient L_1 et L_2 deux* q*-modules sur $\mathbb{Z}$. On suppose que le* q*-espace vectoriel sur $\mathbb{R}$, $\mathbb{R} \otimes_{\mathbb{Z}} L_1$ est indéfini, alors les deux conditions suivantes sont équivalentes :*
(i) L_1 et L_2 sont isomorphes ;
(ii) les deux q*-espaces vectoriels sur $\mathbb{R}$, $\mathbb{R}\otimes_{\mathbb{Z}} L_1$ et $\mathbb{R}\otimes_{\mathbb{Z}} L_2$, sont isomorphes.*

Théorème 2.8. *Soient L_1 et L_2 deux* q*-modules sur $\mathbb{Z}$ et p un nombre premier. Les deux conditions suivantes sont équivalentes :*
(i) les deux q*-modules sur $\mathbb{Z}[\frac{1}{p}]$, $\mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} L_1$ et $\mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} L_2$, sont isomorphes ;*
(ii) les deux q*-espaces vectoriels sur $\mathbb{R}$, $\mathbb{R}\otimes_{\mathbb{Z}} L_1$ et $\mathbb{R}\otimes_{\mathbb{Z}} L_2$, sont isomorphes.*

Les deux énoncés peuvent se démontrer à l'aide du théorème d'approximation forte pour les groupes Spin [PR94]. On peut aussi démontrer 2.7 de la façon suivante : commencer par observer que 2.1 implique qu'un b-module sur $\mathbb{Z}$ indéfini représente zéro et achever comme le fait Serre dans [Ser70, Ch. V, §3].

Terminologie classique dans le cas défini positif

Soit V un espace euclidien, en clair un $\mathbb{R}$-espace vectoriel de dimension finie muni d'une forme bilinéaire symétrique définie positive (appelée produit

scalaire). Dans ce contexte, un *réseau* de V est un sous-groupe discret cocompact. Soit L un tel réseau, on dit que L est *entier* si le produit scalaire $x.y$ est entier pour tous x et y dans L ; muni de la forme bilinéaire symétrique induite par le produit scalaire, L est un $\widetilde{\mathrm{b}}$-module sur $\mathbb{Z}$, défini positif (c'est-à-dire que le $\widetilde{\mathrm{b}}$-espace vectoriel $\mathbb{R} \otimes_{\mathbb{Z}} L$ est défini positif). Réciproquement un $\widetilde{\mathrm{b}}$-module sur $\mathbb{Z}$ défini positif L est un réseau entier dans l'espace euclidien $\mathbb{R} \otimes_{\mathbb{Z}} L$. Un réseau entier L de V est appelé *réseau unimodulaire* s'il est de covolume 1 (l'adjectif entier est donc implicite dans ce cas), en d'autres termes si le $\widetilde{\mathrm{b}}$-module L est en fait un b-module. Un réseau entier L de V est dit *pair* si $x.x$ est pair pour tout x dans L, en d'autres termes si le $\widetilde{\mathrm{b}}$-module L est en fait un $\widetilde{\mathrm{q}}$-module. Un q-module sur $\mathbb{Z}$ défini positif L est donc un réseau unimodulaire pair dans l'espace euclidien $\mathbb{R} \otimes_{\mathbb{Z}} L$.

Dans ce mémoire nous emploierons plus souvent la terminologie classique, réseau unimodulaire pair (resp. réseau unimodulaire, réseau entier pair, réseau entier), que la terminologie q-module (resp. b-module, $\widetilde{\mathrm{q}}$-module, $\widetilde{\mathrm{b}}$-module) sur $\mathbb{Z}$ défini positif (en vérité, la terminologie "q-module", "b-module", ..., n'est guère employée que par le second auteur !).

3. Systèmes de racines et réseaux unimodulaires pairs

Les réseaux unimodulaires pairs qui apparaissent en dimension 8, 16 et 24, à l'exception du réseau de Leech, sont tous construits à partir de certains systèmes de racines par un procédé que nous allons décrire.

En fait les systèmes de racines en question sont certaines sommes directes de systèmes de racines de type $\mathbf{A}_l$, $\mathbf{D}_l$, $\mathbf{E}_6$, $\mathbf{E}_7$ et $\mathbf{E}_8$; nous dirons que de telles sommes directes sont des sytèmes de racines de *type ADE* (la terminologie anglo-saxonne, justifiée par la considération du graphe de Dynkin, est *simply laced*). Il est clair que les systèmes de racines irréductibles de type ADE sont caractérisés, parmi tous les systèmes de racines irréductibles, par la propriété que toutes les racines sont de même longueur. Le lecteur vérifiera sans peine que l'on peut prendre comme définition des systèmes de racines de type ADE, la définition *ad hoc* suivante, variante de [Bou81b, Ch. VI, §1, Déf. 1] :

Définition 3.1. *Soient V un espace euclidien et R un sous-ensemble de V constitué de vecteurs α vérifiant $\alpha.\alpha = 2$. Nous dirons que R est un* système de racines de type ADE *dans V si les conditions suivantes sont vérifiées :*

(I) *Le sous-ensemble R est fini et engendre V.*

(II) *Pour tout α dans R la réflexion orthogonale $x \mapsto x - (\alpha.x)\,\alpha$ de V (notée s_α) laisse stable R.*

(III) *Pour tous α et β dans R le produit scalaire $\alpha.\beta$ est entier.*

Le groupe de Weyl $\mathrm{W}(R)$ engendré par les s_α apparaît ici comme un sous-groupe du groupe orthogonal de V ; il en est de même du groupe (fini) $\mathrm{A}(R)$ constitué des automorphismes du $\mathbb{R}$-espace vectoriel V qui laissent stable R (ceci résulte par exemple de [Bou81b, Ch. VI, §1, Prop. 3 et Prop. 7]). Si l'on identifie V et V^* *via* le produit scalaire alors l'application structurelle $\alpha \mapsto \alpha^\vee$ est l'identité, en particulier les deux systèmes de racines R et $R^\vee$ coïncident.

Soit $R \subset V$ un système de racines de type ADE ; le réseau de V engendré par R, noté $\mathrm{Q}(R)$, est un réseau entier pair et R s'identifie au sous-ensemble de $\mathrm{Q}(R)$ constitué des éléments α vérifiant $\alpha.\alpha = 2$ (cette dernière propriété n'est pas, *a priori*, une conséquence immédiate de 3.1, on peut se convaincre de ce qu'elle est satisfaite en observant qu'elle l'est pour les systèmes de racines $\mathbf{A}_l$, $\mathbf{D}_l$, $\mathbf{E}_6$, $\mathbf{E}_7$ et $\mathbf{E}_8$). On observera que $\mathrm{A}(R)$ s'identifie au groupe des automorphismes de $\mathrm{Q}(R)$, comme $\widetilde{\mathrm{q}}$-module sur $\mathbb{Z}$. La notation $\mathrm{Q}(R)$ est celle de Bourbaki [Bou81b] qui appelle *poids radiciels* les éléments de ce réseau. Réciproquement, soient L un réseau entier (en d'autres termes un $\widetilde{\mathrm{b}}$-module sur $\mathbb{Z}$, défini positif), $\mathrm{R}(L)$ le sous-ensemble (fini) de L constitué des éléments α vérifiant $\alpha.\alpha = 2$, que l'on appelle les *racines* de L, et $\mathrm{V}(L)$ le sous-espace de $\mathbb{R}\otimes_{\mathbb{Z}} L$ engendré par $\mathrm{R}(L)$, alors $\mathrm{R}(L)$ est un système de racines dans $\mathrm{V}(L)$ de type ADE (prendre $\Lambda = \{2\}$ au début du n° 4 de [Bou81b, Ch. VI, §4]). En conclusion, la classification des systèmes de racines de type ADE coïncide avec celle des réseaux entiers (pairs) engendrés par leurs racines.

Le procédé qui permet d'obtenir un réseau unimodulaire pair à partir de certains systèmes de racines de type ADE est simplement un cas particulier du procédé général fourni par la proposition 1.1. Soit R un système de racines de type ADE. Supposons que le qe-module $\operatorname{rés}\mathrm{Q}(R)$ possède un lagrangien I, alors l'image réciproque de I dans le réseau $\mathrm{Q}(R)^\sharp$, par l'application canonique $\mathrm{Q}(R)^\sharp \to \mathrm{Q}(R)^\sharp/\mathrm{Q}(R) =: \operatorname{rés}\mathrm{Q}(R)$, est un q-module (voir les points (b) et (c) de la proposition 1.1) sur $\mathbb{Z}$ défini positif, en d'autres termes un réseau unimodulaire pair. Le réseau $\mathrm{Q}(R)^\sharp$ est le réseau des *poids* du système de racines R ; il est noté $\mathrm{P}(R)$ dans [Bou81b].

Exemple

Soit $n \geq 1$ un entier ; on munit le $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$ de sa structure euclidienne canonique et on note $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ sa base canonique.

Considérons à nouveau le réseau entier pair $\mathrm{D}_n \subset \mathrm{I}_n := \mathbb{Z}^n \subset \mathbb{R}^n$ introduit au paragraphe 2. Le système de racines $\mathbf{D}_n$, $n \geq 3$, est défini par l'égalité $\mathbf{D}_n := \mathrm{R}(\mathrm{D}_n)$; $\mathrm{R}(\mathrm{D}_n)$ engendre D_n pour $n \geq 2$. Rappelons ce que l'on a vu au paragraphe 2 :

– Le qe-module rés D_n possède un lagrangien si et seulement si n est divisible par 8, ce que l'on suppose ci-après.

– On a dans ce cas un isomorphisme de qe-modules rés $\mathrm{D}_n \cong \mathrm{H}(\mathbb{Z}/2)$ et les deux lagrangiens de rés D_n sont respectivement engendrés par les classes des vecteurs $\frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)$ et $\frac{1}{2}(-\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)$; on observera incidemment que ces deux vecteurs sont échangés par l'automorphisme involutif $(x_1, x_2, \ldots x_n) \mapsto (-x_1, x_2, \ldots x_n)$ de D_n.

On a noté E_n le réseau engendré par D_n et $\frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)$; E_n est l'exemple le plus simple de réseau unimodulaire pair obtenu par le procédé décrit ci-dessus (pour des exemples plus sophistiqués, voir la classification des réseaux unimodulaires pairs de dimension 24 évoquée ci-après).

Le système de racines $\mathbf{E}_8$ est défini par l'égalité $\mathbf{E}_8 := \mathrm{R}(\mathrm{E}_8)$; $\mathrm{R}(\mathrm{E}_8)$ engendre E_8, en d'autres termes on a l'égalité $\mathrm{E}_8 := \mathrm{Q}(\mathbf{E}_8)$.

Pour $n \geq 16$ (et $n \equiv 0 \bmod 8$) on a $\mathrm{R}(\mathrm{E}_n) = \mathrm{R}(\mathrm{D}_n) = \mathbf{D}_n$; le sous-groupe engendré par $\mathrm{R}(\mathrm{E}_n)$ est d'indice 2 dans E_n.

Le réseau unimodulaire pair E_n est aussi noté D_n^+ (au moins pour $n \geq 16$) ; cette notation est justifiée par le fait que le groupe des automorphismes de D_n opère transitivement sur l'ensemble des deux lagrangiens de rés D_n.

Classification des réseaux unimodulaires pairs en dimension 8, 16 et 24

Cette classification est due à Louis J. Mordell en dimension 8, à Ernst Witt en dimension 16 et à Hans-Volker Niemeier en dimension 24 [Ni73]. Ci-après, nous évoquons la stratégie ingénieuse développée par Boris Venkov [Ven80] pour retrouver la classification de Niemeier. Sa stratégie fonctionne également en dimension 8 et 16. En effet, l'idée de départ de Venkov est de considérer des séries thêta "à coefficients harmoniques de degré 2" et d'observer que ces séries sont identiquement nulles car toute forme modulaire parabolique pour $\mathrm{SL}_2(\mathbb{Z})$ de poids $14 = \frac{24}{2} + 2$ est nulle, les arguments qu'il utilise ensuite ne font plus intervenir de façon essentielle que la dimension des réseaux est 24 ; or toute forme modulaire parabolique pour $\mathrm{SL}_2(\mathbb{Z})$ de poids $\frac{n}{2} + 2$ est également nulle pour $n = 8, 16$.

En considérant le "coefficient de $e^{2\imath\pi\tau}$" dans les séries thêta évoquées ci-dessus, Venkov obtient l'identité suivante :

Proposition 3.2. *Soit L un réseau unimodulaire pair de dimension $n = 8, 16, 24$. Alors on a l'identité*

$$\sum_{\alpha \in \mathrm{R}(L)} (\alpha.x)^2 \;=\; \frac{2\,|\mathrm{R}(L)|}{n}\; x.x$$

pour tout x dans l'espace euclidien $\mathbb{R} \otimes_{\mathbb{Z}} L$ (la notation $|-|$ désignant le cardinal d'un ensemble fini).

Venkov déduit ensuite de cette identité l'énoncé ci-dessous :

Proposition-Définition 3.3. *Soit L un réseau unimodulaire pair de dimension $n = 8, 16, 24$. Si l'ensemble $\mathrm{R}(L)$ des racines de L (rappelons qu'il s'agit là des éléments α de L vérifiant $\alpha.\alpha = 2$) est non vide alors il vérifie les propriétés suivantes :*

(a) *L'ensemble $\mathrm{R}(L)$ est un système de racines (de type ADE) de rang n (dans $\mathbb{R} \otimes_{\mathbb{Z}} L$), en d'autres termes $\mathrm{R}(L)$ engendre le $\mathbb{R}$-espace vectoriel $\mathbb{R} \otimes_{\mathbb{Z}} L$.*

(b) *Toutes les composantes irréductibles du système de racines $\mathrm{R}(L)$ ont le même nombre de Coxeter, que l'on appelle le nombre de Coxeter de L et que l'on note $\mathrm{h}(L)$; un tel système de racines sera dit* équicoxeter.

(c) *On a $|\mathrm{R}(L)| = n\,\mathrm{h}(L)$.*

Remarques

– Venkov démontre simultanément (b) et (c) à l'aide de 3.2 et [Bou81b, Ch. VI, §1, Prop. 32]. On peut également démontrer (c) à partir de (b) en invoquant la relation $|R| = nh$ qui lie nombre de racines, rang et nombre de Coxeter, pour tout système de racines irréductible réduit (voir [Hu90, 3.18][Bou81b, Ch. VI, §1, Exc. 20]).

– Puisque le nombre de Coxeter de la somme directe de deux systèmes de racines est le p.p.c.m. de leurs nombres de Coxeter (se rappeler que le nombre de Coxeter d'un système de racines est défini comme l'ordre d'une transformation de Coxeter), $\mathrm{h}(L)$ est aussi le nombre de Coxeter du système de racines $\mathrm{R}(L)$.

Scholie 3.4. *Soit L un réseau unimodulaire pair de dimension 24 avec $\mathrm{R}(L) \neq \emptyset$. Alors on a l'identité*

$$\sum_{\alpha \in \mathrm{R}(L)} (\alpha.x)^2 \;=\; 2\,\mathrm{h}(L)\; x.x$$

pour tout x dans l'espace euclidien $\mathbb{R} \otimes_{\mathbb{Z}} L$.

Corollaire 3.5. *Tout réseau unimodulaire pair de dimension* 8 *est isomorphe à* E_8.

Démonstration. Soit L un tel réseau. La série thêta de L, modulaire de poids 4 pour $\mathrm{SL}_2(\mathbb{Z})$, est nécessairement égale à la série d'Eisenstein normalisée $\mathbb{E}_4$ (la surutilisation des E est responsable de cette notation inhabituelle). On en déduit $|\mathrm{R}(L)| = 240$ et $\mathrm{h}(L) = 30$. Cette dernière égalité force par inspection $\mathrm{R}(L) \simeq \mathbf{E}_8$. Comme le réseau $\mathrm{E}_8 = \mathrm{Q}(\mathbf{E}_8)$ est unimodulaire, on a bien $L \simeq \mathrm{E}_8$. □

Corollaire 3.6. *Tout réseau unimodulaire pair de dimension* 16 *est isomorphe à* D_{16}^+ *ou à* $\mathrm{E}_8 \oplus \mathrm{E}_8$ *(et ces deux réseaux ne sont pas isomorphes).*

Démonstration. Soit L un tel réseau. La série thêta de L est nécessairement égale à la série d'Eisenstein normalisée $\mathbb{E}_8 = \mathbb{E}_4^2$. On en déduit $|\mathrm{R}(L)| = 480$ et $\mathrm{h}(L) = 30$. Cette dernière égalité force par inspection $\mathrm{R}(L) \simeq \mathbf{D}_{16}$ ou $\mathrm{R}(L) \simeq \mathbf{E}_8 \coprod \mathbf{E}_8$ (nous notons $\coprod$ la *somme directe des systèmes de racines*).

Dans le cas $\mathrm{R}(L) \simeq \mathbf{E}_8 \coprod \mathbf{E}_8$ on conclut comme précédemment que l'on a $L \simeq \mathrm{E}_8 \oplus \mathrm{E}_8$.

Dans le cas $\mathrm{R}(L) \simeq \mathbf{D}_{16}$, D_{16} apparaît, à isomorphisme près, comme un sous-réseau de L ; on peut donc supposer que l'on a dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ les inclusions $\mathrm{D}_{16} \subset L \subset \mathrm{D}_{16}^\sharp$. Alors L/D_{16} est un lagrangien du qe-module $\mathrm{rés}\,\mathrm{D}_{16}$ et l'on voit que l'on a $L \simeq \mathrm{D}_{16}^+$. □

Venons-en maintenant au choses sérieuses, c'est-à-dire à la détermination des classes d'isomorphisme de réseaux unimodulaires pairs de dimension 24.

Soit L un réseau unimodulaire pair de dimension 24 avec $\mathrm{R}(L) \neq \emptyset$. Les propriétés (a) et (b) de la proposition 3.3 nous disent que $\mathrm{R}(L)$ est un système de racines de type ADE, de rang 24 et équicoxeter. Venkov commence par expliciter (par inspection) la liste des classes d'isomorphisme de tels systèmes de racines. Cette liste comporte 23 éléments $\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_{23}$. Pour la liste complète nous renvoyons à la deuxième colonne de [CS99, Ch. 16, Table 16.1] (Table I.1 de notre mémoire) ; le lecteur notera que nous indexons les termes de cette colonne par les entiers $1, 2, \ldots, 23$, plutôt que par les lettres grecques $\alpha, \beta, \ldots, \psi$, comme le font Conway et Sloane. Voici quelques exemples :

$\mathbf{R}_1 = \mathbf{D}_{24}$, $\mathbf{R}_2 = \mathbf{D}_{16} \coprod \mathbf{E}_8$, $\mathbf{R}_3 = \mathbf{E}_8 \coprod \mathbf{E}_8 \coprod \mathbf{E}_8$, $\mathbf{R}_4 = \mathbf{A}_{24}$, $\mathbf{R}_5 = \mathbf{D}_{12} \coprod \mathbf{D}_{12}$, $\mathbf{R}_6 = \mathbf{A}_{17} \coprod \mathbf{E}_7$, $\mathbf{R}_7 = \mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{E}_7$, $\mathbf{R}_{23} = \mathbf{A}_1 \coprod \mathbf{A}_1 \coprod \cdots \coprod \mathbf{A}_1$ (24 composantes irréductibles toutes égales à $\mathbf{A}_1$).

Avant de poursuivre notre exposition des arguments de Venkov il nous faut faire quelques observations et rappels numérotés 1, 2 et 3 ci-aprés.

1) Soit M un $\widetilde{\mathrm{q}}$-module sur $\mathbb{Z}$. Si M est défini positif alors le quotient $\operatorname{rés} M := M^\sharp/M$ possède, en plus de sa structure de qe-module, une structure supplémentaire que nous nous proposons de décrire. Soient ξ un élément de $\operatorname{rés} M$ et $\gamma : M^\sharp \to \operatorname{rés} M$ la surjection canonique, on définit une application qm : $\operatorname{rés} M \to \mathbb{Q} \cap [0, \infty[$ en posant

$$\mathrm{qm}(\xi) = \inf_{x \in \gamma^{-1}(\xi)} \mathrm{q}(x) \qquad .$$

Il est clair que cette application fait commuter le diagramme suivant

$$\begin{tikzcd} & \mathbb{Q} \cap [0, \infty[\arrow[d] \\ \operatorname{rés} M \arrow[ur, "\mathrm{qm}"] \arrow[r, "\mathrm{q}"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

dans lequel la flèche verticale est la restriction de la réduction modulo $\mathbb{Z}$. Nous dirons que $\operatorname{rés} M$ muni de cette structure supplémentaire est un qe-*module de Venkov*.

Exemple. Soit $n > 0$ un entier divisible par 8 ; on prend $M = \mathrm{D}_n$. On a vu au paragraphe 2 que $\operatorname{rés} \mathrm{D}_n$ est isomorphe à $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ muni de la forme quadratique d'enlacement définie par $\mathrm{q}(\bar{0}, \bar{0}) = 0$, $\mathrm{q}(\bar{1}, \bar{0}) = 0$, $\mathrm{q}(\bar{0}, \bar{1}) = 0$ et $\mathrm{q}(\bar{1}, \bar{1}) = \frac{1}{2}$; l'application qm est donnée quant à elle par $\mathrm{qm}(\bar{0}, \bar{0}) = 0$, $\mathrm{qm}(\bar{1}, \bar{0}) = \frac{n}{8}$, $\mathrm{qm}(\bar{0}, \bar{1}) = \frac{n}{8}$ et $\mathrm{qm}(\bar{1}, \bar{1}) = \frac{1}{2}$.

La proposition suivante est évidente :

Proposition 3.7. *Soit M un réseau entier pair. Soient I un sous-module de $\operatorname{rés} M$ avec $I \subset I^\perp$ et L le réseau entier associé. Alors les deux conditions suivantes sont équivalentes :*
(i) on a $\mathrm{R}(L) = \mathrm{R}(M)$;
(ii) on a $\mathrm{qm}(\xi) > 1$ pour tout ξ dans $I - \{0\}$.

Exemple. On reprend l'exemple précédent. La proposition montre que l'on a $\mathrm{R}(\mathrm{E}_n) = \mathrm{R}(\mathrm{D}_n)$ pour $n \geq 16$ et $\mathrm{R}(\mathrm{E}_8) \supsetneqq \mathrm{R}(\mathrm{D}_8)$.

2) Soit $R \subset V$ un système de racines de type ADE ; on rappelle maintenant comment déterminer l'application qm : $\operatorname{rés} \mathrm{Q}(R) \to \mathbb{Q} \cap [0, \infty[$. Il est clair que l'on peut supposer R irréductible, ce que l'on fait ci-dessous.

On fixe une chambre C de R ; on note respectivement $(\alpha_1, \alpha_2, \ldots, \alpha_l)$ et $\widetilde{\alpha}$, la base de R et la plus grande racine correspondantes. On rappelle que C est le sous-ensemble de V constitué des éléments ξ vérifiant $\alpha_i.\xi > 0$ pour $i = 1, 2, \ldots, l$. On rappelle également que l'on a $\widetilde{\alpha} = n_1\alpha_1 + n_2\alpha_2 + \cdots + n_l\alpha_l$ avec

$n_i \in \mathbb{N} - \{0\}$ pour $i = 1, 2, \ldots, l$; on note J le sous-ensemble de $\{1, 2, \ldots, l\}$ constitué des indices i pour lesquels on a $n_i = 1$. On note $\varpi_1, \varpi_2, \ldots, \varpi_l$ les *poids fondamentaux*, c'est-à-dire les éléments de V définis par $\alpha_i.\varpi_j = \delta_{i,j}$ (symbole de Kronecker) ; $(\varpi_1, \varpi_2, \ldots, \varpi_l)$ est une base du $\mathbb{Z}$-module $\mathrm{Q}(R)^\sharp$ et C est le cône ouvert de V engendré par cette base.

Proposition 3.8. *Soit R un système de racines irréductible de type ADE, muni d'une chambre C. On note $\gamma : \mathrm{Q}(R)^\sharp \to \mathrm{rés}\,\mathrm{Q}(R)$ l'application canonique et $\Pi(R)$ le sous-ensemble $\{0\} \coprod \{\varpi_j ; j \in \mathrm{J}\}$ de $\mathrm{Q}(R)^\sharp$.*

(a) *La restriction de γ à $\Pi(R)$ est une bijection.*

(b) *Pour tout ξ dans $\Pi(R)$, on a $\mathrm{qm}(\gamma(\xi)) = \mathrm{q}(\xi)$.*

Les deux points de la proposition ci-dessus permettent la détermination de l'application $\mathrm{qm} : \mathrm{rés}\,\mathrm{Q}(R) \to \mathbb{Q} \cap [0, \infty[$. Une référence pour le point (a) est [Bou81b, Ch. VI, §2, Cor. de Prop. 6] ; le point (b) est implicite dans [Ven80]. Pour le confort du lecteur nous donnons ci-après, en petits caractères, une démonstration de ces deux points fondée sur la proposition 3.9 ci-dessous (pour laquelle une référence est [Bou81b, Ch. V, §3, Th. 2]) qui est un résultat fondamental (c'est le cas de le dire !) concernant l'action du groupe de Weyl affine sur V.

Avant d'énoncer cette proposition, rappelons la définition de l'*alcove*, notée *Alc* dans ce mémoire, associée à la chambre C :

$$Alc \;:=\; \{\, \xi \,;\, \xi \in V,\ \alpha_i.\xi > 0 \text{ pour } i = 1, 2, \ldots, l \text{ et } \widetilde{\alpha}.\xi < 1 \,\} \qquad ;$$

la fermeture $\overline{Alc}$ de *Alc* dans V est bien sûr définie par les inégalités larges $\alpha_i.\xi \geq 0$ et $\widetilde{\alpha}.\xi \leq 1$.

Proposition 3.9. *Toute orbite de l'action canonique du produit semi-direct $\mathrm{W}(R) \ltimes \mathrm{Q}(R)$ (le groupe de Weyl affine) sur V rencontre $\overline{Alc}$ en un et un seul point.*

Démonstration du point (a) de la proposition 3.8.

Par définition $\Pi(R)$ est contenu dans $\overline{Alc}$ puisque pour tout j dans J (qui peut être vide) les produits scalaires $\alpha_i.\xi$, $i = 1, 2, \ldots, l$, et $\widetilde{\alpha}.\xi$ sont 0 ou 1. En fait, il n'est pas difficile de se convaincre de ce que l'on a $\Pi(R) = \mathrm{Q}(R)^\sharp \cap \overline{Alc}$: Soit ξ un élément de $\mathrm{Q}(R)^\sharp$; on écrit $\xi = \sum_{i=1}^{l} (\alpha_i.\xi)\varpi_i$, si ξ est dans $\overline{C}$ alors les entiers $\alpha_i.\xi$ sont positifs ou nuls, si ξ est non nul et que l'on a en outre $\widetilde{\alpha}.\xi \leq 1$ alors ξ est forcément l'un des ϖ_j avec j dans J.

Compte tenu de ce qui précède, le point (a) de la proposition 3.8 est conséquence de la proposition 3.9 :

– La partie "unicité" de cette proposition montre que la restriction de γ à $\Pi(R)$ est injective.

– La partie “existence” montre qu'elle est aussi surjective. En effet, soit ξ un élément de $\mathrm{Q}(R)^\sharp$ alors il existe η dans $\overline{Alc}$, w dans $\mathrm{W}(R)$ et x dans $\mathrm{Q}(R)$, tels que l'on a $\xi = w\eta + x$; on en déduit $\eta \in \Pi(R)$, puis $\gamma(\xi) = \gamma(w\eta)$ et enfin $\gamma(\xi) = \gamma(\eta)$ car l'action de $\mathrm{W}(R)$ sur $\mathrm{rés}\,\mathrm{Q}(R)$, induite par celle de $\mathrm{W}(R)$ sur $\mathrm{Q}(R)$, est triviale [Bou81b, Ch. VI, §1, Prop. 27].

Démonstration du point (b) de la proposition 3.8.

Ce point est conséquence de l'implication $(v) \Rightarrow (i)$ de la proposition ci-dessous.

Proposition 3.10. *Soit $R \subset V$ un système de racines irréductible de type ADE. Soit ξ un élément de V. Les conditions suivantes sont équivalentes :*
(i) On a $\mathrm{q}(\xi) \leq \mathrm{q}(\xi + x)$ pour tout x dans $\mathrm{Q}(R)$.
(ii) On a $\mathrm{q}(\xi) \leq \mathrm{q}(\xi + \alpha)$ pour tout α dans R.
(iii) On a $\alpha.\xi \leq 1$ pour tout α dans R.
(iv) On a $|\alpha.\xi| \leq 1$ pour tout α dans R.
(v) Il existe un élément w de $\mathrm{W}(R)$ tel que $w\xi$ appartient à $\overline{Alc}$ (on suppose ici R muni d'une chambre C).

Démonstration. Les implications $(i) \Rightarrow (ii) \Rightarrow (iii) \iff (iv)$ sont triviales (pour $(ii) \Rightarrow (iii) \iff (iv)$, observer que si α est une racine alors il en est de même pour $-\alpha$).

Démonstration de $(iv) \iff (v)$. On pose

$$\Psi \;:=\; \{\, \xi \,;\, \xi \in V,\ \alpha.\xi \leq 1 \text{ pour tout } \alpha \text{ dans } R \,\} \qquad ;$$

il s'agit de montrer que l'on a $\Psi = \bigcup_{w \in \mathrm{W}(R)} w\,\overline{Alc}$.

Soit ξ un élément de V, alors il existe un élément w de $\mathrm{W}(R)$ avec $w^{-1}\xi \in \overline{C}$. Si l'on suppose en outre $\xi \in \Psi$ alors on a $(w\widetilde{\alpha}).\xi = \widetilde{\alpha}.(w\xi) \leq 1$ et donc $w^{-1}\xi \in \overline{Alc}$; ceci montre l'inclusion $\Psi \subset \bigcup_{w \in \mathrm{W}(R)} w\,\overline{Alc}$.

Soit α une racine positive (pour la chambre C) ; comme α s'écrit $\sum_{i=1}^{l} \nu_i \alpha_i$ avec $0 \leq \nu_i \leq n_i$, on a $0 \leq \alpha.\xi \leq \widetilde{\alpha}.\xi$ pour tout ξ dans $\overline{C}$. L'inclusion $\overline{Alc} \subset \Psi$ en résulte ; on en déduit $\bigcup_{w \in \mathrm{W}(R)} w\,\overline{Alc} \subset \Psi$ puisque Ψ est stable sous l'action de $\mathrm{W}(R)$. □

Démonstration de $(iii) \Rightarrow (i)$. Soit Γ un réseau arbitraire de l'espace euclidien V. On pose

$$\Phi_\Gamma \;:=\; \{\, \xi \,;\, \xi \in V,\ \mathrm{q}(\xi) \leq \mathrm{q}(\xi - x) \text{ pour tout } x \text{ dans } \Gamma \,\} \qquad ,$$

en clair, Φ_Γ est le sous-ensembe de V constitué des points dont la distance à l'origine est inférieure ou égale à la distance à tout point de Γ. L'étude de ces sous-ensembles est bien sûr fort classique ! Par définition Φ_Γ est l'intersection des demi-espaces $x.\xi \leq \mathrm{q}(x)$, x parcourant Γ ; il est facile de se convaincre de ce que Φ_Γ est compact et intersection d'une sous-famille finie de ces demi-espaces. Le sous-ensemble Φ_Γ vérifie les trois propriétés suivantes :
(1) Φ_Γ est la fermeture dans V de son intérieur ;
(2) les translatés $\Phi_\Gamma + x$, x parcourant Γ, recouvrent V ;
(3) les translatés $\mathring{\Phi}_\Gamma + x$, x parcourant Γ, sont deux à deux disjoints (la notation $\mathring{\Phi}_\Gamma$ désigne l'intérieur de Φ_Γ).

Lemme 3.11. *Soit Φ (resp. Φ') un sous-ensemble de V vérifiant les propriétés (1), (2) et (3) (resp. (1) et (3)). Si l'on a $\Phi \subset \Phi'$ alors on a $\Phi = \Phi'$.*

Démonstration. Supposons $\Phi' \not\subset \Phi$. Dans ce cas on a aussi $\mathring{\Phi}' \not\subset \Phi$ puisque Φ est fermé et que Φ' est la fermeture de son intérieur. Soit ξ un élément de V avec $\xi \in \mathring{\Phi}'$ et $\xi \notin \Phi$. Puisque Φ vérifie (2) il existe x dans Γ tel que l'on $\xi + x \in \Phi$ et *a fortiori* $\xi + x \in \Phi'$. On a donc $\mathring{\Phi}' \cap (\Phi' + x) \neq \emptyset$; par un argument de topologie générale analogue au précédent on a aussi $\mathring{\Phi}' \cap (\mathring{\Phi}' + x) \neq \emptyset$. Puisque Φ vérifie (3), on a $x = 0$. Contradiction. □

Le lemme ci-dessus fournit une démonstration de l'implication $(iii) \Rightarrow (i)$. On pose $\Phi := \Phi_{\mathrm{Q}(R)}$; Φ est donc le sous-ensemble de V constitué des ξ qui vérifient la condition (i). Il s'agit de montrer que l'on a $\Phi = \Psi$. Il est clair que Ψ vérifie la propriété (1) ; pour conclure il suffit de montrer qu'il vérifie aussi la propriété (3). Soit ξ un élément de $\mathrm{Q}(R)$ avec $\mathring{\Psi} \cap (\mathring{\Psi} + x) \neq \emptyset$; soit ξ un élément de cette intersection. Les inégalités $-1 < \alpha.\xi < 1$ et $-1 < \alpha.(\xi + x) < 1$ impliquent $-2 < \alpha.x < 2$; comme $\alpha.x$ est entier, on a aussi $-1 \leq \alpha.x \leq 1$, c'est-à-dire $x \in \Psi$. La proposition ci-dessous dit que x est nul.

Proposition 3.12. *On a* $\Psi \cap \mathrm{Q}(R) = \{0\}$.

Démonstration. Compte tenu de l'égalité $\Psi = \bigcup_{w \in \mathrm{W}(R)} w\,\overline{Alc}$ il sufit de montrer que l'on a $\overline{Alc} \cap \mathrm{Q}(R) = \{0\}$. Cette égalité est à nouveau impliquée par la proposition 3.9. □□

Remarque terminologique. Les éléments ξ de $\mathrm{Q}(R)^\sharp$ vérifiant $\mathrm{q}(\xi) \leq \mathrm{q}(\xi + x)$ pour tout x dans Q sont appelés *poids minuscules* ; cependant on réserve souvent l'appellation "poids minuscules" aux poids fondamentaux ϖ_j, $j \in J$, considérés plus haut (voir par exemple [ST98]).

3) Soit R un système de racines de type ADE. L'action de $\mathrm{A}(R)$ sur $\mathrm{Q}(R)$ induit une action de $\mathrm{A}(R)$ sur le qe-module de Venkov $\mathrm{rés}\,\mathrm{Q}(R)$. La restriction à $\mathrm{W}(R)$ de l'action de $\mathrm{A}(R)$ sur $\mathrm{rés}\,\mathrm{Q}(R)$ est triviale (voir plus haut) ; comme $\mathrm{W}(R)$ est distingué dans $\mathrm{A}(R)$ [BOU81b, Ch. VI, §1, Prop. 16], on dispose d'une action canonique (en fait fidèle [BOU81b, Ch. VI, §4, Exc. 7]) du groupe quotient $\mathrm{G}(R) := \mathrm{A}(R)/\mathrm{W}(R)$ sur $\mathrm{rés}\,\mathrm{Q}(R)$.

On revient maintenant à la classification des réseaux unimodulaires pairs de dimension 24 dont l'ensemble des racines est non vide. Pour achever cette classification, Venkov vérifie au cas par cas l'énoncé (miraculeux !) suivant :

Proposition 3.13. *Soit R un système de racines de type ADE, de rang* 24 *et équicoxeter.*

(a) *Le* qe-*module de Venkov* $\mathrm{rés}\,\mathrm{Q}(R)$ *possède un lagrangien I avec* $\mathrm{qm}(\xi) > 1$ *pour tout ξ dans $I - \{0\}$.*

(b) *Un tel lagrangien est unique à l'action de* $\mathrm{G}(R)$ *près.*

Corollaire 3.14. *L'application $L \mapsto \mathrm{R}(L)$ induit une bijection, de l'ensemble des classes d'isomorphisme de réseaux unimodulaires pairs de dimension* 24 *avec* $\mathrm{R}(L) \neq \emptyset$*, sur l'ensemble des classes d'isomorphisme de systèmes de racines de type ADE de rang* 24 *et équicoxeter.*

Scholie 3.15. *Soit L un réseau unimodulaire pair de dimension 24 avec* $\mathrm{R}(L) \neq \emptyset$.

(a) *L'action du groupe de Weyl* $\mathrm{W}(\mathrm{R}(L))$ *sur* $\mathrm{R}(L)$ *se prolonge en une action (orthogonale) sur L si bien que* $\mathrm{W}(\mathrm{R}(L))$ *s'identifie à un sous-groupe du groupe orthogonal* $\mathrm{O}(L)$.

(b) *Le groupe* $\mathrm{W}(\mathrm{R}(L))$ *est distingué dans* $\mathrm{O}(L)$ *et le quotient* $\mathrm{O}(L)/\mathrm{W}(\mathrm{R}(L))$ *est canoniquement isomorphe au sous-groupe de* $\mathrm{G}(R)$ *qui stabilise le lagrangien* $L/\mathrm{Q}(\mathrm{R}(L))$ *du* qe-*module* $\mathrm{rés}\,\mathrm{Q}(R)$ *(lagrangien qui est l'un de ceux considérés dans la proposition 3.13).*

(Le point (a) du scholie ci-dessus résulte de ce que l'action canonique de $\mathrm{W}(\mathrm{R}(L))$ sur $\mathrm{rés}\,\mathrm{Q}(R)$ est triviale.)

Exemples

1) $\mathrm{R}(L) \cong \mathbf{D}_{24}$, $\mathrm{R}(L) \cong \mathbf{D}_{16} \coprod \mathbf{E}_8$, $\mathrm{R}(L) \cong \mathbf{E}_8 \coprod \mathbf{E}_8 \coprod \mathbf{E}_8$

Il résulte de ce que l'on a déjà vu que l'on a dans ces trois cas respectivement $L \cong \mathrm{D}_{24}^+$, $L \cong \mathrm{D}_{16}^+ \oplus \mathrm{E}_8$, $L \cong \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8$.

2) $\mathrm{R}(L) \cong \mathbf{A}_{24}$

Soit $n \geq 1$ un entier ; on munit le $\mathbb{R}$-espace vectoriel $\mathbb{R}^{n+1}$ de sa structure euclidienne canonique et on note $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n+1})$ sa base canonique. On note A_n le sous-module de $\mathrm{I}_{n+1} := \mathbb{Z}^{n+1} \subset \mathbb{R}^{n+1}$ constitué des $(n+1)$-uples $(x_1, x_2, \ldots, x_{n+1})$ avec $x_1 + x_2 + \ldots + x_{n+1} = 0$; A_n est un réseau entier pair (dans l'hyperplan de $\mathbb{R}^{n+1}$ constitué des $(n+1)$-uples $(\xi_1, \xi_2, \ldots, \xi_{n+1})$ avec $\xi_1 + \xi_2 + \ldots + \xi_{n+1} = 0$). Le système de racines $\mathbf{A}_n$ est défini par l'égalité $\mathbf{A}_n := \mathrm{R}(\mathrm{A}_n)$ (si bien que l'on a aussi l'égalité $\mathrm{A}_n = \mathrm{Q}(\mathbf{A}_n)$).

Le groupe abélien sous-jacent au qe-module de Venkov $\mathrm{rés}\,\mathrm{A}_n$ est cyclique d'ordre $n+1$ engendré par la classe de la projection orthogonale de ε_1 sur l'hyperplan $\sum_{i=1}^{n+1} \xi_i = 0$, disons ϖ. La forme quadratique d'enlacement $\mathrm{q} : \mathbb{Z}/(n+1) \to \mathbb{Q}/\mathbb{Z}$, définie par transport de structure, est donnée par

$$\mathrm{q}(\bar{k}) = k^2\,\mathrm{q}(\varpi) = \frac{n\,k^2}{2(n+1)} \qquad .$$

L'application $\mathrm{qm} : \mathbb{Z}/(n+1) \to \mathbb{Q} \cap [0, \infty[$ est donnée quant à elle par

$$\mathrm{qm}(\bar{k}) = \frac{k\,(n+1-k)}{2(n+1)} \qquad \text{pour } \ 0 \leq k \leq n$$

(dans le cas de $\mathbf{A}_n$, tous les poids fondamentaux sont minuscules).

Il est clair que $\operatorname{rés} \mathrm{A}_n$ possède un lagrangien, au sens bilinéaire, si et seulement si l'entier $n+1$ est un carré, $n+1=r^2$, à savoir le sous-module engendré par $r\varpi$, et que dans ce cas ce lagrangien est unique.

On suppose $n+1=r^2$ et on note I le sous-module engendré par $r\varpi$; on constate que I est un lagrangien au sens quadratique si et seulement si n est pair, c'est-à-dire r impair, et que dans ce cas I vérifie la condition (ii) de la proposition 3.7 si et seulement on a l'inégalité $r \geq 5$.

On note A_{24}^+ le réseau de $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{A}_{24}$ engendré par A_{24} et 5ϖ. La discussion précédente montre que A_{24}^+ est un réseau unimodulaire pair de dimension 24 avec $\mathrm{R}(\mathrm{A}_{24}^+) \cong \mathbf{A}_{24}$ et que cette propriété caractérise, à isomorphisme près, A_{24}^+ parmi les réseaux unimodulaires pairs de dimension 24.

3) $\mathrm{R}(L) \cong \mathbf{D}_{12} \coprod \mathbf{D}_{12}$

Le qe-module de Venkov $\operatorname{rés} \mathrm{D}_{12}$ est isomorphe à $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ muni des applications q et qm définies respectivement par :
$\mathrm{q}(\bar{0},\bar{0})=0$, $\mathrm{q}(\bar{1},\bar{0})=\frac{1}{2}$, $\mathrm{q}(\bar{0},\bar{1})=\frac{1}{2}$, $\mathrm{q}(\bar{1},\bar{1})=\frac{1}{2}$;
$\mathrm{qm}(\bar{0},\bar{0})=0$, $\mathrm{qm}(\bar{1},\bar{0})=\frac{3}{2}$, $\mathrm{qm}(\bar{0},\bar{1})=\frac{3}{2}$ et $\mathrm{qm}(\bar{1},\bar{1})=\frac{1}{2}$.
Le qe-module de Venkov $\operatorname{rés}(\mathrm{D}_{12} \oplus \mathrm{D}_{12})$ est isomorphe à $\operatorname{rés} \mathrm{D}_{12} \oplus \operatorname{rés} \mathrm{D}_{12}$. On constate que les lagrangiens de $\operatorname{rés}(\mathrm{D}_{12} \oplus \mathrm{D}_{12})$ sont les graphes des permutations ϕ de $\operatorname{rés} \mathrm{D}_{12}$ qui préservent 0 (une telle permutation est linéaire et préserve la forme quadratique d'enlacement). Le graphe de ϕ vérifie la condition (ii) de la proposition 3.7 si et seulement si l'on a $\phi(\mathrm{qm}^{-1}(\frac{1}{2})) \neq \mathrm{qm}^{-1}(\frac{1}{2})$; de tels ϕ sont au nombre de 4 et l'on constate que le groupe $\mathrm{G}(\mathbf{D}_{12} \coprod \mathbf{D}_{12})$ (qui est isomorphe à $\mathfrak{S}_2 \wr \mathrm{G}(\mathbf{D}_{12}) = \mathfrak{S}_2 \wr \mathfrak{S}_2$) agit bien transitivement sur l'ensemble des 4 graphes correspondants.

4) $\mathrm{R}(L) \cong \mathbf{A}_{17} \coprod \mathbf{E}_7$

Le qe-module de Venkov $\operatorname{rés}(\mathrm{A}_{17} \oplus \mathrm{E}_7)$ est isomorphe à $\operatorname{rés} \mathrm{A}_{17} \oplus \operatorname{rés} \mathrm{E}_7$. La structure du qe-module de Venkov $\operatorname{rés} \mathrm{A}_n$, pour tout n, a déja été explicitée dans le deuxième exemple ci-dessus. Le qe-module $\operatorname{rés} \mathrm{E}_7$ est quant à lui isomorphe à $\mathbb{Z}/2$ muni de la forme quadratique d'enlacement définie par $\mathrm{q}(\bar{1}) = -\frac{1}{4}$ (voir le point (d) de B.2.2) ; on vérifie que l'on a $\mathrm{qm}(\bar{1}) = \frac{3}{4}$. On constate que l'unique lagrangien du qe-module $\operatorname{rés}(\mathrm{A}_{17} \oplus \mathrm{E}_7)$ satisfait bien la condition (ii) de la proposition 3.7.

5) $\mathrm{R}(L) \cong \mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{E}_7$

La structure du qe-module de Venkov $\operatorname{rés}(\mathrm{D}_{10} \oplus \mathrm{E}_7 \oplus \mathrm{E}_7)$ est déterminée par celle de $\operatorname{rés} \mathrm{E}_7$ que nous venons d'expliciter et celle de $\operatorname{rés} \mathrm{D}_{10}$. Celle-ci est la

suivante : $\text{rés}\,\mathrm{D}_{10}$ est isomorphe à $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ muni de l'application qm définie par $\mathrm{qm}(\bar{0},\bar{0}) = 0$, $\mathrm{qm}(\bar{1},\bar{0}) = \frac{5}{4}$, $\mathrm{qm}(\bar{0},\bar{1}) = \frac{5}{4}$ et $\mathrm{qm}(\bar{1},\bar{1}) = \frac{1}{2}$.

Le qe-module $\text{rés}(\mathrm{D}_{10} \oplus \mathrm{E}_7 \oplus \mathrm{E}_7)$ possède deux lagrangiens, disons I_1 et I_2, à savoir les graphes des deux isomorphismes de qe-modules de $\text{rés}\,\mathrm{D}_{10}$ sur $\langle -1 \rangle \otimes \text{rés}(\mathrm{E}_7 \oplus \mathrm{E}_7)$. On constate que I_1 et I_2 satisfont tous deux la condition (ii) de la proposition 3.7.

Le groupe $G := \mathrm{G}(\mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{E}_7)$ s'identife à $\mathbb{Z}/2 \times \mathbb{Z}/2$ car il est isomorphe au produit des groupes $\mathrm{G}(\mathbf{D}_{10})$ et $\mathrm{G}(\mathbf{E}_7 \coprod \mathbf{E}_7)$ qui sont tous deux cycliques d'ordre 2. On constate que G agit bien transitivement sur l'ensemble $\{I_1, I_2\}$; on observe également que le $\mathbb{Z}/2$ diagonal agit trivialement (cette observation sera utilisée à la fin du paragraphe 2 de l'appendice B).

6) $\mathrm{R}(L) \cong 24\,\mathbf{A}_1$ (cette notation désigne la somme directe de 24 copies du système de racines $\mathbf{A}_1$)

Le qe-module de Venkov $\text{rés}\,\mathrm{A}_1$ est isomorphe à $\mathbb{Z}/2$ muni de l'application qm définie par $\mathrm{qm}(x) = \frac{\lambda(x)}{4}$, $\lambda : \mathbb{Z}/2 \to \mathbb{N}$ désignant l'application définie par $\lambda(\bar{0}) = 0$ et $\lambda(\bar{1}) = 1$; il en résulte que le qe-module de Venkov $\text{rés}(\mathrm{A}_1^{\oplus 24})$ est isomorphe à $(\mathbb{Z}/2)^{24}$ muni de l'application qm définie par

$$\mathrm{qm}(x_1, x_2, \ldots, x_{24}) \;=\; \frac{1}{4} \sum_{i=1}^{24} \lambda(x_i) \;=:\; \frac{1}{4}\,\mathrm{wt}(x_1, x_2, \ldots, x_{24}) \qquad .$$

Le groupe $\mathrm{G}(24\,\mathbf{A}_1)$ est isomorphe à $\mathfrak{S}_{24} \wr \mathrm{G}(\mathbf{A}_1) = \mathfrak{S}_{24}$ et son action sur $\text{rés}(\mathrm{A}_1^{\oplus 24})$ s'identifie à l'action évidente de $\mathfrak{S}_{24}$ sur $(\mathbb{Z}/2)^{24}$.

Un lagrangien de $\text{rés}(\mathrm{A}_1^{\oplus 24})$ s'identifie à un sous-espace vectoriel I de $(\mathbb{Z}/2)^{24}$ avec $\dim I = 12$ et $\mathrm{wt}(x) \equiv 0 \bmod 4$ pour tout x dans I ; un tel I est ce qu'on appelle un *code binaire auto-dual pair* de longueur 24. A isomorphisme près (en d'autres termes, modulo l'action de $\mathfrak{S}_{24}$), il existe 9 codes binaires auto-duaux pairs de longueur 24 [PLS74].

Le lagrangien I vérifie en outre la condition (ii) de la proposition 3.7 si et seulement si l'on a $\mathrm{wt}(x) \geq 8$ pour tout x dans $I - \{0\}$. Là encore, il existe un code binaire auto-dual pair de longueur 24 vérifiant cette propriété, et à isomorphisme près un seul, à savoir le code de Golay [PL68].

L'énoncé suivant permet de compléter l'énoncé 3.14 :

Théorème 3.16. *Tout réseau unimodulaire pair dont l'ensemble des racines est vide est isomorphe au réseau de Leech.*

On obtient :

Théorème 3.17. *L'application* $L \mapsto \mathrm{R}(L)$ *induit une bijection, de l'ensemble des classes d'isomorphisme de réseaux unimodulaires pairs de dimension* 24*, sur l'ensemble à* 24 *éléments constitué, des classes d'isomorphisme de systèmes de racines de type ADE de rang* 24 *et équicoxeter, et de l'ensemble vide.*

Le théorème 3.16 est dû à Conway (voir [Co69b]). Venkov en propose dans [Ven80] une démonstration qui utilise la notion de voisin de Kneser dont traite le prochain chapitre.

III. Voisins à la Kneser

1. Variations sur la notion de voisins à la Kneser

La notion de réseaux unimodulaires 2-voisins a été introduite par Martin Kneser dans [Kn57]. Dans l'article en question, Kneser décrit, à l'aide de cette notion, un algorithme pour classifier les réseaux unimodulaires (l'exhaustivité est essentiellement due au théorème II.2.8) et met en oeuvre cet algorithme pour expliciter la liste des classes d'isomorphisme de réseaux unimodulaires de dimension inférieure ou égale à 15 (voir aussi [O'M73, §106F]).

Commençons nos variations par deux observations très générales (nous faisons intervenir ci-dessous un anneau de Dedekind R arbitraire, mais les deux applications que nous avons en tête sont $R = \mathbb{Z}$ et $R = \mathbb{Z}_p$) :

Proposition 1.1. *Soient R un anneau de Dedekind et K son corps des fractions. Soit V un* q*-espace vectoriel sur K, de dimension finie ; soient L_1 et L_2 deux réseaux entiers auto-duaux de V (les réseaux L_1 et L_2 sont donc en particulier deux* q*-modules et le réseau $L_1 \cap L_2$ un $\widetilde{\mathrm{q}}$-module, sur R).*

On pose $I_1 = L_1/(L_1 \cap L_2)$ et $I_2 = L_2/(L_1 \cap L_2)$.

(a) *Les sous-modules I_1 et I_2 sont deux lagrangiens transverses du* qe*-module* $\mathrm{rés}(L_1 \cap L_2)$. *La forme d'enlacement de ce* qe*-module induit un isomorphisme de I_2 sur $I_1^\vee$, disons ι, et l'homomorphisme composé*

$$\mathrm{H}(I_1) = I_1 \oplus I_1^\vee \xrightarrow{\mathrm{id}\oplus\iota^{-1}} I_1 \oplus I_2 \longrightarrow \mathrm{rés}(L_1 \cap L_2)$$

est un isomorphisme de qe*-modules sur R (on rappelle que la notation $\mathrm{H}(I_1)$ désigne le* qe*-module hyperbolique sur le R-module de torsion de type fini I_1).*

(b) *Soit r le nombre minimum de générateurs du R-module I_1 ; on a l'inégalité*

$$2\,r \;\leq\; \dim_K V \qquad .$$

Démonstration. La première partie du point (a) est évidente ; la seconde est la reprise du point (a) de II.1.3. Passons au point (b). Soit I un R-module de

torsion de type fini, on note $\mathrm{r}(I)$ le nombre minimum de générateurs de cet R-module ; $\mathrm{r}(I)$ peut être vu, par exemple, comme le plus grand des entiers k tels que la puissance extérieure $\Lambda^k I$ est non nulle. Comme le dual $I^\vee$ est isomorphe (non canoniquement) à I (pour s'en convaincre, observer que R est "localement principal") on a $\mathrm{r}(I) = \mathrm{r}(I^\vee)$; on a donc, d'après le point (a), l'égalité $\mathrm{r}(\text{rés}(L_1 \cap L_2)) = 2\mathrm{r}(I_1)$. Comme $\text{rés}(L_1 \cap L_2)$ est un quotient du réseau $(L_1 \cap L_2)^\sharp$ on a $\mathrm{r}(\text{rés}(L_1 \cap L_2)) \leq \dim_K V$. □

On spécialise au cas $R = \mathbb{Z}$.

Scholie-Définition 1.2. *Soit V un* q*-espace vectoriel sur $\mathbb{Q}$; soient L_1 et L_2 deux réseaux entiers auto-duaux de V (les réseaux L_1 et L_2 sont donc en particulier deux* q*-modules et le réseau $L_1 \cap L_2$ un $\widetilde{\mathrm{q}}$-module, sur $\mathbb{Z}$).*

Soit A un groupe abélien fini ; les conditions suivantes sont équivalentes :
(i) le quotient $L_1/(L_1 \cap L_2)$ est isomorphe à A ;
(ii) le quotient $L_2/(L_1 \cap L_2)$ est isomorphe à A.

*Si ces conditions sont vérifiées alors on dit que L_1 et L_2 sont A-*voisins *(ou que L_2 est un A-*voisin *de L_1).*

d-VOISINS, POINT DE VUE ASYMÉTRIQUE

La spécificité de la notion de A-voisins pour A cyclique tient à l'énoncé ci-dessous, qui peut être vu comme un corollaire du point (b) de II.1.3. :

Proposition 1.3. *Soit A un groupe cyclique fini ; alors $A^\vee$ est l'unique lagrangien du* qe*-module $\mathrm{H}(A)$ transverse (au sens de II.1.3) au lagrangien A.*

On fixe maintenant un q-module L sur $\mathbb{Z}$, un entier $d \geq 2$, et on analyse l'ensemble des $\mathbb{Z}/d$-voisins de L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ (qui est un q-espace vectoriel sur $\mathbb{Q}$). On allège la terminologie $\mathbb{Z}/d$-voisin en *d-voisin.*

Dans ce contexte, un d-voisin de L est un réseau entier L' dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ avec $L'^\sharp = L'$ et $L/(L \cap L') \simeq \mathbb{Z}/d$. On pose $M = L \cap L'$. D'après ce qui précède :

– Le réseau dL' est contenu dans M.

– L'image de l'homomorphisme composé $dL' \subset M \subset L \to L/dL$ est une droite isotrope, disons c, de L/dL muni de sa structure de q-module sur $\mathbb{Z}/d$. Précisons ce que l'on entend ici par *droite isotrope* de L/dL : c est un sous-module libre de dimension 1 du $\mathbb{Z}/d$-module L/dL (nécessairement facteur direct car $\mathbb{Z}/d$ est un $\mathbb{Z}/d$-module injectif) tel que la restriction de la forme quadratique $\mathrm{q} : L/dL \to \mathbb{Z}/d$ à c est nulle.

– Le réseau M est l'image inverse par l'homomorphisme $L \to L/dL$ de $c^\perp$, $c^\perp$ désignant le sous-module du $\mathbb{Z}/d$-module L/dL orthogonal de la droite c.

– Le réseau L' est l'image inverse par l'homomorphisme $M^\sharp \to \text{rés}\, M$ de l'unique lagrangien transverse au lagrangien L/M.

Ce qui précède montre que l'application $L' \mapsto c$ est injective, la proposition ci-dessous montre qu'elle est aussi surjective.

Proposition 1.4. *Soit c une droite isotrope de L/dL ; soit M le sous-module de L image inverse de $c^\perp$ par l'homomorphisme $L \to L/dL$. Alors le* qe-*module* $\text{rés}\, M$ *est isomorphe à* $\mathrm{H}(\mathbb{Z}/d)$*, le quotient L/M en est un lagrangien et l'image inverse par l'homomorphisme $M^\sharp \to \text{rés}\, M$ de l'unique lagrangien qui lui est transverse est un d-voisin L' de L avec $L \cap L' = M$.*

Avant de vérifier cet énoncé nous introduisons une terminologie et une notation que nous utiliserons dans la suite du chapitre.

Soit L un $\mathbb{Z}$-module libre de dimension finie ; on dit qu'un élément u de L est indivisible ou *primitif* s'il est non nul et si le quotient $L/\mathbb{Z}u$ est sans torsion. Tout élément non nul u de L s'écrit de façon unique $\mathrm{c}(u)v$ avec v primitif et $\mathrm{c}(u)$ dans $\mathbb{N} - \{0\}$. Soit $d \geq 2$ un entier, nous dirons qu'un élément u de L est *d-primitif*, s'il est non nul et si d est premier avec $\mathrm{c}(u)$. En d'autres termes, u est d-primitif si le sous-module de L/dL engendré par la classe de u est un $\mathbb{Z}/d$-module libre de dimension 1. Comme nous l'avons déjà observé, un tel sous-module est nécessairement facteur direct si bien qu'un élément d-primitif u de L définit un élément de $\mathrm{P}_L(\mathbb{Z}/d)$, la notation P_L désignant le schéma dont les R-points, pour tout anneau commutatif R, sont les facteurs directs de rang 1 du R-module libre $R \otimes_{\mathbb{Z}} L$. Cet élément sera noté $[u]$.

Démonstration de 1.4. Il est clair qu'il suffit de vérifier que $\text{rés}\, M$ est isomorphe à $\mathrm{H}(\mathbb{Z}/d)$. Soit u un élément d-primitif de L dont la classe modulo d engendre la droite c ; puisque cette droite est isotrope on a $\mathrm{q}(u) \equiv 0 \bmod d$. Soit v un élément de L avec $u.v \equiv 1 \bmod d$. On constate que v et $\frac{u}{d}$ appartiennent à $M^\sharp$ et que $\text{rés}\,\mathrm{M}$ est un $\mathbb{Z}/d$-module libre de dimension 2 dont une base est constituée des classes de ces deux éléments. On pose $w = \frac{u}{d} - \frac{\mathrm{q}(u)}{d} v$; on constate également que l'on a dans $\mathbb{Q}/\mathbb{Z}$ les égalités $\mathrm{q}(v) = 0$, $\mathrm{q}(w) = 0$ et $v.w = \frac{1}{d}$. $\square$

On voit donc au bout du compte que le réseau L' est entièrement déterminé par la donnée de c. On met en place ci-après une notation qui souligne cette dépendance.

On note $\mathrm{C}_L(\mathbb{Z}/d)$ l'ensemble des droites isotropes de L/dL. La justification de cette notation est la suivante : on note $\mathrm{C}_L \subset \mathrm{P}_L$ la quadrique définie

par la forme quadratique dont L est muni. On observera incidemment que la non dégénérescence de cette forme quadratique fait que C_L est lisse sur $\mathbb{Z}$ (version projective du critère jacobien de lissité). Il est clair que les $\mathbb{Z}/d$-points de C_L sont les droites isotropes de L/dL. Soit c un élément de $\mathrm{C}_L(\mathbb{Z}/d)$, les réseaux M et L' introduits dans la proposition 1.4 seront respectivement notés $\mathrm{M}_d(L;c)$ et $\mathrm{vois}_d(L;c)$. On note enfin $\mathrm{Vois}_d(L)$ l'ensemble des d-voisins de L dans $\mathbb{Q}\otimes_{\mathbb{Z}} L$. On a tout fait pour avoir l'énoncé suivant :

Proposition 1.5. *L'application*

$$\mathrm{C}_L(\mathbb{Z}/d) \to \mathrm{Vois}_d(L) \qquad , \qquad c \mapsto \mathrm{vois}_d(L;c)$$

est une bijection.

Soit u un élément d-primitif de L avec $\mathrm{q}(u) \equiv 0 \bmod d$; les réseaux $\mathrm{M}_d(L;[u])$ et $\mathrm{vois}_d(L;[u])$ seront aussi notés $\mathrm{M}_d(L;u)$ et $\mathrm{vois}_d(L;u)$. Pour mémoire, nous explicitons ci-après l'algorithme $u \rightsquigarrow \mathrm{vois}_d(L;u)$ fourni par la démonstration de 1.4 :

Soit v un élément de L avec $u.v \equiv 1 \bmod d$ alors $\mathrm{vois}_d(L;u)$ est le réseau de $\mathbb{Q}\otimes_{\mathbb{Z}} L$ engendré par

$$\mathrm{M}_d(L;u) := \{\, x\,;\, x \in L\,,\, u.x \equiv 0 \bmod d \,\} \qquad \text{et} \qquad \frac{u - \mathrm{q}(u)v}{d} \qquad .$$

Posons $\widetilde{u} = u - \mathrm{q}(u)v$; on observera que l'on a $\widetilde{u} \equiv u \bmod d$, en d'autres termes $[\widetilde{u}] = [u]$ dans $\mathrm{C}_L(\mathbb{Z}/d)$, et $\mathrm{q}(\widetilde{u}) \equiv 0 \bmod d^2$. Cette observation conduit de façon évidente à une présentation alternative de l'algorithme : u étant donné, on détermine un élément $\widetilde{u}$ de L avec $\widetilde{u} \equiv u \bmod d$ et $\mathrm{q}(\widetilde{u}) \equiv 0 \bmod d^2$, $\mathrm{vois}_d(L;u)$ est alors le réseau de $\mathbb{Q}\otimes_{\mathbb{Z}} L$ engendré par $\mathrm{M}_p(L;u)$ et $\frac{\widetilde{u}}{d}$.

d-voisins, point de vue abstrait

Soient L_1 et L_2 deux q-modules sur $\mathbb{Z}$, disons de même dimension n. Sans surprises, on dit que L_2 est d-voisin de L_1 si L_2 est isomorphe, comme q-module, à un d-voisin de L_1 dans $\mathbb{Q}\otimes_{\mathbb{Z}} L_1$. Compte tenu de ce qui précède, si L_2 est d-voisin de L_1 alors L_1 est d-voisin de L_2 ; on dit donc aussi que L_1 et L_2 sont d-voisins. Pour éviter la confusion, il sera parfois commode de parler de voisinage "abstrait" pour la notion que nous venons d'introduire et de voisinage "concret" pour celle introduite dans la définition 1.2. Si le q-espace vectoriel sur $\mathbb{R}\otimes_{\mathbb{Z}} L_1$ est indéfini alors L_2 est d-voisin de L_1 si et seulement si les deux q-espaces vectoriels sur $\mathbb{R}\otimes_{\mathbb{Z}} L_1$ et $\mathbb{R}\otimes_{\mathbb{Z}} L_2$ sont isomorphes (Théorème II.2.7) : la relation de d-voisinage abstrait ne présente

pas grand intérêt dans ce cas ! On suppose donc ci-après que L_1 et L_2 sont définis positifs (ce qui force n à être divisible par 8). Comme convenu, on abandonne la terminologie "q-module sur $\mathbb{Z}$ défini positif" pour la terminologie "réseau unimodulaire pair".

Soient L_1 et L_2 deux réseaux unimodulaires pairs. On note $\widetilde{\mathrm{Vois}}_d(L_1, L_2)$ l'ensemble des isomorphismes de q-espaces vectoriels $\phi : \mathbb{Q} \otimes_{\mathbb{Z}} L_2 \to \mathbb{Q} \otimes_{\mathbb{Z}} L_1$ avec $L_1/(L_1 \cap \phi(L_2))$ cyclique d'ordre d. On observera que $\widetilde{\mathrm{Vois}}_d(L_1, L_2)$ est un ensemble fini ; par définition cet ensemble est non vide si et seulement si L_1 et L_2 sont d-voisins. On observera également que $\widetilde{\mathrm{Vois}}_d(L_1, L_2)$ est muni d'une action à gauche libre du groupe orthogonal $\mathrm{O}(L_1)$ et d'une action à droite libre du groupe orthogonal $\mathrm{O}(L_2)$, actions qui commutent. On note $\mathrm{Vois}_d(L_1, L_2)$ le sous-ensemble de $\mathrm{Vois}_d(L_1)$ constitué des d-voisins de L_1 dans $\mathbb{Q} \otimes_{\mathbb{Z}} L_1$ qui sont isomorphes, comme q-module, à L_2 ; $\mathrm{Vois}_d(L_1, L_2)$ est canoniquement muni d'une action à gauche de $\mathrm{O}(L_1)$. Par définition encore, l'application $\widetilde{\mathrm{Vois}}_d(L_1, L_2) \to \mathrm{Vois}_d(L_1, L_2)$, $\phi \mapsto \phi(L_2)$ induit une bijection $\mathrm{O}(L_1)$-équivariante

$$\widetilde{\mathrm{Vois}}_d(L_1, L_2)/\mathrm{O}(L_2) \;\cong\; \mathrm{Vois}_d(L_1, L_2) \qquad .$$

Le cardinal de l'ensemble $\mathrm{Vois}_d(L_1, L_2)$ est noté $\mathrm{N}_d(L_1, L_2)$.

Attention : l'introduction de cette notation n'est pas anodine, l'étude de ces cardinaux, en dimension 16 et 24, pour d premier, est le thème principal de notre mémoire (voir chapitre I) !

On note $[-]$ la classe d'isomorphisme d'un réseau unimodulaire pair ; il est clair que $\mathrm{N}_d(L_1, L_2)$ ne dépend que de $[L_1]$ et $[L_2]$, pour cette raison cet entier sera aussi noté $\mathrm{N}_d([L_1], [L_2])$

Lemme 1.6. *L'application $\phi \mapsto \phi^{-1}$ induit une bijection de $\widetilde{\mathrm{Vois}}_d(L_1, L_2)$ sur $\widetilde{\mathrm{Vois}}_d(L_2, L_1)$.*

Démonstration. Conséquence du "point de vue symétrique" sur les d-voisins, en clair de la proposition 1.1. □

Scholie 1.7. *On a la relation*

$$\frac{1}{|\mathrm{O}(L_1)|}\ \mathrm{N}_d(L_1, L_2) \;=\; \frac{1}{|\mathrm{O}(L_2)|}\ \mathrm{N}_d(L_2, L_1)$$

(la notation $|-|$ désigne le cardinal d'un ensemble fini).

Démonstration. Observer que l'on a $|\widetilde{\mathrm{Vois}}_d(L_1, L_2)| = \mathrm{N}_d(L_1, L_2)\,|\mathrm{O}(L_2)|$. □

L'énoncé 1.7 peut être précisé en l'énoncé 1.8 ci-dessous ; pour une illustration de 1.8 voir 3.1 et 3.2.

Ce qui précède montre que l'ensemble quotient $\mathrm{O}(L_1)\backslash\widetilde{\mathrm{Vois}}_d(L_1,L_2)/\mathrm{O}(L_2)$ est canoniquement en bijection avec l'ensemble quotient $\mathrm{O}(L_1)\backslash\mathrm{Vois}_d(L_1,L_2)$ et l'ensemble quotient $\mathrm{O}(L_2)\backslash\mathrm{Vois}_d(L_2,L_1)$ si bien que l'on dispose d'une bijection canonique entre ces deux derniers ensembles quotients.

Scholie 1.8. *Soient* Ω_1 *une* $\mathrm{O}(L_1)$*-orbite dans* $\mathrm{Vois}_d(L_1,L_2)$ *et* Ω_2 *une* $\mathrm{O}(L_2)$*-orbite dans* $\mathrm{Vois}_d(L_2,L_1)$ *qui se correspondent par la bijection canonique*

$$\mathrm{O}(L_1)\backslash\mathrm{Vois}_d(L_1,L_2) \;\cong\; \mathrm{O}(L_2)\backslash\mathrm{Vois}_d(L_2,L_1) \qquad ;$$

alors on a la relation

$$\frac{|\Omega_1|}{|\mathrm{O}(L_1)|} \;=\; \frac{|\Omega_2|}{|\mathrm{O}(L_2)|} \qquad .$$

On peut se convaincre plus directement de l'égalité ci-dessus, en revenant à la notion concrète de d-voisinage.

Proposition 1.9. *Soit* V *un* q*-espace vectoriel sur* $\mathbb{Q}$*, défini positif ; on suppose que* V *contient deux réseaux unimodulaires pairs* L_1 *et* L_2 *et que ces réseaux sont* d*-voisins dans* V*. Soient* Ω_1 *la* $\mathrm{O}(L_1)$*-orbite de* L_2 *et* Ω_2 *la* $\mathrm{O}(L_2)$*-orbite de* L_1 *; alors on a la relation*

$$\frac{|\Omega_1|}{|\mathrm{O}(L_1)|} \;=\; \frac{|\Omega_2|}{|\mathrm{O}(L_2)|} \;=\; \frac{1}{|\mathrm{O}(L_1)\cap\mathrm{O}(L_2)|}$$

($\mathrm{O}(L_1)$ *et* $\mathrm{O}(L_2)$ *s'identifient à des sous-groupes de* $\mathrm{O}(V)$ *et l'intersection qui apparaît ci-dessus est effectuée dans* $\mathrm{O}(V)$*).*

Démonstration. Observer que les stabilisateurs de L_2 pour l'action de $\mathrm{O}(L_1)$ et de L_1 pour l'action de $\mathrm{O}(L_2)$ s'identifie tous deux à $\mathrm{O}(L_1)\cap\mathrm{O}(L_2)$. □

2-voisins, le point de vue de Borcherds [CS99, Chap. 17]

On commence par deux remarques concernant la proposition 1.9. On en reprend les notations et on considère le réseau $L_1\cap L_2$.

– Ce réseau est un $\widetilde{\mathrm{q}}$-module dont le résidu est muni d'un couple de lagrangiens, tous deux cycliques d'ordre d et transverses l'un à l'autre, à savoir $\omega := (L_1/(L_1\cap L_2), L_2/(L_1\cap L_2))$. On observe que le groupe $\mathrm{O}(L_1)\cap\mathrm{O}(L_2)$

s'identifie au sous-groupe de $\mathrm{O}(L_1 \cap L_2)$, disons $\mathrm{O}(L_1 \cap L_2; \omega)$, constitué des éléments qui préservent ω. Les égalités de 1.9 peuvent donc être réécrites sous la forme suivante :

$$|\Omega_1| \;=\; \frac{|\mathrm{O}(L_1)|}{|\mathrm{O}(L_1 \cap L_2; \omega)|} \qquad , \qquad |\Omega_2| \;=\; \frac{|\mathrm{O}(L_2)|}{|\mathrm{O}(L_1 \cap L_2; \omega)|} \qquad .$$

– Dans le cas où d est premier, la paire de lagrangiens sous-jacente au couple de lagrangiens ω, est uniquement déterminée en fonction de $L_1 \cap L_2$. Ceci implique que $\mathrm{O}(L_1 \cap L_2; \omega)$ est au plus d'indice 2 dans $\mathrm{O}(L_1 \cap L_2)$. En particulier, on a $\mathrm{O}(L_1 \cap L_2; \omega) = \mathrm{O}(L_1 \cap L_2)$ si L_1 et L_2 ne sont pas isomorphes.

Ces remarques étant faites, nous pourrions continuer à traiter de d-voisins avec $d \geq 2$ quelconque, mais pour simplifier l'exposition, nous traitons ci-dessous seulement de p-voisins avec p premier ; en fait, le cas que nous avons en vue est $p = 2$.

Soit $n > 0$ un entier divisible par 8 ; on rappelle que l'on note X_n l'ensemble fini des classes d'isomorphisme des réseaux unimodulaires pairs de dimension n. Soit p un nombre premier ; on introduit trois autres ensembles finis.

– On note $\mathrm{Y}_n(p)$ l'ensemble des classes d'isomorphisme des couples (L_1, L_2), L_1 désignant un réseau unimodulaire pair de dimension n et L_2 un p-voisin de L_1 dans $\mathbb{Q} \otimes_{\mathbb{Z}} L_1$.

– On note $\mathrm{B}_n(p)$ l'ensemble des classes d'isomorphisme des $\widetilde{\mathrm{q}}$-modules M sur $\mathbb{Z}$, avec $\dim M = n$, $\mathbb{R} \otimes_{\mathbb{Z}} M > 0$ et $\mathrm{rés}\, M \simeq \mathrm{H}(\mathbb{Z}/p)$.

– On note $\widetilde{\mathrm{B}}_n(p)$ l'ensemble des classes d'isomorphisme de couples $(M; \omega)$ avec M comme précédemment et ω une bijection de l'ensemble des lagrangiens de $\mathrm{rés}\, M$ sur l'ensemble $\{1, 2\}$. Par définition $\widetilde{\mathrm{B}}_n(p)$ est muni d'une action à gauche du groupe symétrique $\mathfrak{S}_2$ et l'ensemble quotient $\mathfrak{S}_2 \backslash \widetilde{\mathrm{B}}_n(p)$ s'identifie à $\mathrm{B}_n(p)$.

Nous avons tout fait pour que les ensembles $\mathrm{Y}_n(p)$ et $\widetilde{\mathrm{B}}_n(p)$ soient canoniquement en bijection. Soit $(M; \omega)$ comme ci-dessus, on note $\mathrm{d}_i(M; \omega)$, $i = 1, 2$, l'image réciproque par la surjection $M^\sharp \to \mathrm{rés}\, M$ de $\omega^{-1}(i)$; $\mathrm{d}_1(M; \omega)$ et $\mathrm{d}_2(M; \omega)$ sont deux réseaux unimodulaires pairs (de dimension n) p-voisins dans $\mathbb{Q} \otimes_{\mathbb{Z}} M$. En passant aux classes d'isomorphisme on obtient deux applications que l'on note encore d_1 et d_2 de $\widetilde{\mathrm{B}}_n(p)$ dans X_n.

Là encore, nous avons tout fait pour avoir l'énoncé suivant.

Proposition 1.10. *Soit p un nombre premier ; soient x_1 et x_2 deux éléments de X_n. On a :*

$$\mathrm{N}_p(x_1, x_2) \;=\; \sum_{\beta \,\in\, \mathrm{d}_1^{-1}(x_1) \cap \mathrm{d}_2^{-1}(x_2)} \frac{|\mathrm{O}(x_1)|}{|\mathrm{O}(\beta)|}$$

(nous laissons au lecteur le soin de décoder les notations $|\mathrm{O}(x_1)|$ et $|\mathrm{O}(\beta)|$).

La proposition ci-dessus a un avatar un peu plus concret pour $p = 2$ parce que la donnée d'un $\widetilde{\mathrm{q}}$-module M sur $\mathbb{Z}$, avec $\dim M = n$, $\mathbb{R} \otimes_{\mathbb{Z}} M > 0$ et $\mathrm{rés}\, M \simeq \mathrm{H}(\mathbb{Z}/2)$, est équivalente à celle d'un réseau unimodulaire impair L avec $\dim L = n$. Expliquons pourquoi (en suivant Borcherds).

– A un M comme ci-dessus on associe le réseau L image réciproque par la surjection $M^\sharp \to \mathrm{rés}\, M$ de la droite du $\mathbb{Z}/2$-espace vectoriel $\mathrm{rés}\, M$ qui n'est pas isotrope au sens quadratique ; cette droite est isotrope au sens bilinéaire si bien que L est un réseau unimodulaire impair.

– A un réseau unimodulaire impair L de dimension n on associe le sous-module M constitué des éléments x avec $x.x \equiv 0 \bmod 2$ (voir Scholie II.2.3).

De plus l'ensemble des deux lagrangiens de $\mathrm{rés}\, M$ est naturellement en bijection avec l'ensemble des deux classes de vecteurs de Wu de L (voir la discussion qui suit le scholie II.2.3).

On est donc amené à introduire les notations suivantes.

– On note B_n l'ensemble fini des classes d'isomorphisme de réseaux unimodulaires L impairs de dimension n.

– On note $\widetilde{\mathrm{B}}_n$ l'ensemble fini des classes d'isomorphisme des couples $(L; \omega)$, L désignant un réseau unimodulaire impair de dimension n et ω une bijection de l'ensemble des deux classes de vecteurs de Wu de L sur $\{1, 2\}$. Par définition, $\widetilde{\mathrm{B}}_n$ est muni d'une action à gauche du groupe symétrique $\mathfrak{S}_2$ et l'ensemble quotient $\mathfrak{S}_2 \backslash \widetilde{\mathrm{B}}_n$ s'identifie à B_n.

– Soit L_i, $i = 1, 2$, le réseau unimodulaire pair de $\mathbb{Q} \otimes_{\mathbb{Z}} L$, engendré par le sous-module de L constitué des éléments x avec $x.x \equiv 0 \bmod 2$ et $\frac{1}{2}\omega^{-1}(i)$. On note encore $\mathrm{d}_i : \widetilde{\mathrm{B}}_n \to \mathrm{X}_n$, $i = 1, 2$, l'application qui associe à la classe d'isomorphisme de $(L; \omega)$, la classe d'isomorphisme de L_i.

Par construction, les réseaux unimodulaires L et L_i, $i = 1, 2$, sont 2-voisins "au sens bilinéaire" : $L \cap L_i$ est d'indice 2 dans L et L_i. Le lecteur vérifiera que L_1 et L_2 sont caractérisés, parmi les réseaux unimodulaires de $\mathbb{Q} \otimes_{\mathbb{Z}} L$ qui sont 2-voisins de L, par le fait qu'ils sont pairs. Nous dirons que L_1 et L_2 sont les 2-*voisins pairs* de L.

Voici enfin l'avatar annoncé de la proposition 1.10 pour $p = 2$. Son énoncé semble identique ; les seules différences sont en fait les suivantes : d_1 et d_2 désignent maintenant les applications de $\widetilde{\mathrm{B}}_n$ dans X_n introduites ci-dessus, β appartient à $\widetilde{\mathrm{B}}_n$ et si β est représenté par un réseau unimodulaire impair L muni d'une bijection ω de l'ensemble de ses deux classes de vecteurs de Wu sur $\{1, 2\}$ alors $\mathrm{O}(\beta)$ est le sous-groupe de $\mathrm{O}(L)$ qui préserve ω.

Proposition 1.11. *Soient x_1 et x_2 deux éléments de X_n. On a :*

$$\mathrm{N}_2(x_1, x_2) \;=\; \sum_{\beta \,\in\, \mathrm{d}_1^{-1}(x_1) \cap \mathrm{d}_2^{-1}(x_2)} \frac{|\mathrm{O}(x_1)|}{|\mathrm{O}(\beta)|} \qquad .$$

Les graphes des p-voisins

Soient $n > 0$ un nombre entier divisible par 8 et p un nombre premier ; le *graphe des p-voisins* $\mathrm{K}_n(p)$ est le graphe dont l'ensemble des sommets est l'ensemble X_n des classes de réseaux unimodulaires pairs de dimension n et dont l'ensemble des arêtes est l'ensemble des parties à deux éléments $\{[L_1], [L_2]\}$ de X_n avec L_1 et L_2 p-voisins (on rappelle que l'on note $[L]$ la classe d'isomorphisme d'un réseau unimodulaire pair L).

Théorème 1.12 (M. Kneser)**.** *Pour tout n et tout p le graphe $\mathrm{K}_n(p)$ est connexe.*

Démonstration. Soient L et M deux réseaux unimodulaires pairs de même dimension ; il faut montrer qu'il existe une suite finie de réseaux unimodulaires pairs

$$L = L_0\,,\, L_1\,,\, L_2\,,\, \ldots\,,\, L_{m-1}\,,\, L_m = M$$

avec L_k et L_{k+1} (abstraitement) p-voisins pour $0 \leq k \leq m-1$.

Le théorème II.2.8 montre qu'il existe un isomorphisme de q-modules ϕ : $\mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} L \to \mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} M$. Quitte à remplacer M par $\phi^{-1}(M)$, on peut donc supposer $M \subset \mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} L \subset \mathbb{Q} \otimes_{\mathbb{Z}} L$; on pose $V = \mathbb{Q} \otimes_{\mathbb{Z}} L = \mathbb{Q} \otimes_{\mathbb{Z}} M$. On rappelle maintenant ce que dit le point (a) de 1.1. On considère L et M comme des réseaux de V et on pose $N = L \cap M$. On a $N^\sharp = L + M$ et $\operatorname{rés} N = L/N \oplus M/N$ (comme groupe abélien). On pose $I = L/N$ et $J = M/N$; l'accouplement $I \times J \to \mathbb{Q}/\mathbb{Z}$, induit par la forme d'enlacement de $\operatorname{rés} N$, est non dégénéré. On en déduit que J et $\operatorname{rés} N$ sont canoniquement isomorphes, respectivement

au dual de Pontryagin $I^\vee$ et au qe-module d'enlacement hyperbolique $\mathrm{H}(I)$. Puisque l'on a $M \subset \mathbb{Z}[\frac{1}{p}] \otimes_{\mathbb{Z}} L$, le groupe abélien fini I est un p-groupe ; soit

$$I = I_0 \supset I_1 \supset I_2 \supset \ldots \supset I_{m-1} \supset I_m = 0$$

une suite finie décroissante de sous-groupes de I avec $I_k/I_{k+1} \simeq \mathbb{Z}/p$ pour $0 \leq k \leq m-1$. Soit

$$0 = J_0 \subset J_1 \subset I_2 \subset \ldots \subset J_{m-1} \subset J_m = J$$

la suite "orthogonale" de sous-groupes de J. On pose $K_k = I_k \oplus J_k$; on constate que K_k est un lagrangien de $\mathrm{rés}\, N$. On note L_k l'image inverse de K_k par l'homomorphisme canonique $N^\sharp \to \mathrm{rés}\, N$. Par construction

$$L = L_0\,,\, L_1\,,\, L_2\,,\, \ldots\,,\, L_{m-1}\,,\, L_m = M$$

est une suite de réseaux unimodulaires pairs avec L_k et L_{k+1} (concrètement) p-voisins pour $0 \leq k \leq m-1$. □

Miscellanées

On rassemble sous cet intertitre quatre énoncés plus ou moins techniques (1.13, 1.14, 1.16 et 1.17), concernant la notion de d-voisinage, que nous invoquerons par la suite.

Le moins technique des quatre est l'énoncé 1.13 ci-dessous ; sa démonstration, qui est une illustration de la proposition II.1.1, est laissée au lecteur.

Proposition 1.13. *Soient L un* q*-module sur $\mathbb{Z}$ et $d \geq 2$ un nombre entier ; soit u un élément d-primitif de L avec $\mathrm{q}(u) \equiv 0 \bmod d^2$. On suppose $d = d_1 d_2$ avec $d_1 \geq 2$ et $d_2 \geq 2$. Alors $\frac{u}{d_1}$ est un élément d_2-primitif de $\mathrm{vois}_{d_1}(L;u)$ et l'on a, dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$, l'égalité suivante*

$$\mathrm{vois}_d(L;u) \;=\; \mathrm{vois}_{d_2}(\mathrm{vois}_{d_1}(L;u); \frac{u}{d_1}) \qquad .$$

Proposition 1.14. *Soient L un* q*-module sur $\mathbb{Z}$ et $d \geq 2$ un nombre entier ; soit u un élément d-primitif de L avec $\mathrm{q}(u) = d$. On note s_u la symétrie orthogonale de $\mathbb{Q} \otimes_{\mathbb{Z}} L$ par rapport à l'hyperplan $u^\perp$.*

(a) *On a dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ l'égalité*

$$\mathrm{vois}_d(L;u) \;=\; \mathrm{s}_u(L) \qquad ;$$

en particulier $\mathrm{vois}_d(L;u)$ est isomorphe à L.

(b) *On suppose* $d = d_1 d_2$ *avec* $d_1 \geq 2$ *et* $d_2 \geq 2$. *Alors* u *est* d_i*-primitif pour* $i = 1, 2$ *et l'on a dans* $\mathbb{Q} \otimes_{\mathbb{Z}} L$ *l'égalité*

$$\mathrm{vois}_{d_2}(L; u) \;=\; \mathrm{s}_u(\mathrm{vois}_{d_1}(L; u)) \qquad ;$$

en particulier $\mathrm{vois}_{d_1}(L; u)$ *et* $\mathrm{vois}_{d_2}(L; u)$ *sont isomorphes.*

Démonstration. Explicitons s_u :

$$\mathrm{s}_u(x) \;=\; x - \frac{u.x}{d}\, u$$

pour tout x dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$. Cette expression montre que s_u induit un automorphisme de $\mathrm{M}_d(L; u)$ comme $\widetilde{\mathrm{q}}$-module sur $\mathbb{Z}$ et donc un automorphisme de $\mathrm{rés}\, \mathrm{M}_d(L; u)$ comme qe-module sur $\mathbb{Z}$. Soient I et J les deux lagrangiens transverses de $\mathrm{rés}\, \mathrm{M}_d(L; u)$ correspondant respectivement, *via* le point (b) de II.1.1, aux réseaux L et $\mathrm{vois}_d(L; u)$. Soit v un élément de L avec $u.v \equiv 1 \bmod d$; on rappelle que I et J sont respectivement engendrés par les classes dans $\mathrm{rés}\, \mathrm{M}_d(L; u)$ de v et $\frac{1}{d}(u - \mathrm{q}(u)v)$. On constate que l'on a $\mathrm{s}_u(I) = J$; cette égalité implique le point (a) de la proposition.

On constate que les réseaux $\mathrm{vois}_{d_1}(L; u)$ et $\mathrm{vois}_{d_2}(L; u)$ correspondent, *via* la bijection du point (b) de II.1.1, respectivement aux lagrangiens $d_1 I \oplus d_2 J$ et $d_2 I \oplus d_1 J$ de $\mathrm{rés}\, \mathrm{M}_d(L; u)$. D'après ce qui précède, on a $\mathrm{s}_u(d_1 I \oplus d_2 J) = d_2 I \oplus d_1 J$; cette égalité implique le point (b) de la proposition. □

Remarque. Si l'on convient que L est le seul 1-voisin de L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ alors le point (a) de la proposition 1.14 apparaît comme un cas particulier de son point (b).

Proposition 1.15. *Soit* L *un* b*-module sur* $\mathbb{Z}$. *On suppose qu'il existe un élément* e *de* L *avec* $e.e = 1$ *(et donc que* L *est impair). Alors la symétrie orthogonale de* L *par rapport à l'hyperplan* $e^{\perp}$ *échange les deux classes de vecteurs de Wu de* L.

Démonstration. Soient s_e la symétrie en question et u un vecteur de Wu de L ; l'égalité $\mathrm{s}_e(u) = u - 2(e.u)e$ et la congruence $e.u \equiv e.e \bmod 2$ montrent que les vecteurs de Wu u et $\mathrm{s}_e(u)$ sont non équivalents. □

Corollaire 1.16. *Soit* L *un réseau unimodulaire impair de dimension divisible par* 8. *On suppose qu'il existe un élément* e *de* L *avec* $e.e = 1$. *Alors la symétrie orthogonale de* $\mathbb{Q} \otimes_{\mathbb{Z}} L$ *par rapport à l'hyperplan* $e^{\perp}$ *échange les deux réseaux unimodulaires pairs* 2*-voisins de* L.

La proposition suivante, dont la vérification est immédiate, montre que le point (a) de la proposition 1.14, dans le cas particulier $d = 2$, et le corollaire 1.16 sont intimement reliés.

Proposition 1.17. *Soient L un réseau unimodulaire pair et u un élément de L avec $\mathrm{q}(u) = 2$ (égalité qui implique que u est 2-primitif). Soit B le réseau impair de $\mathbb{Q} \otimes_{\mathbb{Z}} L$ dont les 2-voisins pairs sont L et $\mathrm{vois}_2(L; u)$ (voir la fin de la discussion intitulée "2-voisins, le point de vue de Borcherds"). On note e l'élément $\frac{u}{2}$ de $\mathbb{Q} \otimes_{\mathbb{Z}} L$. Alors :*
– on a $e.e = 1$;
– le réseau B est engendré dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ par $\mathrm{M}_2(L; u)$ et e ;
- les symétries orthogonales s_u et s_e de $\mathbb{Q} \otimes_{\mathbb{Z}} L$ coïncident.

2. Sur les opérateurs de Hecke associés à la notion de voisinage

Soit $n > 0$ un entier divisible par 8 ; on rappelle que l'on note X_n l'ensemble fini des classes d'isomorphisme de réseaux unimodulaires de dimension n.

On note $\mathbb{Z}[\mathrm{X}_n]$ le $\mathbb{Z}$-module libre engendré par l'ensemble X_n.

Soient A un groupe abélien fini et L un réseau unimodulaire pair de dimension n ; on note $\mathrm{Vois}_A(L)$ l'ensemble fini constitué des A-voisins de L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ (la notation $\mathrm{Vois}_d(-)$ introduite dans le paragraphe précédent est donc une abréviation de $\mathrm{Vois}_{\mathbb{Z}/d}(-)$).

L'opérateur de Hecke T_A est l'endomorphisme de $\mathbb{Z}[\mathrm{X}_n]$ défini par

$$\mathrm{T}_A[L] \ := \sum_{L' \in \mathrm{Vois}_A(L)} [L'] \qquad ,$$

pour tout réseau unimodulaire pair L de dimension n.

Remarques
– Soit $\mathrm{r}(A)$ le nombre minimum de générateurs du groupe abélien A. Le point (b) de 1.1 montre que T_A est nul si l'on a $2\mathrm{r}(A) > n$. On pourrait donc supposer $2\mathrm{r}(A) \leq n$ dans la définition ci-dessus.
– Soient A et B deux groupes abéliens finis ; il n'est pas trop difficile de se convaincre de ce que les opérateurs de Hecke T_A et T_B commutent si les cardinaux de A et B sont premiers entre eux. En fait, T_A et T_B commutent pour tous A et B ; ceci sera démontré et largement généralisé au chapitre IV.

Soit $d \geq 2$ un entier ; on abrégera la notation $\mathrm{T}_{\mathbb{Z}/d}$ en T_d. Par définition même des entiers $\mathrm{N}_d(x, y)$ on a :

$$\mathrm{T}_d\, x \ = \sum_{y \in \mathrm{X}_n} \mathrm{N}_d(x, y)\, y$$

pour tout x dans X_n. En d'autres termes, si l'on considère T_d comme une $(\mathrm{X}_n, \mathrm{X}_n)$-matrice, alors son coefficient d'indice (y, x) est $\mathrm{N}_d(x, y)$.

La proposition 1.5 montre que l'on a aussi

$$\mathrm{T}_d[L] \;=\; \sum_{c \in \mathrm{C}_L(\mathbb{Z}/d)} [\mathrm{Vois}_d(L; c)]$$

pour tout réseau unimodulaire pair L.

Nous dégageons l'énoncé 2.2 ci-dessous en vue de futures références. Cet énoncé est impliqué par 2.1 et 1.5 ; l'énoncé 2.1 est quant à lui essentiellement conséquence de II.2.5.

Proposition-Définition 2.1. *Soient L un réseau unimodulaire pair et $d \geq 2$ un entier. Alors le* q*-module $\mathbb{Z}/d \otimes_{\mathbb{Z}} L$ est hyperbolique. En particulier, le cardinal de la quadrique $\mathrm{C}_L(\mathbb{Z}/d)$ ne dépend que la dimension de L, disons n, on le note $\mathrm{c}_n(d)$. On a*

$$\mathrm{c}_n(p) \;=\; \sum_{m=0}^{n-2} p^m \;+\; p^{\frac{n}{2}-1}$$

pour tout nombre premier p.

Remarque (suite). Le calcul de $\mathrm{c}_n(d)$ pour tout d, se déduit facilement du calcul pour d premier et du fait que les quadriques C_L sont lisses sur $\mathbb{Z}$.

Proposition 2.2. *Soit $d \geq 2$ un entier. On a*

$$\sum_{y \in \mathrm{X}_n} \mathrm{N}_d(x, y) \;=\; \mathrm{c}_n(d)$$

pour tout x dans X_n.

Remarques (suite et fin)

– Le scholie 1.7 peut être reformulé de la façon suivante :

Proposition 2.3. *Soit $d \geq 2$ un entier. L'endomorphisme T_d de $\mathbb{Z}[\mathrm{X}_n]$ est auto-adjoint pour le produit scalaire, disons $(-|-)$, défini par*

$$(x|y) \;=\; |\mathrm{O}(x)|\; \delta_{x,y}$$

pour x et y dans X_n (la notation $\delta_{x,y}$ désignant le symbole de Kronecker).

Là encore, cet énoncé sera largement généralisé au chapitre IV.

– Soit $\epsilon : \mathbb{Z}[\mathrm{X}_n] \to \mathbb{Z}$ l'homomorphisme de $\mathbb{Z}$-modules défini par $\epsilon(x) = 1$ pour tout x dans X_n ; la proposition 2.2 dit que l'on a $\epsilon \circ \mathrm{T}_d = \mathrm{c}_n(d)\epsilon$, en d'autres termes, que ϵ est vecteur propre de l'endomorphisme T_d^* de $(\mathbb{Z}[\mathrm{X}_n])^*$, pour la valeur propre $\mathrm{c}_n(d)$ (la notation T_d^* est une notation alternative pour la notation $\mathrm{T}_d^{\mathrm{t}}$ utilisée par ailleurs). Cette observation et la proposition 2.3 conduisent à l'énoncé suivant :

Proposition 2.4. *Soit $d \geq 2$ un entier. L'élément*

$$\sum_{x \in \mathrm{X}_n} \frac{1}{|\mathrm{O}(x)|}\, x$$

de $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{X}_n]$ est vecteur propre de T_d pour la valeur propre $\mathrm{c}_n(d)$.

– La proposition 2.3 implique que T_d est diagonalisable, au moins après extension des scalaires à $\mathbb{R}$. En fait, pour $n = 8, 16, 24$, les valeurs propres de T_d sont entières. C'est trivial pour $n = 8$ puisque l'on a $|\mathrm{X}_8| = 1$; cela l'est presque autant pour $n = 16$ puisque l'on a $|\mathrm{X}_{16}| = 2$ et que l'on connaît déjà une valeur propre entière, à savoir $\mathrm{c}_{16}(d)$. Le cas $n = 24$ requiert davantage d'efforts. Nous expliquerons en 3.3 comment Gabriele Nebe et Boris Venkov ont déterminé T_2, à partir de travaux de Borcherds ; on constate (merci `PARI`) que les racines du polynôme caractéristique de T_2 sont entières et simples. Puisque T_d commute avec T_2 pour tout d, les vecteurs propres de T_2 sont aussi propres pour T_d et les valeurs propres de T_d sont entières.

L'étude des propriétés arithmétiques de ces valeurs propres, pour d premier, est la motivation du présent travail.

3. Exemples

3.1. Détermination de T_2 pour $n = 16$

Il est bien connu que l'homomorphisme canonique $\mathrm{O}(\mathrm{E}_8) \to \mathrm{O}(\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8)$ induit un isomorphisme $\mathrm{O}(\mathrm{E}_8)/\{\pm 1\} \cong \mathrm{O}(\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8)$ (voir par exemple [Bou81b, Ch. VI, §4, Exc. 1]). Il en résulte que l'action de $\mathrm{O}(\mathrm{E}_8)$ partitionne $\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8 - \{0\}$ en deux orbites à savoir $\mathrm{q}^{-1}(0)$ et $\mathrm{q}^{-1}(1)$; ces deux orbites ont respectivement 135 et 120 éléments.

On considère maintenant les réseaux $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16} que l'on plonge de façon standard dans $\mathbb{Q}^{16}$; on note $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{16})$ la base canonique de $\mathbb{Q}^{16}$.

Il est clair que le groupe $\mathrm{O}(\mathrm{E}_8 \oplus \mathrm{E}_8)$ est canoniquement isomorphe au produit en couronne $\mathfrak{S}_2 \wr \mathrm{O}(\mathrm{E}_8)$. D'après ce qui précède, l'action de $\mathrm{O}(\mathrm{E}_8 \oplus \mathrm{E}_8)$ partitionne la quadrique $\mathrm{C}_{\mathrm{E}_8 \oplus \mathrm{E}_8}(\mathbb{F}_2)$ en trois orbites :

– l'orbite du point $[2\varepsilon_1]$ (le vecteur $2\varepsilon_1$ appartient au réseau $\mathrm{E}_8 \oplus \mathrm{E}_8$ et vérifie $\mathrm{q}(2\varepsilon_1) = 2$, la notation $[2\varepsilon_1]$ désigne sa classe dans $\mathrm{C}_{\mathrm{E}_8 \oplus \mathrm{E}_8}(\mathbb{F}_2)$), cette orbite a $2 \times 135 = 270$ éléments ;

– l'orbite du point $[\varepsilon_1 + \varepsilon_2 + \varepsilon_9 + \varepsilon_{10}]$ (on observera que l'on a à nouveau $\mathrm{q}(\varepsilon_1 + \varepsilon_2 + \varepsilon_9 + \varepsilon_{10}) = 2$), cette orbite a $120^2 = 14400$ éléments ;

– l'orbite du point $[2\varepsilon_1 + 2\varepsilon_9]$ (on observera que l'on a cette fois $\mathrm{q}(2\varepsilon_1 + 2\varepsilon_9) = 4$), cette orbite a $135^2 = 18225$ éléments.

D'après le point (a) de 1.14, le réseau $\mathrm{vois}_2(\mathrm{E}_8 \oplus \mathrm{E}_8; c)$ est isomorphe (comme q-module) à $\mathrm{E}_8 \oplus \mathrm{E}_8$ pour tout c dans l'une des deux premières orbites.

Comme le graphe des 2-voisins est connexe (Théorème 1.12), on a forcément $\mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16}) = 18225$. Compte tenu de 1.7 et 2.2, cette égalité détermine l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{16}] \to \mathbb{Z}[\mathrm{X}_{16}]$; sa matrice dans la base $(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)$, disons encore T_2, est la suivante :

$$\mathrm{T}_2 = \begin{bmatrix} 20025 & 18225 \\ 12870 & 14670 \end{bmatrix} \qquad .$$

En fait, il est facile de vérifier que l'on a $\mathrm{vois}_2(\mathrm{E}_8 \oplus \mathrm{E}_8; [2\varepsilon_1 + 2\varepsilon_9]) = \mathrm{E}_{16}$ (ce qui implique $\mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16}) = 18225$). En effet, on constate que le réseau $\mathrm{M}_2(\mathrm{E}_8 \oplus \mathrm{E}_8; [2\varepsilon_1 + 2\varepsilon_9])$ est engendré par $\mathrm{D}_8 \oplus \mathrm{D}_8$ et $\frac{1}{2}\sum_{i=1}^{16} \varepsilon_i$ [le premier (resp. second) D_8 est l'orthogonal modulo 2 dans le premier (resp. second) E_8 du vecteur $2\varepsilon_1$ (resp. $2\varepsilon_9$)]. Comme l'on a $\mathrm{q}(2\varepsilon_1 + 2\varepsilon_9) = 4$, le réseau $\mathrm{vois}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, [2\varepsilon_1 + 2\varepsilon_9])$ est engendré par $\mathrm{M}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, [2\varepsilon_1 + 2\varepsilon_9])$ et $\varepsilon_1 + \varepsilon_9$ (se rappeler l'algorithme $u \rightsquigarrow \mathrm{vois}_d(L; u)$). Or le réseau engendré par $\mathrm{D}_8 \oplus \mathrm{D}_8$ et $\varepsilon_1 + \varepsilon_9$ est D_{16} si bien que le réseau $\mathrm{vois}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, [2\varepsilon_1 + 2\varepsilon_9])$ coïncide avec le réseau engendré par D_{16} et $\frac{1}{2}\sum_{i=1}^{16} \varepsilon_i$, c'est-à-dire E_{16}.

Variante. Pour illustrer 1.8, et accessoirement pour nous rassurer, nous considérons maintenant les 2-voisins de E_{16}.

Le groupe $\mathrm{O}(\mathrm{E}_{16})$ s'identifie au sous-groupe de $\mathrm{O}(\mathrm{I}_{16})$ constitué des éléments qui préservent la classe (au sens de la discussion qui suit le scholie II.2.3) du vecteur de Wu $\sum_{i=1}^{16} \varepsilon_i$. On a donc un isomorphisme canonique $\mathrm{O}(\mathrm{E}_{16}) \cong \mathfrak{S}_{16} \ltimes (\{\pm 1\}^{16})^0$, la notation $(\{\pm 1\}^{16})^0$ désignant le sous-groupe de $\{\pm 1\}^{16}$ constitué des 16-uples $(\eta_1, \eta_2, \ldots, \eta_{16})$ avec $\eta_1 \eta_2 \ldots \eta_{16} = 1$.

On constate que l'action de $\mathrm{O}(\mathrm{E}_{16})$ partitionne la quadrique $\mathrm{C}_{\mathrm{E}_{16}}(\mathbb{F}_2)$ en quatre orbites :

– l'orbite du point $[2\varepsilon_1]$ (le vecteur $2\varepsilon_1$ appartient au réseau E_{16} et vérifie $\mathrm{q}(2\varepsilon_1) = 2$), cette orbite a un seul élément ;

– l'orbite du point $[\sum_{i=1}^{4} \varepsilon_i]$ (on observera que l'on a $\mathrm{q}(\sum_{i=1}^{4} \varepsilon_i) = 2$), cette orbite a $2\binom{16}{4} = 3640$ éléments ;

– l'orbite du point $[\sum_{i=1}^{8} \varepsilon_i]$ (on observera que l'on a $\mathrm{q}(\sum_{i=1}^{8} \varepsilon_i) = 4$), cette orbite a $\binom{16}{8} = 12870$ éléments.

– l'orbite du point $[\frac{1}{2}\sum_{i=1}^{16} \varepsilon_i]$ (on observera que l'on a $\mathrm{q}(\frac{1}{2}\sum_{i=1}^{16} \varepsilon_i) = 2$), cette orbite a $2^{14} = 16384$ éléments.

Toujours d'après le point (a) de 1.14, le réseau $\mathrm{vois}_2(\mathrm{E}_{16}; c)$ est isomorphe (comme q-module) à E_{16} pour tout c qui n'est pas dans la troisième orbite.

On conclut comme précedemment : comme le graphe des 2-voisins est connexe, on a forcément $\mathrm{N}_2(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8) = 12870$.

3.2. Détermination de T_3 pour $n = 16$

On plonge toujours E_{16} de façon standard dans $\mathbb{Q}^{16}$. On constate que l'action de $\mathrm{O}(\mathrm{E}_{16})$ partitionne la quadrique $\mathrm{C}_{\mathrm{E}_{16}}(\mathbb{F}_3)$ en cinq orbites, à savoir les orbites des classes des vecteurs suivants de E_{16} (qui appartiennent en fait à D_{16}) :

– $u_1 = 2\varepsilon_1 + \varepsilon_2 + \varepsilon_3$;

– $u_2 = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_6$;

– $u_3 = 2\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \ldots + \varepsilon_9$;

– $u_4 = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{12}$;

– $u_5 = 2\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \ldots + \varepsilon_{15}$.

On constate que l'on a $(\mathrm{q}(u_i))_{i=1,2,\ldots,5} = (3, 3, 6, 6, 9)$. D'après 1.14 (a), le réseau $\mathrm{vois}_3(\mathrm{E}_{16}, [u_i])$ est isomorphe (comme q-module) à E_{16} pour $i = 1, 2$. On constate que le cardinal de l'orbite de $[u_i]$ est $\binom{16}{3i} 2^{3i-1}$. Ce cardinal n'est pas divisible par 286 pour $i = 4, 5$; d'après 1.8 le réseau $\mathrm{vois}_3(\mathrm{E}_{16}; [u_i])$ est encore isomorphe (comme q-module) à E_{16} pour $i = 4, 5$. En effet, on a

$$\frac{|\mathrm{O}(\mathrm{E}_8 \oplus \mathrm{E}_8)|}{|\mathrm{O}(\mathrm{E}_{16})|} = \frac{405}{286}$$

avec 405 et 286 premiers entre eux ; le scholie 1.8 montre que si $\mathrm{vois}_3(\mathrm{E}_{16}; [u_i])$ est isomorphe à $\mathrm{E}_8 \oplus \mathrm{E}_8$ alors le cardinal de l'orbite de $[u_i]$ est divisible par 286.

Puisque le graphe des 3-voisins est connexe, le réseau $\mathrm{vois}_3(\mathrm{E}_{16}; [u_3])$ doit être isomorphe (comme q-module) à $\mathrm{E}_8 \oplus \mathrm{E}_8$ (ce que le logiciel `PARI` confirme) et

on a $\mathrm{N}_3(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8) = \binom{16}{9} 2^8 = 2928640$. Compte tenu de 1.7 et 2.2, cette égalité détermine l'opérateur de Hecke $\mathrm{T}_3 : \mathbb{Z}[\mathrm{X}_{16}] \to \mathbb{Z}[\mathrm{X}_{16}]$; sa matrice dans la base $(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)$, disons encore T_3, est la suivante :

$$\mathrm{T}_3 = \begin{bmatrix} 4248000 & 4147200 \\ 2928640 & 3029440 \end{bmatrix} \qquad .$$

3.3. Détermination de T_2 pour $n = 24$ (d'après Nebe-Venkov [NV01])

Soit $n > 0$ un entier divisible par 8.

Nous avons expliqué au paragraphe 1, en suivant Borcherds, pourquoi l'ensemble $\mathrm{Y}_n(2)$ des classes d'isomorphisme des couples (L_1, L_2), L_1 désignant un réseau unimodulaire pair de dimension n et L_2 un 2-voisin de L_1 dans $\mathbb{Q} \otimes_{\mathbb{Z}} L_1$, est naturellement en bijection avec l'ensemble $\widetilde{\mathrm{B}}_n$ des classes d'isomorphismes des couples $(L; \omega)$, L désignant un réseau unimodulaire impair de dimension n et ω une bijection de l'ensemble des deux classes de vecteurs de Wu de L sur $\{1, 2\}$. Rappelons que nous avons noté B_n l'ensemble des classes d'isomorphisme de réseaux unimodulaires L impairs de dimension n ; nous notons en outre B_n^1 le sous-ensemble de B_n constitué des $[L]$ telles que L représente 1 (en clair, tels qu'il existe e dans L avec $e.e = 1$) et B_n^2 le complémentaire $\mathrm{B}_n - \mathrm{B}_n^1$. Dans [Bor84], Borcherds utilise la bijection $\mathrm{Y}_{24}(2) \cong \widetilde{\mathrm{B}}_{24}$ pour déterminer B_{24}. Il explicite dans [CS99, Chap. 17] la liste des 156 éléments b de B_{24}^2 et donne, pour chacun de ces b, suffisamment d'informations pour déterminer $|\mathrm{O}(b)|$. La raison pour laquelle il se limite à B_{24}^2 est qu'un réseau L qui représente 1 est isomorphe à une somme orthogonale $\mathrm{I}_1 \oplus L'$ et que l'énumération des réseaux unimodulaires, ne représentant pas 1, de dimension strictement inférieure à 23, avait déjà été faite (voir [CS99, Chap. 16, Table 16.7], B_{24}^1 a 117 éléments). On observera, avec Nebe et Venkov, que si un réseau unimodulaire impair L, de dimension n, représente 1, alors les deux réseaux unimodulaires pairs 2-voisins de L sont isomorphes d'après 1.16. Soit $\mathrm{B}_n^{2,0}$ le sous-ensemble de B_n^2 constitué des classes d'isomorphisme des réseaux unimodulaires impairs L, de dimension n, tels que les deux réseaux unimodulaires pairs 2-voisins de L, disons L_1 et L_2, sont non isomorphes ; soit e l'application de $\mathrm{B}_n^{2,0}$ dans l'ensemble des paires d'éléments de X_n, qui associe à $[L]$ la paire $\{[L_1], [L_2]\}$. La proposition 1.11 se spécialise de la façon suivante :

Proposition 3.3.1. *Soient x_1 et x_2 deux éléments distincts de X_n. On a :*

$$\mathrm{N}_2(x_1, x_2) \;=\; \sum_{b \,\in\, \mathrm{e}^{-1}(\{x_1, x_2\})} \frac{|\mathrm{O}(x_1)|}{|\mathrm{O}(b)|} \qquad .$$

Nebe et Venkov déterminent T_2 à l'aide de l'énoncé ci-dessus et de la table de Borcherds, en tenant compte de 2.2 ; attention, nos conventions font que la matrice $(24, 24)$ de [NV01, page 59] est la transposée de notre T_2.

Remarques

– La proposition 1.11 donne pour $n = 8$ la relation

$$\frac{|\mathrm{O}(\mathrm{E}_8)|}{|\mathrm{O}(\mathrm{I}_8)|} = \frac{\mathrm{c}_8(2)}{2} \quad .$$

Plus généralement, la proposition 1.11 conduit, pour tout n divisible par 8, à la relation suivante entre formules de masses

$$(*) \qquad \sum_{b \in \mathrm{B}_n} \frac{1}{|\mathrm{O}(b)|} = \frac{\mathrm{c}_n(2)}{2} \sum_{x \in \mathrm{X}_n} \frac{1}{|\mathrm{O}(x)|}$$

(voir [CS99, Chap. 16, §2]). Expliquons pourquoi. La proposition 1.11 dit que l'on a

$$\mathrm{N}_2(x, y) \, \frac{1}{|\mathrm{O}(x)|} = \sum_{\mathrm{d}_1(\beta)=x \, , \, \mathrm{d}_2(\beta)=y} \frac{1}{|\mathrm{O}(\beta)|}$$

pour tous x et y dans X_n ; en sommant en y puis en x on obtient

$$(**) \qquad \sum_{\beta \in \widetilde{\mathrm{B}}_n} \frac{1}{|\mathrm{O}(\beta)|} = \mathrm{c}_n(2) \sum_{x \in \mathrm{X}_n} \frac{1}{|\mathrm{O}(x)|} \quad .$$

Soit $\mathrm{p} : \widetilde{\mathrm{B}}_n \to \mathrm{B}_n$ l'application évidente ; l'égalité

$$\sum_{\beta \in \mathrm{p}^{-1}(b)} \frac{1}{|\mathrm{O}(\beta)|} = \frac{2}{|\mathrm{O}(b)|}$$

montre que les relations $(*)$ et $(**)$ sont équivalentes.

– L'analyse que nous avons faite en 3.1 des 2-voisinages entre réseaux unimodulaires pairs de dimension 16 conduit à l'énoncé ci-dessous que nous utiliserons dans l'appendice A. Comme en 3.1, on identifie de façon standard les réseaux E_{16}, $\mathrm{E}_8 \oplus \mathrm{E}_8$ et $\mathrm{D}_8 \oplus \mathrm{D}_8$ à des réseaux de $\mathbb{Q}^{16}$ dont on note $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{16})$ la base canonique.

Scholie-Définition 3.3.2. *Le réseau de* $\mathbb{Q}^{16}$ *engendré par*

$$\mathrm{D}_8 \oplus \mathrm{D}_8 \qquad , \qquad \frac{1}{2}\sum_{i=1}^{16} \varepsilon_i \qquad , \qquad -\varepsilon_1 - \varepsilon_9 + \frac{1}{2}\sum_{i=1}^{8} \varepsilon_i$$

est un réseau unimodulaire impair que l'on note Bor_{16} *; ses* 2*-voisins pairs sont* E_{16} *et* $\mathrm{E}_8 \oplus \mathrm{E}_8$*. Le réseau* Bor_{16} *est, à isomorphisme près, le seul réseau unimodulaire impair de dimension* 16 *qui ne représente pas* 1*. Le système de racines* $\mathrm{R}(\mathrm{Bor}_{16})$ *est isomorphe à* $\mathbf{D}_8 \coprod \mathbf{D}_8$*.*

Démonstration. Soit B un réseau unimodulaire impair de dimension 16 dont les 2-voisins pairs sont isomorphes ; l'analyse évoquée ci-dessus et la proposition 1.17 montrent que B représente 1. Soit maintenant B un réseau unimodulaire impair de dimension 16 qui ne représente pas 1 ; d'après ce qui précède les 2-voisins pairs de B sont isomorphes, l'un à E_{16}, l'autre à $\mathrm{E}_8 \oplus \mathrm{E}_8$. Soit M le sous-module de B constitué des éléments x avec $x.x$ pair ; d'après l'analyse en question M est isomorphe (comme $\widetilde{\mathrm{q}}$-module) à la fois, au sous-module de E_{16} orthogonal modulo 2 de l'élément $\sum_{i=1}^{8} \varepsilon_i$ et au sous-module de $\mathrm{E}_8 \oplus \mathrm{E}_8$ orthogonal modulo 2 de l'élément $2\varepsilon_1 + 2\varepsilon_9$. On constate que ces deux orthogonaux modulo 2, vus comme des réseaux de $\mathbb{Q}^{16}$, coïncident avec le réseau, disons M_{16}, engendré par $\mathrm{D}_8 \oplus \mathrm{D}_8$ et $\frac{1}{2}\sum_{i=1}^{16} \varepsilon_i$; en effet M_{16} est d'indice 2 à la fois dans E_{16} et $\mathrm{E}_8 \oplus \mathrm{E}_8$ et l'on a $(\sum_{i=1}^{8} \varepsilon_i).x \equiv 0 \bmod 2$ (resp. $(2\varepsilon_1 + 2\varepsilon_9).x \equiv 0 \bmod 2$) pour tout x dans M_{16}. Incidemment, ceci montre que l'on a $\mathrm{M}_{16} = \mathrm{E}_{16} \cap (\mathrm{E}_8 \oplus \mathrm{E}_8)$. Soit ξ l'élément $-\varepsilon_1 - \varepsilon_9 + \frac{1}{2}\sum_{i=1}^{8} \varepsilon_i$ de $\mathbb{Q}^{16}$; on constate que ξ appartient à $\mathrm{M}_{16}^{\sharp}$ et que l'on a $\xi.\xi = 3$, il en résulte que ξ engendre la droite "non quadratiquement isotrope" de $\mathrm{rés}\,\mathrm{M}_{16}$, si bien que Bor_{16} est le réseau unimodulaire impair correspondant à M_{16} par la théorie de Borcherds. D'après cette théorie $M \simeq \mathrm{M}_{16}$ implique $B \simeq \mathrm{Bor}_{16}$ (Bor_{16} ne représente pas 1 car ses 2-voisins pairs ne sont pas isomorphes). La dernière assertion du scholie se démontre à l'aide de II.3.7 (observer que l'on a $\mathrm{R}(\mathrm{M}_{16}) = \mathrm{R}(\mathrm{E}_{16}) \cap \mathrm{R}(\mathrm{E}_8 \oplus \mathrm{E}_8) \simeq \mathbf{D}_8 \coprod \mathbf{D}_8$ et que l'image par la fonction qm de la classe de ξ dans $\mathrm{rés}\,\mathrm{M}_{16}$ est forcément $\frac{3}{2}$ car $\xi.\xi = 1$ est interdit). $\square$

4. Sur les d-voisinages entre un réseau de Niemeier avec racines et le réseau de Leech

La raison d'être de ce paragraphe est la suivante :

Soit $d \geq 2$ un entier ; la détermination des entiers $\mathrm{N}_d(L, \mathrm{Leech})$, pour tout réseau de Niemeier avec racines L, entraîne celle de l'opérateur de Hecke T_d (dans l'expression $\mathrm{N}_d(L, \mathrm{Leech})$, "Leech" est une abréviation pour "réseau de Leech", celle-ci sera fréquemment utilisée dans la suite du mémoire).

Expliquons pourquoi. On a vu en 3.3, que l'on connaît explicitement, grâce à Nebe-Venkov, l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{24}] \to \mathbb{Z}[\mathrm{X}_{24}]$; on peut vérifier (merci `PARI`) que les éléments $\mathrm{T}_2^k[\text{Leech}]$, $0 \leq k \leq 23$, sont linéairement indépendants. Comme les opérateurs de Hecke T_d et T_2 commutent, la détermination de $\mathrm{T}_d[\text{Leech}]$ entraîne celle de T_d. Compte tenu de 1.7 et 2.2, la détermination de $\mathrm{T}_d[\text{Leech}]$ est quant à elle équivalente à celle des entiers $\mathrm{N}_d(x, [\text{Leech}])$, x décrivant l'ensemble $\mathrm{X}_{24} - \{[\text{Leech}]\}$.

4.1. Conditions nécessaires pour qu'un réseau de Niemeier avec racines puisse avoir un d-voisin sans racines

Proposition 4.1.1. *Soient L un réseau de Niemeier avec racines et $d \geq 2$ un entier ; soit $\mathrm{h}(L)$ le nombre de Coxeter de L (voir Proposition-Définition II.3.3). Si L a un d-voisin sans racines alors on a l'inégalité*

$$d \;\geq\; \mathrm{h}(L) \qquad .$$

Démonstration. On suppose qu'il existe un élément c de $\mathrm{C}_L(\mathbb{Z}/d)$ tel que l'on a $\mathrm{R}(\mathrm{vois}_d(L;c)) = \emptyset$. On a *a fortiori* $\mathrm{R}(\mathrm{M}_d(L;c)) = \emptyset$ (on rappelle que $\mathrm{M}_d(L;c)$ est l'intersection dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ des réseaux L et $\mathrm{vois}_d(L;c)$) ou encore $\mathrm{R}(L) \cap \mathrm{M}_d(L;c) = \emptyset$. Soit u un élément de L qui représente c, la condition $\mathrm{R}(\mathrm{vois}_d(L;c)) = \emptyset$ implique donc

$$\alpha.u \;\not\equiv\; 0 \pmod{d} \text{ pour tout } \alpha \text{ dans } \mathrm{R}(L) \qquad .$$

On constate que l'on a nécessairement l'inégalité $d \geq \mathrm{h}(L)$ en prenant dans la proposition ci-dessous, pour R une composante irréductible de $\mathrm{R}(L)$, et pour f la forme linéaire $x \mapsto x.u$. □

Proposition 4.1.2. *Soient V un $\mathbb{R}$-espace vectoriel de dimension finie et $R \subset V$ un système de racines irréductible et réduit ; soit h le nombre de Coxeter de R. Soit $f : V \to \mathbb{R}$ une forme linéaire dont la restriction à R prend des valeurs entières ; soit $d \geq 2$ un entier avec $d < h$. Alors il existe une racine α dans R telle que l'on a*

$$f(\alpha) \equiv 0 \pmod{d} \qquad .$$

Démonstration. On fixe une chambre C du système de racines R ; on note respectivement $\{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ et $\widetilde{\alpha}$, la base de R et la plus grande racine

correspondantes. On rappelle que l'on a $\widetilde{\alpha} = n_1\alpha_1 + n_2\alpha_2 + \cdots + n_l\alpha_l$ avec $n_i \in \mathbb{N} - \{0\}$ pour $i = 1, 2, \ldots, l$ et

$$\text{(hm)} \qquad n_1 + n_2 + \cdots + n_l = h - 1$$

[Bou81b, Ch. VI, §1, Prop. 31] (hm est pour "hauteur maximale"). On note enfin Alc l'alcôve de V^* contenue dans C à laquelle 0 est adhérent [Bou81b, Ch. VI, §2, Prop. 4] ; Alc (resp. $\overline{Alc}$) est donc l'ouvert (resp. le fermé) de V^* constitué des éléments ϕ vérifiant les inégalités $\langle \alpha_i, \phi \rangle > 0$ (resp. $\langle \alpha_i, \phi \rangle \geq 0$) pour $i = 1, 2, \ldots, l$ et $\langle \widetilde{\alpha}, \phi \rangle < 1$ (resp. $\langle \widetilde{\alpha}, \phi \rangle \leq 1$).

Soit ϕ un élément de V^*. Puisque $\overline{Alc}$ est un domaine fondamental pour l'action du groupe de Weyl affine sur V^* (voir par exemple [Bou81b, Ch. VI, §2, n° 1 et n° 2]), il existe un élément w du groupe de Weyl de R et un élément θ du réseau $\mathrm{Q}(R^\vee)$ de V^* tels que l'on a les inégalités

$$\langle w\alpha_i, \phi - \theta \rangle \geq 0 \ \text{ pour } i = 1, 2, \ldots, l \qquad \text{et} \qquad \langle w\widetilde{\alpha}, \phi - \theta \rangle \leq 1 \qquad .$$

On obtient une preuve de la proposition en prenant $\phi = \frac{1}{d} f$: il existe w et θ comme ci-dessus tels que l'on a les inégalités

$$f(w\alpha_i) - d\theta(w\alpha_i) \geq 0 \qquad \text{et} \qquad f(w\widetilde{\alpha}) - d\theta(w\widetilde{\alpha}) \leq d \qquad .$$

On observe que les $w\alpha_i$ et $w\widetilde{\alpha}$ sont des racines et que les $f(w\alpha_i)$, $\theta(w\alpha_i)$, $f(w\widetilde{\alpha})$ et $\theta(w\widetilde{\alpha})$ sont des entiers ; on pose $x_i = f(w\alpha_i) - d\theta(w\alpha_i)$ et $y = d - (f(w\widetilde{\alpha}) - d\theta(w\widetilde{\alpha}))$. On a $x_i \geq 0$, $y \geq 0$ et

$$n_1 x_1 + n_2 x_2 + \cdots + n_l x_l + y = d \qquad .$$

Compte tenu de l'égalité (hm), l'un des entiers x_1, x_2, …, x_l, y doit être nul, ce qui démontre bien la proposition. □

Remarque. En fait, nous n'utilisons la proposition 4.1.2 que pour des systèmes de racines irréductibles de type ADE, c'est à dire pour $R = \mathbf{A}_n$ $(n \geq 1)$, $R = \mathbf{D}_n$ $(n \geq 3)$, $R = \mathbf{E}_6$, $R = \mathbf{E}_7$, et $R = \mathbf{E}_8$. Il existe des démonstrations très simples de l'énoncé 4.1.2 dans les deux premiers cas. Nous traitons ci-dessous le second ; le traitement du premier est similaire (et d'ailleurs plus facile).

On munit $\mathbb{R}^n$ de sa structure euclidienne canonique ; on rappelle que l'on a $\mathbf{D}_n = \mathrm{R}(\mathrm{D}_n)$, D_n désignant le sous-module de $\mathbb{Z}^n$ constitué des n-uples $(x_1, x_2, \ldots, x_n)$ avec $\sum_{i=1}^n x_i$ pair. Une forme linéaire $f : \mathbb{R}^n \to \mathbb{R}$ qui prend des valeurs entières sur D_n induit une application linéaire $\mathbb{Z}^n \to \frac{1}{2}\mathbb{Z}$. On pose

$\lambda = 0$ (resp. $\lambda = 1$) si l'homomorphisme composé $\mathrm{D}_n \xrightarrow{f} \mathbb{Z} \to \mathbb{Z}/2$ est trivial (resp. non trivial) ; on pose $\nu_i = f(\varepsilon_i) - \frac{\lambda}{2}$, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ désignant la base canonique de $\mathbb{R}^n$ (les ν_i sont donc des entiers). On constate que si l'on a $f(\alpha) \not\equiv 0 \pmod{d}$ pour tout α dans $\mathbf{D}_n$ alors l'application de $\{1, 2, \ldots, n\}$ dans $\mathbb{Z}/d$ qui associe à i la classe modulo d de ν_i induit une injection de $\{1, 2, \ldots, n\}$ dans l'ensemble quotient de $\mathbb{Z}/d$ par l'involution $t \mapsto -t - \lambda$ (se rappeler que $\mathbf{D}_n$ est constitué des éléments $\pm\varepsilon_i \pm \varepsilon_j$, $i \neq j$). Or le cardinal du quotient en question est majoré par $\frac{d}{2} + 1$, on a donc $n \leq \frac{d}{2} + 1$ soit encore $d \geq 2n - 2$. $\square$

Notations relatives aux réseaux de Niemeier avec racines

Comme tous les énoncés de la suite de ce paragraphe 4 concernent les réseaux de Niemeier avec racines, nous récapitulons et complétons ci-dessous la liste des notations que nous utilisons pour ces réseaux.

Soit L un réseau de Niemeier avec racines :

– $R = \mathrm{R}(L)$ désigne l'ensemble des racines de L ;

– on pose $V = \mathbb{R} \otimes_{\mathbb{Z}} L$, V est un espace euclidien de dimension 24 et $R \subset V$ est un système de racines de type ADE, equicoxeter, de rang 24 ;

– $W = \mathrm{W}(L)$ désigne le groupe de Weyl du système de racines R, on rappelle que W s'identifie à un sous-groupe du groupe orthogonal $\mathrm{O}(L)$ (point (a) du scholie II.3.15) ;

– $Q = \mathrm{Q}(R) \subset L$ est le réseau de V engendré par R ;

– $Q^\sharp = (\mathrm{Q}(R))^\sharp \supset L$ est le réseau dual de Q ;

– $f = \mathrm{f}(L)$ désigne l'indice de Q dans $Q^\sharp$ (que Bourbaki appelle *indice de connexion* du système de racines R) ;

– $g = \mathrm{g}(L)$ désigne l'indice de Q dans L (compte tenu du fait que L/Q est un lagrangien du qe-module $Q^\sharp/Q$, on a $f = g^2$).

On note $R_1, R_2, \ldots, R_c$ les composantes irréductibles de R :

– le nombre de ces composantes irréductibles est donc $c = \mathrm{c}(L)$;

– toutes ces composantes irréductibles ont le même nombre de Coxeter, à savoir $h = \mathrm{h}(L)$.

On choisit une chambre C de R :

– $B \subset R$ désigne la base de R correspondant à ce choix ;

– $R_+ \subset R$ est l'ensemble des racines positives pour la relation d'ordre sur V définie par C ;

– $H \subset R_+ \subset R$ désigne l'ensemble des éléments maximaux de R pour l'ordre en question (l'ensemble H a c éléments, plus précisément on a $H \cap R_k = \{\widetilde{\alpha}_k\}$, $\widetilde{\alpha}_k$ désignant la plus grande racine de R_k).

On note Alc l'alcôve de V contenue dans C à laquelle 0 est adhérent ; Alc (resp. $\overline{Alc}$) est l'ouvert (resp. le fermé) de V constitué des éléments x vérifiant les inégalités $\alpha.x > 0$ (resp. $\alpha.x \geq 0$) pour $\alpha \in B$ et $\alpha.x < 1$ (resp. $\alpha.x \leq 1$) pour $\alpha \in H$.

On pose enfin $\Pi := Q^\sharp \cap \overline{Alc}$. Le sous-ensemble Π de $Q^\sharp$ s'identifie au produit d'ensembles $\prod_{k=1}^{c} \Pi(R_i)$ (la notation $\Pi(-)$ est introduite dans la proposition II.3.8, l'égalité $\Pi(S) = \mathrm{Q}(S)^\sharp \cap \overline{Alc}$ pour S un sytème de racines irréductible de type ADE est établie dans la démonstration de II.3.8 (a)).

La démonstration de la proposition 4.1.2 conduit au scholie suivant :

Scholie 4.1.3. *Soit L un réseau de Niemeier avec racines. Soient ξ un élément de $Q^\sharp$ et $d \geq 1$ un entier. Alors il existe un élément w de W et un élément x de Q tels que l'élément $\eta := w\xi + dx$ de $Q^\sharp$ appartient à $d\,\overline{Alc}$, en clair, tels que l'on a les inégalités $\alpha.\eta \geq 0$ pour $\alpha \in B$ et $\alpha.\eta \leq d$ pour $\alpha \in H$. De plus si l'on a $\alpha.\xi \not\equiv 0 \bmod d$ pour tout α dans R alors le couple (w, x) qui apparaît ci-dessus est uniquement déterminé en fonction de ξ.*

Soit x un élément de V ; on dit que x est *régulier* si l'on a $\alpha.x \neq 0$ pour tout α dans R (en d'autres termes, si x est dans une chambre). Soit $d \geq 1$ un entier ; nous dirons que x de V est *d-régulier* si l'on a $\alpha.x \notin d\mathbb{Z}$ pour tout α dans R (en d'autres termes, si $\frac{1}{d}x$ est dans une alcôve). Soit $d \geq 2$ un entier ; nous dirons qu'un élément de $\mathrm{P}_L(\mathbb{Z}/d)$ est *régulier* s'il est représenté par un élément d-régulier u de L, en clair vérifiant $\alpha.u \not\equiv 0 \bmod d$ pour tout α dans R (cette condition est indépendante du choix de u) ; le sous-ensemble de $\mathrm{P}_L(\mathbb{Z}/d)$ constitué de ces éléments sera noté $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$. On posera enfin $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/d) := \mathrm{C}_L(\mathbb{Z}/d) \cap \mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$. La démonstration que nous avons donnée de la proposition 4.1.1 revient en fait à vérifier l'énoncé plus précis suivant (le point (a) étant évident) :

Scholie 4.1.4. *Soient L un réseau de Niemeier avec racines et $d \geq 2$ un entier.*

(a) *Soit c un élément de $\mathrm{C}_L(\mathbb{Z}/d)$; si le réseau $\mathrm{vois}_d(L; c)$ est sans racines alors c appartient à $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/d)$.*

(b) *Si l'ensemble $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$ est non vide alors on a l'inégalité $d \geq \mathrm{h}(L)$.*

4.2. Sur les h-voisinages et $h+1$-voisinages entre un réseau de Niemeier avec racines de nombre de Coxeter h et le réseau de Leech

Soit L un réseau de Niemeier avec racines, de nombre de Coxeter h. On a vu dans le sous-paragraphe 4.1 qu'une condition nécessaire pour que L

ait pour d-voisin le réseau de Leech est l'inégalité $d \geq h$. On montre en particulier ci-après que cette inégalité est optimale ; ceci est intimement relié aux *holy constructions* du réseau de Leech dues à Conway et Sloane [CS82]. On détermine également l'entier $\mathrm{N}_d(L, \mathrm{Leech})$ pour $d = h, h+1$; ce calcul sera exploité en X.3.

Nous commençons par rappeler ce qu'est un vecteur de Weyl d'un réseau de Niemeier et par rassembler quelques-unes des propriétés de ces vecteurs que nous serons amenés à utiliser.

Vecteurs de Weyl

Soient L un réseau de Niemeier avec racines et $C \subset V$ une chambre du système de racines R. Soit ρ la demi-somme des racines positives (pour la relation d'ordre sur V définie par C) :

$$2\rho \;=\; \sum_{\alpha \in R_+} \alpha$$

(cette égalité montre que ρ appartient à $\frac{1}{2}L$, la proposition 4.2.1 ci-dessous dit que ρ appartient en fait à L). On dit que ρ est un *vecteur de Weyl* du système de racines R ou du réseau L. Soit α une racine de R alors α appartient à B si et seulement si l'on a $\rho.\alpha = 1$ (voir [Bou81b, Ch. VI, §1, Prop. 29]) ; cette observation montre que l'application $C \mapsto \rho$ est bijective. Il en résulte que l'action de W sur l'ensemble des vecteurs de Weyl est simplement transitive.

Proposition 4.2.1 (Borcherds)**.** *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors ρ appartient à L.*

Démonstration. Avant de reproduire l'argument donné par Borcherds dans [Bor84][Bor85], nous dégageons quelques énoncés qui nous seront utiles par la suite.

Proposition 4.2.2. *Soit L un réseau de Niemeier avec racines.*

(a) *On a*

$$h\, x.y \;=\; \sum_{\alpha \in R_+} (\alpha.x)(\alpha.y)$$

pour tous x et y dans V.

(b) *Soit ρ un vecteur de Weyl de L, on a*

$$h\mathrm{q}(x) - \rho.x \;=\; \sum_{\alpha \in R_+} \frac{(\alpha.x)^2 - \alpha.x}{2}$$

pour tout x dans V.

Démonstration. Le point (a) est un avatar de II.3.4. Le point (b) (dû à Borcherds) est conséquence du point (a) et de la définition de ρ. Le point (a) implique l'énoncé suivant :

Corollaire 4.2.3. *Soit L un réseau de Niemeier avec racines. Alors le quotient $Q^\sharp/Q$ est annulé par h.*

En effet, le point (a) de 4.2.2 montre que si ξ et η sont deux éléments de $Q^\sharp$ alors $h\xi.\eta$ est entier et donc que $h\xi$ appartient à Q. □

Soit ρ un vecteur de Weyl de L. Comme l'action canonique de W sur $Q^\sharp/Q$ est triviale l'image de ρ dans $Q^\sharp/Q$ est indépendante du choix de ce vecteur de Weyl. Voici une autre explication de ce phénomène. On fait intervenir la structure de qe-module de $Q^\sharp/Q =: \operatorname{rés} Q$. D'après 4.2.3, l'application $Q^\sharp/Q \to \mathbb{Q}/\mathbb{Z}$, $\xi \mapsto h\,\mathrm{q}(\xi)$ est linéaire (et à valeurs dans $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$) ; il existe donc un élément σ de $Q^\sharp/Q$, uniquement déterminé (et annulé par 2), tel que l'on a $h\,\mathrm{q}(\xi) = \sigma.\xi$ pour tout ξ dans $Q^\sharp/Q$. Le point (b) de 4.2.2 montre que σ est la classe de ρ. En effet ce point montre que $h\,\mathrm{q}(\xi) - \rho.\xi$ est entier pour tout ξ dans $Q^\sharp$. Nous avons obtenu :

Proposition 4.2.4. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors l'image de ρ dans $Q^\sharp/Q$, disons $\overline{\rho}$, est caractérisée par la propriété*

$$h\,\mathrm{q}(\xi) \;=\; \overline{\rho}.\xi$$

pour tout ξ dans $Q^\sharp/Q$.

Exprimé avec le formalisme introduit ci-dessus, l'argument de Borcherds pour démontrer 4.2.1 est le suivant : Soit I un lagrangien du qe-module $Q^\sharp/Q$, $\mathrm{q}(I) = 0$ implique $\overline{\rho} \in I^\perp = I$; en prenant $I = L/Q$ on obtient $\rho \in L$. □

Proposition 4.2.5 (Venkov)**.** *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors on a*

$$\mathrm{q}(\rho) \;=\; h(h+1) \qquad .$$

Démonstration. Il suffit par exemple de constater que l'on a $\rho.\rho = \frac{n}{12}h(h+1)$ pour tout système de racines de type ADE irréductible de rang n et d'invoquer le point (b) de la proposition-définition II.3.3. □

Proposition 4.2.6. *Soit L un réseau de Niemeier avec racines. Pour tout élément x de V, on a l'inégalité*

$$\inf_{\alpha\in R}\,(\alpha.x)^2 \;\leq\; \frac{\mathrm{q}(x)}{h(h+1)} \qquad .$$

De plus, on a l'égalité si et seulement s'il existe un vecteur de Weyl ρ de L et un nombre réel $\lambda \geq 0$ tels que l'on a $x = \lambda\rho$.

Démonstration. Soit $C \subset V$ une chambre de R telle que x appartienne à $\overline{C}$. Soient respectivement B et ρ la base de R et le vecteur de Weyl associés à C ; soit $\{\varpi_\alpha\}_{\alpha\in B}$ la base duale de B (par rapport au produit scalaire). On considère l'égalité

$$x.x = \sum_{(\alpha,\beta)\in B\times B} (\alpha.x)(\beta.x)\ \varpi_\alpha.\varpi_\beta \qquad ;$$

en observant que l'on a $\alpha.x \geq 0$ et $\beta.x \geq 0$ (par définition de C), $\varpi_\alpha.\varpi_\beta \geq 0$ (voir par exemple [Bou81b, Ch. VI, §1, Th. 2, Rem. 2]) et $\rho.\rho = \sum_{(\alpha,\beta)} \varpi_\alpha.\varpi_\beta$ (spécialisation de l'égalité ci-dessus), on constate que l'on a l'inégalité

$$(*) \qquad x.x \ \geq\ \rho.\rho \inf_{\alpha\in B}(\alpha.x)^2 \qquad .$$

Posons $\lambda = \inf_{\alpha\in B} \alpha.x$; l'inégalité ci-dessus peut-être affinée en

$$x.x \ \geq\ \rho.\rho \inf_{\alpha\in B}(\alpha.x)^2 + \sum_{\alpha\in B} \left((\alpha.x)^2 - \lambda^2\right) \varpi_\alpha.\varpi_\alpha \qquad .$$

Ceci montre que si l'on a égalité dans l'inégalité (*) alors on a $\alpha.x = \lambda$ pour tout α dans B et donc $x = \lambda\rho$. □

Scholie 4.2.7 *Soit L un réseau de Niemeier avec racines. Pour tout élément régulier ξ de $\mathrm{Q}(R)^\sharp$, en clair vérifiant $\alpha.\xi \neq 0$ pour tout α dans R, on a l'inégalité*

$$\mathrm{q}(\xi) \ \geq\ h(h+1) \qquad .$$

De plus on a l'égalité si et seulement ξ est un vecteur de Weyl de L.

Le point (a) de la proposition ci-dessous dit en particulier que le point (b) de 4.1.4 est "optimal".

Proposition 4.2.8. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L.*

(a) *Le vecteur de Weyl ρ est un élément primitif (*a fortiori *h-primitif) et h-régulier de L.*

(b) *Soit ξ un élément de $Q^\sharp$; les deux conditions suivantes sont équivalentes :*

(i) l'élément ξ est h-régulier ;

(ii) il existe un élément w de W et un élément x de Q tels que l'on a $\xi = w\rho + hx$.

De plus si ces conditions sont vérifiées alors le couple (w, x) qui apparaît dans la condition (ii) est uniquement déterminé en fonction de ξ.

Démonstration du point (a). L'égalité $\alpha.\rho = 1$ pour $\alpha \in B$ montre que ρ est primitif. Avant de démontrer que ρ est h-régulier, rappelons la définition et quelques propriétés de la fonction *hauteur*, disons $\mathrm{H} : R_+ \to \mathbb{N} - \{0\}$. Soit β un élément de R_+ ; β s'écrit $\sum_{\alpha \in B} n_\alpha \alpha$ avec n_α dans $\mathbb{N}$ [Bou81b, Ch. VI, §1, Th. 3] et l'on pose $\mathrm{H}(\beta) := \sum_{\alpha \in B} n_\alpha$. La fonction H vérifie les propriétés suivantes :

- $\mathrm{H}(\beta) = \beta.\rho$;
- $\mathrm{H}(\beta) \geq 1$ et $\mathrm{H}(\beta) = 1 \iff \beta \in B$;
- $\mathrm{H}(\beta) \leq h - 1$ et $\mathrm{H}(\beta) = h - 1 \iff \beta \in H$.

La dernière propriété ci-dessus résulte de [Bou81b, Ch. VI, §1, Prop. 31] (référence que nous avons déjà invoquée lors de la démonstration de 4.1.2) et de la définition même du sous-ensembe $H \subset R_+$. L'égalité $R = R_+ \coprod -R_+$ et les inégalités $1 \leq \beta.\rho \leq h - 1$ pour tout β dans R_+ montre que l'on a $\alpha.\rho \not\equiv 0 \bmod h$ pour tout α dans R. □

Démonstration du point (b). L'implication $(ii) \Rightarrow (i)$ résulte du fait que ρ est h-régulier. On démontre $(i) \Rightarrow (ii)$. Compte tenu de 4.1.3, on peut supposer $\xi \in h\overline{Alc}$, c'est-à-dire :

- $\alpha.\xi \geq 0$ pour tout α dans B ;
- $\widetilde{\alpha}.\xi \leq h$ pour tout $\widetilde{\alpha}$ dans H.

La première inégalité montre que si ξ est h-régulier alors on a $\alpha.\xi \geq 1$ pour tout α dans B (par définition $\beta.\xi$ est dans $\mathbb{Z}$ pour tout β dans R) ; soit encore $\alpha.(\xi - \rho) \geq 0$ pour tout α dans B. Pareillement, la seconde montre que l'on a $\widetilde{\alpha}.\xi \leq h - 1$ pour tout $\widetilde{\alpha}$ dans H ; soit encore $\widetilde{\alpha}.(\xi - \rho) \leq 0$ pour tout $\widetilde{\alpha}$ dans H. Or un élément η de V qui vérifie $\alpha.\eta \geq 0$ pour tout α dans B et $\widetilde{\alpha}.\eta \leq 0$ pour tout $\widetilde{\alpha}$ dans H est nul (par exemple, parce qu'il appartient à $\epsilon\overline{Alc}$ pour tout $\epsilon > 0$). On a donc $\xi = \rho$. La dernière partie du point (b), concernant l'unicité du couple (w, x) qui apparaît dans la condition (ii), est un sous-produit de la démonstration que nous venons de faire. □

Nous en arrivons au dernier énoncé concernant les vecteurs de Weyl des réseaux de Niemeier que nous voulons dégager ; les points (b) et (c), sont encore dûs à Borcherds.

Proposition 4.2.9. *Soient L un réseau de Niemeier avec racines, ρ un vecteur de Weyl de L et ξ un élément de $Q^\sharp$.*

(a) *L'élément $\rho - h\xi$ de $Q^\sharp$ appartient à L et est h-régulier.*

(b) *On a l'inégalité*

$$\mathrm{q}(\rho - h\xi) \ \geq \ \mathrm{q}(\rho) \ = \ h(h+1) \qquad .$$

(c) *Les conditions suivantes sont équivalentes :*

(i) on a l'égalité dans l'inégalité ci-dessus ;

(ii) ξ *appartient à* Π *;*

(iii) $\rho - h\xi$ *est un vecteur de Weyl de* L*.*

Démonstration. L'élément $\rho - h\xi$ appartient à L d'après 4.2.1 et 4.2.3. Il est h-régulier d'après le point (a) de 4.2.8. Il est *a fortiori* régulier, si bien que l'inégalité du point (b) peut être vue comme une conséquence du scholie 4.2.7. Cependant l'argument de Borcherds [Bor84][Bor85], qui utilise le point (b) de 4.2.2, est plus efficace pour traiter des cas d'égalité. En effet, on a $\mathrm{q}(\rho - h\xi) - \mathrm{q}(\rho) = h\,(h\mathrm{q}(\xi) - \rho.\xi)$. Puisque l'on a $t^2 - t \geq 0$ pour tout t dans $\mathbb{Z}$, le second membre de l'égalité du point en question, avec $x = \xi$, est positif ou nul et il est nul si et seulement si l'on a $\alpha.\xi \in \{0, 1\}$ pour tout α dans R_+ ; or cette dernière propriété caractérise les éléments de Π (voir la démonstration du point (a) de la proposition II.3.8). Ceci démontre l'équivalence $(i) \iff (ii)$ du point (c). L'équivalence $(i) \iff (iii)$ résulte quant à elle de 4.2.7 (cas d'égalité). $\square$

Holy constructions

Nous en arrivons maintenant à l'énoncé principal du sous-paragraphe 4.2. Cet énoncé mérite le nom de théorème à cause du point (c) qui est implicite dans [CS82], au moins en ce qui concerne le réseau $\mathrm{vois}_h(L;\rho)$.

Théorème 4.2.10. *Soient* L *un réseau de Niemeier avec racines et* ρ *un vecteur de Weyl de* L*. On note* s_ρ *la réflexion orthogonale de* $\mathbb{Q} \otimes_{\mathbb{Z}} L$ *par rapport à l'hyperplan orthogonal à* ρ*.*

(a) *La classe de* ρ *dans l'espace projectif* $\mathrm{P}_L(\mathbb{Z}/h)$ *(resp.* $\mathrm{P}_L(\mathbb{Z}/(h+1))$*) appartient à la quadrique* $\mathrm{C}_L(\mathbb{Z}/h)$ *(resp.* $\mathrm{C}_L(\mathbb{Z}/(h+1))$*).*

(b) *Les réseaux* $\mathrm{vois}_h(L;\rho)$ *et* $\mathrm{vois}_{h+1}(L;\rho)$ *sont échangés par la réflexion* s_ρ *:*

$$\mathrm{vois}_{h+1}(L;\rho) \ = \ \mathrm{s}_\rho(\mathrm{vois}_h(L;\rho)) \qquad .$$

(c) *Les réseaux* $\mathrm{vois}_h(L;\rho)$ *et* $\mathrm{vois}_{h+1}(L;\rho)$ *sont sans racines :*

$$\mathrm{vois}_h(L;\rho) \ \simeq \ \mathrm{Leech} \qquad , \qquad \mathrm{vois}_{h+1}(L;\rho) \ \simeq \ \mathrm{Leech} \qquad .$$

(d) *On a :*

$$\mathrm{N}_h(L, \mathrm{Leech}) \;=\; \frac{|W|}{\varphi(h)\,g} \qquad , \qquad \mathrm{N}_{h+1}(L, \mathrm{Leech}) \;=\; \frac{|W|}{\varphi(h+1)} \qquad .$$

(la notation $\varphi(-)$ désigne ci-dessus l'indicateur d'Euler d'un entier naturel et la notation $|-|$ le cardinal d'un ensemble fini, on rappelle que g désigne l'indice de Q dans L ou encore la racine carrée de l'indice de connexion f de R).

Démonstration des points (a) et (b). Le point (a) est conséquence de 4.2.5 ; le point (b) est un cas particulier du point (b) de 1.14.

Démonstration du point (c). Compte tenu du point (b) il suffit de montrer que $\mathrm{vois}_h(L;\rho)$ ou $\mathrm{vois}_{h+1}(L;\rho)$ est sans racines. Nous proposons trois démonstrations.

1) La première est très prosaïque. Le logiciel `PARI` permet de calculer sans problèmes le *minimum* d'un réseau entier Λ, disons $\mathrm{m}(\Lambda)$, à savoir l'entier $\inf_{x\in\Lambda-\{0\}} x.x$, pour $\dim\Lambda = 24$ et donc de vérifier que l'on a bien $\mathrm{m}(\mathrm{vois}_h(L;\rho)) = 4$ pour les 23 réseaux de Niemeier avec racines.

2) La deuxième démonstration consiste à identifier le réseau $\mathrm{vois}_h(L;\rho)$ avec la construction du réseau de Leech donnée par Conway et Sloane dans [CS82] où, comme nous l'avons déjà dit, cette identification est implicite. La construction en question, que Conway et Sloane dénomment *holy construction*, est rappelée ci-dessous.

Conway et Sloane associent d'abord à la donnée $(L;\rho)$ deux sous-ensembles finis de L :

– Le premier, disons F, est la réunion disjointe $B \coprod -H$; on rappelle que les éléments de H sont les plus grandes racines, $\widetilde{\alpha}_1, \widetilde{\alpha}_2, \ldots, \widetilde{\alpha}_c$, des composantes irréductibles, $R_1, R_2, \ldots, R_c$, de R. Pour allèger la notation on note $\alpha_1, \alpha_2, \ldots, \alpha_{24}$ les éléments de B et on pose $\alpha_{24+i} = -\widetilde{\alpha}_i$; les éléments de F (qui sont tous des racines de R) correspondent aux sommets du *graphe de Dynkin complété* de R.

– Le second, disons G, est constitué des poids minuscules de R (voir la remarque qui suit la proposition II.3.12) qui sont dans $L \cap \overline{C}$. On a donc $G = L \cap \Pi$ et l'application canonique de G dans L/Q est une bijection ; on note $\mu_0, \mu_1, \ldots, \mu_{g-1}$ les éléments de G avec $\mu_0 = 0$.

Conway et Sloane considèrent ensuite le réseau de $\mathbb{Q} \otimes_{\mathbb{Z}} L$, disons $\mathrm{HC}(L;\rho)$, constitué des éléments de la forme

$$\sum_{i=1}^{24+c} m_i \alpha_i \ + \ \sum_{j=0}^{g-1} n_j (\frac{\rho}{h} - \mu_j) \qquad ,$$

les m_i et n_j désignant des entiers vérifiant $\sum_i m_i + \sum_j n_j = 0$.

La proposition suivante montre que le réseau $\mathrm{HC}(L;\rho)$ peut être décrit en termes de voisinage à la Kneser.

Proposition 4.2.11. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Le réseau* $\mathrm{HC}(L;\rho)$ *de Conway et Sloane coïncide avec le réseau* $\mathrm{vois}_h(L;\rho)$.

Démonstration. Il s'agit plutôt d'une vérification d'où les petits caractères. On a vu (voir la discussion qui suit 1.5) que le réseau $\mathrm{vois}_h(L;\rho)$ est le sous-$\mathbb{Z}$-module de $\mathbb{Q}\otimes_{\mathbb{Z}} L$ engendré par M et $\frac{\widetilde{\rho}}{h}$, M désignant le noyau de l'homomorphisme de L dans $\mathbb{Z}/h$ qui associe à un élément x de L la réduction $\bmod h$ de l'entier $\rho.x$ et $\widetilde{\rho}$ désignant un élément de L avec $\widetilde{\rho} \equiv \rho \bmod h$ et $\mathrm{q}(\widetilde{\rho}) \equiv 0 \bmod h^2$. On constate que l'on peut prendre $\widetilde{\rho} = \rho - h\alpha_1$; en effet on a $\mathrm{q}(\rho - h\alpha_1) = h(h+1) - h + h^2 = 2h^2$.

Ce rappel étant fait, on observe que les $\alpha_1 - \alpha_i$ apartiennent à M ; en effet on a $\rho.\alpha_i = 1$ pour $i \leq 24$ et $\rho.\alpha_i = 1 - h$ pour $i > 24$. On observe également que les μ_j appartiennent à M ; en effet le point (c) de 4.2.9 montre que l'on a $\mathrm{q}(\rho - h\mu_j) = \mathrm{q}(\rho)$, égalité qui équivaut à $\rho.\mu_j = h\,\mathrm{q}(\mu_j)$.

Soit maintenant x un élément de $\mathbb{Q}\otimes_{\mathbb{Z}} L$ de la forme considérée par Conway et Sloane. Les observations ci-dessus montrent que x s'écrit aussi $y + (\sum_j n_j)\frac{\widetilde{\rho}}{h}$ avec y dans M, en d'autres termes que l'on a dans $\mathbb{Q}\otimes_{\mathbb{Z}} L$ l'inclusion $\mathrm{HC}(L;\rho) \subset \mathrm{vois}_h(L;\rho)$. L'inclusion $\mathrm{vois}_h(L;\rho) \subset \mathrm{HC}(L;\rho)$ résulte du fait que L est engendré par $\mathrm{Q}(R)$ et les μ_j. Détaillons un peu. On déduit du fait en question que M est engendré par les μ_j, les $\alpha_1 - \alpha_i$ et $h\alpha_1$. On se convainc de ce que les μ_j appartiennent à $\mathrm{HC}(L;\rho)$ en contemplant l'égalité $\mu_j = (\frac{\rho}{h} - \mu_0) - (\frac{\rho}{h} - \mu_j)$. Il est clair qu'il en est de même pour les $\alpha_1 - \alpha_i$. On suppose $\alpha_1 \in R_1$; on se convainc de ce que $h\alpha_1$ appartient à $\mathrm{HC}(L;\rho)$ en observant que l'on a $\widetilde{\alpha}_1 = \sum_{\beta \in B \cap R_1} m_\beta\, \beta$, les m_β étant des entiers avec $\sum_{\beta \in B \cap R_1} m_\beta = h - 1$. Enfin, on se convainc de ce que $\frac{\widetilde{\rho}}{h}$ appartient à $\mathrm{HC}(L;\rho)$ en écrivant $\frac{\widetilde{\rho}}{h} = -\alpha_1 + (\frac{\rho}{h} - \mu_0)$. □

Dans [CS82] Conway et Sloane disent avoir vérifié au cas par cas le fait que $\mathrm{HC}(L;\rho)$ est sans racines... si bien que la démonstration du point (c) grâce à [CS82] paraît très semblable à celle que nous avons proposée en premier. Il faut cependant signaler que Borcherds [Bor84][Bor85] a découvert, peu après la parution de [CS82], une preuve uniforme en termes de réseaux "lorentziens".

3) La troisième démonstration du point (c) que nous proposons fait un usage systématique de la théorie des voisins à la Kneser. Il s'agit d'une démonstration par l'absurde : on suppose $\mathrm{R}(\mathrm{vois}_h(L;\rho)) \neq \emptyset$ et on produit une contradiction.

On commence par dégager un énoncé *ad hoc* concernant la théorie générale des d-voisins :

Lemme 4.2.12. *Soit L un* q*-module sur $\mathbb{Z}$; soient $d \geq 2$ un entier et u un élément d-primitif de L avec $\mathrm{q}(u) \equiv 0 \bmod d$. Soit x un élément de $\mathrm{vois}_d(L;u)$, alors $\mathrm{q}(u)x$ appartient à $\mathrm{M}_d(L;u)$ et l'on a dans L la congruence suivante :*

$$\mathrm{q}(u)x \;\equiv\; (u.x)\,u \mod d$$

(observer que u appartient à $\mathrm{M}_d(L;u) \subset \mathrm{vois}_d(L;u)$ si bien que $u.x$ est entier et que $(u.x)\,u$ appartient également à $\mathrm{M}_d(L;u)$).

Démonstration. On pose $M = \mathrm{M}_d(L;u)$ et $L' = \mathrm{vois}_d(L;u)$. L'élément $\mathrm{q}(u)x$ appartient à M puisque le quotient L'/M est cyclique d'ordre d et que $\mathrm{q}(u)$ est divisible par d. Soit v un élément de L avec $u.v \equiv 1 \bmod d$, puisque L' est engendré par M et $\frac{u-\mathrm{q}(u)v}{d}$ il suffit de vérifier la congruence de l'énoncé pour $x \in M$ et pour $x = \frac{u-\mathrm{q}(u)v}{d}$. Dans le premier cas les deux membres sont divisibles par d ; la vérification dans le second cas est immédiate. □

Scholie 4.2.13. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Soit x un élément de $\mathrm{vois}_h(L;\rho)$, alors $\rho.x$ est entier, hx et $(h+1)\mathrm{s}_\rho(x)$ appartiennent respectivement à $\mathrm{M}_h(L;\rho)$ et $\mathrm{M}_{h+1}(L;\rho)$, et l'on a dans L les congruences suivantes :*

$$hx \;\equiv\; (\rho.x)\,\rho \mod h \quad , \quad (h+1)\mathrm{s}_\rho(x) \;\equiv\; (\rho.x)\,\rho \mod (h+1) \quad .$$

Démonstration. Elle résulte du lemme 4.2.12 et des égalités $\mathrm{q}(\rho) = h(h+1)$, $\mathrm{vois}_{h+1}(L;\rho) = \mathrm{s}_\rho(\mathrm{vois}_h(L;\rho))$ et $\rho.\mathrm{s}_\rho(x) = -\rho.x$. □

On analyse maintenant les contraintes que la condition $\mathrm{R}(\mathrm{vois}_h(L;\rho)) \neq \emptyset$ impose.

Proposition 4.2.14. *Soient L un réseau de Niemeier avec racines, ρ un vecteur de Weyl de L et α' une racine du réseau $\mathrm{vois}_h(L;\rho)$.*

(a.1) *L'entier $\rho.\alpha'$ n'est pas divisible par h.*

(a.2) *Les entiers $\rho.\alpha'$ et h ne sont pas premiers entre eux.*

(b.1) *L'entier $\rho.\alpha'$ n'est pas divisible par $h+1$.*

(b.2) *Les entiers $\rho.\alpha'$ et $h+1$ ne sont pas premiers entre eux.*

Démonstration. On pose $L' = \mathrm{vois}_h(L;\rho)$ et $M = \mathrm{M}_h(L;\rho)$; on rappelle que l'on a $M = L \cap L'$.

Démonstration du point (a.1). Le scholie 4.2.13 montre que si $\rho.\alpha'$ est divisible par h alors α' appartient à L, ce qui est interdit par $\mathrm{R}(M) = \emptyset$. □

Démonstration du point (a.2). Le scholie 4.2.13 montre que si l'entier $\rho.\alpha'$ est premier avec h alors $h\alpha'$ est un élément h-primitif de L et la classe de cet élément dans la quadrique $\mathrm{C}_L(\mathbb{Z}/h)$ est égale à celle de ρ. Ceci est interdit par l'égalité $\mathrm{q}(h\alpha') = h^2$ et 4.2.7. □

Démonstration des points (b.1) et (b.2). On observe tout d'abord que si α' est une racine de L' alors $\mathrm{s}_\rho(\alpha')$ est une racine de $\mathrm{s}_\rho(L') = \mathrm{vois}_{h+1}(L;\rho)$ et que l'on a $\rho.\mathrm{s}_\rho(\alpha') = -\rho.\alpha'$. On procède ensuite comme précédemment. Pour la démonstration du point (b.2), on utilise les énoncés 4.2.15, 4.2.16 et 4.2.17 ci-après ; 4.2.15 est le pendant de 4.2.8, 4.2.16 est semblable au point (b) de 4.2.9 et 4.2.17 à 4.2.7.

Proposition 4.2.15. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L.*

(a) *Le vecteur de Weyl ρ est $h+1$-régulier.*

(b) *Soit ξ un élément de $Q^\sharp$; les deux conditions suivantes sont équivalentes :*

(i) l'élément ξ est $h+1$-régulier ;

(ii) il existe un élément w de W, un élément ϖ de Π et un élément x de Q tels que l'on a $\xi = w(\rho + \varpi) + (h+1)x$.

De plus si ces conditions sont vérifiées alors le triplet (w, ϖ, x) qui apparaît dans la condition (ii) est uniquement déterminé en fonction de ξ.

(c) *Soit u un élément de L ; les deux conditions suivantes sont équivalentes :*

(i) l'élément u est $h+1$-régulier ;

(ii) il existe un élément w de W et un élément x de L tels que l'on a $u = w\rho + (h+1)x$.

De plus si ces conditions sont vérifiées alors le couple (w, x) qui apparaît dans la condition (ii) est uniquement déterminé en fonction de u.

Démonstration des points (a) et (b). Ce sont des variantes de celles des points (a) et (b) de 4.2.8. Démontrons par exemple l'implication $(i) \Rightarrow (ii)$ du point (b). Compte tenu de 4.1.3, on peut supposer $\xi \in (h+1)\overline{Alc}$ (à nouveau la dernière partie du point (b), concernant l'unicité du triplet (w, ϖ, x), sera un sous-produit de notre démonstration). Si ξ est $h+1$-régulier, alors on a cette fois les inégalités $\alpha.(\xi - \rho) \geq 0$ pour tout α dans B et $\widetilde{\alpha}.(\xi - \rho) \leq 1$ pour tout $\widetilde{\alpha}$ dans H. On a donc $\xi - \rho \in Q^\sharp \cap \overline{Alc} =: \Pi$. □

Démonstration du point (c). L'implication $(ii) \Rightarrow (i)$ du point (c) résulte du fait que ρ est $h+1$-régulier. L'implication $(i) \Rightarrow (ii)$ du point (c) résulte de l'implication $(i) \Rightarrow (ii)$ du point (b). En effet si u est $h+1$-régulier, alors il s'écrit de façon unique $u = w_0(\rho+\varpi)+(h+1)x_0$ avec $(w_0, \varpi, x_0) \in W \times \Pi \times Q$. On observe que puisque u est dans L alors il en est de même pour ϖ : $\varpi \in \Pi \cap L$. On écrit $u = w_0(\rho - h\varpi) + (h+1)(w_0\varpi + x_0)$. D'après 4.2.9 (c), $\rho - h\varpi$ est un vecteur de Weyl de L, il existe donc un élément w_1 de W, uniquement déterminé en fonction de ϖ, tel que l'on a $\rho - h\varpi = w_1\rho$. En posant $w = w_0w_1$ et $x = w_0\varpi + x_0$ on a bien $u = w\rho + (h+1)x$. L'unicité du couple (w, x) résulte de ce que l'application canonique $\Pi \cap L \to L/Q$ est une bijection. □

Proposition 4.2.16. *Soit x un élément non nul de L, alors on a l'inégalité*

$$\mathrm{q}(\rho - (h+1)x) \ \geq \ (h+1)(h+2) \qquad .$$

Démonstration. On adapte l'argument de Borcherds utilisé dans la démonstration de 4.2.9. Soit x un élément de L, on vérifie que l'on a cette fois l'égalité

$$\mathrm{q}(\rho - (h+1)x) \ = \ (h+1)\,(\,h + \mathrm{q}(x) + \sum_{\alpha \in R_+} \frac{(\alpha.x)^2 - \alpha.x}{2}\,) \qquad .$$

Pour estimer le second membre de cette égalité, on distingue deux cas :

1) Il existe une racine positive α telle que l'on a $\alpha.x \notin \{0,1\}$. On constate que l'on a dans ce cas $(\alpha.x)^2 - \alpha.x \geq 2$ et donc $\mathrm{q}(x) + \sum_{\alpha \in R_+} \frac{(\alpha.x)^2 - \alpha.x}{2} \geq 2$.

2) On a $\alpha.x \in \{0,1\}$ pour tout α dans R_+. Si x est non nul alors on a $\mathrm{q}(x) \geq 2$; en effet x ne peut être une racine puisque x ou $-x$ serait une racine positive, disons β, avec $\beta.x \notin \{0,1\}$. □

Corollaire 4.2.17. *Soit u un élément de L. Si u est $(h+1)$-primitif et si l'on a $\mathrm{q}(u) = (h+1)^2$ alors u n'est pas $(h+1)$-régulier.*

Démonstration. D'après le point (c) de 4.2.15, si un tel u est $(h+1)$-régulier alors il existe un élément w du groupe de Weyl de R et un élément x de L tel que l'on a $u = w\rho + (h+1)x$. Les propositions 4.2.5 et 4.2.16 montrent que l'on a $\mathrm{q}(u) = h(h+1)$ ou $\mathrm{q}(u) \geq (h+1)(h+2)$. □

La proposition 4.2.14 montre que le réseau $\mathrm{vois}_h(L;\rho)$ est sans racines si h ou $h+1$ est premier. C'est le cas pour 19 des réseaux de Niemeier sans racines. Les 4 qui font de la résistance correspondent à $h = 25, 14, 9, 8$. Pour en venir à bout, on raffine l'argument précédent.

Proposition 4.2.18. *Soit L un réseau de Niemeier avec racines. On suppose que le réseau* $\mathrm{vois}_h(L;\rho)$ *possède aussi des racines et on note h' son nombre de Coxeter. Alors il existe un entier ν vérifiant les trois conditions suivantes :*

(1) $\nu > 0$ *;*

(2) $\nu^2 \leq \frac{h(h+1)}{h'(h'+1)}$ *;*

(3) $\mathrm{p.g.c.d.}(\nu, h) \neq 1$ *et* $\mathrm{p.g.c.d.}(\nu, h+1) \neq 1$.

Démonstration. On pose $L' = \mathrm{vois}_h(L;\rho)$. On applique la proposition 4.2.6 au réseau L' en prenant pour x l'élément ρ : il existe une racine α' de L' telle que l'on a $(\rho.\alpha')^2 \leq \frac{h(h+1)}{h'(h'+1)}$. On pose $\nu = |\rho.\alpha'|$. Ce qui précède montre que ν est un nombre entier qui vérifie les trois conditions ci-dessus. □

On note $\mathrm{S}(h, h')$ le sous-ensemble de $\mathbb{Z}$ constitué des entiers ν vérifiant les trois conditions de la proposition 4.2.18 ; il est clair que l'on a $\mathrm{S}(h, h'_1) \subset \mathrm{S}(h, h'_2)$ pour $h'_1 \geq h'_2$. On constate que $\mathrm{S}(h, 2)$ est vide pour $h \neq 25$. Le réseau $\mathrm{vois}_h(L;\rho)$ est donc sans racines pour $h \neq 25$.

Il reste à faire un dernier effort pour $h = 25$. On a $\mathrm{S}(25, 2) = \{10\}$ et $\mathrm{S}(25, 3) = \emptyset$. La seconde égalité force $h' = 2$ et donc $\mathrm{R}(L') = 24\mathbf{A}_1$. On contemple alors l'égalité (Scholie II.3.4)

$$\sum_{\beta \in R'_+} (\rho.\beta)^2 \;=\; 2600 \qquad ,$$

R'_+ désignant l'ensemble à 24 éléments constitué des racines positives de L', pour un certain choix de chambre. Cette égalité montre que l'on ne peut avoir $|\rho.\beta| = 10$ pour tout β dans R'_+ ; la proposition 4.2.14 montre qu'il existe β_1 dans R'_+ avec $|\rho.\beta_1| \geq 20$. Il en résulte qu'il existe β_2 dans R'_+ avec $|\rho.\beta_2| \leq 9$ (observer que l'on a $23 \times 10^2 > 2600 - 20^2$). Contradiction avec la proposition 4.2.14.

Cette contradiction achève notre troisième démonstration du point (c) du théorème 4.2.10. □□

Démonstration du point (d) du théorème 4.2.10

La proposition 4.2.8 montre que la classe de ρ dans $\mathrm{P}_L(\mathbb{Z}/h)$ appartient à $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/h)$ et que l'action de W sur cet ensemble est transitive. Comme la classe de ρ appartient à $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/h)$, on constate que l'on a $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/h) = \mathrm{P}_L^{\text{rég}}(\mathbb{Z}/h)$. Pareillement, la proposition 4.2.15 montre que la classe de ρ dans $\mathrm{P}_L(\mathbb{Z}/(h+1))$ appartient à $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/(h+1))$, que l'action de W sur cet ensemble est transitive (4.2.15 (c)) et que l'on a $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/(h+1)) = \mathrm{P}_L^{\text{rég}}(\mathbb{Z}/(h+1))$. Compte tenu du fait qu'une condition nécéssaire pour que $\mathrm{vois}_d(L;c)$ soit

isomorphe au réseau de Leech est que c appartienne à $\mathrm{C}_L^{\text{rég}}(\mathbb{Z}/d)$ (4.1.4 (a)), la démonstration du point (d) de 4.2.10 consiste à vérifier que le cardinal du stabilisateur, pour l'action de W, de la classe de ρ dans $\mathrm{P}_L(\mathbb{Z}/h)$ (resp. $\mathrm{P}_L(\mathbb{Z}/(h+1))$), est $\phi(h)g$ (resp. $\phi(h+1)$). Ceci résulte des énoncés 4.2.19 et 4.2.20 ci-dessous.

Proposition 4.2.19. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors le stabilisateur, pour l'action de W, de la classe de ρ dans $\mathrm{P}_L(\mathbb{Z}/h)$, est une extension canonique de $(\mathbb{Z}/h)^\times$ par L/Q.*

Démonstration. Soient $S \subset W$ le stabilisateur en question et w un élément de S. On a par définition $w\rho = \lambda\rho + hx$ avec λ dans $\mathbb{Z}$ premier à h et x dans L. On constate que la classe $\overline{\lambda}$ de λ dans $(\mathbb{Z}/h)^\times$ ne dépend que de w et que l'application $w \mapsto \overline{\lambda}$ est un homomorphisme de groupes, disons $\pi : S \to (\mathbb{Z}/h)^\times$. L'implication $(i) \Rightarrow (ii)$ de 4.2.8 (b) montre que π est surjectif puisque $\lambda\rho$ est h-régulier pour tout λ dans $\mathbb{Z}$ premier à h. On considère maintenant le sous-groupe $\ker\pi$. Soit w dans $\ker\pi$; on a cette fois $w\rho = \rho + hx$ avec x dans L. On constate que l'application qui associe à w la classe de x dans L/Q est un homomorphisme de groupes, disons $\iota : \ker\pi \to L/Q$ (on utilise ici que l'action de W sur $Q^\sharp/Q$ est triviale). Le même argument que précédemment montre que ι est surjectif. La propriété d'unicité qui apparaît dans 4.2.8 (b) montre que ι est injectif. □

Remarques

1) Le $\mathbb{Z}$-module L/Q est un $\mathbb{Z}/h$-module d'après 4.2.3, si bien que l'on dispose d'une action naturelle de $(\mathbb{Z}/h)^\times$ sur L/Q ; cette action coïncide avec celle définie par l'extension de 4.2.19. Si ρ appartient à Q (ce qui n'est pas toujours le cas, voir 4.2.4), alors la démonstration de 4.2.19 montre implicitement que S est canoniquement isomorphe au produit semi-direct $L/Q \rtimes (\mathbb{Z}/h)^\times$. En fait, on peut vérifier que l'extension de 4.2.19 est toujours triviale.

2) Par construction l'homomorphisme ι qui apparaît dans la démonstration de 4.2.19 se factorise par une application ensembliste de $\ker\pi$ dans L. Ceci montre que l'on dispose d'une section ensembliste (ne dépendant que du choix de ρ) de l'homomorphisme $L \to L/Q$. L'image de cette section est $\Pi \cap L$ et cette seconde remarque est intimement reliée à la remarque qui suit 4.2.9.

Proposition 4.2.20. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors le stabilisateur, pour l'action de W, de la classe de ρ dans $\mathrm{P}_L(\mathbb{Z}/(h+1))$, est canoniquement isomorphe à $(\mathbb{Z}/(h+1))^\times$.*

Démonstration. Elle est analogue à la précédente, la proposition 4.2.15 remplaçant la proposition 4.2.8. Elle est en réalité plus simple. Cette fois l'homomorphisme $\pi : S \to (\mathbb{Z}/(h+1))^\times$ est un isomorphisme. La raison de cette simplification est la suivante : dans le point (b) de 4.2.8 l'élément x appartient à Q, dans le point (c) de 4.2.15 il appartient à L. □□□

4.3. Sur les stabilisateurs de l'action de W sur $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$, pour L un réseau de Niemeier avec racines

On majore dans ce sous-paragraphe la taille des stabilisateurs en question. Notre motivation est l'énoncé 4.3.3 dont on verra l'utilité en IX.3.1.

Soient L un réseau de Niemeier avec racines et $d \geq 2$ un entier.

On suppose ci-après que d est premier avec l'indice g de Q dans L. Dans ce cas l'homomorphisme canonique $Q/dQ \to L/dL$ est un isomorphisme. On introduit, *mutatis mutandis*, les notations P_Q, C_Q (cette fois ce schéma est seulement lisse sur $\mathbb{Z}[\frac{1}{g}]$), $\mathrm{P}_Q(\mathbb{Z}/d)$, $\mathrm{P}_Q(\mathbb{Z}/d)$, $\mathrm{P}_Q^{\text{rég}}(\mathbb{Z}/d)$ et $\mathrm{C}_Q^{\text{rég}}(\mathbb{Z}/d)$, ainsi que la terminologie correspondante ; il est clair que les bijections canoniques $\mathrm{P}_Q(\mathbb{Z}/d) \cong \mathrm{P}_L(\mathbb{Z}/d)$, $\mathrm{C}_Q(\mathbb{Z}/d) \cong \mathrm{C}_L(\mathbb{Z}/d)$, $\mathrm{P}_Q^{\text{rég}}(\mathbb{Z}/d) \cong \mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$ et $\mathrm{C}_Q^{\text{rég}}(\mathbb{Z}/d) \cong \mathrm{C}_L^{\text{rég}}(\mathbb{Z}/d)$ sont W-équivariantes.

Proposition 4.3.1. *Soient L un réseau de Niemeier avec racines et $d \geq 2$ un entier premier avec l'indice de Q dans L ; soit S le stabilisateur, pour l'action de W, d'un élément de $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/d)$.*

(a) *Le groupe S est canoniquement isomorphe à un sous-groupe de $(\mathbb{Z}/d)^\times$.*

(b) *Si d est premier, alors l'action de S sur R (induite par celle de W) est libre.*

Démonstration du point (a). Compte tenu de ce que l'on a dit plus haut, on peut remplacer $\mathrm{P}_L(\mathbb{Z}/d)$ par $\mathrm{P}_Q(\mathbb{Z}/d)$. Soient u un élément d-primitif de Q, $S \subset W$ le stabilisateur de la classe de u dans $\mathrm{P}_Q(\mathbb{Z}/d)$ et w un élément de S. On procède comme dans la démonstration de 4.2.19. On a par définition $wu = \lambda u + dx$ avec λ dans $\mathbb{Z}$ premier à d et x dans Q, la classe $\overline{\lambda}$ de λ dans $(\mathbb{Z}/d)^\times$ ne dépend que de w et l'application $\pi : S \to (\mathbb{Z}/d)^\times$, $w \mapsto \overline{\lambda}$ est un homomorphisme de groupes. On vérifie que π est injectif si u est d-régulier à l'aide du scholie 4.1.3. □

Démonstration du point (b). L'égalité $wu = \lambda u + dx$ implique la congruence $\alpha.(wu) \equiv \lambda(\alpha.u) \bmod d$, pour tout α dans R, ou encore $(w^{-1}\alpha).u \equiv \lambda(\alpha.u) \bmod d$. On constate que si l'on a $w\alpha = \alpha$ (et donc $w^{-1}\alpha = \alpha$) alors on a $(\lambda - 1)(\alpha.u) \equiv 0 \bmod d$, soit encore $(\alpha.u)(\pi(w) - 1) = 0$ dans $\mathbb{Z}/d$. Si u est

d-régulier et si d est premier alors on obtient $\pi(w) = 1$. Comme π est injectif quand u est d-régulier, on a bien l'implication $w\alpha = \alpha \Rightarrow w = \mathrm{id}$. $\square$

Remarque. La proposition 4.2.20 est une illustration de l'énoncé 4.3.1 (a) ; la proposition 4.2.19 montre que l'hypothèse faite sur d n'est pas superflue.

Corollaire-Définition 4.3.2. *Soient L un réseau de Niemeier avec racines et p un nombre premier ; on note $\mathrm{D}_p(L)$ le p.g.c.d. des entiers $p-1$, $24h$ et $|W|$. Si p ne divise pas l'indice de Q dans L, alors le stabilisateur, pour l'action de W, d'un élément de $\mathrm{P}_L^{\text{rég}}(\mathbb{F}_p)$ est canoniquement isomorphe à un sous-groupe du groupe $\mu_{\mathrm{D}_p(L)}(\mathbb{F}_p)$ (qui est cyclique d'ordre $\mathrm{D}_p(L)$).*

Démonstration. Soit $S \subset W$ l'un de ces stabilisateurs. D'après 4.3.1 (a), S s'identifie à un sous-groupe de $\mathbb{F}_p^\times$; d'après 4.3.1 (b) le cardinal de S divise le cardinal de R à savoir $24h$. $\square$

Remarque. On constate par inspection que $24\mathrm{h}(L)$ divise $|\mathrm{W}(L)|$ sauf pour $\mathrm{R}(L) = 24\mathbf{A}_1$ auquel cas le p.g.c.d. des entiers $24\mathrm{h}(L)$ et $|\mathrm{W}(L)|$ est 16 ; on a donc $\text{p.g.c.d.}\,(p-1, 24\mathrm{h}(L), |\mathrm{W}(L)|) = \text{p.g.c.d.}\,(p-1, 24\mathrm{h}(L))$ en dehors de ce cas.

Scholie-Définition 4.3.3. *Soient L un réseau de Niemeier avec racines et p un nombre premier ; on note $\mathrm{pas}\,(L;p)$ l'entier défini par*

$$\mathrm{pas}\,(L;p) \;:=\; \frac{|\mathrm{W}(L)|}{\text{p.g.c.d.}\,(p-1, 24\mathrm{h}(L), |\mathrm{W}(L)|)} \qquad .$$

Si p ne divise pas l'indice de Q dans L alors $\mathrm{N}_p(L, \mathrm{Leech})$ est divisible par $\mathrm{pas}\,(L;p)$; on note dans ce cas $\mathrm{n}_p(L)$ l'entier défini par

$$\mathrm{N}_p(L, \mathrm{Leech}) \;=\; \mathrm{n}_p(L)\ \mathrm{pas}\,(L;p) \qquad .$$

Démonstration. L'entier $\mathrm{N}_p(L, \mathrm{Leech})$ est la somme des cardinaux des W-orbites des points c de $\mathrm{C}_L(\mathbb{F}_p)$ avec $\mathrm{vois}_p(L;c) \simeq \mathrm{Leech}$, or ces points appartiennent à $\mathrm{P}_L^{\text{rég}}(\mathbb{F}_p)$ d'après 4.1.4 (a). $\square$

Remarque. L'entier $\mathrm{pas}\,(L;p)$ est le produit de l'entier $\mathrm{pas}_1(L)$ (indépendant de p) et de l'entier $\mathrm{pas}_2\,(L;p)$ respectivement définis par

$$\mathrm{pas}_1(L) = \frac{|\mathrm{W}(L)|}{\text{p.g.c.d.}\,(24\mathrm{h}(L), |\mathrm{W}(L)|)}\ ,\ \mathrm{pas}_2(L;p) = \frac{24\mathrm{h}(L)}{\text{p.g.c.d.}\,(p-1, 24\mathrm{h}(L))}\ .$$

Exemples

On illustre ce qui précède en considérant le réseau de Niemeier A_{24}^{+} associé au système de racines $\mathbf{A}_{24}$ (voir le deuxième des exemples qui suivent II.3.15) et les nombres premiers 29 et 31 ; cette illustration est intéressée : le calcul des entiers $\mathrm{N}_{29}(\mathrm{A}_{24}^{+}, \mathrm{Leech})$ et $\mathrm{N}_{31}(\mathrm{A}_{24}^{+}, \mathrm{Leech})$ sera utilisé en IX.3.1.

On rappelle que l'on a par construction $\mathrm{Q}(\mathbf{A}_{24}) = \mathrm{A}_{24}$, A_{24} désignant le sous-$\mathbb{Z}$-module de $\mathbb{Z}^{25}$ constitué des 25-uples $(x_1, x_2, \ldots, x_{25})$ avec $\sum_i x_i = 0$, muni de la forme bilinéaire paire induite par la structure euclidienne de $\mathbb{R}^{25}$. Le groupe de Weyl W s'identifie au groupe symétrique $\mathfrak{S}_{25}$, son action sur A_{24} étant l'action évidente. Il en résulte que le $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathrm{A}_{24}$ s'identifie au sous-espace vectoriel de $\mathbb{F}_p^{25}$ constitué des éléments $(x_1, x_2, \ldots, x_{25})$ avec $\sum_i x_i = 0$, l'action induite de $\mathfrak{S}_{25}$ étant toujours l'action évidente.

On note respectivement $\widetilde{\mathrm{C}}_{\mathrm{A}_{24}}(\mathbb{F}_p)$ et $\widetilde{\mathrm{C}}_{\mathrm{A}_{24}}^{\text{rég}}(\mathbb{F}_p)$ les images inverses de $\mathrm{C}_{\mathrm{A}_{24}}(\mathbb{F}_p)$ et $\mathrm{C}_{\mathrm{A}_{24}}^{\text{rég}}(\mathbb{F}_p)$ dans $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathrm{A}_{24} - \{0\}$; pour $p \neq 2$, $\widetilde{\mathrm{C}}_{\mathrm{A}_{24}}(\mathbb{F}_p)$ s'identifie, comme $(\mathfrak{S}_{25} \times \mathbb{F}_p^{\times})$-ensemble, au sous-ensemble de $\mathbb{F}_p^{25} - \{(0, 0, \ldots, 0)\}$ constitué des éléments $(x_1, x_2, \ldots, x_{25})$ vérifiant

$$(*) \qquad x_1 + x_2 + \ldots + x_{25} = 0 \qquad \text{et} \qquad x_1^2 + x_2^2 + \ldots + x_{25}^2 = 0 \qquad .$$

Par définition le 25-uple $(x_1, x_2, \ldots, x_{25})$ est une application ensembliste de $\{1, 2, \ldots, 25\}$ dans $\mathbb{F}_p$; on la note x. On constate que x appartient à $\widetilde{\mathrm{C}}_{\mathrm{A}_{24}}^{\text{rég}}(\mathbb{F}_p)$ si et seulement si l'application x est injective. En effet, si l'on voit le système de racines $\mathbf{A}_{24}$, de la façon habituelle, comme un sous-ensemble de l'espace euclidien $\mathbb{R}^{25}$ muni de sa base canonique $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{25}\}$ [Bou81b, Planche I], alors les racines sont les $\varepsilon_i - \varepsilon_j$, $i \neq j$. On remarquera incidemment que cette observation permet de se convaincre, à peu de frais, que si l'ensemble $\mathrm{P}_{\mathrm{A}_{24}^{+}}^{\text{rég}}(\mathbb{F}_p)$ est non vide alors on a nécessairement $p \geq 25$, au moins pour $p \neq 5$).

On en vient maintenant aux deux exemples que nous avions en vue.

1) Sur les réseaux $\mathrm{vois}_{29}(\mathrm{A}_{24}^{+}; c)$ pour c dans $\mathrm{C}_{\mathrm{A}_{24}^{+}}^{\text{rég}}(\mathbb{F}_{29})$

Soit $x : \{1, 2, \ldots, 25\} \to \mathbb{F}_{29}$ une application injective ; on note $\{y_1, y_2, y_3, y_4\}$ la partie à 4 éléments de $\mathbb{F}_{29}$ complémentaire de l'image de x. Comme l'on a $\sum_{z \in \mathbb{F}_{29}} z = 0$ et $\sum_{z \in \mathbb{F}_{29}} z^2 = 0$, l'application x vérifie (*) si et seulement cette partie à 4 éléments vérifie

$$y_1 + y_2 + y_3 + y_4 = 0 \qquad \text{et} \qquad y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0 \qquad .$$

On note $\mathcal{C}$ (resp. $\widetilde{\mathcal{C}}$) le sous-schéma de $\mathbf{P}^3$ (resp. $\mathbf{A}^4 - \{0\}$), disons sur $\mathbb{F}_{29}$, défini par les équations ci-dessus ; il est clair que $\mathcal{C}$ est isomorphe à $\mathbf{P}^1$.

On note enfin $\mathcal{C}^{\text{rég}}$ (resp. $\widetilde{\mathcal{C}}^{\text{rég}}$) l'ouvert de $\mathcal{C}$ (resp. $\widetilde{\mathcal{C}}$) défini par $y_i \neq y_j$ pour $i \neq j$; comme -2 n'est pas un carré dans $\mathbb{F}_{29}$ on a en fait $\mathcal{C}(\mathbb{F}_{29}) = \mathcal{C}^{\text{rég}}(\mathbb{F}_{29})$ et $\widetilde{\mathcal{C}}(\mathbb{F}_{29}) = \widetilde{\mathcal{C}}^{\text{rég}}(\mathbb{F}_{29})$.

Nous avons introduit le formalisme ci-dessus pour en arriver aux énoncés suivants :

– L'ensemble $\mathfrak{S}_{25}\backslash\widetilde{\mathrm{C}}^{\text{rég}}_{\mathrm{A}_{24}}(\mathbb{F}_{29})$ quotient de l'action de $\mathfrak{S}_{25}$ sur $\widetilde{\mathrm{C}}^{\text{rég}}_{\mathrm{A}_{24}}(\mathbb{F}_{29})$ et l'ensemble $\mathfrak{S}_4\backslash\widetilde{\mathcal{C}}^{\text{rég}}(\mathbb{F}_{29})$ quotient de l'action évidente de $\mathfrak{S}_4$ sur $\widetilde{\mathcal{C}}^{\text{rég}}(\mathbb{F}_{29})$ sont canoniquement en bijection. De plus ces deux quotients sont munis d'actions naturelles de $\mathbb{F}_{29}^\times$ et la bijection que l'on vient d'évoquer est équivariante.

– On dispose d'une bijection canonique, disons

$$\kappa : \mathfrak{S}_4\backslash\mathcal{C}^{\text{rég}}(\mathbb{F}_{29}) \xrightarrow{\cong} \mathfrak{S}_{25}\backslash\mathrm{C}^{\text{rég}}_{\mathrm{A}_{24}}(\mathbb{F}_{29}) \qquad .$$

De plus, pour toute $\mathfrak{S}_4$-orbite $\mathcal{O}$ de $\mathcal{C}^{\text{rég}}(\mathbb{F}_{29})$, les stabilisateurs de $\mathcal{O}$ et $\kappa(\mathcal{O})$, qui s'identifient tous deux à des sous-groupes de $\mathbb{F}_{29}^\times$, sont canoniquement isomorphes.

On analyse enfin l'action de $\mathfrak{S}_4$ sur l'ensemble $\mathcal{C}(\mathbb{F}_{29}) = \mathcal{C}^{\text{rég}}(\mathbb{F}_{29})$; pour cela il peut être utile d'observer que le fait que -3 n'est pas un carré dans $\mathbb{F}_{29}$ implique que tout élément (y_1, y_2, y_3, y_4) de $\widetilde{\mathcal{C}}(\mathbb{F}_{29})$ vérifie $y_i \neq 0$ pour tout i.

On vérifie que l'action du groupe $\mathfrak{S}_4$ sur l'ensemble à 30 éléments $\mathcal{C}(\mathbb{F}_{29})$ a exactement deux orbites :

– l'orbite, disons $\mathcal{O}_1$, de la classe du point $(1, 12, -1, -12)$ de $\mathbb{F}_{29}^4$ dont le stabilisateur est isomorphe à $\mu_4(\mathbb{F}_{29})$ (observer que $\{1, 12, -1, -12\} \subset \mathbb{F}_{29}^\times$ est le sous-groupe $\mu_4(\mathbb{F}_{29})$),

– l'orbite, disons $\mathcal{O}_2$, de la classe du point $(1, 4, 6, -11)$ qui est libre.

Il en résulte que l'action du groupe $\mathfrak{S}_{25}$ sur l'ensemble $\mathrm{C}^{\text{rég}}_{\mathrm{A}_{24}}(\mathbb{F}_{29})$ a exactement deux orbites à savoir $\Omega_1 = \kappa(\mathcal{O}_1)$ dont le stabilisateur est isomorphe à $\mu_4(\mathbb{F}_{29})$ et $\Omega_2 = \kappa(\mathcal{O}_2)$ qui est libre ; on observera que ceci confirme 4.3.2 puisque l'on a $\mathrm{D}_{29}(\mathrm{A}_{24}^+) = 4$.

`PARI` nous dit que les réseaux $\mathrm{vois}_{29}(\mathrm{A}_{24}^+; \Omega_1)$ et $\mathrm{vois}_{29}(\mathrm{A}_{24}^+; \Omega_2)$ (l'abus de notation est véniel) sont tous deux isomorphes au réseau de Leech. On obtient donc finalement :

$$\mathrm{N}_{29}(\mathrm{A}_{24}^+, \text{Leech}) \;=\; \frac{5}{4}\,|\mathrm{W}(\mathbf{A}_{24})| \;=\; 1938901255416373248000000 0$$

(soit encore, avec la notation introduite en 4.3.3, $\mathrm{n}_{29}(\mathrm{A}_{24}^+) = 5$).

En fait, on peut éviter ci-dessus le recours à `PARI`, en invoquant la proposition *ad hoc* suivante :

Proposition 4.3.4. *Soient L un réseau de Niemeier avec racines, ρ un vecteur de Weyl et α une racine de L ; on note d l'entier $2h+1-\rho.\alpha$. Alors :*

(1) *On a $d \geq h+2$.*

(2) *On a $\mathrm{q}(\rho - h\alpha) = hd$.*

(3) *Il existe β appartenant à B (en clair, la base de $\mathrm{R}(L)$ déterminée par ρ) avec $\alpha.\beta = 0$.*

(4) *L'élément $\rho - h\alpha$ de L est primitif.*

(5) *Le réseau $\mathrm{vois}_d(L;\rho - h\alpha)$ (qui est bien défini d'après (2) et (4)) est isomorphe au réseau $\mathrm{vois}_h(L;\rho)$ (qui est isomorphe au réseau de Leech d'après 4.2.10 (c)).*

Démonstration. La propriété (1) résulte de l'inégalité $|\rho.\alpha| \leq h-1$; (2) est immédiate. La propriété (3) est claire si le système de R n'est pas irréductible ; on peut s'en convaincre par inspection dans le cas contraire ($R = \mathbf{A}_{24}, \mathbf{D}_{24}$). La propriété (3) implique la propriété (4) : observer que l'on a $(\rho - h\alpha).\beta = 1$. Enfin la propriété (5) est conséquence du point (b) de 1.14. □

Pour appliquer cette proposition au cas qui nous intéresse, à savoir $L = \mathrm{A}_{24}^+$ et $d = 29$, nous devons choisir ρ et α avec $\rho.\alpha = 22$. Suivant Bourbaki, on prend $\rho = \sum_{i=1}^{25}(13-i)\varepsilon_i$; il y a alors trois choix possibles pour α : $\alpha_i = \varepsilon_i - \varepsilon_{i+22}$, $i = 1,2,3$. Soit c_i la classe de $\rho - 25\alpha_i$ dans $\mathrm{C}_{\mathrm{A}_{24}}^{\text{rég}}(\mathbb{F}_{29})$ (c_i est nécessairement 29-régulière puisque l'on a $\mathrm{vois}_{29}(\mathrm{A}_{24}^+;\rho) \simeq$ Leech) ; on constate que c_2 est dans l'orbite Ω_1 et c_1 et c_3 dans l'orbite Ω_2 (soit $w_0 \in \mathfrak{S}_{25}$ la permutation $i \mapsto 26-i$, on observera que w_0 fixe c_2 et échange c_1 et c_3).

2) Sur les réseaux $\mathrm{vois}_{31}(\mathrm{A}_{24}^+;c)$ pour c dans $\mathrm{C}_{\mathrm{A}_{24}^+}^{\text{rég}}(\mathbb{F}_{31})$

On peut à nouveau appliquer la méthode précédente pour déterminer l'entier $\mathrm{N}_{31}(\mathrm{A}_{24}^+, \text{Leech})$. Cette fois $\mathcal{C}$ est la quadrique projective définie par les équations

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 = 0 \quad \text{et} \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_3^2 + y_4^2 = 0 \quad .$$

Cependant les cardinaux des ensembles $\mathcal{C}(\mathbb{F}_{31})$ et $\mathcal{C}^{\text{rég}}(\mathbb{F}_{31})$ sont respectivement 30784 et 18864 si bien que le volume des calculs est plus important. Nous donnons seulement ci-dessous le résultat de ces calculs, en épargnant les détails au lecteur.

Les stabilisateurs non triviaux de l'action de $\mathfrak{S}_6$ sur $\mathcal{C}^{\text{rég}}(\mathbb{F}_{31})$ sont les sous-groupes $\mu_6(\mathbb{F}_{31})$, $\mu_3(\mathbb{F}_{31})$ et $\mu_2(\mathbb{F}_{31})$ (en accord avec l'égalité $\mathrm{D}_{31}(\mathrm{A}_{24}^+) = 30$).
– Il existe une seule orbite avec stabilisateur $\mu_6(\mathbb{F}_{31})$; le voisin de A_{24}^+ qui lui est associé est Leech.

– Il existe une seule orbite avec stabilisateur $\mu_5(\mathbb{F}_{31})$; le voisin associé est à nouveau Leech.

– Il existe exactement 4 orbites avec stabilisateur $\mu_3(\mathbb{F}_{31})$; une conduit à Leech, deux au réseau de Niemeier dont le système de racines est $24\mathbf{A}_1$ et une au réseau de Niemeier dont le système de racines est $12\mathbf{A}_2$.

– Il existe une seule orbite avec stabilisateur $\mu_2(\mathbb{F}_{31})$; le voisin associé est Leech.

– Il existe exactement 24 orbites libres ; 8 conduisent à Leech, 15 au réseau de Niemeier dont le système de racines est $24\mathbf{A}_1$ et une seule au réseau de Niemeier dont le système de racines est $12\mathbf{A}_2$.

(On observera au passage que l'inventaire que nous venons de faire montre en particulier que 4.1.4 (a) n'admet pas de réciproque.)

On en déduit :

$$\mathrm{N}_{31}(\mathrm{A}_{24}^{+}, \mathrm{Leech}) \;=\; \frac{46}{5}\,|\mathrm{W}(\mathbf{A}_{24})| \;=\; 1427031323986450710528000 00$$

(soit encore $\mathrm{n}_{31}(\mathrm{A}_{24}^{+}) = 276$).

4.4. Complément : Sur les 2-voisins, associés à un vecteur de Weyl, d'un réseau de Niemeier avec racines

Ce sous-paragraphe s'inspire de [Bor84], en particulier les commentaires par lesquels il s'achève sont à comparer aux arguments que donnent Borcherds dans cet article pour prouver l'existence *a priori* d'un réseau unimodulaire pair de dimension 24 sans racines.

Soient L un réseau de Niemeier avec racines et ρ l'un de ses vecteurs de Weyl. L'égalité $\mathrm{q}(\rho) = h(h+1)$ (Proposition 4.2.5) implique la congruence $\mathrm{q}(\rho) \equiv 0 \bmod 2$, si bien que l'on peut considérer le réseau $\mathrm{vois}_2(L;\rho)$ (ρ est primitif donc *a fortiori* 2-primitif). Nous étudions ci-après ce 2-voisin de L.

On étend la définition du nombre de Coxeter d'un réseau de Niemeier avec racines (Proposition-Définition II.3.3), à tous les réseaux de Niemeier, en convenant que le nombre de Coxeter du réseau de Leech est 0.

Proposition 4.4.1. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. On a l'inégalité*

$$\mathrm{h}(\mathrm{vois}_2(L;\rho)) \;\leq\; \frac{\mathrm{h}(L)+1}{2} \qquad .$$

Démonstration. On pose $h = \mathrm{h}(L)$ et $h' = \mathrm{h}(\mathrm{vois}_2(L;\rho))$.

On suppose tout d'abord h pair. Soit $\widetilde{\rho}$ un élément de L avec $\widetilde{\rho} \equiv \rho \bmod h$ et $\mathrm{q}(\widetilde{\rho}) \equiv 0 \bmod h^2$. On a vu, lors de l'étude de l'algorithme des voisins, qu'un tel élément existe ; ici on peut prendre $\widetilde{\rho} = \rho - h\alpha$, α désignant une racine de la base de $\mathrm{R}(L)$ définie par ρ. La proposition 1.13 dit que $\frac{\widetilde{\rho}}{2}$ est un élément $\frac{h}{2}$-primitif de $\mathrm{vois}_2(L;\rho)$ et que l'on a dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ l'égalité

$$\mathrm{vois}_h(L;\rho) \;=\; \mathrm{vois}_{\frac{h}{2}}(\mathrm{vois}_2(L;\rho);\frac{\widetilde{\rho}}{2}) \qquad .$$

Cette égalité montre que le réseau $\mathrm{vois}_2(L;\rho)$ possède un $\frac{h}{2}$-voisin sans racines puisque le point (c) de 4.2.10 dit que le réseau $\mathrm{vois}_h(L;\rho)$ est sans racines. On en déduit $\frac{h}{2} \geq h'$ grâce à 4.1.1.

Le cas h impair est similaire. On contemple cette fois l'égalité

$$\mathrm{vois}_{h+1}(L;\rho) \;=\; \mathrm{vois}_{\frac{h+1}{2}}(\mathrm{vois}_2(L;\rho);\frac{\widetilde{\rho}}{2})$$

avec par exemple $\widetilde{\rho} = \rho + (h+1)\alpha$. □

On vient de voir que la démonstration de la proposition 4.4.1 repose sur la proposition 4.1.1 et le point (c) du théorème 4.2.10 ("holy constructions") ; on se propose maintenant de donner une démonstration *ab initio* de l'énoncé ci-dessous qui affine 4.4.1.

Proposition 4.4.2. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. On a l'égalité*

$$\mathrm{h}(\mathrm{vois}_2(L;\rho)) \;=\; \frac{\mathrm{h}(L)}{2} - \frac{\iota(\mathrm{R}(L))}{8} + 2 \qquad ,$$

la notation $\iota(\mathrm{R}(L))$ désignant ci-dessus le nombre d'exposants impairs du groupe de Weyl de $\mathrm{R}(L)$ [Bou81b, Ch. V, §6, Déf. 2].

Avant d'expliquer la démonstration de cette proposition, donnons quelques informations sur le nombre d'exposants impairs, disons $\iota(R)$, du groupe de Weyl d'un système de racines R.

(1) L'invariant ι est additif en le sens suivant : $\iota(R_1 \coprod R_2) = \iota(R_1) + \iota(R_2)$.

(2) La valeur de ι sur les systèmes de racines irréductibles de type ADE est la suivante : $\iota(\mathbf{A}_l) = [\frac{l+1}{2}]$, $\iota(\mathbf{D}_l) = 2[\frac{l}{2}]$, $\iota(\mathbf{E}_6) = 4$, $\iota(\mathbf{E}_7) = 7$, $\iota(\mathbf{E}_8) = 8$.

(3) Soit R un système de racines de rang l et de nombre de Coxeter h. Comme l'ensemble des exposants de R est stable sous l'involution $m \mapsto h - m$ et que son cardinal est l [Bou81b, Ch. V, §6, n° 2], on constate que si h est impair alors on a $l = 2\iota(R)$.

Soit R un système de racines de type ADE de rang l et de nombre de Coxeter h. Les points (1) et (2) montrent que l'on a l'inégalité $l \geq 2\iota(R)$ et que l'on a l'égalité si et seulement si toutes les composantes irréductibles de R sont de type $\mathbf{A}_d$ avec d pair. Cette dernière condition équivaut à h impair, ce qui est en accord avec le point (3).

Ce qui précède montre que la proposition 4.4.2 implique bien la proposition 4.4.1 et que l'on a l'égalité dans l'inégalité de 4.4.1 si et seulement si $\mathrm{R}(L)$ est isomorphe à la somme directe de $\frac{24}{d}$ copies de $\mathbf{A}_d$ avec d un diviseur pair de 24 (se rappeler que $\mathrm{R}(L)$ est équicoxeter). On observera incidemment que les trois conditions suivantes sont équivalentes :

– $\mathrm{h}(L)$ est impair ;

– $\mathrm{R}(L)$ est isomorphe à la somme directe de $\frac{24}{d}$ copies de $\mathbf{A}_d$ avec d un diviseur pair de 24 ;

– on a l'égalité $\mathrm{h}(\mathrm{vois}_2(L;\rho)) = \frac{\mathrm{h}(L)+1}{2}$.

La démonstration de la proposition 4.4.2 est basée sur les deux propositions 4.4.3 et 4.4.4 ci-après.

Proposition 4.4.3. *Soient L un réseau de Niemeier avec racines et ρ un vecteur de Weyl de L. Alors le nombre de racines α de L avec $\rho.\alpha$ pair est* $12\mathrm{h}(L) - \iota(\mathrm{R}(L))$.

Démonstration. Soient R un système de racines, C une chambre de R, $B \subset R$ la base et $R_+ \subset R$ le sous-ensemble des racines positives, définis par C ; la démonstration de 4.4.3 est conséquence de la relation, dégagée par Bertram Kostant dans [Kos59], entre la fonction hauteur $\mathrm{R}_+ \to \mathbb{N} - 0$ et les exposants du groupe de Weyl de R. Nous rappelons cette théorie ci-dessous.

La fonction *hauteur*, disons $\mathrm{H} : R_+ \to \mathbb{N} - \{0\}$, associe à une racine positive la somme de ses coordonnées dans la base B ; nous notons $\mathrm{Exp}(R)$ l'ensemble des exposants de R.

Soient A un groupe abélien et $f : \mathbb{N} - \{0\} \to A$ une application (ensembliste). Soit $F : \mathbb{N} - \{0\} \to A$ la "primitive" de f, c'est-à-dire l'application définie par

$$F(m) \;=\; \sum_{k=1}^{m} f(k) \qquad .$$

Alors on a dans A l'égalité suivante :

$$\text{(Ko)} \qquad \sum_{\alpha \in R_+} f(\mathrm{H}(\alpha)) \;=\; \sum_{m \in \mathrm{Exp}(R)} F(m) \qquad .$$

Cette égalité est conséquence de la relation de Kostant évoquée plus haut. Expliquons pourquoi. Soient i un élément de $\mathbb{N} - \{0\}$ et $\delta_{(i)} : \mathbb{N} - \{0\} \to \mathbb{Z}$ la "masse de Dirac" correspondante. L'égalité ci-dessus dit, dans le cas particulier $f = \delta_{(i)}$, que le cardinal de $\mathrm{H}^{-1}(i)$ est égal au cardinal du sous-ensemble de $\mathrm{Exp}(R)$ constitué des m avec $m \geq i$; ceci est le résultat de Kostant. Le cas général en résulte par linéarité.

On revient maintenant à la démonstration de 4.4.3. Soit ν (resp. ν_+) le nombre de racines (resp. de racines positives, pour la chambre associée à ρ) α de L avec $\rho.\alpha$ pair ; il est clair que l'on a $\nu = 2\nu_+$. Dans le contexte de 4.4.3, on a $\mathrm{H}(\alpha) = \rho.\alpha$; en prenant pour f, dans l'égalité (Ko), la fonction $\mathbb{N} - \{0\} \to \mathbb{Z}, k \mapsto (-1)^k$, on obtient :

$$|\mathrm{R}_+(L;\rho)| - 2\,\nu_+ \;=\; \iota(\mathrm{R}(L)) \qquad ,$$

$\mathrm{R}_+(L;\rho)$ désignant le sous-ensemble constitué des racines positives pour la chambre associée à ρ, soit encore

$$\nu \;=\; \frac{|\mathrm{R}(L)|}{2} - \iota(\mathrm{R}(L)) \qquad .$$

Or on a $|\mathrm{R}(L)| = 24\mathrm{h}(L)$ d'après II.3.3 (c). □

Soient Λ un réseau entier et $k \geq 0$ un entier, on note $\mathrm{r}_k(\Lambda)$ le nombre de représentations de k par Λ, c'est-à-dire le nombre d'éléments x de Λ avec $x.x = k$.

Proposition 4.4.4 (Borcherds)**.** *Soit B un réseau unimodulaire impair de dimension 24 ; soient L_1 et L_2 les deux 2-voisins pairs de B. Alors on a :*

$$\mathrm{r}_2(L_1) + \mathrm{r}_2(L_2) \;=\; 3\,\mathrm{r}_2(B) \;-\; 24\,\mathrm{r}_1(B) \;+\; 48 \qquad .$$

Démonstration (esquisse). Soient $n > 0$ un entier divisible par 8 et B un réseau unimodulaire de dimension n ; on considère la série thêta

$$\vartheta_B(\tau) \;=\; \sum_{x \in B} e^{\imath\pi\tau x.x}$$

(τ dans le demi-plan de Poincaré). La fonction ϑ_B est une forme modulaire de poids $\frac{n}{2}$ pour le sous-groupe, disons Γ', du groupe $\Gamma := \mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{I}\}$, engendré par les transformations $\tau \mapsto \tau + 2$ et $\tau \mapsto \frac{-1}{\tau}$; elle est en outre modulaire pour Γ si B est pair. On note respectivement $\mathrm{M}_{\frac{n}{2}}(\Gamma)$ et $\mathrm{M}_{\frac{n}{2}}(\Gamma')$ les $\mathbb{C}$-espaces vectoriels constitués des formes modulaires de poids $\frac{n}{2}$ pour les groupes Γ et Γ' ; comme Γ' est d'indice fini (à savoir 3) dans Γ on dispose d'un homomorphisme de transfert, disons $\mathrm{tr} : \mathrm{M}_{\frac{n}{2}}(\Gamma') \to \mathrm{M}_{\frac{n}{2}}(\Gamma)$. La démonstration de l'énoncé suivant est laissée en exercice au lecteur.

Lemme 4.4.5. *Soient $n > 0$ un entier divisible par 8 et B un réseau unimodulaire impair de dimension n ; soient L_1 et L_2 les deux 2-voisins pairs de B. Alors on a :*

$$\vartheta_{L_1} + \vartheta_{L_2} \;=\; \mathrm{tr}(\vartheta_B) \qquad .$$

On vérifie que $\mathcal{B} := (\mathbb{E}_4^3, \mathbb{E}_4^2\vartheta_{\mathrm{I}_8}, \mathbb{E}_4\vartheta_{\mathrm{I}_{16}}, \Delta)$ est une base de $\mathrm{M}_{12}(\Gamma')$ (on rappelle que la notation $\mathbb{E}_4$ désigne la série d'Eiseinstein normalisée, modulaire de poids 4 pour Γ, que l'on a $\vartheta_{\mathrm{E}_8} = \mathbb{E}_4$, que Δ est l'unique forme parabolique normalisée de poids 12 pour Γ et que $(\mathbb{E}_4^3, \Delta)$ est une base de $\mathrm{M}_{12}(\Gamma)$).

Puisque $\mathbb{E}_4$ et Δ sont modulaires pour Γ on a $\mathrm{tr}(\mathbb{E}_4^3) = 3\mathbb{E}_4^3$ et $\mathrm{tr}(\Delta) = 3\Delta$; d'autre part le lemme 4.4.5 implique $\mathrm{tr}(\vartheta_{\mathrm{I}_8}) = 2\mathbb{E}_4$ et $\mathrm{tr}(\vartheta_{\mathrm{I}_{16}}) = 2\mathbb{E}_4^2$. Comme le transfert est $\mathrm{M}(\Gamma)$-linéaire, $\mathrm{M}(\Gamma)$ désignant la $\mathbb{C}$-algèbre graduée des formes modulaires pour Γ, on constate au bout du compte que l'image de la base $\mathcal{B}$, par l'homomorphisme de transfert, est $(3\mathbb{E}_4^3, 2\mathbb{E}_4^3, 2\mathbb{E}_4^3, 3\Delta)$.

Soit maintenant B un réseau unimodulaire impair de dimension 24. Soient (c_0, c_1, c_2, c_3) les coordonnées de ϑ_B dans la base $\mathcal{B}$:

$$\vartheta_B = c_0\mathbb{E}_4^3 + c_1\mathbb{E}_4^2\vartheta_{\mathrm{I}_8} + c_2\mathbb{E}_4\vartheta_{\mathrm{I}_{16}} + c_3\Delta \qquad .$$

Puisque le terme constant du développement de Fourier de ϑ_B est 1, on a $c_0+c_1+c_2 = 1$. Comme B est impair, le lemme 4.4.5 dit que le terme constant du développement de Fourier de $\mathrm{tr}(\vartheta_B)$ est 2 ; on a donc $3c_0 + 2c_1 + 2c_2 = 2$. On en déduit $c_0 = 0$.

On note $\mathrm{M}_{12}^0(\Gamma')$ le sous-espace vectoriel de $\mathrm{M}_{12}(\Gamma')$ engendré par $\mathbb{E}_4^2\vartheta_{\mathrm{I}_8}$, $\mathbb{E}_4\vartheta_{\mathrm{I}_{16}}$ et Δ. Soient f un élément de $\mathrm{M}_{12}^0(\Gamma')$ et

$$f \;=\; \mathrm{r}_0(f) \;+\; \mathrm{r}_1(f)\,e^{\imath\pi\tau} \;+\; \mathrm{r}_2(f)\,e^{2\imath\pi\tau} \;+\; \ldots$$

le début de son développement de Fourier ; on constate que l'application linéaire $\mathrm{M}_{12}^0(\Gamma') \to \mathbb{C}^3$, $f \mapsto (\mathrm{r}_0(f), \mathrm{r}_1(f), \mathrm{r}_2(f))$ est un isomorphisme. Il en

résulte que le coefficient de $e^{2\imath\pi\tau}$ dans le développement de Fourier de $\mathrm{tr}(f)$ s'exprime linéairement en fonction de $(\mathrm{r}_0(f), \mathrm{r}_1(f), \mathrm{r}_2(f))$. En résolvant un système linéaire on trouve que ce coefficient est $48\mathrm{r}_0(f) - 24\mathrm{r}_1(f) + 3\mathrm{r}_2(f)$. Compte tenu de 4.4.5, on obtient 4.4.4 en prenant $f = \vartheta_B$. □

Démonstration de 4.4.2 à l'aide de 4.4.3 et 4.4.4

Soit B le réseau unimodulaire impair de dimension 24 dont les deux 2-voisins pairs sont L et $\mathrm{vois}_2(L;\rho)$. Comme l'on a $\mathrm{r}_2(\Lambda) = 24\mathrm{h}(\Lambda)$ pour tout réseau unimodulaire pair Λ de dimension 24 (point (c) de II.3.3 pour $\mathrm{r}_2(\Lambda) \neq 0$ et convention pour $\mathrm{r}_2(\Lambda) = 0$) la proposition 4.4.4 donne

$$(1) \qquad 24\,\mathrm{h}(L) + 24\,\mathrm{h}(\mathrm{vois}_2(L;\rho)) \;=\; 3\,\mathrm{r}_2(B) \;-\; 24\,\mathrm{r}_1(B) \;+\; 48 \qquad .$$

Par construction le sous-module de B constitué des éléments x avec $x.x$ pair est le réseau $\mathrm{M}_2(L;\rho)$; on a donc $\mathrm{r}_2(B) = \mathrm{r}_2(\mathrm{M}_2(L;\rho))$. Par construction encore, $\mathrm{r}_2(\mathrm{M}_2(L;\rho))$ est le nombre de racines α de L avec $\rho.\alpha$ pair ; on a donc

$$(2) \qquad \mathrm{r}_2(\mathrm{M}_2(L;\rho)) \;=\; 12\,\mathrm{h}(L) - \iota(\mathrm{R}(L))$$

d'après 4.4.3. Les égalités (1) et (2) entraînent

$$(3) \qquad \mathrm{h}(\mathrm{vois}_2(L;\rho)) \;=\; \frac{\mathrm{h}(L)}{2} - \frac{\iota(\mathrm{R}(L))}{8} + 2 - \mathrm{r}_1(B) \qquad .$$

Il reste à montrer $\mathrm{r}_1(B) = 0$. On procède par l'absurde. Si l'on a $\mathrm{r}_1(B) \neq 0$ alors on a $\mathrm{r}_1(B) \geq 2$ et l'égalité (3) implique l'inégalité $\mathrm{h}(\mathrm{vois}_2(L;\rho)) < \mathrm{h}(L)$ qui montre que les réseaux L et $\mathrm{vois}_2(L;\rho)$ ne sont pas isomorphes. Or le corollaire 1.16 montre que si l'on a $\mathrm{r}_1(B) \neq 0$ alors les réseaux L et $\mathrm{vois}_2(L;\rho)$ sont isomorphes. □□

Commentaires

On note XR_{24} le sous-ensemble de X_{24} constitué des classes d'isomorphisme de réseaux unimodulaires pairs de dimension 24 avec racines. On note YR_{24} l'ensemble des classes d'isomorphisme de systèmes de racines équicoxeter de rang 24 ; on note Y_{24} la réunion disjointe de YR_{24} et du singleton $\{\emptyset\}$. D'après les points (a) et (b) de II.3.3, l'application $L \mapsto \mathrm{R}(L)$ induit des applications $\mathrm{XR}_{24} \to \mathrm{YR}_{24}$ et $\mathrm{X}_{24} \to \mathrm{Y}_{24}$, la seconde prolongeant la première, que l'on note encore R. On oublie ci-dessous que l'on sait que l'application $\mathrm{R} : \mathrm{X}_{24} \to \mathrm{Y}_{24}$ est bijective.

Soit L un réseau unimodulaire pair de dimension 24 et ρ un vecteur de Weyl de L. Comme le groupe $\mathrm{W}(\mathrm{R}(L))$ permute transitivement les vecteurs de

Weyl de L, l'application $L \mapsto \mathrm{vois}_2(L;\rho)$ induit une application $\mathrm{XR}_{24} \to \mathrm{X}_{24}$ que l'on note φ.

Soit R un élément de YR_{24}, on pose

$$\mathrm{h}'(R) \;=\; \frac{\mathrm{h}(R)}{2} - \frac{\iota(R)}{8} + 2 \qquad ;$$

on vérifie que $\mathrm{h}'(R)$ appartient à $\mathbb{N}$. La proposition 4.4.2 dit que l'on a l'égalité suivante :

$$(1) \qquad \mathrm{h}(\mathrm{R}(\varphi([L])) \;=\; \mathrm{h}'(\mathrm{R}([L])) \qquad .$$

Cette égalité suffit à déterminer $\mathrm{R}(\varphi([L]))$ si $\mathrm{h}'(\mathrm{R}(L))$ est différent de 12, 10 ou 6. En effet, les fibres $\mathrm{h}^{-1}(k)$ de l'application $\mathrm{h} : \mathrm{X}_{24} \to \mathbb{N}$ ont 0 ou 1 élément sauf pour $k = 12, 10, 6$, auxquels cas on a $\mathrm{h}^{-1}(12) = \{\mathbf{A}_{11}\mathbf{D}_7\mathbf{E}_6, 4\mathbf{E}_6\}$, $\mathrm{h}^{-1}(10) = \{2\mathbf{A}_9\mathbf{D}_6, 4\mathbf{D}_6\}$ et $\mathrm{h}^{-1}(6) = \{4\mathbf{A}_5\mathbf{D}_4, 6\mathbf{D}_4\}$. On vérifie par inspection que $\mathrm{h}'^{-1}(12)$ est vide et que l'on a $\mathrm{h}'^{-1}(10) = \{2\mathbf{D}_{12}\}$ et $\mathrm{h}'^{-1}(6) = \{3\mathbf{D}_8, \mathbf{A}_{11}\mathbf{D}_7\mathbf{E}_6, 4\mathbf{E}_6\}$. Dans les cas $R = 2\mathbf{D}_{12}, 3\mathbf{D}_8, \mathbf{A}_{11}\mathbf{D}_7\mathbf{E}_6, 4\mathbf{E}_6$, on détermine $\mathrm{R}(\varphi([L]))$ à l'aide de la condition (2) ci-après.

Soit R un système de racines de type ADE muni d'une chambre C, ou ce qui revient au même d'un vecteur de Weyl ρ. On note $R/2$ le sous-système de racines de R constitué des racines de hauteur paire, pour la fonction hauteur définie par C. Le système de racines $R/2$ est encore de type ADE ; on observera que $R/2$ est canoniquement muni d'une chambre : les racines positives pour cette chambre sont celles qui le sont pour C. Il est clair que la classe d'isomorphisme de $R/2$ est indépendante du choix de C. Au niveau des classes d'isomorphisme, l'application $R \mapsto R/2$ est déterminée par les deux propriétés ci-dessous :

– On a l'égalité $(R_1 \coprod R_2)/2 = R_1/2 \coprod R_2/2$.

– Pour R irréductible le système de racines $R/2$ est le suivant : $\mathbf{A}_{2m}/2 = \mathbf{A}_m \coprod \mathbf{A}_{m-1}$, $\mathbf{A}_{2m+1}/2 = \mathbf{A}_m \coprod \mathbf{A}_m$, $\mathbf{D}_{2m}/2 = \mathbf{D}_m \coprod \mathbf{D}_m$, $\mathbf{D}_{2m+1}/2 = \mathbf{D}_{m+1} \coprod \mathbf{D}_m$, $\mathbf{E}_6/2 = \mathbf{A}_5 \coprod \mathbf{A}_1$, $\mathbf{E}_7/2 = \mathbf{A}_7$, $\mathbf{E}_8/2 = \mathbf{D}_8$ (avec les conventions $\mathbf{A}_0 = \emptyset$, $\mathbf{D}_2 = \mathbf{A}_1 \coprod \mathbf{A}_1$ et $\mathbf{D}_3 = \mathbf{A}_3$).

On a par définition $\mathrm{R}(L)/2 = \mathrm{R}(\mathrm{M}_2(L;\rho))$ et donc

$$(2) \qquad \mathrm{R}([L])/2 \;\subset\; \mathrm{R}(\varphi([L]))$$

pour tout $[L]$ dans XR_{24}. Cette inclusion permet de déterminer $\mathrm{R}(\varphi([L]))$ pour $\mathrm{h}'(\mathrm{R}([L])) \in \{10, 6\}$. En effet, on a :

– $(2\mathbf{D}_{12})/2 = 4\mathbf{D}_6 \not\subset 2\mathbf{A}_9\mathbf{D}_6$;

– $(3\mathbf{D}_8)/2 = 6\mathbf{D}_4 \not\subset 4\mathbf{A}_5\mathbf{D}_4$;

– $(\mathbf{A}_{11}\mathbf{D}_7\mathbf{E}_6)/2 = \mathbf{A}_1\,\mathbf{A}_3\,\mathbf{A}_4 3\mathbf{A}_5 \not\subset 6\mathbf{D}_4$;
– $(4\mathbf{E}_6)/2 = 4\mathbf{A}_1 4\mathbf{A}_5 \not\subset 6\mathbf{D}_4$.

La discussion précédente conduit aux énoncés suivants :

Proposition-Définition 4.4.6. *Il existe une unique application*

$$\psi : \mathrm{YR}_{24} \to \mathrm{Y}_{24} \qquad ,$$

telle que l'on a $\mathrm{h}(\psi(R)) = \mathrm{h}'(R)$ *et* $R/2 \subset \psi(R)$.

Remarque. Soit R un élément de YR_{24}, les conditions suivantes sont équivalentes :
– $\psi(R) = R/2$;
– $\iota(R) = 24$;
– les composantes irréductibles de R sont de type $\mathbf{A}_1$, $\mathbf{D}_l$ avec l pair, $\mathbf{E}_7$ ou $\mathbf{E}_8$.

On prolonge ψ en une application $\psi : \mathrm{Y}_{24} \to \mathrm{Y}_{24}$ en posant $\psi(\emptyset) = \emptyset$; pareillement, on prolonge φ en une application $\varphi : \mathrm{X}_{24} \to \mathrm{X}_{24}$ en posant $\varphi([L]) = [L]$ si L est sans racines.

Proposition 4.4.7. *Soient R un élément de Y_{24} et k un entier naturel. On a $\psi^k(R) = \emptyset$ pour* $\mathrm{h}(R) < 2^k + 1$.

(Observer que l'on a $\mathrm{h}(\psi(R)) - 1 \leq \frac{1}{2}\,(\mathrm{h}(R) - 1)$.)

Proposition 4.4.8. *Le diagramme*

$$\begin{array}{ccc} \mathrm{X}_{24} & \xrightarrow{\varphi} & \mathrm{X}_{24} \\ {\scriptstyle \mathrm{R}}\downarrow & & {\scriptstyle \mathrm{R}}\downarrow \\ \mathrm{Y}_{24} & \xrightarrow{\varphi} & \mathrm{Y}_{24} \end{array}$$

est commutatif.

Scholie 4.4.9. *Soient L un réseau unimodulaire pair de dimension 24 et k un entier naturel. Alors $\varphi^k([L])$ est sans racines pour* $\mathrm{h}(L) < 2^k + 1$.

Le graphe orienté de la figure III.1 explicite l'application ψ : ses sommets sont les éléments de Y_{24} et ses arêtes les couples (x, y) de $\mathrm{Y}_{24} \times \mathrm{Y}_{24} -$ diagonale, avec $x \in \mathrm{YR}_{24}$ et $y = \psi(x)$.

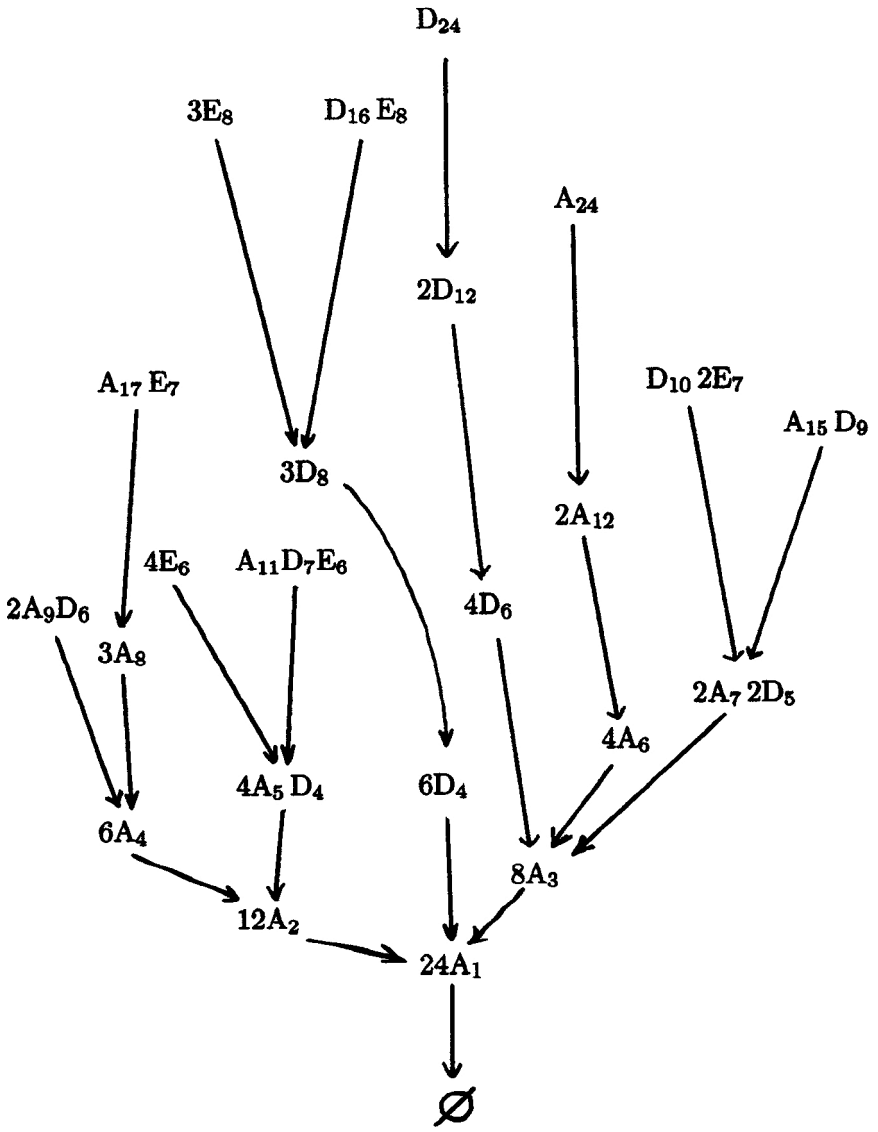

FIGURE III.1 – Système de racines du 2-voisin associé à un vecteur de Weyl d'un réseau unimodulaire pair de dimension 24, en fonction du système de racines de ce dernier.

IV. Formes automorphes et opérateurs de Hecke

1. Réseaux et ensembles de classes des $\mathbb{Z}$-groupes

On note P l'ensemble des nombres premiers. Soient $\widehat{\mathbb{Z}} = \prod_{p\in \mathrm{P}} \mathbb{Z}_p$ et $\mathbb{A}_f = \mathbb{Q}\otimes\widehat{\mathbb{Z}}$ l'anneau des adèles finis de $\mathbb{Q}$. Fixons G un $\mathbb{Z}$-groupe, c'est-à-dire un schéma en groupes affine de type fini sur $\mathbb{Z}$. Le groupe $G(\mathbb{A}_f)$ s'identifie canoniquement au sous-groupe de $\prod_{p\in \mathrm{P}} G(\mathbb{Q}_p)$ dont les éléments (g_p) vérifient $g_p \in G(\mathbb{Z}_p)$ pour *presque tout* p, c'est-à-dire pour tout $p \in \mathrm{P}$ sauf éventuellement un nombre fini d'entre eux. Les groupes $G(\mathbb{Q})$ et $G(\widehat{\mathbb{Z}})$ se plongent naturellement dans $G(\mathbb{A}_f)$ et satisfont $G(\widehat{\mathbb{Z}}) = \prod_{p\in \mathrm{P}} G(\mathbb{Z}_p)$ et $G(\mathbb{Z}) = G(\mathbb{Q}) \cap G(\widehat{\mathbb{Z}})$. Le $G(\mathbb{A}_f)$-ensemble

$$\mathcal{R}(G) = G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$$

jouera un rôle important dans ce chapitre. Nous le notons $\mathcal{R}$, comme "réseau", car il s'identifie en général à l'ensemble des réseaux d'un certain type d'un $\mathbb{Q}$-espace vectoriel.

Un résultat classique de Borel [Bor63, §5] assure que l'*ensemble des classes de* G :

$$\mathrm{Cl}(G) = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}}) = G(\mathbb{Q})\backslash\mathcal{R}(G)$$

est fini. Son cardinal $\mathrm{h}(G) = |\mathrm{Cl}(G)|$ est appelé *nombre de classes* de G. Dans ce qui suit nous décrivons $\mathcal{R}(G)$ et $\mathrm{Cl}(G)$ dans les quelques cas standards qui vont nous intéresser (voir par exemple [Bor63, §2]).

1.1. Groupes linéaires

Commençons par le cas de GL_n. Si V est un espace vectoriel de dimension finie n sur le corps des fractions d'un anneau principal A, nous désignerons par $\mathcal{R}_A(V)$ l'ensemble des réseaux de V relativement à A, c'est-à-dire des sous-A-modules libres de rang n de V (§II.1). Il est muni d'une action transitive de $\mathrm{GL}(V)$, le stabilisateur de $L \in \mathcal{R}_A(V)$ étant $\mathrm{GL}(L)$.

Soit V un $\mathbb{Q}$-espace vectoriel de dimension n. Si p est premier, et si l'on pose $V_p = V \otimes \mathbb{Q}_p$, on dispose d'une application naturelle $\mathcal{R}_{\mathbb{Z}}(V) \to \mathcal{R}_{\mathbb{Z}_p}(V_p)$, $M \mapsto M_p := M \otimes \mathbb{Z}_p$. Fixons $L \in \mathcal{R}_{\mathbb{Z}}(V)$ et posons $G = \mathrm{GL}_L$. Il est élémentaire de vérifier, suivant Eichler [Eic52, §13], que l'application

$$\mathcal{R}_{\mathbb{Z}}(V) \to \prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p), \quad M \mapsto (M_p), \tag{1.1}$$

est une injection de $\mathcal{R}_{\mathbb{Z}}(V)$ sur le sous-ensemble $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p) \subset \prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ constitué des familles (M_p) telles que $M_p = L_p$ pour presque tout p (ce sous-ensemble ne dépendant d'ailleurs pas du choix de L). L'action naturelle de $G(\mathbb{A}_f)$ sur $\prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ préserve $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$, et elle est transitive sur ce dernier. Ainsi, si l'on identifie $\mathcal{R}_{\mathbb{Z}}(V)$ à $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ au moyen de l'application (1.1), ce que l'on fera systématiquement par la suite, on obtient par transport de structure une action transitive de $G(\mathbb{A}_f)$ sur $\mathcal{R}_{\mathbb{Z}}(V)$ étendant l'opération évidente de $G(\mathbb{Q}) = \mathrm{GL}(V)$. Le stabilisateur du réseau L étant $G(\widehat{\mathbb{Z}})$, on en déduit un isomorphisme de $G(\mathbb{A}_f)$-ensembles

$$\mathcal{R}(G) \xrightarrow{\sim} \mathcal{R}_{\mathbb{Z}}(V)$$

Comme $G(\mathbb{Q})$ agit aussi transitivement sur $\mathcal{R}_{\mathbb{Z}}(V)$, il vient en particulier que

$$\mathrm{h}(\mathrm{GL}_n) = 1.$$

Quand $G = \mathrm{PGL}_L$ (resp. $G = \mathrm{SL}_L$), $\mathcal{R}(G)$ s'interprète également comme le quotient de $\mathcal{R}_{\mathbb{Z}}(V)$ par $\mathbb{Q}^\times$ pour l'action par homothéties (resp. comme le sous-ensemble de $\mathcal{R}_{\mathbb{Z}}(V)$ constitué des M possédant une $\mathbb{Z}$-base de déterminant 1 relativement à une $\mathbb{Z}$-base de L). On a encore $\mathrm{h}(\mathrm{PGL}_n) = \mathrm{h}(\mathrm{SL}_n) = 1$.

1.2. Groupes orthogonaux et symplectiques

Supposons de plus que le $\mathbb{Q}$-espace vectoriel V est muni d'une forme bilinéaire non dégénérée φ, supposée symétrique ou alternée. Soit $L \in \mathcal{R}_{\mathbb{Z}}(V)$. Rappelons que son *réseau dual* est le réseau $L^\sharp \in \mathcal{R}_{\mathbb{Z}}(V)$ défini par (§II.1)

$$L^\sharp = \{v \in V, \varphi(v, x) \in \mathbb{Z}, \forall x \in L\}.$$

Nous dirons que L est *homodual*, pour "homothétique à son dual", s'il existe $\lambda \in \mathbb{Q}^\times$ tel que $L^\sharp = \lambda L$; il existe alors un unique tel λ qui soit > 0, que l'on notera λ_L. Le réseau L est dit *autodual* si $L^\sharp = L$. Si L est homodual, et si φ est symétrique (resp. alternée), la forme bilinéaire $\lambda_L \varphi$ munit L d'une structure de b-module (resp. a-module) sur $\mathbb{Z}$ au sens du §II.1. On dira alors

que L est *pair* si $\lambda_L\varphi(x,x) \in 2\mathbb{Z}$ pour tout $x \in L$. C'est automatique si φ est alternée, et si φ est symétrique cela permet de voir L comme un q-module sur $\mathbb{Z}$ en posant $\mathrm{q}(x) = \lambda_L \frac{\varphi(x,x)}{2}$ pour $x \in L$. Notons

$$\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \subset \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$$

les sous-ensembles de $\mathcal{R}_{\mathbb{Z}}(V)$ constitués des réseaux autoduaux (resp. homoduaux) pairs.

Posons $n = \dim V$. Fixons $L \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$. L'existence d'un tel L entraîne, par réduction modulo 2, la congruence $n \equiv 0 \bmod 2$. Considérons le sous-$\mathbb{Z}$-groupe $G \subset \mathrm{GL}_L$ défini par :

$$G = \begin{cases} \mathrm{Sp}_L & \text{si } \varphi \text{ est alternée,} \\ \mathrm{O}_L & \text{sinon.} \end{cases}$$

Nous noterons également $\widetilde{G}$ le $\mathbb{Z}$-groupe de similitudes correspondant, de sorte que $G \subset \widetilde{G} \subset \mathrm{GL}_L$, ainsi que $\mathrm{P}\widetilde{G}$ le $\mathbb{Z}$-groupe des *similitudes projectives*, quotient de $\widetilde{G}$ par son sous-$\mathbb{Z}$-groupe central isomorphe à $\mathbb{G}_m$ constitué des homothéties (§II.1).

Lemme 1.3. *La restriction à $\widetilde{G}(\mathbb{A}_f)$ (resp. $G(\mathbb{A}_f)$) de l'action de $\mathrm{GL}_L(\mathbb{A}_f)$ sur $\mathcal{R}_{\mathbb{Z}}(V)$ préserve $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ (resp. $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$).*

Avant de procéder à la démonstration, introduisons les analogues locaux des définitions précédentes. Soit p premier. Si $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$, il y a encore un sens à considérer le réseau dual $M^\sharp \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$ (relativement à $\mathbb{Z}_p$, voir §II.1). On note $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) \subset \mathcal{R}_{\mathbb{Z}_p}(V_p)$ le sous-ensemble des réseaux M tels qu'il existe $\lambda \in \mathbb{Q}_p^\times$ tel que $M^\sharp = \lambda M$ et $\lambda\varphi(x,x) \in 2\mathbb{Z}_p$ pour tout $x \in M$. Notons également $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p) \subset \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ le sous ensemble des M tels que $M^\sharp = M$. Si $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$, il existe un unique $\lambda_M \in p^{\mathbb{Z}}$ tel que $M^\sharp = \lambda_M M$. Si φ est symétrique (resp. alternée), la forme quadratique $x \mapsto \lambda_M \frac{\varphi(x,x)}{2}$ (resp. la forme alternée $\lambda_M\varphi$) munit alors M d'une structure de q-module (resp. a-module) sur $\mathbb{Z}_p$.

Démonstration. Soit $M \in \mathcal{R}_{\mathbb{Z}}(V)$. Commençons par observer que M est dans $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ si, et seulement si, M_p est dans $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ pour tout p premier, auquel cas on a de plus $\lambda_M = \prod_p \lambda_{M_p}$ (bien entendu, λ_{M_p} vaut 1 pour presque tout p). Cela découle en effet de l'identité $\mathbb{A}_f^\times = \mathbb{Q}^\times \cdot \widehat{\mathbb{Z}}^\times$ (i.e. $\mathrm{h}(\mathbb{G}_m) = 1$) et de la relation immédiate $(N^\sharp)_p = (N_p)^\sharp$, valable pour tout p premier et tout $N \in \mathcal{R}_{\mathbb{Z}}(V)$. En particulier, $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ si, et seulement si, $M_p \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p)$ pour tout p.

Pour conclure la démonstration, il suffit d'observer que si $g \in \widetilde{G}(\mathbb{Q}_p)$ a pour facteur de similitude $\nu(g)$ (§II.1), et si $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$, on a la relation $g(M)^\sharp = \nu(g)^{-1} g(M^\sharp)$. $\square$

Observons que les homothéties $\mathbb{Q}^\times$ agissent sur $\mathcal{R}_\mathbb{Z}(V)$ en préservant $\mathcal{R}^{\mathrm{h}}_\mathbb{Z}(V)$. D'après le lemme ci-dessus, l'ensemble quotient

$$\underline{\mathcal{R}}^{\mathrm{h}}_\mathbb{Z}(V) := \mathbb{Q}^\times \backslash \mathcal{R}^{\mathrm{h}}_\mathbb{Z}(V)$$

est donc muni d'une action de $\mathrm{P}\widetilde{G}(\mathbb{A}_f)$ étendant l'action évidente de $\mathrm{P}\widetilde{G}(\mathbb{Q})$. Nous noterons $\underline{M}$ la classe d'homothétie d'un $M \in \mathcal{R}_\mathbb{Z}(V)$. Nous disposons au final d'un diagramme commutatif :

$$\begin{tikzcd}
\mathcal{R}(G) \arrow[r, hook] \arrow[d, "\omega_1"] & \mathcal{R}(\widetilde{G}) \arrow[r, two heads] \arrow[d, "\omega_2"] & \mathcal{R}(\mathrm{P}\widetilde{G}) \arrow[d, "\omega_3"] \\
\mathcal{R}^{\mathrm{a}}_\mathbb{Z}(V) \arrow[r, hook] \arrow[d, two heads] & \mathcal{R}^{\mathrm{h}}_\mathbb{Z}(V) \arrow[r, two heads] \arrow[d, two heads] & \underline{\mathcal{R}}^{\mathrm{h}}_\mathbb{Z}(V) \arrow[d, two heads] \\
G(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{a}}_\mathbb{Z}(V) \arrow[r, "\xi_1"] & \widetilde{G}(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{h}}_\mathbb{Z}(V) \arrow[r, two heads, "\xi_2"] & \mathrm{P}\widetilde{G}(\mathbb{Q})\backslash\underline{\mathcal{R}}^{\mathrm{h}}_\mathbb{Z}(V)
\end{tikzcd}$$

Les ω_i, pour $i = 1, 2, 3$, sont respectivement les applications "orbite" de L, L, et $\underline{L}$, sous les actions de $G(\mathbb{A}_f)$, $\widetilde{G}(\mathbb{A}_f)$ et $\mathrm{P}\widetilde{G}(\mathbb{A}_f)$. Toutes les autres flèches désignent les applications canoniques.

Proposition 1.4. *Les applications ω_i et ξ_j sont bijectives. En particulier, l'action de $G(\mathbb{A}_f)$ sur $\mathcal{R}^{\mathrm{a}}_\mathbb{Z}(V)$ est transitive, l'orbite de L définissant un isomorphisme de $G(\mathbb{A}_f)$-ensembles $\mathcal{R}(G) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_\mathbb{Z}(V)$.*

Démonstration. L'injectivité des ω_i est évidente. Commençons par vérifier la dernière assertion, qui n'est autre que la surjectivité de ω_1. Si φ est symétrique, le scholie II.2.5 affirme que pour tout $M \in \mathcal{R}^{\mathrm{a}}_\mathbb{Z}(V)$, le q-module M_p sur $\mathbb{Z}_p$ est hyperbolique. Il est en particulier isomorphe à L_p, ce qui conclut car toute isométrie $L_p \to M_p$ est nécessairement induite par un élément de $\mathrm{O}(V_p) = G(\mathbb{Q}_p)$. Supposons donc φ alternée. Il est bien connu que si A est un anneau principal, il existe à équivalence près une et une seule forme bilinéaire alternée non dégénérée sur le A-module A^n (n pair). On conclut en considérant le cas $A = \mathbb{Z}_p$.

La surjectivité de ω_3 (resp. de ω_2) est conséquence de celle de ω_2 (resp. de celles de ω_1 et ξ_1). Montrons la surjectivité de ξ_1. Si $M \in \mathcal{R}^{\mathrm{h}}_\mathbb{Z}(V)$, et $g \in \widetilde{G}(\mathbb{Q})$ a pour facteur de similitude $\nu(g)$, on a $\lambda_{g(M)} = \pm\, \nu(g)^{-1}\, \lambda_M$. Il suffit donc de voir que $\nu(\widetilde{G}(\mathbb{Q}))$ contient l'ensemble $\mathbb{Q}_{>0}$ des rationnels strictement positifs. C'est évident dans le cas alterné, et plus généralement si V est hyperbolique. Dans le cas symétrique, il s'agit de voir que si $\lambda \in \mathbb{Q}_{>0}$ alors V et $V \otimes \langle\lambda\rangle$ (obtenu en multipliant la forme quadratique sur V par λ) sont isomorphes

en tant que q-modules sur $\mathbb{Q}$. Mais ils le sont sur $\mathbb{Q}_p$ pour tout premier p, les $V \otimes \mathbb{Q}_p$ étant hyperboliques d'après le scholie II.2.5. Ils le sont sur $\mathbb{R}$ car $\lambda > 0$. On conclut par le théorème de Hasse-Minkowski.

L'application ξ_2 est bijective car $\mathrm{P}\widetilde{G}(\mathbb{Q}) = \widetilde{G}(\mathbb{Q})/\mathbb{Q}^\times$. Vérifions enfin l'injectivité de ξ_1. On peut supposer φ symétrique, car l'argument du premier paragraphe montre que $h(G) = 1$ si φ est alternée. Supposons donc qu'il existe $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ et $g \in \widetilde{G}(\mathbb{Q})$ tels que $g(M) = L$. On en déduit $\nu(g) = \pm 1$. Si $\nu(g) = 1$ alors $g \in G(\mathbb{Q})$: on a terminé. Sinon, M est isométrique au q-module $L \otimes \langle -1 \rangle$, d'espace sous-jacent L mais de forme quadratique opposée. Cela entraîne que $V \otimes \mathbb{R}$ est hyperbolique, puis que L et M sont isomorphes d'après le théorème II.2.7. $\square$

Corollaire 1.5. $\mathrm{h}(G) = \mathrm{h}(\widetilde{G}) = \mathrm{h}(\mathrm{P}\widetilde{G})$.

Quand φ est alternée, la classification sus-mentionnée des formes alternées non dégénérées appliquée à l'anneau $\mathbb{Z}$ entraîne[1] $\mathrm{h}(G) = 1$, puis $\mathrm{h}(\mathrm{Sp}_{2g}) = \mathrm{h}(\mathrm{GSp}_{2g}) = \mathrm{h}(\mathrm{PGSp}_{2g}) = 1$ pour tout $g \geq 1$.

Supposons φ symétrique. Si le q-module $L \otimes \mathbb{R}$ n'est pas défini, il résulte de même du théorème II.2.7 que $\mathrm{h}(\mathrm{O}_L) = 1$. La situation est bien différente si $L \otimes \mathbb{R}$ est défini positif, ce que l'on suppose désormais. Rappelons que L peut alors être vu comme un réseau unimodulaire pair de l'espace euclidien $V \otimes \mathbb{R}$ de dimension n. En particulier $n \equiv 0 \bmod 8$. Dans ce cas, $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ est par définition l'ensemble des réseaux unimodulaires pairs de $V \otimes \mathbb{R}$ qui sont inclus dans $L \otimes \mathbb{Q}$. Rappelons que X_n désigne l'ensemble des classes d'isométrie de réseaux unimodulaires pairs de l'espace euclidien $V \otimes \mathbb{R}$. D'après le scholie II.2.1, l'inclusion naturelle $\mathrm{O}(V)\backslash\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \to \mathrm{X}_n$ est bijective, et induit donc un isomorphisme $\mathrm{Cl}(\mathrm{O}_L) \xrightarrow{\sim} \mathrm{X}_n$. En particulier, si O_n désigne le $\mathbb{Z}$-groupe orthogonal du réseau $L = \mathrm{E}_n$ (§I.3), on obtient l'égalité

$$\mathrm{h}(\mathrm{O}_n) = |\mathrm{X}_n|,$$

qui montre que $\mathrm{h}(\mathrm{O}_n)$ est un nombre tout à fait intéressant.

1. Les assertions $\mathrm{h}(\mathrm{SL}_n) = \mathrm{h}(\mathrm{Sp}_{2g}) = 1$ rappelées ci-dessus sont également des cas très particuliers du théorème d'approximation forte de Kneser (voir [Kn66] [PR94, Thm. 7.12]). Il affirme que $\mathrm{h}(G) = 1$ dès que le $\mathbb{C}$-groupe $G_{\mathbb{C}}$ est semi-simple, simplement connexe, et que le groupe topologique $G(\mathbb{R})$ n'a pas de sous-groupe distingué compact connexe non trivial.

1.6. SO_L versus O_L

On poursuit l'étude du paragraphe précédent en supposant φ symétrique, de sorte que $G, \widetilde{G}$ et $\mathrm{P}\widetilde{G}$ sont respectivement O_L, GO_L et PGO_L. On s'intéresse à leurs sous-$\mathbb{Z}$-groupes respectifs SO_L, GSO_L et PGSO_L (§II.1). Les groupes $\mathrm{SO}_L(\mathbb{A}_f)$, $\mathrm{GSO}_L(\mathbb{A}_f)$ et $\mathrm{PGSO}_L(\mathbb{A}_f)$ agissent respectivement sur $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ et $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V)$ (Proposition 1.3). Considérons le diagramme commutatif suivant, étendant celui du §1.2.

$$\begin{tikzcd}
 & \mathcal{R}(\mathrm{SO}_L) \arrow[rr] \arrow[dl, "\mu_1"'] \arrow[dd, "\widetilde{\omega}_1"] & & \mathcal{R}(\mathrm{GSO}_L) \arrow[rr] \arrow[dl, "\mu_2"'] \arrow[dd, "\widetilde{\omega}_2"] & & \mathcal{R}(\mathrm{PGSO}_L) \arrow[dl, "\mu_3"'] \arrow[dd, "\widetilde{\omega}_3"] \\
\mathcal{R}(\mathrm{O}_L) \arrow[rr] \arrow[dd, "\omega_1"] & & \mathcal{R}(\mathrm{GO}_L) \arrow[rr] \arrow[dd, "\omega_2"] & & \mathcal{R}(\mathrm{PGO}_L) \arrow[dd, "\omega_3"] & \\
 & \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \arrow[rr, hook] \arrow[dl, "\mathrm{Id}"'] \arrow[dd] & & \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[rr] \arrow[dl, "\mathrm{Id}"'] \arrow[dd] & & \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[dl, "\mathrm{Id}"'] \arrow[dd] \\
\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \arrow[rr] \arrow[dd] & & \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[rr] \arrow[dd] & & \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[dd] & \\
 & \mathrm{SO}_L(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \arrow[rr, "\widetilde{\xi}_1"'] \arrow[dl] & & \mathrm{GSO}_L(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[rr, "\widetilde{\xi}_2"'] \arrow[dl] & & \mathrm{PGSO}_L(\mathbb{Q})\backslash\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[dl] \\
\mathrm{O}_L(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \arrow[rr, "\xi_1"'] & & \mathrm{GO}_L(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) \arrow[rr, "\xi_2"'] & & \mathrm{PGO}_L(\mathbb{Q})\backslash\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) &
\end{tikzcd}$$

Les applications verticales $\widetilde{\omega}_i$ sont encore les applications "orbites" de L (resp. L, resp. $\underline{L}$) et les autres flèches sont les applications canoniques.

Proposition 1.7. *Les applications $\widetilde{\omega}_i$, μ_i et $\widetilde{\xi}_j$ sont bijectives. En particulier, l'action de $\mathrm{SO}_L(\mathbb{A}_f)$ sur $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ est encore transitive, l'orbite de L définissant un isomorphisme $\mathcal{R}(\mathrm{SO}_L) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$.*

Démonstration. Nous avons déjà vu que l'action naturelle de $\mathrm{O}_L(\mathbb{A}_f)$ sur $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ est transitive (Proposition 1.4). Il en va de même de la restriction de cette action à son sous-groupe $\mathrm{SO}_L(\mathbb{A}_f)$ car le groupe orthogonal d'un q-module hyperbolique non trivial sur $\mathbb{Z}_p$ contient toujours un élément de déterminant -1. Cette même raison montre que les μ_i sont bijectifs, car $\mathrm{O}_L(\mathbb{Z}_p)/\mathrm{SO}_L(\mathbb{Z}_p) \to \mathrm{GO}_L(\mathbb{Q}_p)/\mathrm{GSO}_L(\mathbb{Q}_p)$ est bijective pour tout premier p (§II.1). Les ω_i étant bijectifs, on en déduit la bijectivité des $\widetilde{\omega}_i$.

La bijectivité de $\widetilde{\xi}_2$ est évidente. La surjectivité de $\widetilde{\xi}_1$ se déduit de celle de ξ_1 et de ce que $-1 \in \mathrm{dét}(\mathrm{O}(V))$. Enfin, l'injectivité de $\widetilde{\xi}_1$ se démontre de manière similaire à celle de ξ_1 (Proposition 1.4), en utilisant que $-1 \in \mathrm{dét}(\mathrm{O}(\mathrm{H}(\mathbb{Z}^{n/2})))$. $\square$

Corollaire 1.8. *Si L est un* q*-module sur $\mathbb{Z}$, on a* $\mathrm{h}(\mathrm{SO}_L) = \mathrm{h}(\mathrm{GSO}_L) = \mathrm{h}(\mathrm{PGSO}_L)$. *Si de plus $L \otimes \mathbb{R}$ est indéfini, ces entiers sont égaux à* 1.

Démonstration. La première assertion est conséquence de la bijectivité des applications ξ_i (Proposition 1.7). Quand $L \otimes \mathbb{R}$ n'est pas défini, nous avons déjà expliqué au §1.2 l'égalité $\mathrm{h}(\mathrm{O}_L) = 1$. Il reste à voir qu'il existe $s \in \mathrm{O}(L)$ tel que $\operatorname{dét} s = -1$. L'hypothèse sur L et le théorème II.2.7 montrent qu'il existe un q-module sur $\mathbb{Z}$, disons L', tel que $L \simeq L' \oplus \mathrm{H}(\mathbb{Z})$ (somme orthogonale). On conclut car $\mathrm{H}(\mathbb{Z})$ contient un automorphisme de déterminant -1. □

Supposons finalement L défini positif. On dispose alors comme précédemment d'une bijection canonique $\mathrm{Cl}(\mathrm{SO}_L) \xrightarrow{\sim} \widetilde{\mathrm{X}}_n$, où $\widetilde{\mathrm{X}}_n$ désigne l'ensemble des classes d'isométries *directes* de réseaux unimodulaires pairs de $V \otimes \mathbb{R}$ (autrement dit, l'ensemble des orbites de l'action de $\mathrm{SO}(V \otimes \mathbb{R})$ sur ces derniers). La classe d'isométrie d'un réseau unimodulaire pair $M \subset V \otimes \mathbb{R}$ admet exactement 1 ou 2 antécédents par la projection canonique

$$\widetilde{\mathrm{X}}_n \to \mathrm{X}_n$$

selon que $\mathrm{O}(M)$ possède un élément de déterminant -1 ou non. C'est par exemple le cas si M possède au moins une racine, c'est-à-dire un $\alpha \in M$ tel que $\alpha \cdot \alpha = 2$, car la symétrie orthogonale associée est dans $\mathrm{O}(M)$ (§II.3). En revanche, si M est le réseau de Leech alors $\mathrm{O}(M) = \mathrm{SO}(M)$ d'après Conway [Co69a]. Les rappels du §II.3 entraînent le corollaire suivant. Pour $n \equiv 0 \bmod 8$, on pose $\mathrm{SO}_n = \mathrm{SO}_{\mathrm{E}_n}$.

Corollaire 1.9. *On a* $\mathrm{h}(\mathrm{SO}_8) = 1$, $\mathrm{h}(\mathrm{SO}_{16}) = 2$ *et* $\mathrm{h}(\mathrm{SO}_{24}) = 25$.

1.10. Groupes orthogonaux en dimension impaire

On se place encore dans le cadre du §1.2, en supposant φ symétrique. On considère plutôt l'ensemble

$$\mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V) \subset \mathcal{R}_{\mathbb{Z}}(V)$$

constitué des $L \in \mathcal{R}_{\mathbb{Z}}(V)$ tels que $\varphi(x, x) \in 2\mathbb{Z}$ pour tout $x \in L$ et tels que $L^\sharp/L \simeq \mathbb{Z}/2\mathbb{Z}$. Cette dernière condition équivaut à demander que $\varphi_{|L \times L}$ est de déterminant ± 2. Nous renvoyons à l'appendice B pour une étude de ces réseaux.

Fixons $L \in \mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$, ce qui nécessite que la dimension n de V soit impaire. Alors $\mathrm{SO}_L(\mathbb{A}_f)$ agit transitivement sur $\mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$ d'après la proposition B.2.5,

le stabilisateur de L étant $\mathrm{SO}_L(\widehat{\mathbb{Z}})$. Si $L \otimes \mathbb{R}$ n'est pas défini, le nombre de classes de SO_L est 1 : c'est un résultat classique qu'il ne serait pas difficile de déduire de la proposition B.2.5 (iii) et du théorème II.2.7. La situation est plus intéressante si $L \otimes \mathbb{R}$ est défini, disons positif pour fixer les idées, ce que l'on suppose désormais.

Dans ce cas, on a la congruence $n \equiv \pm 1 \bmod 8$ et $\mathrm{Cl}(\mathrm{SO}_L)$ s'identifie à l'ensemble des classes d'isométrie de réseaux pairs et de déterminant 2 dans $\mathbb{R}^n$ (§B.2). Il n'y a pas lieu ici de distinguer isométries directes et indirectes car $x \mapsto -x$ est dans $\mathrm{O}(M)$ et de déterminant -1 pour tout $M \in \mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$. Si $n \equiv 1 \bmod 8$, on pose $\mathrm{L}_n = \mathrm{E}_{n-1} \oplus \mathrm{A}_1$. Si $n \equiv -1 \bmod 8$, on note L_n l'orthogonal d'une racine quelconque de E_{n+1} ; ces racines étant permutées transitivement par le groupe orthogonal de E_{n+1}, la classe d'isométrie d'un tel réseau ne dépend d'aucun choix. Si $n \equiv \pm 1 \bmod 8$ le réseau L_n est donc pair de déterminant 2 (§B.2), et l'on pose $\mathrm{SO}_n = \mathrm{SO}_{\mathrm{L}_n}$ (§B.1).

Les valeurs connues de $\mathrm{h}(\mathrm{SO}_n)$ avec n impair sont rassemblées dans le corollaire qui suit (voir aussi [CS99]). Les cas $n \leq 23$ sont traités en exemple dans l'appendice B.2 ; le cas $n = 25$ est dû à Borcherds [Bor84, Table -2].

Corollaire 1.11. *On a* $\mathrm{h}(\mathrm{SO}_1) = \mathrm{h}(\mathrm{SO}_7) = \mathrm{h}(\mathrm{SO}_9) = 1$, $\mathrm{h}(\mathrm{SO}_{15}) = 2$, $\mathrm{h}(\mathrm{SO}_{17}) = 4$, $\mathrm{h}(\mathrm{SO}_{23}) = 32$ *et* $\mathrm{h}(\mathrm{SO}_{25}) = 121$.

2. Correspondances de Hecke

2.1. Formalisme général

Soit Γ un groupe (abstrait) et soit X un Γ-ensemble transitif. L'anneau des *correspondances (ou opérateurs) de Hecke* de X est l'anneau

$$\mathrm{H}(X) = \mathrm{End}_{\mathbb{Z}[\Gamma]}(\mathbb{Z}[X]).$$

À chaque $T \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$ est associé une matrice à coefficients entiers $(T_{x,y})_{(x,y)\in X\times X}$, qui le détermine uniquement, définie par la formule

$$\forall y \in X, \quad T(y) = \sum_{x\in X} T_{x,y}\ x.$$

Par définition, un tel élément T est dans $\mathrm{H}(X)$ si et seulement si la fonction $X \times X \to \mathbb{Z}, (x, y) \mapsto T_{x,y}$, est constante sur les orbites du groupe Γ opérant diagonalement sur $X \times X$. La fonction $\Gamma\backslash(X \times X) \to \mathbb{Z}$ qui en résulte est alors à support fini, par finitude de $\{x \in X, T_{x,y} \neq 0\}$ pour $y \in X$ et par transitivité de X. Nous disposons donc d'une application injective

$$\mathrm{H}(X) \to \mathrm{Hom}_{\mathrm{sf}}(\Gamma\backslash(X \times X), \mathbb{Z}), \qquad T \mapsto ((x, y) \mapsto T_{x,y}), \tag{2.1}$$

$\mathrm{Hom}_{\mathrm{sf}}(Y, \mathbb{Z})$ désignant le groupe abélien des fonctions à support fini sur l'ensemble Y, et à valeurs dans $\mathbb{Z}$.

Si $x \in X$ on note $\Gamma_x \subset \Gamma$ le stabilisateur de x. On suppose que les propriétés équivalentes suivantes sont satisfaites :

(i) Pour toute orbite Ω de Γ dans $X \times X$, et pour tout $x \in X$, l'intersection $\Omega \cap (X \times \{x\})$ est finie.

(ii) Pour tout $x \in X$, les orbites de Γ_x sur X sont finies. Autrement dit, pour tout $x, y \in X$, l'intersection $\Gamma_x \cap \Gamma_y$ est d'indice fini dans Γ_x.

Ces conditions assurent que l'application (2.1) est bijective. En particulier, $\mathrm{H}(X)$ est un $\mathbb{Z}$-module libre ayant pour base naturelle les fonctions caractéristiques des orbites de Γ sur $X \times X$.

Fixons $x \in X$. La transitivité de X assure que l'application $\Gamma \to X \times X, \gamma \mapsto (\gamma(x), x)$, induit des bijections

$$\Gamma_x \backslash \Gamma / \Gamma_x \xrightarrow{\sim} \Gamma_x \backslash (X \times \{x\}) \xrightarrow{\sim} \Gamma \backslash (X \times X). \tag{2.2}$$

Cela identifie en particulier $\mathrm{H}(X)$ à $\mathrm{Hom}_{\mathrm{sf}}(\Gamma_x \backslash \Gamma / \Gamma_x, \mathbb{Z})$. Par transport de structure, ce dernier hérite de $\mathrm{H}(X)$ une structure d'anneau : on retombe sur les présentations plus standards des anneaux de Hecke, comme par exemple dans [Sat63], [Shi71, §3], [Car79], [Fre83, Kap. IV] ou [Gro98]. On prendra garde que suivant les références, la structure d'anneau considérée sur $\mathrm{Hom}_{\mathrm{sf}}(\Gamma_x \backslash \Gamma / \Gamma_x, \mathbb{Z})$ (définie en général par un produit de convolution explicite) peut légèrement différer de la nôtre : c'est notamment le cas des articles de Cartier et Gross, auxquels nous réfèrerons au §VI.2, pour lesquels l'anneau $\mathrm{H}(X)$ est précisément l'anneau opposé du nôtre.

Observons que la seconde formulation de la condition (ii) étant symétrique en x, y, la condition (i) équivaut encore à demander que pour toute orbite Ω de Γ dans $X \times X$, et pour tout $x \in X$, l'intersection $\Omega \cap (\{x\} \times X)$ est finie. Ainsi, si $T \in \mathrm{H}(X)$, il existe un unique $T^{\mathrm{t}} \in \mathrm{H}(X)$ tel que $T^{\mathrm{t}}_{x,y} = T_{y,x}$ pour tout $x, y \in X$. L'endomorphisme

$$T \mapsto T^{\mathrm{t}}$$

de $\mathrm{H}(X)$ est une anti-involution, i.e. satisfait $(ST)^{\mathrm{t}} = T^{\mathrm{t}} S^{\mathrm{t}}$ et $(T^{\mathrm{t}})^{\mathrm{t}} = T$ pour tout $S, T \in \mathrm{H}(X)$, qui correspond simplement à la transposée sur les matrices associées. Observons que cette anti-involution est l'identité si, et seulement si, les Γ-orbites de $X \times X$ sont invariantes par $(x, y) \mapsto (y, x)$, auquel cas $\mathrm{H}(X)$ est commutative : c'est un cas particulier du critère de Gelfand.

2.2. Le foncteur des Γ-modules vers les $\mathrm{H}(X)^{\mathrm{opp}}$-modules

Soit X un Γ-ensemble transitif satisfaisant les conditions (i) et (ii) du §2.1. L'anneau $\mathrm{H}(X)$ intervient de la manière suivante dans la théorie des représentations de Γ. Si M est un $\mathbb{Z}[\Gamma]$-module, alors le groupe abélien

$$M_X = \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathbb{Z}[X], M)$$

hérite d'une action <u>à droite</u> de $\mathrm{H}(X)$ par composition à la source. Il est évident que $M \mapsto M_X$ est un foncteur des Γ-modules (à gauche) vers les $\mathrm{H}(X)$-modules à droite.

Si M est un $\mathbb{Z}[\Gamma]$-module, et si $x \in X$, l'application $\varphi \mapsto \varphi(x)$ identifie M_X au sous-groupe des invariants $M^{\Gamma_x} \subset M$, ce qui munit également ce sous-groupe d'une structure de $\mathrm{H}(X)$-module. Supposons que $T \in \mathrm{H}(X)$ a pour matrice la fonction caractéristique de la double classe $\Gamma_x \gamma \Gamma_x$ via l'identification $\Gamma_x \backslash \Gamma / \Gamma_x \xrightarrow{\sim} \Gamma \backslash (X \times X)$ choisie au §2.1. On a la formule classique

$$T(m) = \sum_i \gamma_i(m)\,, \quad \forall m \in M^{\Gamma_x}, \tag{2.3}$$

pour toute décomposition $\Gamma_x \gamma \Gamma_x = \coprod_i \gamma_i \Gamma_x$ (réunion finie).

Dans ce contexte, l'anti-involution $T \mapsto T^{\mathrm{t}}$ définie au §2.1 prend le sens suivant. Soient M, M' deux $\mathbb{Z}[\Gamma]$-modules, N un groupe abélien, et $(-|-)$: $M \times M' \to N$ une application bilinéaire telle que $(\gamma m|\gamma m') = (m|m')$ pour tout $\gamma \in \Gamma$ et tout $(m, m') \in M \times M'$. Observons que si $(\varphi, \varphi') \in M_X \times M'_X$, alors

$$(\varphi, \varphi') := (\varphi(x)|\varphi'(x))$$

ne dépend pas du choix de $x \in X$, et définit une application bilinéaire $M_X \times M'_X \to N$. Si l'on identifie M_X à M^{Γ_x} comme plus haut, cette application bilinéaire n'est autre que la restriction de $(-|-)$ à $M^{\Gamma_x} \times M'^{\Gamma_x}$.

On dira que X est *symétrique* s'il vérifie, en plus des conditions (i) et (ii) du §2.1, les propriétés équivalentes suivantes [2] :

(iii) Pour toute orbite Ω de Γ dans $X \times X$, et pour tout $x \in X$, alors $|\Omega \cap (X \times \{x\})| = |\Omega \cap (\{x\} \times X)|$.

(iv) Pour tout $x, y \in X$, $\Gamma_x \cap \Gamma_y$ a même indice dans Γ_x et Γ_y.

2. Cette propriété n'est pas automatique si X est infini. On pourra par exemple considérer le groupe $\Gamma = \mathbb{Q} \rtimes \mathbb{Q}^\times$ des transformations affines de $\mathbb{Q}$, et le Γ-ensemble X constitué des parties de $\mathbb{Q}$ de la forme $a\mathbb{Z} + b$ avec $a \in \mathbb{Q}^\times$ et $b \in \mathbb{Q}$.

Lemme 2.3. *Supposons X symétrique. Si $T \in \mathrm{H}(X)$, et si $(\varphi, \varphi') \in M_X \times M'_X$, alors $(T(\varphi), \varphi') = (\varphi, T^{\mathrm{t}}(\varphi'))$.*

Démonstration. Soit $\psi : X \times X \to N$ une application constante sur chaque Γ-orbite dans $X \times X$, et nulle hors d'un nombre fini d'entre elles. La propriété de symétrie de X entraîne, pour tout $x \in X$, la relation $\sum_{y \in X} \psi(y, x) = \sum_{y \in X} \psi(x, y)$. On applique ceci à la fonction $(x, y) \mapsto T_{x,y} \cdot (\varphi(x) | \varphi'(y))$. $\square$

Remarque 2.4. Supposons que V est un $\mathrm{H}(X)$-module à droite. L'application $\mathrm{H}(X) \times V \to V$, $(T, v) \mapsto T^{\mathrm{t}}\, v$, définit une structure de $\mathrm{H}(X)$-module (à gauche) sur V, que l'on notera V^{t}.

2.5. L'anneau de Hecke d'un $\mathbb{Z}$-groupe

Soit maintenant G un $\mathbb{Z}$-groupe. Nous allons appliquer les définitions précédentes à $\Gamma = G(\mathbb{A}_f)$ et $X = \mathcal{R}(G)$. *L'anneau de Hecke de G* est l'anneau

$$\mathrm{H}(G) := \mathrm{H}(\mathcal{R}(G)).$$

Rappelons que pour tout premier p, le groupe $G(\mathbb{Q}_p)$ hérite de $\mathbb{Q}_p$ une structure de groupe topologique localement compact (séparé, réunion dénombrable de compacts), le sous-groupe $G(\mathbb{Z}_p)$ étant à la fois compact et ouvert. Le groupe $G(\mathbb{A}_f)$ est également un groupe topologique localement compact pour la topologie ayant pour base de voisinages de l'unité les ouverts de la forme $\prod_{p \in \mathrm{P}} U_p$ où chaque U_p pour p premier est un voisinage ouvert de l'unité dans $G(\mathbb{Q}_p)$, tel que $U_p = G(\mathbb{Z}_p)$ pour presque tout p. En particulier, $G(\widehat{\mathbb{Z}})$ est un sous-groupe ouvert compact de $G(\mathbb{A}_f)$. Cela entraîne que $\mathcal{R}(G)$ satisfait la propriété (ii) du §2.1, ainsi que les $G(\mathbb{Q}_p)$-ensembles

$$\mathcal{R}_p(G) := G(\mathbb{Q}_p)/G(\mathbb{Z}_p).$$

Le $G(\mathbb{A}_f)$-ensemble $\mathcal{R}(G)$, ainsi que les $\mathcal{R}_p(G)$, sont symétriques au sens du §2.2 si $G(\mathbb{A}_f)$ est unimodulaire, ce qui est notamment le cas si la composante neutre de $G(\mathbb{C})$ est réductive [Bor63, §5.5].

Si p est premier, on définit également $\mathrm{H}_p(G)$ comme l'anneau de Hecke du $G(\mathbb{Q}_p)$-ensemble $\mathcal{R}_p(G)$. Observons que le $G(\mathbb{A}_f)$-ensemble $\mathcal{R}(G)$ s'identifie canoniquement au sous-ensemble de $\prod_{p \in \mathrm{P}} \mathcal{R}_p(G)$ constitué des (x_p) tels que $x_p = G(\mathbb{Z}_p)$ pour presque tout p. Nous avons déjà vu une manifestation de ce fait dans le plongement d'Eichler (1.1). On dispose en particulier, pour chaque premier p, d'un homomorphisme d'anneaux injectif canonique

$$\mathrm{H}_p(G) \to \mathrm{H}(G)$$

associant à un $T \in \mathrm{H}_p(G)$ l'endomorphisme de $\mathbb{Z}[\mathcal{R}(G)]$ envoyant $y = (y_\ell)_{\ell \in \mathrm{P}}$ sur $\sum_x T_{x_p, y_p}\, x$, où x parcourt les éléments de $\mathcal{R}(G)$ tels que $x_\ell = y_\ell$ dans $\mathcal{R}_\ell(G)$ pour tout $\ell \neq p$. On écrira simplement

$$\mathrm{H}_p(G) \subset \mathrm{H}(G).$$

Si $p \neq q$, $S \in \mathrm{H}_p(G)$ et $T \in \mathrm{H}_q(G)$ alors $TS = ST$.

Si l'on se donne pour tout premier p une $G(\mathbb{Q}_p)$-orbite $\Omega_p \subset \mathcal{R}_p(G) \times \mathcal{R}_p(G)$, et si de plus Ω_p est l'orbite de $G(\mathbb{Z}_p) \times G(\mathbb{Z}_p)$ pour presque tout p, alors le sous-ensemble des éléments (ω_p) de $\prod_p \Omega_p$ tels que $\omega_p = G(\mathbb{Z}_p) \times G(\mathbb{Z}_p)$ pour presque tout p s'identifie naturellement à une $G(\mathbb{A}_f)$-orbite dans $\mathcal{R}(G) \times \mathcal{R}(G)$. Réciproquement, toute $G(\mathbb{A}_f)$-orbite $\Omega \subset \mathcal{R}(G) \times \mathcal{R}(G)$ est de cette forme, et ce pour une unique famille (Ω_p), la $G(\mathbb{Q}_p)$-orbite Ω_p étant l'image de Ω par la projection canonique $\mathcal{R}(G) \times \mathcal{R}(G) \to \mathcal{R}_p(G) \times \mathcal{R}_p(G)$. Il resulte de ces observations et de la bijectivité de l'application (2.1) que $\mathrm{H}(G)$ est isomorphe au produit tensoriel de ses sous-anneaux $\mathrm{H}_p(G)$:

$$\bigotimes_{p \in \mathrm{P}} \mathrm{H}_p(G) \xrightarrow{\sim} \mathrm{H}(G).$$

La compréhension de $\mathrm{H}(G)$ se ramène donc entièrement à celle des $\mathrm{H}_p(G)$.

L'anneau $\mathrm{H}_p(G)$ ne dépend que du $\mathbb{Z}_p$-groupe $G_{\mathbb{Z}_p} = G \times_{\mathbb{Z}} \mathbb{Z}_p$. Lorsque $G_{\mathbb{Z}_p}$ est réductif, les résultats généraux de Satake et Bruhat-Tits entraînent que $\mathrm{H}_p(G)$ est commutative : nous y reviendrons au §VI.2. Il en va donc de même de $\mathrm{H}(G)$ si G est réductif sur $\mathbb{Z}$. Cette propriété est toutefois élémentaire dans les cas les plus classiques, que nous allons rappeler ci-dessous.

2.6. Quelques anneaux de Hecke classiques

Supposons d'abord $G = \mathrm{PGL}_n$. Nous avons vu que $\mathcal{R}(G)$ s'identifie à

$$\underline{\mathcal{R}}_{\mathbb{Z}}(V) := \mathbb{Q}^\times \backslash \mathcal{R}_{\mathbb{Z}}(V)$$

où $V = \mathbb{Q}^n$. Rappelons que $\underline{M} \in \underline{\mathcal{R}}_{\mathbb{Z}}(V)$ désigne la classe d'homothétie d'un réseau $M \in \mathcal{R}_{\mathbb{Z}}(V)$.

Si $M, N \in \mathcal{R}_{\mathbb{Z}}(V)$, il existe un plus petit entier $d \geq 1$ tel que $dN \subset M$. La classe d'isomorphisme du groupe abélien M/dN ne dépend que de la $G(\mathbb{A}_f)$-orbite de $(\underline{N}, \underline{M})$ dans $\underline{\mathcal{R}}_{\mathbb{Z}}(V) \times \underline{\mathcal{R}}_{\mathbb{Z}}(V)$. La théorie des diviseurs élémentaires montre alors que l'application ainsi définie

$$G(\mathbb{A}_f) \backslash (\underline{\mathcal{R}}_{\mathbb{Z}}(V) \times \underline{\mathcal{R}}_{\mathbb{Z}}(V)) \to \mathrm{AF},$$

AF désignant l'ensemble des classes d'isomorphisme de groupes abéliens finis, est une injection dont l'image est constituée des groupes engendrés par $n-1$ éléments. Si A est un tel groupe, l'opérateur de Hecke associé $\mathrm{T}_A \in \mathrm{H}(G)$ vérifie par définition

$$\mathrm{T}_A(\underline{M}) = \sum_N \underline{N},$$

où N parcourt les sous-groupes de M tels que $M/N \simeq A$. Ces opérateurs T_A, avec A parcourant les groupes abéliens finis engendrés par $n-1$ éléments, forment donc une $\mathbb{Z}$-base de $\mathrm{H}(G)$. Il est clair que $\mathrm{T}_{A\times B} = \mathrm{T}_A\mathrm{T}_B$ si $|A|$ et $|B|$ sont premiers entre eux, et que $\mathrm{T}_A \in \mathrm{H}_p(G)$ si, et seulement si, A est un p-groupe.

Si $n = 2$, on vérifie aisément que $\mathrm{T}_A^{\mathrm{t}} = \mathrm{T}_A$ pour tout A, en particulier $\mathrm{H}(G)$ est commutative (la notation T^{t} est définie au §2.1). Le premier point ne vaut plus pour $n > 2$, mais $\mathrm{H}(G)$ reste commutative. On peut le voir simplement en munissant V d'une forme bilinéaire symétrique non dégénérée. L'application $\underline{M} \mapsto \underline{M^\sharp}$ est une involution de $\underline{\mathcal{R}}_{\mathbb{Z}}(V)$. Elle induit une involution linéaire de $\mathbb{Z}[\,\underline{\mathcal{R}}_{\mathbb{Z}}(V)\,]$, puis par conjugaison une involution ι de $\mathrm{H}(G)$, qui n'est autre que $(T_{\underline{N},\underline{M}}) \mapsto (T_{\underline{N^\sharp},\underline{M^\sharp}})$ sur les matrices associées. Mais si $N \subset M$ alors $N^\sharp/M^\sharp$ est en dualité parfaite avec M/N, et donc ι coïncide avec l'anti-involution canonique de $\mathrm{H}(G)$: $\iota(T) = T^{\mathrm{t}}$ pour tout $T \in \mathrm{H}(G)$ (voir aussi [Shi71, §3]).

Discutons maintenant le cas particulièrement important pour ce mémoire des $\mathbb{Z}$-groupes orthogonaux et symplectiques [Sat63] [Fre83] [And87]. On reprend les notations du §1.2, en particulier $V = L \otimes \mathbb{Q}$ est de dimension n paire, φ est une forme bilinéaire sur V qui est symétrique (resp. alternée), pour laquelle L est autodual pair, et $G \subset \mathrm{GL}_L$ est le groupe O_L (resp. Sp_L).

Dans ce cas nous avons vu que $\mathcal{R}(G)$ s'identifie au $G(\mathbb{A}_f)$-ensemble $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ des réseaux autoduaux de V (Proposition 1.4). Si $(N, M) \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, la classe d'isomorphisme du groupe abélien $M/(N \cap M)$ ne dépend que de la $G(\mathbb{A}_f)$-orbite de (N, M). On a donc défini une application naturelle

$$G(\mathbb{A}_f)\backslash(\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)) \to \mathrm{AF}, \quad (N, M) \mapsto M/(N \cap M). \tag{2.4}$$

Proposition 2.7. *L'application* (2.4) *est une injection dont l'image est constituée des groupes engendrés par $n/2$ éléments.*

Cette proposition est bien connue, nous en redonnerons une démonstration à la fin de ce paragraphe pour le confort du lecteur. Soit A un groupe abélien fini engendré par au plus $n/2$ éléments. Il lui est donc associé un opérateur de Hecke

$$\mathrm{T}_A \in \mathrm{H}(G)$$

défini par $\mathrm{T}_A(M) = \sum_N N$, la somme portant sur les N tels que $M/(N \cap M) \simeq A$, soit encore sur les A-voisins de M au sens de la définition III.1.2 dans le cas quadratique. Ces opérateurs T_A forment donc une $\mathbb{Z}$-base de $\mathrm{H}(G)$. On a bien sûr encore $\mathrm{T}_{A\times B} = \mathrm{T}_A\mathrm{T}_B$ si $|A|$ et $|B|$ sont premiers entre eux, et $\mathrm{T}_A \in \mathrm{H}_p(G)$ si, et seulement si, A est un p-groupe. Du point de vue du chapitre III, un opérateur tout particulièrement important pour nous est l'opérateur $\mathrm{T}_{\mathbb{Z}/d\mathbb{Z}}$ pour $d \geq 1$, que l'on note également simplement T_d.

Proposition 2.8. *Soit A un groupe abélien fini engendré par $n/2$ éléments. Alors $\mathrm{T}_A^{\mathrm{t}} = \mathrm{T}_{A^\vee} = \mathrm{T}_A$. En particulier, l'anneau $\mathrm{H}(G)$ est commutatif.*

Démonstration. En effet, la première assertion est conséquence du scholie-définition III.1.2 quand φ est symétrique, et de manière similaire dans le cas alterné. La seconde se déduit de la première d'après la fin du paragraphe 2.1. Voir également [Sat63, Ch. III], [Fre83, Kap. IV] et le §V.2.8. □

Discutons enfin du groupe des similitudes projectives $\mathrm{P}\widetilde{G}$. Soient p un nombre premier et $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ l'ensemble des réseaux homoduaux pairs de V_p, introduit après l'énoncé du lemme 1.3. Si φ est symétrique (resp. alternée), on rappelle qu'un réseau $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$ est homodual si et seulement s'il existe $\lambda_M \in p^{\mathbb{Z}}$, nécessairement unique, tel que $x \mapsto \lambda_M \frac{\varphi(x,x)}{2}$ (resp. $\lambda_M\varphi$) munisse M d'une structure de q-module (resp. a-module) sur $\mathbb{Z}_p$. Comme le q-module V_p est hyperbolique d'après le scholie II.2.5, il en va de même de $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ en tant que q-module sur $\mathbb{Z}_p$ d'après la proposition II.1.2. Cela montre que l'application $g \mapsto g(L)$ induit des isomorphismes $\mathcal{R}_p(\widetilde{G}) \xrightarrow{\sim} \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ et $\mathcal{R}_p(G) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p)$. En particulier, l'ensemble $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) := \mathbb{Q}_p^\times\backslash\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ s'identifie naturellement à $\mathcal{R}_p(\mathrm{P}\widetilde{G})$.

Soit $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$. On note $\mathrm{v}_M \in \mathbb{Z}$ l'unique élément tel que $\lambda_M = p^{-\mathrm{v}_M}$. Si $g \in \widetilde{G}(\mathbb{Q}_p)$, alors $\mathrm{v}_{g(M)} = \mathrm{v}_M + v$ où v est la valuation p-adique de $\nu(g)$. Soit $(\underline{N}, \underline{M})$ un couple d'éléments de $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$. Quitte à changer de représentant N, on peut supposer $\mathrm{v}_M - \mathrm{v}_N \in \{0,1\}$. Le couple $(M/N\cap M, \mathrm{v}_M - \mathrm{v}_N)$ ne dépend alors que de la $\mathrm{P}\widetilde{G}(\mathbb{Q}_p)$-orbite de $(\underline{N}, \underline{M})$, ce qui définit une application

$$\mathrm{P}\widetilde{G}(\mathbb{Q}_p)\backslash(\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) \times \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)) \to \mathrm{AF} \times \{0,1\}. \tag{2.5}$$

Proposition 2.9. *L'application* (2.5) *est une injection d'image l'ensemble des couples $(A, -)$ où A est un p-groupe abélien engendré par $n/2$ éléments.*

Nous reportons au §V.2.8 la démonstration de cette proposition. Soit $(A, i) \in \mathrm{AF} \times \{0,1\}$ où A est un p-groupe engendré par au plus $n/2$ éléments.

Nous dirons que $\underline{N} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ est un A-voisin de type i de $\underline{M} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$, si l'image de $(\underline{N}, \underline{M})$ par l'application (2.5) est (A, i). L'opérateur de Hecke correspondant est noté

$$\mathrm{T}_{(A,i)} \in \mathrm{H}_p(\mathrm{P}\widetilde{G});$$

ils forment une $\mathbb{Z}$-base de $\mathrm{H}_p(\mathrm{P}\widetilde{G})$. Si $M^\sharp = M$, on constate que $\underline{N}$ est un A-voisin de type 0 de $\underline{M}$ si, et seulement si, $\underline{N}$ possède un représentant autodual, alors unique, et si ce dernier est un A-voisin de M au sens précédent. La notion de A-voisin de type 1 de $\underline{M}$ est en revanche "nouvelle". L'exemple qui suit sera particulièrement important dans ce mémoire.

Soient $M, N \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$. Suivant Koch et Venkov dans le cas quadratique [KV89], nous dirons que N est une *perestroïka* de M relativement à p si

$$pM \subsetneq N \subsetneq M.$$

Il est aisé de vérifier que N est une perestroïka de M relativement à p si, et seulement si, $\mathrm{v}_M - \mathrm{v}_{p^{-1}N} = 1$ et $\underline{N}$ est un 0-voisin de $\underline{M}$ de type 1. De plus, la proposition suivante est immédiate.

Proposition 2.10. *Soient $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ et p un nombre premier. L'application $N \mapsto N/pM$ définit une bijection de l'ensemble des perestroïkas de M relativement à p sur l'ensemble des lagrangiens de $M \otimes \mathbb{F}_p$.*

L'opérateur des perestroïkas relativement à p est l'opérateur

$$\mathrm{K}_p := \mathrm{T}_{(0,1)} \in \mathrm{H}_p(\mathrm{P}\widetilde{G}).$$

Si $(N, M) \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$, N est une perestroïka de M relativement à p si, et seulement si, pM est une perestroïka de N relativement à p. En particulier, $\mathrm{K}_p^{\mathrm{t}} = \mathrm{K}_p$. En fait, on a $T^{\mathrm{t}} = T$ pour tout $T \in \mathrm{H}(\mathrm{P}\widetilde{G})$ comme on le verra au §V.2.8.

Terminons ce paragraphe, comme prévu, par une démonstration de la proposition 2.7.

Démonstration. On se place dans le cas quadratique, i.e. φ symétrique et $\mathrm{q}(x) = \frac{\varphi(x,x)}{2}$, auquel cas L est un q-module sur $\mathbb{Z}$. La démonstration dans le cas alterné est similaire (et même plus simple).

Il s'agit de montrer que si U est un q-module hyperbolique sur $\mathbb{Q}_p$, et si (L_1, L_2) et (L'_1, L'_2) sont deux couples de réseaux autoduaux de U tels que $L_1/(L_1 \cap L_2) \simeq L'_1/(L'_1 \cap L'_2)$ alors il existe $\alpha \in \mathrm{O}(U)$ tel que $\alpha(L_i) = L'_i$ pour $i = 1, 2$. On raisonne par récurrence sur $\dim(U)$.

Les cas $U = 0$ et $L_1 = L_2$ sont triviaux. On suppose donc que $L_1 \neq L_2$. L'idéal annulateur du quotient $L_1/(L_1 \cap L_2)$ est donc de la forme $p^\nu \mathbb{Z}_p$ avec $\nu \geq 1$. Nous affirmons qu'il existe un élément e_1 de L_1 et un élément e_2 de L_2 tels que

$$\mathrm{q}(e_1) = 0 \qquad , \qquad \mathrm{q}(e_2) = 0 \qquad , \qquad e_1.e_2 = p^{-\nu} \qquad .$$

En effet, il est tout d'abord facile de se convaincre de ce qu'il existe un élément ϵ_1 de L_1 et un élément ϵ_2 de L_2 avec $\epsilon_1.\epsilon_2 = p^{-\nu}$. Le lemme de Hensel montre ensuite qu'il existe une matrice

$$P = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \qquad ,$$

à coefficients dans $\mathbb{Z}_p$, avec $P \equiv \mathrm{I} \bmod p^\nu$ telle que l'on a :

$${}^{\mathrm{t}}P \begin{bmatrix} 2\mathrm{q}(\epsilon_1) & p^{-\nu} \\ p^{-\nu} & 2\mathrm{q}(\epsilon_2) \end{bmatrix} P \;=\; \begin{bmatrix} 0 & p^{-\nu} \\ p^{-\nu} & 0 \end{bmatrix} \qquad .$$

On prend $e_1 = a_{1,1}\epsilon_1 + a_{2,1}\epsilon_2$ et $e_2 = a_{1,2}\epsilon_1 + a_{2,2}\epsilon_2 \in L_2$ (la congruence $P \equiv \mathrm{I} \bmod p^\nu$ implique $e_1 \in L_1$ et $e_2 \in L_2$). Ce qui termine la démonstration de l'affirmation.

Achevons maintenant la récurrence. On note respectivement H, H_1 H_2, le sous-espace vectoriel de U engendré par e_1 et e_2, le sous-module de L_1 engendré par e_1 et $p^\nu e_2$, le sous-module de L_2 engendré par $p^\nu e_1$ et e_2. On munit H, H_1 et H_2 des formes quadratiques induites par celle de U. Par construction, $H \approx \mathrm{H}(\mathbb{Q}_p)$ et $H_i \approx \mathrm{H}(\mathbb{Z}_p)$ pour $i = 1, 2$. On note respectivement W, M_1 et M_2, l'orthogonal de H dans U, l'orthogonal de H_1 dans L_1 et l'orthogonal de H_2 dans L_2. On a des décompositions en somme orthogonale

$$U = H \oplus W \qquad , \qquad L_1 = H_1 \oplus M_1 \qquad , \qquad L_2 = H_2 \oplus M_2$$

et des isomorphismes

$$L_1/(L_1 \cap L_2) \cong H_1/(H_1 \cap H_2) \oplus M_1/(M_1 \cap M_2) \quad , \quad H_1/(H_1 \cap H_2) \cong \mathbb{Z}_p/p^\nu \mathbb{Z}_p \quad .$$

On remplace le couple (L_1, L_2) par le couple (L_1', L_2') et on introduit pareillement les q-espaces vectoriels H', W' et les q-modules H_1', H_2', M_1', M_2'. On obtient l'automorphisme cherché $\alpha : U \to U$ comme somme orthogonale d'isomorphismes adéquats de q-espaces vectoriels $H \to H'$ et $W \to W'$, l'existence du second étant assurée par l'hypothèse de récurrence. $\square$

2.11. $\mathrm{H}(\mathrm{SO}_L)$ versus $\mathrm{H}(\mathrm{O}_L)$

Soit L un q-module sur $\mathbb{Z}$. Discutons brièvement du lien entre $\mathrm{H}(\mathrm{SO}_L)$ et $\mathrm{H}(\mathrm{O}_L)$. Les cas de PGSO_L et PGO_L pourraient se traiter de manière similaire.

D'après la proposition 1.7, l'inclusion $\mathrm{SO}_L \to \mathrm{O}_L$ induit une bijection $\mathrm{SO}_L(\mathbb{A}_f)$-équivariante $\mathcal{R}(\mathrm{SO}_L) \xrightarrow{\sim} \mathcal{R}(\mathrm{O}_L)$. Il en résulte que $\mathrm{H}(\mathrm{O}_L)$ s'identifie canoniquement à un sous-anneau de $\mathrm{H}(\mathrm{SO_L})$: ce sont les sous-anneaux de $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)])$ constitués respectivement des endomorphismes $\mathrm{O}_L(\mathbb{A}_f)$-équivariants et $\mathrm{SO}_L(\mathbb{A}_f)$-équivariants. Le groupe quotient

$$\mathrm{O}_L(\mathbb{A}_f)/\mathrm{SO}_L(\mathbb{A}_f) \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathrm{P}}$$

agit naturellement par conjugaison sur $\mathrm{H}(\mathrm{SO}_L)$, avec pour anneau des invariants $\mathrm{H}(\mathrm{O}_L)$. Cette action respecte la décomposition de $\mathrm{H}(G)$ en produit tensoriel des $\mathrm{H}_p(G)$ sur les $p \in \mathrm{P}$, et identifie également $\mathrm{H}_p(\mathrm{O}_L)$ avec $\mathrm{H}_p(\mathrm{SO}_L)^{\mathbb{Z}/2\mathbb{Z}}$.

Donnons un exemple d'un élément de $\mathrm{H}_p(\mathrm{SO}_L)$ qui n'est pas dans $\mathrm{H}_p(\mathrm{O}_L)$. Soit $A = (\mathbb{Z}/p\mathbb{Z})^{n/2}$ où n est le rang de L. Considérons l'ensemble Ω des couples (N, M) d'éléments de $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ tels que N est un A-voisin de M. La proposition 2.7 assure que Ω est une $\mathrm{O}_L(\mathbb{Q}_p)$-orbite. En revanche, il est réunion disjointe de deux orbites sous l'action de $\mathrm{SO}_L(\mathbb{Q}_p)$. Pour le voir, on commence par vérifier, par des considérations similaires à celles du §III.1, que l'application

$$N \mapsto (M \cap N)/pM$$

induit une surjection (non bijective en général) entre les A-voisins de M et les lagrangiens du q-module hyperbolique $M \otimes \mathbb{F}_p$. Mais il est bien connu que pour tout corps k, et tout k-module hyperbolique V, il y a exactement deux orbites de lagrangiens de V sous l'action de $\mathrm{SO}(V)$ (et une seule sous $\mathrm{O}(V)$, par le théorème de Witt). Par lissité de SO_M sur $\mathbb{Z}_p$, chacune de ces deux orbites définit donc une $\mathrm{SO}(M)$-orbite de A-voisins de M, et par conséquent deux opérateurs de Hecke distincts $\mathrm{T}_A^{\pm} \in \mathrm{H}(\mathrm{SO}_L)$ dont la somme vaut T_A, qui sont échangés sous l'action de $\mathrm{O}_L(\mathbb{Q}_p)/\mathrm{SO}_L(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$.

2.12. Isogénies

Nous discutons maintenant des isogénies entre Γ-ensembles transitifs, en exposant une variante des considérations dans [Sat63, II §7].

Soient X un Γ-ensemble et X' un Γ'-ensemble. Rappelons qu'un morphisme $X \to X'$ est un couple (f, g) où $g : X \to X'$ est une application et $f : \Gamma \to \Gamma'$ est un morphisme de groupes, tels que $g(\gamma x) = f(\gamma)g(x)$ pour

tout $x \in X$ et tout $\gamma \in \Gamma$. Dans ce qui suit, il sera commode de convenir qu'un ensemble transitif est non vide.

Lemme 2.13. *Soient X un Γ-ensemble transitif, X' un Γ'-ensemble, et (f, g) un morphisme $X \to X'$ tel que $f(\Gamma)$ est distingué dans Γ'. Soit S le stabilisateur de $g(X)$ dans Γ', c'est-à-dire $S = \{\gamma \in \Gamma', \gamma g(X) \subset g(X)\}$.*

(i) Pour tout $x \in g(X)$ on a $S = f(\Gamma)\Gamma'_x$.

(ii) $S = \{\gamma \in \Gamma', \gamma g(X) \cap g(X) \neq \emptyset\}$.

Démonstration. Soit $x \in g(X)$. Le sous-groupe $f(\Gamma)$ étant distingué dans Γ', le sous-ensemble $E_x := f(\Gamma)\Gamma'_x \subset \Gamma'$ est un sous-groupe. La transitivité de X montre alors que :

– E_x ne dépend pas du choix de $x \in g(X)$,

– E_x est l'ensemble des $\gamma \in \Gamma'$ tels que $\gamma(x) \in g(X)$.

On a donc $S = \bigcap_{x \in g(X)} E_x = \bigcup_{x \in g(X)} E_x = \{\gamma \in \Gamma', \gamma g(X) \cap g(X) \neq \emptyset\}$. □

Soient X un Γ-ensemble transitif, X' un Γ'-ensemble, et (f, g) un morphisme $X \to X'$. On suppose comme dans le lemme ci-dessus que $f(\Gamma)$ est distingué dans Γ' et de plus que l'application g est injective.[3] Soit S le stabilisateur de $g(X)$ dans Γ'. L'application $(s, x) \mapsto g^{-1}(s(g(x))$, qui a un sens par injectivité de g, définit une action de S sur X, dont la restriction à $f : \Gamma \to S$ est le Γ-ensemble X. Elle induit donc une action de $S/f(\Gamma)$ sur $\mathrm{H}(X)$ par automorphismes d'anneaux, dont nous noterons $\mathrm{H}(X)^{\mathrm{inv}} \subset \mathrm{H}(X)$ le sous-anneau des invariants, qui est également $\mathrm{End}_{\mathbb{Z}[S]}(\mathbb{Z}[X])$.

Proposition-Définition 2.14. *Soit $u = (f, g) : X \to X'$ un morphisme entre le Γ-ensemble transitif X et le Γ'-ensemble transitif X'. On suppose que $f(\Gamma)$ est distingué dans Γ' et que g est injectif.*

(i) Si $T \in \mathrm{H}(X)^{\mathrm{inv}}$ il existe un unique $T' \in \mathrm{H}(X')$ qui s'annule sur $(X' - g(X)) \times g(X)$ et tel que $T'_{g(x),g(y)} = T_{x,y}$ pour tout $x, y \in X$.

(ii) L'application ainsi définie $\mathrm{H}(u) : \mathrm{H}(X)^{\mathrm{inv}} \to \mathrm{H}(X'), T \mapsto T'$, est un homomorphisme injectif d'anneaux.

3. Nous renvoyons à l'article de Satake pour une variante sans l'hypothèse d'injectivité de g. Le lecteur ne perdrait pas grand chose ici à supposer que $\Gamma \subset \Gamma'$, $X \subset X'$, et que f et g sont les inclusions correspondantes.

Démonstration. L'assertion d'unicité dans le (i) découle de l'injectivité de g et de la transitivité de X'. L'assertion (ii) se déduit immédiatement du (i). Il ne reste donc qu'à justifier l'existence de T' dans le (i). Mais le point (ii) du lemme 2.13 montre que l'injection $g : X \to X'$ induit une bijection $\mathrm{Ind}_S^{\Gamma'} X \xrightarrow{\sim} X'$, et donc un isomorphisme $\mathbb{Z}[\Gamma'] \otimes_{\mathbb{Z}[S]} \mathbb{Z}[X] \xrightarrow{\sim} \mathbb{Z}[X']$. Ainsi, toute application linéaire S-équivariante $T : \mathbb{Z}[X] \to \mathbb{Z}[X]$, composée avec $g : \mathbb{Z}[X] \to \mathbb{Z}[X']$, s'étend de manière unique en une application Γ'-équivariante $T' : \mathbb{Z}[X'] \to \mathbb{Z}[X']$; elle a les propriétés de l'énoncé. □

Dans tous les exemples que nous aurons à considérer, il se trouve que le groupe S préservera chaque Γ-orbite de $X \times X$, de sorte que l'on aura $\mathrm{H}(X)^{\mathrm{inv}} = \mathrm{H}(X)$. Un cas particulièrement simple est celui où $\Gamma' = \Gamma$, $X' = X$, et f et g sont bijectifs. Dans ce cas $S = f(\Gamma)$ et $\mathrm{H}(u)$ est par définition l'automorphisme de $\mathrm{H}(X)$ qui vaut matriciellement $(T_{x,y}) \mapsto (T_{g^{-1}x,g^{-1}y})$.

Plaçons-nous dans les hypothèses de la proposition-définition 2.14. Si M est un Γ'-module, notons $M_{|\Gamma}$ le Γ-module obtenu par restriction de M par $f : \Gamma \to \Gamma'$. On dispose alors d'une application injective canonique

$$M_{X'} \to (M_{|\Gamma})_X, \quad \varphi \mapsto \varphi_{|X} := \varphi \circ g.$$

Le lemme suivant est immédiat.

Lemme 2.15. *On reprend les hypothèses de la proposition-définition 2.14. Soient M un Γ'-module, $T \in \mathrm{H}(X)^{\mathrm{inv}}$ et $\varphi \in M_{X'}$, alors $T(\varphi_{|X}) = \mathrm{H}(u)(T)(\varphi)$.*

Exemple 2.16. En guise d'exemple, replaçons-nous dans le contexte des groupes de similitudes (§1.2) et considérons le $\mathbb{Z}$-morphisme naturel $\mu : G \to \mathrm{P}\widetilde{G}$. Le paragraphe précédent s'applique et définit un morphisme d'anneaux

$$\mathrm{H}(\mu) : \mathrm{H}(G) \to \mathrm{H}(\mathrm{P}\widetilde{G})$$

tel que $\mathrm{H}(\mu)(\mathrm{T}_A) = \mathrm{T}_{(A,0)}$ pour tout groupe abélien fini A engendré par au plus $n/2$ éléments.

En effet, on considère $\Gamma = G(\mathbb{A}_f)$, $X = \mathcal{R}(G)$, $\Gamma' = \mathrm{P}\widetilde{G}(\mathbb{A}_f)$, $X' = \mathcal{R}(\mathrm{P}\widetilde{G})$, et on prend pour f et g les applications naturelles déduites de μ. Le groupe Γ est distingué dans $\widetilde{G}(\mathbb{A}_f)$, ainsi donc que $f(\Gamma)$ dans Γ'. De plus, g s'identifie à l'injection naturelle $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \to \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V)$, $M \mapsto \underline{M}$, d'après la proposition 1.4. Le groupe S est le sous-groupe des éléments $g \in \widetilde{G}(\mathbb{A}_f)$ tels que $\nu(g)$ est de la forme $a^2 b$ avec $a \in \mathbb{A}_f^\times$ et $b \in \widehat{\mathbb{Z}}^\times$. Il agit trivialement sur $\Gamma \backslash (\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V))$. En effet, si $N, M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, $g \in \widetilde{G}(\mathbb{A}_f)$, et si p est un nombre premier, g induit un isomorphisme $M_p/(N_p \cap M_p) \simeq g(M)_p/(g(N)_p \cap g(M)_p)$, ce qui conclut par la proposition 2.7. L'assertion sur T_A se déduit de la discussion consécutive à la proposition 2.9.

3. Formes automorphes d'un $\mathbb{Z}$-groupe

L'anneau des adèles de $\mathbb{Q}$ est l'anneau $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$. Soit G un $\mathbb{Z}$-groupe. Le groupe $G(\mathbb{R})$ est un groupe de Lie de manière naturelle, et le groupe

$$G(\mathbb{A}) = G(\mathbb{R}) \times G(\mathbb{A}_f)$$

est encore localement compact et séparé pour la topologie produit, la topologie sur $G(\mathbb{A}_f)$ ayant déjà été rappelée au §2.5. Le groupe $G(\mathbb{Q})$ se plonge naturellement diagonalement dans $G(\mathbb{A})$: c'est un sous-groupe fermé discret (voir [GGPS66, Ch. II §3] pour les rudiments sur ces constructions).

3.1. Formes automorphes de carré intégrable

Rappelons quelques résultats classiques dûs à Borel et Harish-Chandra, pour lesquels nous renvoyons à [Bor63, §5]. Supposons que la composante neutre de $G(\mathbb{C})$ est semi-simple [Hu75] [Bor91]. Le groupe localement compact $G(\mathbb{A})$ est alors unimodulaire. L'espace homogène

$$G(\mathbb{Q})\backslash G(\mathbb{A})$$

hérite d'après Weil d'une mesure de Radon μ positive (non nulle) invariante par translations à droite sous $G(\mathbb{A})$ [Wei40, Chap. II] [Rud87, Chap. 2]. Il est de mesure finie.

L'espace des *formes automorphes de carré intégrable pour* G est le sous-espace

$$\mathcal{A}^2(G) \subset \mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$$

des éléments qui sont invariants par translations à droite sous $G(\widehat{\mathbb{Z}})$ [GGPS66, Ch. 3] [BJ79, §4]. C'est un espace de Hilbert pour le produit scalaire hermitien

$$\langle f, f' \rangle_{\mathrm{Pe}} := \int \overline{f} f' \ \mathrm{d}\mu,$$

appelé aussi *produit de Petersson*. Alternativement, $\mathcal{A}^2(G)$ peut être vu comme l'espace des fonctions de carré intégrable sur $G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$, muni de la mesure de Radon image de μ par l'application (propre) canonique $G(\mathbb{Q})\backslash G(\mathbb{A}) \to G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$. L'espace $\mathcal{A}^2(G)$ est muni de deux structures additionnelles importantes que nous décrivons maintenant.

D'une part, l'espace $\mathcal{A}^2(G)$ étant l'espace des $G(\widehat{\mathbb{Z}})$-invariants du $G(\mathbb{A}_f)$-module $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$ pour les translations à droite, est muni d'une action à droite de l'anneau de Hecke $\mathrm{H}(G)$ (§2.2, §2.5). Cette action est une

$\star$-*action* pour le produit de Petersson. Nous entendons par là que l'adjoint de $T \in \mathrm{H}(G)$ est l'opérateur T^{t} défini au §2.1 : si $f, f' \in \mathcal{A}^2(G)$ et $T \in \mathrm{H}(G)$,

$$\langle\, T(f), f' \,\rangle_{\mathrm{Pe}} = \langle\, f, T^{\mathrm{t}}(f') \,\rangle_{\mathrm{Pe}}. \tag{3.1}$$

C'est en effet conséquence du lemme 2.3 et de l'unimodularité de $G(\mathbb{A}_f)$.

D'autre part, $\mathcal{A}^2(G)$ est stable sous l'action de $G(\mathbb{R})$ par translations à droite, et cette action commute à celle de $\mathrm{H}(G)$. Elle fait de $\mathcal{A}^2(G)$ une représentation unitaire du groupe de Lie $G(\mathbb{R})$ (nous renvoyons à [Kna86] comme référence générale sur les représentations unitaires). Une description plus classique de cette représentation s'obtient en écrivant

$$G(\mathbb{A}_f) = \coprod_{i=1}^{\mathrm{h}(G)} G(\mathbb{Q}) g_i G(\widehat{\mathbb{Z}}) \tag{3.2}$$

pour certains éléments $g_i \in G(\mathbb{A}_f)$, par finitude du nombre de classes de G. Pour tout i, $G(\mathbb{Q}) g_i G(\widehat{\mathbb{Z}})$ est un ouvert de $G(\mathbb{A}_f)$ et le groupe "de congruences"

$$\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$$

est un sous-groupe discret de $G(\mathbb{R})$ commensurable à $G(\mathbb{Z})$. L'application $f \mapsto (f_{|G(\mathbb{R})\times g_i})_i$ induit un isomorphisme $G(\mathbb{R})$-équivariant

$$\mathcal{A}^2(G) \xrightarrow{\sim} \prod_{i=1}^{\mathrm{h}(G)} \mathrm{L}^2(\Gamma_i \backslash G(\mathbb{R})), \tag{3.3}$$

chaque $\Gamma_i \backslash G(\mathbb{R})$ héritant naturellement d'une mesure de Radon > 0, invariante à droite par $G(\mathbb{R})$, de masse finie, uniquement déterminée par μ. Cette représentations de $G(\mathbb{R})$ comporte en général une partie "discrète" notoirement difficile à décrire, ainsi qu'une partie "continue" dont l'étude a été ramenée par Langlands à des parties discrètes pour des groupes G' annexes [Lan76].

3.2. L'ensemble $\Pi_{\mathrm{disc}}(G)$

Nous ne nous intéresserons ici qu'à la partie discrète de $\mathcal{A}^2(G)$, c'est-à-dire au sous-espace

$$\mathcal{A}_{\mathrm{disc}}(G) \subset \mathcal{A}^2(G)$$

défini comme étant l'adhérence de la somme des sous-$G(\mathbb{R})$-représentations fermées et topologiquement irréductibles de $\mathcal{A}^2(G)$. C'est une représenta-

tion de $G(\mathbb{R})$ qui est somme orthogonale d'irréductibles par construction [4], chacune n'intervenant qu'avec une multiplicité finie d'après un résultat fondamental dû à Harish-Chandra (voir l'introduction de [HC68] ainsi que le théorème 1 du chapitre 1 loc. cit., voir également [BJ79]). Autrement dit, si U est une représentation irréductible unitaire de $G(\mathbb{R})$, l'espace

$$\mathcal{A}_U(G) := \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}_{\mathrm{disc}}(G)) = \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}^2(G))$$

est de dimension finie sur $\mathbb{C}$. On a bien entendu un isomorphisme canonique

$$\widehat{\bigoplus_{U \in \mathrm{Irr}(G(\mathbb{R}))}} U \otimes \mathcal{A}_U(G) \xrightarrow{\sim} \mathcal{A}_{\mathrm{disc}}(G), \tag{3.4}$$

$\mathrm{Irr}(H)$ désignant l'ensemble des classes d'isomorphisme de représentations unitaires topologiquement irréductibles du groupe localement compact H.

La structure de $\mathrm{H}(G)$-module à droite de $\mathcal{A}^2(G)$ induit naturellement une structure de $\mathrm{H}(G)$-module à droite sur $\mathcal{A}_U(G)$. Ce dernier hérite également d'un produit scalaire hermitien pour lequel l'action de $\mathrm{H}(G)$ est encore une $\star$-action. Par exemple, si $e \in U$ est non nul fixé, et si $\varphi, \varphi' \in \mathcal{A}_U(G)$, on peut poser $\langle \varphi, \varphi' \rangle = \langle \varphi(e), \varphi'(e) \rangle_{\mathrm{Pe}}$. Or il est bien connu qu'une sous-$\mathbb{C}$-algèbre de $\mathrm{M}_n(\mathbb{C})$ stable par $M \mapsto {}^{\mathrm{t}}\overline{M}$ est semi-simple : si X est dans son radical de Jacobson, la matrice hermitienne $X\,{}^{\mathrm{t}}\overline{X}$ est nilpotente, donc nulle, ce qui entraîne que X est nulle. En particulier, $\mathcal{A}_U(G)$ est semi-simple vue comme représentation de la $\mathbb{C}$-algèbre $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$.

Appelons *représentation de* $(G(\mathbb{R}), \mathrm{H}(G))$ la donnée d'un espace de Hilbert muni d'une représentation unitaire de $G(\mathbb{R})$ et d'une structure de module à droite sur $\mathrm{H}(G)$ tels que l'action de tout élément de $G(\mathbb{R})$ commute avec celle de tout élément de $\mathrm{H}(G)$. Ces représentations forment une catégorie $\mathbb{C}$-linéaire de manière naturelle : un morphisme $E \to F$ est une application $\mathbb{C}$-linéaire continue $E \to F$ commutant aux actions de $G(\mathbb{R})$ et $\mathrm{H}(G)$. Si U est une représentation unitaire de $G(\mathbb{R})$, et si V est un $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module supposé de dimension finie comme $\mathbb{C}$-espace vectoriel, alors $U \otimes V$ est une représentation de $(G(\mathbb{R}), \mathrm{H}(G))$ de manière naturelle (le produit tensoriel étant pris au dessus de $\mathbb{C}$). Nous désignerons par $\Pi(G)$ l'ensemble des classes

4. Il est utile à ce stade de rappeler la version suivante du lemme de Schur. Soient U et V des espaces de Hilbert munis de représentations unitaires d'un groupe Γ. On suppose que U est topologiquement irréductible et que $u : U \to V$ est une application linéaire continue Γ-équivariante non nulle. Alors l'adjoint $u^* : V \to U$ (qui est Γ-équivariant) satisfait $u^* \circ u = \lambda \mathrm{Id}_U$ pour un certain $\lambda \in \mathbb{R}^\times$. En effet, $u^* \circ u \in \mathrm{End}(U)$ est hermitien non nul et commute à Γ, son spectre est donc réduit à un point $\{\lambda\}$ d'après le théorème spectral. Il vient que V est somme orthogonale de $\mathrm{Im}(u)$ (qui est fermé) et $\mathrm{Ker}(u^*)$.

d'isomorphisme de représentations de $(G(\mathbb{R}), \mathrm{H}(G))$ de cette forme, telles que de plus U est topologiquement irréductible et V est simple. La restriction à $G(\mathbb{R})$ d'une telle représentation unitaire π est isomorphe à $U^{\dim V}$, de sorte que la classe d'isomorphisme de la représentation unitaire U est entièrement déterminée par la représentation unitaire de $G(\mathbb{R})$ sous-jacente à π : on la note π_∞. De même, le $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module sous-jacent à π est semi-simple et V-isotypique, de sorte que la classe d'isomorphisme du $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module V est uniquement déterminée par celle de π : on la note π_f. En particulier, on a $\pi \simeq \pi_\infty \otimes \pi_f$ pour tout $\pi \in \Pi(G)$. Enfin, le lemme de Schur entraîne que tout $\pi \in \Pi(G)$ est topologiquement irréductible en tant que représentation de $(G(\mathbb{R}), \mathrm{H}(G))$.

D'après la discussion ci-dessus, si $U \in \mathrm{Irr}(G(\mathbb{R}))$ alors l'espace $U \otimes \mathcal{A}_U(G)$ est une représentation de $(G(\mathbb{R}), \mathrm{H}(G))$ de manière naturelle, ainsi bien entendu que $\mathcal{A}_{\mathrm{disc}}(G)$, l'isomorphisme (3.4) commutant trivialement aux actions de $G(\mathbb{R})$ et $\mathrm{H}(G)$. Il en résulte que l'on dispose d'une décomposition comme somme hilbertienne d'éléments de $\Pi(G)$ raffinant la décomposition (3.4)

$$\mathcal{A}_{\mathrm{disc}}(G) = \widehat{\bigoplus_{\pi \in \Pi(G)}} m(\pi)\, \pi \tag{3.5}$$

où $m(\pi) \geq 0$ est un entier appelé *multiplicité de* π. Par définition, si $\pi \in \Pi(G)$ et si $U \simeq \pi_\infty$, alors $\mathrm{m}(\pi)$ est la multiplicité de π_f dans le $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module $\mathcal{A}_U(G)$, qui est semi-simple et de dimension finie. On note

$$\Pi_{\mathrm{disc}}(G) \subset \Pi(G)$$

le sous-ensemble des π telles que $m(\pi) \neq 0$.

Les éléments de $\Pi_{\mathrm{disc}}(G)$ seront appelés *représentations automorphes discrètes*[5] de G. Le seul exemple vraiment évident de telle représentation est la *représentation triviale*, notée 1_G, réalisée comme sous-espace (de dimension 1) des fonctions constantes de $\mathcal{A}^2(G)$ (noter que μ est de masse finie). L'action de $G(\mathbb{R})$ dans 1_G est bien entendu l'action triviale, celle de $\mathrm{H}(G)$ étant la multiplication par le "degré" (voir l'exemple VI.2.3). En général, l'ensemble $\Pi_{\mathrm{disc}}(G)$ est infini dénombrable, ce qui n'est pas le cas de $\Pi(G)$. Nous donnerons quelques exemples concrets dans les chapitres suivants.

5. Le lecteur prendra garde que la définition utilisée ici ne dépend pas que de $G_{\mathbb{Q}}$ mais bien de G comme $\mathbb{Z}$-groupe. Dans la littérature, nos représentations automorphes discrètes de G sont plus communément nommées "représentations automorphes discrètes de $G(\mathbb{A})$, sphériques (ou non ramifiées) relativement à $G(\widehat{\mathbb{Z}})$". La perte apparente de généralité dans notre présentation est toutefois illusoire à ce stade, étant donné que tout sous-groupe compact ouvert de $G(\mathbb{A}_f)$ est de la forme $G'(\widehat{\mathbb{Z}})$ pour un $\mathbb{Z}$-groupe G' bien choisi et tel que $G'_{\mathbb{Q}} \simeq G_{\mathbb{Q}}$.

Un élément $F \in \mathcal{A}_U(G)$ sera dit *propre* s'il est non nul et s'il engendre un $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module irréductible. Quand $\mathrm{H}(G)$ est commutative, il est équivalent de demander que $F \neq 0$ soit un vecteur propre de tous les opérateurs de Hecke dans $\mathrm{H}(G)$. Si F est propre, et si $V \subset \mathcal{A}_U(G)$ désigne le $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module engendré par F, l'image de $U \otimes V$ dans $\mathcal{A}_{\mathrm{disc}}(G)$ par l'application canonique (3.4) est une sous-représentation topologiquement irréductible de $(G(\mathbb{R}), \mathrm{H}(G))$ notée π_F ; c'est la *représentation (automorphe, discrète) engendrée par* F. On note souvent également encore π_F sa classe d'isomorphisme, qui est un élément de $\Pi_{\mathrm{disc}}(G)$.

Enfin, suivant Gelfand, Graev et Piatetski-Shapiro [GGPS66, Ch. 3 §7], on dispose du sous-espace $\mathcal{A}_{\mathrm{cusp}}(G) \subset \mathcal{A}^2(G)$ constitué des *formes paraboliques* (la définition d'une forme parabolique est rappelée ci-dessous). Il s'agit d'un sous-espace fermé, stable par les actions de $G(\mathbb{R})$ et $\mathrm{H}(G)$. Gelfand, Graev et Piatetski-Shapiro démontrent l'inclusion

$$\mathcal{A}_{\mathrm{cusp}}(G) \subset \mathcal{A}_{\mathrm{disc}}(G) \tag{3.6}$$

(voir aussi [Bor97, Theorem 16.2]). On note

$$\Pi_{\mathrm{cusp}}(G) \subset \Pi_{\mathrm{disc}}(G)$$

l'ensemble des $\pi \in \Pi(G)$ qui interviennent dans le sous-espace $\mathcal{A}_{\mathrm{cusp}}(G)$.

Quand $G_{\mathbb{Q}}$ n'admet pas de sous-$\mathbb{Q}$-groupe parabolique strict, ce qui équivaut à dire que $G(\mathbb{Q})$ n'a pas d'élément unipotent non trivial, on a l'égalité évidente $\mathcal{A}_{\mathrm{cusp}}(G) = \mathcal{A}^2(G)$. Dans ce cas[6], l'inclusion (3.6) entraîne $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$.

Rappelons la définition d'une forme parabolique. Soit $P \subset G_{\mathbb{Q}}$ un sous-$\mathbb{Q}$-groupe *parabolique strict*, c'est-à-dire tel que $P(\mathbb{C})$ soit connexe, contienne un sous-groupe de Borel de la composante neutre de $G(\mathbb{C})$, et ne soit pas égal à cette composante toute entière [Hu75][Bor91]. Si N désigne le radical unipotent de P, alors le groupe localement compact $N(\mathbb{A})$ est unimodulaire, et son sous-groupe $N(\mathbb{Q})$ est discret et cocompact. On note $\mathrm{d}n$ une mesure de Radon $\mathrm{N}(\mathbb{A})$-invariante > 0 sur $N(\mathbb{Q})\backslash N(\mathbb{A})$. Soient $f : G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$ une fonction borélienne de carré intégrable et $g \in G(\mathbb{A})$. La fonction $n \mapsto f(ng)$, $N(\mathbb{Q})\backslash N(\mathbb{A}) \to \mathbb{C}$, est alors borélienne, de carré intégrable pour presque tout $g \in G(\mathbb{A})$. On dit que f est parabolique si pour tout sous-$\mathbb{Q}$-groupe parabolique strict P de $G_{\mathbb{Q}}$, on a $\int_{N(\mathbb{Q})\backslash N(\mathbb{A})} f(ng)\,\mathrm{d}n = 0$ pour presque

6. En fait, un résultat fameux de Godement montre que sous cette même hypothèse sur G le groupe $G(\mathbb{Q})$ est cocompact dans $G(\mathbb{A})$, ce qui entraîne plus directement l'égalité $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$ dans ce cas particulier (voir par exemple [Bor97, Lemma 16.1]).

tout $g \in N(\mathbb{A})\backslash G(\mathbb{A})$. On vérifie que le sous-ensemble de $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$ constitué des classes de fonctions paraboliques est un sous-espace vectoriel fermé (voir par exemple [Bor97, Prop. 8.2]). Il est trivialement stable par les translations à droite par les éléments de $G(\mathbb{A})$.

4. Formes automorphes pour O_n

4.1. Formes automorphes des $\mathbb{Z}$-groupes G tels que $G(\mathbb{R})$ est compact.

On se replace dans le cadre du §3.1. Supposons que le $\mathbb{Z}$-groupe G a la propriété que $G(\mathbb{R})$ est compact. Dans ce cas, les groupes $\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$ de la formule (3.2) sont des sous-groupes finis de $G(\mathbb{R})$, car discrets dans un compact. De plus, le quotient $G(\mathbb{Q})\backslash G(\mathbb{A})$ est compact, car homéomorphe à la réunion disjointe des $\Gamma_i \backslash G(\mathbb{R})$. La formule (3.3) entraîne alors $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$, d'après le théorème de Peter-Weyl. Nous allons donner une autre description des $\mathrm{H}(G)$-modules $\mathcal{A}_U(G)$.

Si U est un $\mathbb{Z}[G(\mathbb{Q})]$-module, désignons par $\mathrm{M}_U(G)$ l'espace des fonctions

$$F : \mathcal{R}(G) \longrightarrow U$$

telles que $F(\gamma x) = \gamma \cdot F(x)$ pour tous $\gamma \in G(\mathbb{Q})$ et $x \in \mathcal{R}(G)$. Observons que $\mathrm{M}_U(G)$ s'identifie canoniquement à $\mathrm{Hom}_{\mathbb{Z}[G(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(G)], U)$, ce qui lui confère une action à droite de l'anneau $\mathrm{H}(G)$. Mieux, $U \mapsto \mathrm{M}_U(G)$ définit un foncteur des $G(\mathbb{Q})$-modules vers les $\mathrm{H}(G)^{\mathrm{opp}}$-modules. Sa structure additive est très simple, car $F \mapsto (F(g_i))$ induit un isomorphisme

$$\mathrm{M}_U(G) \longrightarrow \prod_{i=1}^{\mathrm{h}(G)} U^{\Gamma_i}. \tag{4.1}$$

En particulier, on a $\mathrm{M}_{U \oplus V}(G) \simeq \mathrm{M}_U(G) \oplus \mathrm{M}_V(G)$. Observons d'ailleurs que la construction ci-dessus a un sens pour tous les $\mathbb{Z}$-groupes G.

Supposons maintenant que U est une représentation complexe, continue, de dimension finie, de $G(\mathbb{R})$, et notons U^* son dual. Si $F \in \mathrm{M}_U(G)$ et $u \in U^*$, on note $\varphi_F(u)$ la fonction $(h, x) \mapsto \langle u, h^{-1}F(x)\rangle$, $G(\mathbb{R}) \times \mathcal{R}(G) \to \mathbb{C}$. C'est une fonction continue ; elle est donc dans $\mathcal{A}^2(G)$ car $G(\mathbb{Q})\backslash(G(\mathbb{R}) \times \mathcal{R}(G))$ est compact d'après (3.3). La relation évidente $\varphi_F(gu) = g \cdot (\varphi_F(u))$, valable pour $u \in U^*$ et $g \in G(\mathbb{R})$, montre que la fonction $\varphi_F, u \mapsto \varphi_F(u)$, est un élément de $\mathcal{A}_{U^*}(G)$. La démonstration de lemme suivant est immédiate, et laissée au lecteur.

Lemme 4.2. *Supposons que U est une représentation irréductible de $G(\mathbb{R})$. Alors $F \mapsto \varphi_F$ est un isomorphisme $\mathrm{H}(G)$-équivariant $\mathrm{M}_U(G) \xrightarrow{\sim} \mathcal{A}_{U^*}(G)$.*

Depuis l'article de Gross [Gro99], les éléments de $\mathrm{M}_U(G)$ sont parfois appelés *formes modulaires algébriques* de poids U du $\mathbb{Z}$-groupe G ; nous n'utiliserons toutefois pas cette terminologie, qui rentre en conflit avec la notion d'algébricité introduite au §VIII.2.6. Par exemple, si $U = \mathbb{C}$ est la représentation triviale, le $\mathrm{H}(G)^{\mathrm{opp}}$-module $\mathrm{M}_{\mathbb{C}}(G)$ s'identifie canoniquement à l'espace des fonctions $\mathrm{Cl}(G) \to \mathbb{C}$, soit encore au dual du $\mathrm{H}(G)$-module $\mathbb{C}[\mathrm{Cl}(G)]$.

Terminons ces généralités par une assertion de compatibilité à certains morphismes de $\mathbb{Z}$-goupes. Soit $\mu : G \to G'$ un morphisme de $\mathbb{Z}$-groupes. Il induit de manière évidente un morphisme du $G(\mathbb{A}_f)$-ensemble $\mathcal{R}(G)$ vers le $G'(\mathbb{A}_f)$-ensemble $\mathcal{R}(G')$, noté (f_μ, g_μ), au sens du §2.12. On suppose que $f_\mu(G(\mathbb{A}_f))$ et distingué dans $G'(\mathbb{A}_f)$, que g_μ est injective, et que de plus l'action du groupe S défini *loc. cit.* sur $\mathcal{R}(G)$ est triviale. C'est par exemple trivialement le cas si μ est un isomorphisme. On dispose alors d'un homomorphisme injectif d'anneaux $\mathrm{H}(\mu) : \mathrm{H}(G) \to \mathrm{H}(G')$ défini *loc. cit.* Soit U' un $G'(\mathbb{Q})$-module, et soit U sa restriction à $G(\mathbb{Q})$. Le lemme suivant paraphrase le lemme 2.15.

Lemme 4.3. *Le morphisme* $\mu^* : \mathrm{M}_{U'}(G') \longrightarrow \mathrm{M}_U(G)$, $\varphi \mapsto (x \mapsto \varphi(g_\mu(x)))$, *satisfait* $T \circ \mu^* = \mu^* \circ \mathrm{H}(\mu)(T)$ *pour tout* $T \in \mathrm{H}(G')$.

4.4. Cas des groupes O_n et SO_n.

Spécifions maintenant cette construction au $\mathbb{Z}$-groupe orthogonal O_n du réseau unimodulaire pair $\mathrm{E}_n \subset \mathbb{R}^n$, pour $n \equiv 0 \bmod 8$ (§II.3, choisir un autre réseau conduirait à une théorie équivalente à celle qui suit).

Dans ce cas, nous avons vu au §1.2 que le $\mathrm{O}_n(\mathbb{A}_f)$-ensemble $\mathcal{R}(\mathrm{O}_n)$ s'identifie canoniquement à l'ensemble des réseaux unimodulaires pairs de $\mathbb{R}^n$ inclus dans $\mathrm{E}_n \otimes \mathbb{Q}$, puis que $\mathrm{Cl}(\mathrm{O}_n) \xrightarrow{\sim} \mathrm{X}_n$. En particulier,

$$\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n) = \mathbb{C}[\mathrm{X}_n]^*.$$

L'action à droite de $\mathrm{H}(\mathrm{O}_n)$ sur $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ définit par transposée une action à gauche de $\mathrm{H}(\mathrm{O}_n)$ sur $\mathbb{C}[\mathrm{X}_n]$. L'opérateur $\mathrm{T}_{\mathbb{Z}/d\mathbb{Z}} \in \mathrm{H}(\mathrm{O}_n)$ défini au §2.6, vu comme endomorphisme de $\mathbb{C}[\mathrm{X}_n]$, est notamment l'opérateur T_d du §III.2. La description de la structure du $\mathrm{H}(\mathrm{O}_n)^{\mathrm{opp}}$-module $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ quand $n \leq 24$ est donc le thème principal de ce mémoire.

L'anneau $\mathrm{H}(\mathrm{O}_n)$ est commutatif d'après la proposition §2.8. Fixons U une représentation (complexe, continue, de dimension finie) de $\mathrm{O}_n(\mathbb{R})$. D'après le lemme 4.2 et les résultats généraux rappelés au §3.1, l'action de $\mathrm{H}(\mathrm{O}_n)$ est donc co-diagonalisable sur chaque $\mathrm{M}_U(\mathrm{O}_n)$. Les valeurs propres de ces

opérateurs ont des significations arithmétiques importantes. Nous verrons au §VI.2.20 qu'elles sont en fait reliées, de manière assez surprenante *a priori*, aux représentations du groupe de Galois absolu de $\mathbb{Q}$. La droite des fonctions constantes dans $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ est par exemple trivialement stable par T_A pour tout A, la valeur propre de T_p sur cette droite étant bien sûr $\mathrm{c}_n(p)$ (Prop.-Déf. III.2.1). Nous donnerons des exemples nettement plus intéressants aux chapitres suivants.

Remarque 4.5. Soit $\mathcal{L}_n$ l'ensemble de tous les réseaux unimodulaires pairs de $\mathbb{R}^n$ déjà considéré dans l'introduction (§I). Il contient $\mathcal{R}(\mathrm{O}_n)$ et l'action naturelle de $\mathrm{O}_n(\mathbb{R})$ sur $\mathcal{L}_n$ prolonge l'action naturelle de $\mathrm{O}_n(\mathbb{Q})$ sur $\mathcal{R}(\mathrm{O}_n)$. L'application $\mathrm{O}_n(\mathbb{R}) \times \mathrm{O}_n(\mathbb{A}_f) \to \mathcal{L}_n$, $(g_\infty, g_f) \mapsto g_\infty^{-1}(g_f(\mathrm{E}_n))$, se factorise donc en une application

$$\mathrm{O}_n(\mathbb{Q})\backslash\mathrm{O}_n(\mathbb{A})/\mathrm{O}_n(\widehat{\mathbb{Z}}) \to \mathcal{L}_n.$$

C'est une bijection : la surjectivité se déduit du scholie II.2.1 et l'injectivité est immédiate.

Discutons maintenant du cas de SO_n. D'après la proposition 1.7 et le §2.11, l'inclusion $\mathrm{SO}_n \to \mathrm{O}_n$ induit une bijection $\mathcal{R}(\mathrm{SO}_n) \xrightarrow{\sim} \mathcal{R}(\mathrm{O}_n)$ et $\mathrm{H}(\mathrm{O}_n)$ est naturellement un sous-anneau de $\mathrm{H}(\mathrm{SO}_n)$. Soit U un $\mathrm{SO}_n(\mathbb{Q})$-module, et soit

$$U' = \mathrm{Ind}_{\mathrm{SO}_n(\mathbb{Q})}^{\mathrm{O}_n(\mathbb{Q})} U.$$

La propriété universelle des modules induits fournit un isomorphisme canonique $\mathrm{ind} : \mathrm{Hom}_{\mathbb{Z}[\mathrm{SO}_n(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)]_{|\mathrm{SO}_n(\mathbb{Q})}, U) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[\mathrm{O}_n(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)], U')$, qui s'écrit encore

$$\mathrm{ind} : \mathrm{M}_U(\mathrm{SO}_n) \xrightarrow{\sim} \mathrm{M}_{U'}(\mathrm{O}_n).$$

Cet isomorphisme est trivalement $\mathrm{H}(\mathrm{O}_n)$-équivariant, de sorte que l'étude des $\mathrm{H}(\mathrm{O}_n)$-modules $\mathrm{M}_U(\mathrm{SO}_n)$ se ramène à celle des $\mathrm{M}_W(\mathrm{O}_n)$ où W est un $\mathrm{O}_n(\mathbb{Q})$-module. Rajoutons que si U est la restriction à $\mathrm{SO}_n(\mathbb{Q})$ d'un $\mathrm{SO}_n(\mathbb{R})$-module V, et si V' désigne l'induite de V à $\mathrm{O}_n(\mathbb{R})$, alors $V'_{|\mathrm{O}_n(\mathbb{Q})} = \mathrm{Ind}_{\mathrm{SO}_n(\mathbb{Q})}^{\mathrm{O}_n(\mathbb{Q})} U$.

Supposons enfin que W est un $\mathrm{O}_n(\mathbb{Q})$-module et que W' désigne sa restriction à $\mathrm{SO}_n(\mathbb{Q})$. Le groupe $\mathrm{O}_n(\mathbb{Q})$ agit naturellement sur $\mathrm{M}_{W'}(\mathrm{SO}_n)$, par $(\gamma, f) \mapsto (x \mapsto \gamma(f(\gamma^{-1}(x))))$, le sous-groupe $\mathrm{SO}_n(\mathbb{Q})$ agissant trivialement. Soit $s \in \mathrm{End}(\mathrm{M}_{W'}(\mathrm{SO}_n))$ l'opérateur induit par l'élément non-trivial du quotient $\mathrm{O}_n(\mathbb{Q})/\mathrm{SO}_n(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. La restriction des fonctions par l'application bijective $\mathcal{R}(\mathrm{SO}_n) \to \mathcal{R}(\mathrm{O}_n)$ définit alors une injection $\mathrm{H}(\mathrm{O}_n)$-équivariante

$$\mathrm{res} : \mathrm{M}_W(\mathrm{O}_n) \to \mathrm{M}_{W'}(\mathrm{SO}_n)$$

dont l'image est $\mathrm{M}_{W'}(\mathrm{SO}_n)^{s=\mathrm{id}}$.

Exemple 4.6. L'isomorphisme ind induit une décomposition canonique

$$\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_n) \simeq \mathrm{M}_{\mathbb{C}}(\mathrm{O}_n) \oplus \mathrm{M}_{\text{dét}}(\mathrm{O}_n)$$

où dét est la représentation de dimension 1 donnée par le déterminant. Regardant également $\mathbb{C}$ comme restriction à $\mathrm{SO}_n(\mathbb{R})$ de la représentation triviale de $\mathrm{O}_n(\mathbb{R})$, cela munit $\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_n)$ d'une symétrie s qui préserve la décomposition ci-dessus, admettant pour points fixes $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$.

Nous renvoyons à [CR12, §2] pour une étude des espaces $\mathrm{M}_U(\mathrm{SO}_8)$ en fonction de la représentation U, notamment de leur dimension, ainsi qu'au §VII.4 pour des exemples.

4.7. Un produit scalaire hermitien invariant

Considérons le cas d'un $\mathbb{Z}$-groupe G général tel que $G(\mathbb{R})$ est compact. Soit U une représentation complexe, continue, de dimension finie, de $G(\mathbb{R})$. L'isomorphisme $\mathrm{M}_U(G) \xrightarrow{\sim} \mathcal{A}_{U^*}(G)$ munit par transport de structure $\mathrm{M}_U(G)$ d'un produit scalaire hermitien naturel, pour lequel l'action de $\mathrm{H}(G)$ est une $\star$-action, d'après le §3.1, et qu'il ne reste qu'à expliciter. Fixons pour cela un produit scalaire hermitien $G(\mathbb{R})$-invariant sur U, disons $\langle -, - \rangle_U$. Choisissons également des éléments $g_i \in G(\mathbb{A}_f)$ vérifiant l'égalité (3.2) ; on rappelle que $\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$ est un groupe fini.

Proposition 4.8. *Si $F, F' \in \mathrm{M}_U(G)$, $(F, F') = \sum_{i=1}^{\mathrm{h}(G)} \frac{1}{|\Gamma_i|} \langle F(g_i), F'(g_i) \rangle_U$ définit un produit scalaire hermitien sur $\mathrm{M}_U(G)$ indépendant du choix des g_i, et pour lequel l'action de $\mathrm{H}(G)$ est une $\star$-action.*

Par manque de référence adéquate nous donnons une démonstration.

Démonstration. Fixons $e \in U^*$ non nul. D'après l'isomorphisme (4.2) et le §IV.3

$$(F, F') := \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \overline{\varphi_F(e)} \varphi_{F'}(e) \, \mathrm{d}m$$

est un produit scalaire hermitien sur $\mathrm{M}_U(G)$ pour lequel l'action de $\mathrm{H}(G)$ est une $\star$-action. Nous allons vérifier qu'il est proportionnel à celui de l'énoncé.

Soient $\Omega_i \subset G(\mathbb{A})$ l'ouvert compact $g_i(G(\mathbb{R}) \times G(\widehat{\mathbb{Z}}))$, $\pi : G(\mathbb{A}) \to G(\mathbb{Q})\backslash G(\mathbb{A})$ la projection canonique, et $\overline{\Omega_i} = \pi(\Omega_i)$. Par définition, $G(\mathbb{Q})\backslash G(\mathbb{A})$ est réunion disjointe (finie) des $\overline{\Omega_i}$. Vérifions d'abord qu'il existe une mesure de Haar m sur $G(\mathbb{A})$ telle que pour toute fonction continue ψ sur (le compact) $G(\mathbb{Q})\backslash G(\mathbb{A})$, on ait la formule

$$\int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \psi \, \mathrm{d}\mu = \sum_{i=1}^{\mathrm{h}(G)} \frac{1}{|\Gamma_i|} \int_{\Omega_i} \psi \circ \pi \; \mathrm{d}m. \tag{4.2}$$

En effet, rappelons que si f est continue à support compact sur $G(\mathbb{A})$, alors $\tilde{f}(g) := \sum_{\gamma \in G(\mathbb{Q})} f(\gamma g)$ est continue à support compact sur $G(\mathbb{Q})\backslash G(\mathbb{A})$. De plus, par la propriété caractéristique de la mesure quotient μ il existe une unique mesure de Haar m sur $G(\mathbb{A})$ telle que pour toute fonction continue à support compact f sur $G(\mathbb{A})$ alors $\int_{G(\mathbb{A})} f \,\mathrm{d}m = \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \tilde{f} \,\mathrm{d}\mu$ (voir [Wei40, Chap. II]).

Si $g \in G(\mathbb{A})$ posons $n_i(g) = |G(\mathbb{Q})g \cap \Omega_i|$. On a clairement $n_i(\gamma g k) = n_i(g)$ pour tout $\gamma \in G(\mathbb{Q})$ et tout $k \in 1 \times G(\widehat{\mathbb{Z}})$. Par définition, on a également $n_i(g_j) = |\Gamma_i|\delta_{i,j}$, la notation $\delta_{i,j}$ désignant le symbole de Kronecker. Soit ψ une fonction continue sur $G(\mathbb{Q})\backslash G(\mathbb{A})$. La fonction $f_i = 1_{\Omega_i} \times \psi \circ \pi$, $G(\mathbb{A}) \to \mathbb{C}$, est continue à support dans Ω_i, et satisfait $\tilde{f}_i(g) = \psi(\pi(g))\, n_i(g)$ pour tout $g \in G(\mathbb{A})$ (nous notons 1_A la fonction caractéristique de l'ensemble A). Autrement dit, on a $\psi \times 1_{\overline{\Omega_i}} = \frac{1}{|\Gamma_i|}\tilde{f}_i$. Cela démontre la formule (4.2).

Appliquons cette formule à la fonction $\psi = \overline{\varphi_F(e)}\, \varphi_{F'}(e)$. Observons que si $U = \mathbb{C}$, de sorte que ψ est constante égale à $|e(1)|^2 \overline{F(g_i)} F'(g_i)$ sur Ω_i, la proposition résulte de ce que $m(\Omega_i) = m(G(\mathbb{R}) \times G(\mathbb{Z}))$ est indépendant de i. En général, introduisons $\mathrm{d}g$ la mesure de Haar sur $G(\mathbb{R})$ de masse totale 1, et m_f la mesure de Haar sur $G(\mathbb{A}_f)$ telle que $\mathrm{d}m = \mathrm{d}g \times \mathrm{d}m_f$. L'invariance de ψ à droite par $1 \times G(\widehat{\mathbb{Z}})$ et le théorème de Fubini entraînent

$$\int_{\Omega_i} \psi \circ \pi \;\mathrm{d}m = m_f(G(\widehat{\mathbb{Z}})) \int_{G(\mathbb{R})} \overline{\langle e, g^{-1}F(g_i)\rangle} \langle e, g^{-1}F'(g_i)\rangle \,\mathrm{d}g.$$

Soit $E \in U$ tel que $\langle E, x\rangle_U = \langle e, x\rangle$ pour tout $x \in U$. Les relations d'orthogonalité des coefficients matriciels pour les représentations irréductibles des groupes compacts montrent

$$\int_{G(\mathbb{R})} \overline{\langle e, g^{-1}F(g_i)\rangle}\, \langle e, g^{-1}F'(g_i)\rangle \,\mathrm{d}m_\infty = \frac{1}{\dim U} \langle E, E\rangle_U \langle F(g_i), F'(g_i)\rangle_U,$$

ce qui conclut la démonstration de la proposition. □

Supposons par exemple $G = \mathrm{O}_n$ et $U = \mathbb{C}$. Si $L_i \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(\mathrm{E}_n \otimes \mathbb{Q})$ désigne le réseau $g_i(L)$, on a $\Gamma_i = \mathrm{O}(L_i) \subset \mathrm{O}_n(\mathbb{Q})$. La relation $\mathrm{T}_A = \mathrm{T}^{\mathrm{t}}_A$ de la proposition 2.8 et la proposition précédente s'écrivent alors

$$\mathrm{N}_A(L, M)|\mathrm{O}(M)| = \mathrm{N}_A(M, L)|\mathrm{O}(L)|,$$

où $\mathrm{N}_A(L, M)$ désigne le nombre des A-voisins de L isométriques à M (avec $L, M \in \mathcal{R}(\mathrm{O}_n)$). C'est la généralisation que nous avions promise de la proposition III.2.3.

Corollaire 4.9. *La forme bilinéaire sur* $\mathrm{M}_{U^*}(G) \times \mathrm{M}_U(G)$ *définie par*

$$(F, F') = \sum_i \frac{1}{|\Gamma_i|} \langle F(g_i), F'(g_i) \rangle$$

est indépendante du choix des g_i*, et non-dégénérée. Elle satisfait l'identité* $(T(F), F') = (F, T^{\mathrm{t}}(F'))$ *pour tous* $T \in \mathrm{H}(G)$*,* $F \in \mathrm{M}_{U^*}(G)$ *et* $F' \in \mathrm{M}_U(G)$*. En particulier, elle définit un isomorphisme canonique entre le* $\mathrm{H}(G)$*-module* $\mathrm{M}_{U^*}(G)^*$ *et le* $\mathrm{H}(G)$*-module* $\mathrm{M}_U(G)^{\mathrm{t}}$ *(voir la remarque 2.4).*

Démonstration. Si V est un $\mathbb{C}$-espace vectoriel, on note $\overline{V}$ le $\mathbb{C}$-espace vectoriel conjugué (à savoir le groupe abélien V muni de l'action de $\mathbb{C}$ définie par $(\lambda, v) \mapsto \overline{\lambda} v$, $\mathbb{C} \times V \to V$). Si U est comme dans l'énoncé, $\overline{U}$ est une représentation de $G(\mathbb{R})$ de manière naturelle, et l'application $v \mapsto (u \mapsto \langle v, u \rangle_U)$ induit un isomorphisme de représentations $\overline{U} \xrightarrow{\sim} U^*$. On dispose donc d'un isomorphisme naturel $\mathrm{M}_{U^*}(G) \xrightarrow{\sim} \mathrm{M}_{\overline{U}}(G) = \overline{\mathrm{M}_U(G)}$. Via cet isomorphisme, la forme bilinéaire de l'énoncé coïncide avec la forme $\overline{\mathrm{M}_U(G)} \times \mathrm{M}_U(G) \to \mathbb{C}$, $(F, F') \mapsto \sum_i \frac{1}{|\Gamma_i|} \langle F(g_i), F'(g_i) \rangle_U$, qui n'est autre que la forme hermitienne sur $\mathrm{M}_U(G)$ donnée par la proposition 4.8. On en déduit les deux premières assertions, la dernière étant alors évidente. $\square$

Terminons par une dernière observation. Si $L \in \mathcal{R}(G)$ et $u \in U$, l'application $F \mapsto \langle F(L), u \rangle$ est une forme linéaire sur $\mathrm{M}_{U^*}(G)$, notée $\mathrm{ev}_{L,u}$. On dispose d'une unique application linéaire

$$\mathbb{Z}[\mathcal{R}(G)] \otimes U \longrightarrow \mathrm{M}_{U^*}(G)^*$$

envoyant $[L] \otimes u$ sur $\mathrm{ev}_{L,u}$ pour tout $L \in \mathcal{R}(G)$ et tout $u \in U$. Le $\mathbb{C}$-espace vectoriel $\mathbb{Z}[\mathcal{R}(G)] \otimes U$ est muni d'une action diagonale de $G(\mathbb{Q})$, et l'application ci-dessus est constante sur les orbites de cette action. Elle se factorise donc en une application linéaire

$$(\mathbb{Z}[\mathcal{R}(G)] \otimes U)_{G(\mathbb{Q})} \to \mathrm{M}_{U^*}(G)^*, \tag{4.3}$$

la notation V_Γ désignant les co-invariants du Γ-module V. C'est un isomorphisme : cela se déduit en effet simplement de la finitude de $G(\mathbb{Q}) \backslash \mathcal{R}(G)$ et de l'isomorphisme naturel $(U^*)^\Gamma \xrightarrow{\sim} (U_\Gamma)^*$, valable pour tout sous-groupe fini Γ de $G(\mathbb{R})$. L'isomorphisme (4.3) commute trivialement aux actions naturelles (à gauche) de $\mathrm{H}(G)$. Si on le compose avec l'isomorphisme $\mathrm{M}_{U^*}(G)^* \longrightarrow \mathrm{M}_U(G)^{\mathrm{t}}$ donné par le corollaire précédent, on en déduit un isomorphisme canonique de $\mathrm{H}(G)$-modules

$$(\mathbb{Z}[\mathcal{R}(G)] \otimes U)_{G(\mathbb{Q})} \xrightarrow{\sim} \mathrm{M}_U(G)^{\mathrm{t}}. \tag{4.4}$$

Il envoit (la classe de) l'élément $[L] \otimes u$ sur un élément de $\mathrm{M}_U(G)$ que nous noterons $[L, u]$. Concrètement, $[L, u]$ est l'unique fonction $F \in \mathrm{M}_U(G)$ nulle hors de $G(\mathbb{Q}) \cdot L$ telle que $F(L) = \sum_{\gamma \in \Gamma} \gamma(u)$, où $\Gamma = G(\mathbb{Q})_L$ est le stabilisateur de L dans $G(\mathbb{Q})$. L'isomorphisme (4.4) jouera un (petit) rôle dans les considérations de séries thêta au §V.4.1 et au chapitre VII.

5. Formes modulaires de Siegel

Commençons par quelques rappels sur les formes modulaires de Siegel (voir [SCA53], [SCA57], [Fre83], [And87]). Nous suivrons de près l'exposition de van der Geer [vdG08], à laquelle nous renvoyons notamment pour un historique du sujet.

5.1. Point de vue classique

Soit $g \geq 1$ un entier. Si R est un anneau nous noterons $\mathrm{Mat}_g(R)$ l'ensemble des matrices de taille $g \times g$ à coefficients dans R, et $\mathrm{Sym}_g(R) \subset \mathrm{Mat}_g(R)$ le sous-ensemble des matrices symétriques. On note 1_g la matrice identité dans $\mathrm{Mat}_g(R)$ et on désigne par $\mathrm{J}_{2g} \in \mathrm{Mat}_{2g}(R)$ l'élément

$$\mathrm{J}_{2g} = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}.$$

Le demi-espace de Siegel de genre g est l'ouvert

$$\mathbb{H}_g \subset \mathrm{Sym}_g(\mathbb{C})$$

des matrices dont la partie imaginaire est définie positive. Le $\mathbb{Z}$-groupe GSp_{2g} sera vu comme le sous-schéma en groupes de GL_{2g} constitué des γ tels que $\gamma\, \mathrm{J}_{2g}\, {}^{\mathrm{t}}\gamma = \nu(\gamma)\mathrm{J}_{2g}$; le morphisme $\nu : \mathrm{GSp}_{2g} \to \mathbb{G}_m$ désignant le facteur de similitude. Ses éléments sont de la forme

$$\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$$

avec $a_\gamma, b_\gamma, c_\gamma, d_\gamma \in \mathrm{Mat}_g$ satisfaisant les relations $a_\gamma\, {}^{\mathrm{t}}b_\gamma = b_\gamma\, {}^{\mathrm{t}}a_\gamma$, $c_\gamma\, {}^{\mathrm{t}}d_\gamma = d_\gamma\, {}^{\mathrm{t}}c_\gamma$ et $a_\gamma\, {}^{\mathrm{t}}d_\gamma - b_\gamma\, {}^{\mathrm{t}}c_\gamma = \nu(\gamma)1_g$.

Soit $\mathrm{GSp}_{2g}(\mathbb{R})^+$ le sous-groupe de $\mathrm{GSp}_{2g}(\mathbb{R})$ constitué des éléments de facteur de similitude > 0. Si $\gamma \in \mathrm{GSp}_{2g}(\mathbb{R})^+$ et $\tau \in \mathbb{H}_g$, on vérifie que l'élément $\mathrm{j}(\gamma, \tau) := c_\gamma \tau + d_\gamma$ est dans $\mathrm{GL}_g(\mathbb{C})$ et que

$$(\gamma, \tau) \mapsto \gamma\tau = (a_\gamma \tau + b_\gamma)(c_\gamma \tau + d_\gamma)^{-1}$$

définit une action transitive de $\mathrm{GSp}_{2g}(\mathbb{R})^+$ sur $\mathbb{H}_g$ par transformations biholomorphes. De plus, on vérifie la relation de 1-cocyle $\mathrm{j}(\gamma\gamma', \tau) = \mathrm{j}(\gamma, \gamma'\tau)\mathrm{j}(\gamma', \tau)$ pour tous $\gamma, \gamma' \in \mathrm{GSp}_{2g}(\mathbb{R})^+$ et tout $\tau \in \mathbb{H}_g$.

Soit W un $\mathbb{C}$-espace vectoriel de dimension finie muni d'une $\mathbb{C}$-représentation $\rho : \mathrm{GL}_g \to \mathrm{GL}_W$. Une *forme modulaire de Siegel de poids W et de genre $g \geq 1$* est une fonction holomorphe $f : \mathbb{H}_g \to W$ telle que

$$f(\gamma\tau) = \rho(\,\mathrm{j}(\gamma, \tau)\,) \cdot f(\tau), \ \forall \tau \in \mathbb{H}_g, \ \ \forall \gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}).$$

Lorsque $g = 1$ on rajoute l'hypothèse que f est bornée sur $\{\tau \in \mathbb{H}_1, \mathrm{Im}(\tau) > 1\}$. Elles forment un $\mathbb{C}$-espace vectoriel noté

$$\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})),$$

dont la dimension est finie d'après Siegel.

Lorsque $(\rho, W) = (\text{dét}^k, \mathbb{C})$ pour $k \in \mathbb{Z}$, on parle de *formes de Siegel classiques*, ou scalaires, de poids k, et par opposition de formes à valeurs vectorielles sinon. Dans ce cas, on note aussi $\mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ l'espace $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$. Quand $g = 1$, on retrouve comme cas particulier les formes modulaires usuelles pour le groupe $\mathrm{SL}_2(\mathbb{Z})$ qui sont par exemple traitées en détail dans le cours d'arithmétique de Serre [Ser70]. Observons enfin que la présence de l'élément $-1_{2g} \in \mathrm{Sp}_{2g}(\mathbb{Z})$, et la relation $\mathrm{j}(-1_{2g}, \tau) = -1_g$, entraînent $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ si $\rho(-1_g) = -\mathrm{id}_W$.

Terminons cette section par une reformulation de la notion de forme modulaire de Siegel. Supposons que la représentation (ρ, W) est irréductible, ou plus généralement qu'il existe un élément $\mathrm{m}_W \in \mathbb{Z}$, nécessairement unique, tel que $\rho(z1_g) = z^{\mathrm{m}_W}\,\mathrm{id}_W$ pour tout $z \in \mathbb{C}^\times$. Si f est une application $\mathbb{H}_g \to W$, on pose

$$f_{|W}\gamma : \mathbb{H}_g \to W, \quad \tau \mapsto \nu(\gamma)^{\mathrm{m}_W/2}\ \rho(\mathrm{j}(\gamma, \tau))^{-1}\ f(\gamma\tau).$$

L'application $(\gamma, f) \mapsto f_{|W}\gamma$ définit une action à droite du groupe $\mathrm{GSp}_{2g}(\mathbb{R})^+$ sur l'espace des fonctions holomorphes $\mathbb{H}_g \to W$; par construction, cette action est triviale sur le sous-groupe des homothéties de rapport > 0 dans $\mathrm{GSp}_{2g}(\mathbb{R})^+$. Une *forme modulaire de Siegel de poids W et de genre $g \geq 2$* est par définition un élément $\mathrm{Sp}_{2g}(\mathbb{Z})$-invariant pour cette action.

5.2. Développements de Fourier et formes paraboliques

Si $n \in \mathrm{Sym}_g(\mathbb{C})$, on pose

$$q^n = e^{2i\pi\,\mathrm{tr}(n\,\tau)} = \prod_{1 \leq i,j \leq g} e^{2i\pi\, n_{i,j}\tau_{i,j}},$$

c'est une fonction homolorphe sur $\mathbb{H}_g$. Si n est *demi-entier*, c'est-à-dire si $n \in \frac{1}{2}\mathrm{Sym}_g(\mathbb{Z})$ et si $n_{i,i} \in \mathbb{Z}$ pour tout $i = 1, \ldots, g$, alors q^n est invariante par translations par $\mathrm{Sym}_g(\mathbb{Z})$. On montre que chaque $f \in \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ admet un développement de Fourier, normalement convergent sur tout compact de $\mathbb{H}_g$, de la forme

$$f = \sum_{n \geq 0} a_n q^n$$

où $n \in \frac{1}{2}\mathrm{Sym}_g(\mathbb{Z})$ parcourt les éléments positifs (au sens des matrices symétriques réelles) demi-entiers, et où les a_n sont dans W [VDG08, §4]. Pour $g \geq 2$, l'opérateur de Siegel est l'application

$$\Phi_g : \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \longrightarrow \mathrm{M}_{W'}(\mathrm{Sp}_{2g-2}(\mathbb{Z}))$$

définie par $\Phi_g(\sum_n a_n q^n) = \sum_{n'} a_{n'} q^{n'}$, où l'on voit $\mathrm{Sym}_{g-1}(-)$ comme sous-ensemble de $\mathrm{Sym}_g(-)$ de dernière ligne et colonne nulles, et $W' = W_{|\mathrm{GL}_{g-1} \times 1}$ [VDG08, §5]. Le sous-espace des formes paraboliques est

$$\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) := \mathrm{Ker}(\Phi_g) \subset \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})).$$

Une forme de Siegel est donc parabolique si son développement de Fourier $\sum_n a_n q^n$ satisfait $a_n = 0$ pour tout n tel que $\mathrm{dét}(n) = 0$. Quand $(W, \rho) = (\mathbb{C}, \mathrm{dét}^k)$ pour $k \in \mathbb{Z}$, on note $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ pour $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$.

5.3. Relation entre $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ et $\mathcal{A}^2(\mathrm{PGSp}_{2g})$

Nous allons maintenant rappeler le lien classique entre $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ et l'espace $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$. Une référence récente agréable sur ce point est l'article [AS01] auquel nous renverrons dès qu'il sera possible de formuler l'énoncé principal (voir aussi [TAI14, §5]).

On pose $G = \mathrm{PGSp}_{2g}$. Le facteur de similitude $\nu : \mathrm{GSp}_{2g} \to \mathbb{G}_m$ induit un homomorphisme $\nu_\infty : G(\mathbb{R}) \to \mathbb{R}^\times/\mathbb{R}^\times_{>0}$ dont nous noterons $G(\mathbb{R})^+$ le noyau. Le morphisme canonique $\mathrm{Sp}_{2g}(\mathbb{R}) \to G(\mathbb{R})$ induit un isomorphisme

$$\mathrm{Sp}_{2g}(\mathbb{R})/\{\pm 1\} \xrightarrow{\sim} G(\mathbb{R})^+.$$

On pose également $G(A)^+ = G(A) \cap G(\mathbb{R})^+$ si A est un sous-anneau de $\mathbb{R}$.

D'après le §1.2 on a $\mathrm{h}(G) = 1$. Comme $\nu_\infty(G(\mathbb{Z})) = \{\pm 1\}$ on en déduit

$$G(\mathbb{A}) = G(\mathbb{Q})(G(\mathbb{R})^+ \times G(\widehat{\mathbb{Z}})) \tag{5.1}$$

et suivant (3.3) que la restriction $f \mapsto f_{|G^+(\mathbb{R})\times 1}$ induit un isomorphisme $G(\mathbb{R})^+$-équivariant

$$\mathcal{A}^2(\mathrm{PGSp}_{2g}) \xrightarrow{\sim} \mathrm{L}^2(G(\mathbb{Z})^+\backslash G(\mathbb{R})^+). \tag{5.2}$$

L'action de $\mathrm{GSp}_{2g}(\mathbb{R})^+$ sur $\mathbb{H}_g$ rappelée au §5.1 se factorise en une action de $G(\mathbb{R})^+$. Cette dernière est fidèle, transitive, et ses stabilisateurs sont les sous-groupes compacts maximaux de $G(\mathbb{R})^+$. Si K désigne le stabilisateur dans $\mathrm{Sp}_{2g}(\mathbb{R})$ de l'élément $i1_g \in \mathbb{H}_g$, et si K^+ désigne son image dans $G(\mathbb{R})^+$, on a donc une identification naturelle

$$G(\mathbb{R})^+/K^+ \xrightarrow{\sim} \mathbb{H}_g.$$

Soit (ρ, W) une $\mathbb{C}$-représentation de GL_g comme au §5.1, supposée maintenant irréductible et telle que $\mathrm{m}_W \equiv 0 \bmod 2$. Fixons $w \in W^*$ et $f \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, nous allons leur associer une fonction $\varphi_{w,f} \in \mathcal{A}^2(G)$. Observons la fonction $\varphi : G(\mathbb{R})^+ \longrightarrow \mathbb{C}$ définie par

$$\varphi(\gamma) = \langle w, (f_{|W}\gamma)(i1_g)\,\rangle.$$

Par construction, φ est continue et invariante à gauche par $G(\mathbb{Z})^+$, c'est donc la restriction à $G(\mathbb{R})^+ \times 1$ d'une unique fonction continue $\varphi' : G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$, invariante par translations à droite par $G(\widehat{\mathbb{Z}})$, d'après la formule (5.1). On pose alors

$$\varphi_{w,f} := \varphi'.$$

D'après [AS01, Lemma 5], on a $\varphi_{w,f} \in \mathcal{A}_{\mathrm{cusp}}(G)$.

Avant d'énoncer la proposition finale, il nous faut encore définir la notion d'élément holomorphe de $\mathcal{A}^2(G)$. Soient $\mathfrak{g}$ et $\mathfrak{k}$ les algèbres de Lie respectives de $G(\mathbb{R})^+$ et K, et soit $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ la décomposition de Cartan associée. Soit $d : \mathfrak{g} \to \mathrm{T}_{i1_g}$ la différentielle en l'identité de l'application $G(\mathbb{R})^+ \to \mathbb{H}_g$, $h \mapsto h(i1_g)$. Elle induit un isomorphisme $\mathbb{R}$-linéaire

$$\mathfrak{p} \xrightarrow{\sim} \mathrm{T}_{i1_g} = \mathrm{Sym}_g(\mathbb{C}).$$

La structure de $\mathbb{C}$-espace vectoriel de $\mathrm{Sym}_g(\mathbb{C})$ munit donc $\mathfrak{p}$ d'une structure de $\mathbb{C}$-espace vectoriel qui décompose $\mathfrak{p} \otimes_{\mathbb{R}} \mathbb{C}$ en $\mathfrak{p}^+ \oplus \mathfrak{p}^-$ de sorte que d induise un isomorphisme $\mathbb{C}$-linéaire $\mathfrak{p}^+ \xrightarrow{\sim} \mathrm{T}_{i1_g}$. Un élément $f \in \mathcal{A}^2(G)$ sera dit *holomorphe* s'il est continu et si pour tout $g \in G(\mathbb{A})$ la fonction $G(\mathbb{R}) \to \mathbb{C}, h \mapsto f(gh)$, est infiniment différentiable et annulée par $\mathfrak{p}^-$.

Proposition 5.4. *L'application $(w, f) \mapsto \varphi_{w,f}$ définit une injection $\mathbb{C}[K]$-linéaire*

$$W^* \otimes \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \longrightarrow \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$$

dont l'image est l'ensemble des $f \in \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$ qui sont holomorphes et W^*-isotypiques sous l'action de K.

Précisons cet énoncé. L'application $h \mapsto \mathrm{j}(h, i1_g)$ est un morphisme de groupes $K \to \mathrm{GL}_g(\mathbb{C})$, qui réalise $\mathrm{GL}_g(\mathbb{C})$ comme complexification du groupe unitaire compact K. Cela permet notamment de voir W comme une représentation de K par restriction, qui est irréductible car W l'est comme représentation de GL_g. Nous renvoyons à [AS01, Thm. 1, §4.5] pour une démonstration de cette proposition, à l'assertion de surjectivité près, qui est vérifiée dans [Tai14, §5.2].

5.5. Action des opérateurs de Hecke

Il résulte de la proposition 5.4 que l'image de l'application de cet énoncé est stable sous l'action $\mathrm{H}(\mathrm{PGSp}_{2g})$, de sorte que l'espace $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ hérite de $\mathcal{A}^2(\mathrm{PGSp}_{2g})$ une action de $\mathrm{H}(\mathrm{PGSp}_{2g})$. À des constantes de normalisation près éventuellement introduites suivant les auteurs pour des raisons d'intégralité, cette action coïncide avec l'action définie traditionnellement sur $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, et même sur $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, que nous rappelons ci-dessous (voir aussi [Fre83, Kap. IV], [vdG08, §16] et [AS01, §4.3]). Sans rentrer dans les détails, mentionnons qu'elle est particulièrement naturelle lorsque l'on voit $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ comme l'espace des variétés abéliennes complexes de dimension g munies d'une polarisation principale[7] [vdG08, §10].

Soient (W, ρ) une $\mathbb{C}$-représentation irréductible de GL_g, p un nombre premier, et G le $\mathbb{Z}$-groupe PGSp_{2g}. L'application naturelle

$$a : G(\mathbb{Z}[\frac{1}{p}])^+/G(\mathbb{Z})^+ \to G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$$

est bijective puisque $\mathrm{h}(G) = 1$ (Corollaire 1.5) et $\nu_\infty(G(\mathbb{Z})) = \{\pm 1\}$ (§5.3). Elle induit donc de manière évidente un homomorphisme injectif entre l'anneau $\mathrm{H}_p(G)$ et l'anneau de Hecke du $G(\mathbb{Z}[\frac{1}{p}])^+$-ensemble $G(\mathbb{Z}[\frac{1}{p}])^+/G(\mathbb{Z})^+$. Cet homomorphisme est un isomorphisme ; en effet, cela suit de l'isomorphisme (2.1) et de ce que a induit également une bijection

$$G(\mathbb{Z})^+\backslash G(\mathbb{Z}[\frac{1}{p}])^+/G(\mathbb{Z})^+ \to G(\mathbb{Z}_p)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p), \tag{5.3}$$

comme le montre la théorie des diviseurs élémentaires (Propositions 2.7 et 2.9, voir également le §VI.2.5).

7. Une polarisation principale sur un réseau $L \subset \mathbb{C}^g$ est la donnée d'une forme bilinéaire alternée non-dégénérée $\eta : L \times L \to \mathbb{Z}$ dont l'extension des scalaires $\eta_\mathbb{R}$ à $L \otimes \mathbb{R} = \mathbb{C}^g$ satisfait $\eta_\mathbb{R}(ix, iy) = \eta_\mathbb{R}(x, y)$ pour tout $x, y \in \mathbb{C}^g$, et telle que la forme hermitienne associée $(x, y) \mapsto \eta_\mathbb{R}(ix, y) + i\eta_\mathbb{R}(x, y)$ sur $\mathbb{C}^g$ est définie positive. La théorie de Riemann permet d'identifier naturellement $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ à l'ensemble des $\mathrm{GL}_g(\mathbb{C})$-orbites de couples (L, η) où $L \subset \mathbb{C}^g$ est un réseau et η est une polarisation principale sur L.

Supposons que l'élément $T \in \mathrm{H}_p(G)$ ait pour matrice la fonction caractéristique de la double classe $G(\mathbb{Z}_p)\gamma G(\mathbb{Z}_p)$ avec $\gamma \in G(\mathbb{Z}[\frac{1}{p}])^+$, au sens de l'identification (2.2). Si l'on écrit

$$G(\mathbb{Z})^+ \, \gamma \, G(\mathbb{Z})^+ = \coprod_i \gamma_i \, G(\mathbb{Z})^+,$$

on constate immédiatement à l'aide de la formule (2.3) que le diagramme suivant est commutatif

$$\begin{tikzcd} \mathrm{S}_W(\mathrm{Sp}_{2g}) \arrow[r] \arrow[d, "f \mapsto \sum_i f_{|W} \gamma_i^{-1}"'] & \mathrm{Hom}_K(W, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})) \arrow[d, "T"] \\ \mathrm{S}_W(\mathrm{Sp}_{2g}) \arrow[r] & \mathrm{Hom}_K(W, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})) \end{tikzcd} \tag{5.4}$$

les applications verticales étant celles définies par la proposition 5.4 (voir [AS01, Lemma 9] pour le détail de l'argument). Étant donné l'égalité $T = T^{\mathrm{t}}$ pour tout $T \in \mathrm{H}(G)$, il ne sera d'ailleurs pas nécessaire de se souvenir de l'inversion des γ_i dans la formule ci-dessus.

La formule (5.4) permet de déterminer le lien exact entre les opérateurs de Hecke considérés ici et diverses définitions que l'on retrouve dans la littérature. Nous nous contenterons dans ce qui suit de donner le dictionnaire avec les définitions de Serre [Ser70, Ch. VII §2, §5] dans le cas $g = 1$. Des cas particuliers en genre $g = 2$ seront abordés au chapitre IX.

Soit $k \geq 0$ un entier pair. Serre définit dans [Ser70, Ch. VII §5.3] pour tout entier $n \geq 1$ un endomorphisme de $\mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ qu'il note $\mathrm{T}(n)$, et dont il détermine l'effet sur les q-développements. On dispose également d'un autre endomorphisme donné par l'opération définie ci-dessus de l'opérateur $\mathrm{T}_A \in \mathrm{H}(\mathrm{PGL}_2)$ défini au §2.6, où A est un groupe cyclique. La traduction est alors :

$$n^{-\frac{k-1}{2}} \mathrm{T}(n) = n^{-\frac{1}{2}} \sum_{d^2 | n} \mathrm{T}_{\mathbb{Z}/\frac{n}{d^2}\mathbb{Z}}. \tag{5.5}$$

Cela vient notamment du fait que la correspondance $\mathrm{T}(n)$ chez Serre associe à un réseau l'ensemble de ses sous-groupes d'indice n, plutôt que ceux de quotient $\mathbb{Z}/n\mathbb{Z}$.

5.6. $\mathcal{A}_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ se déduit de $\mathcal{A}_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$

Observons que le morphisme $\mathrm{Sp}_{2g}(\mathbb{A}) \to \mathrm{PGSp}_{2g}(\mathbb{A})$ induit, par restriction des fonctions, un isomorphisme

$$\mathrm{Res} : \mathcal{A}^2(\mathrm{PGSp}_{2g}) \xrightarrow{\sim} \mathcal{A}^2(\mathrm{Sp}_{2g}).$$

Cela se déduit en effet de la formule (3.3), sachant que

$$\mathrm{h}(\mathrm{Sp}_{2g}) = \mathrm{h}(\mathrm{PGSp}_{2g}) = 1$$

et que l'homomorphisme naturel $\mathrm{Sp}_{2g}(\mathbb{R}) \to \mathrm{PGSp}_{2g}(\mathbb{R})$ induit un homéomorphisme $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathrm{Sp}_{2g}(\mathbb{R}) \xrightarrow{\sim} \mathrm{PGSp}_{2g}(\mathbb{Z})\backslash\mathrm{PGSp}_{2g}(\mathbb{R})$.

On rappelle que nous avons défini au §2.6 un morphisme d'anneaux injectif $\mathrm{H}(\mathrm{Sp}_{2g}) \to \mathrm{H}(\mathrm{PGSp}_{2g})$, que l'on verra désormais par un léger abus de langage comme une inclusion. La source et le but du morphisme Res sont donc tous deux des $\mathrm{H}(\mathrm{Sp}_{2g})$-modules.

Proposition 5.7. *L'application* Res *commute aux actions de* $\mathrm{Sp}_{2g}(\mathbb{R})$ *et de* $\mathrm{H}(\mathrm{Sp}_{2g})$. *Elle envoie* $\mathcal{A}^2_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$ *sur* $\mathcal{A}^2_{\mathrm{disc}}(\mathrm{Sp}_{2g})$.

Démonstration. La première assertion est évidente et la seconde découle du lemme 2.15. La dernière est conséquence de la première et de ce que l'image de $\mathrm{Sp}_{2g}(\mathbb{R})$ dans $\mathrm{PGSp}_{2g}(\mathbb{R})$ est d'indice fini (égal à 2). □

V. Séries thêta et réseaux unimodulaires pairs

1. Séries thêta de Siegel

Soient $L \subset \mathbb{R}^n$ un réseau unimodulaire pair et $g \geq 1$ un entier. Si v est un g-uple d'éléments de L, c'est-à-dire $v = (v_i) \in L^g$, nous notons $v.v := (v_i \cdot v_j)_{i,j} \in \mathrm{Sym}_g(\mathbb{Z})$ la matrice de Gram associée ; elle est positive et $\frac{v.v}{2}$ est demi-entière au sens du §IV.5.2. La *série thêta de Siegel de genre g de L* est la fonction holomorphe sur $\mathbb{H}_g$:

$$\vartheta_g(L) = \sum_{v \in L^g} q^{\frac{v.v}{2}}.$$

Elle ne dépend que de la classe d'isométrie de L. Son développement de Fourier s'écrit $\sum_{n \geq 0} a_n q^n$ où a_n est le nombre de g-uples d'éléments de L de matrice de Gram n. Quand $g = 1$, on retrouve bien entendu les séries thêta classiques, traitées dans [Ser70], a_n étant simplement le nombre des $x \in L$ tels que $x \cdot x = 2n$. Siegel a démontré

$$\vartheta_g(L) \in \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$$

[Fre83, Kap. I §0]. Soit X_n l'ensemble des classes d'isométrie de réseaux unimodulaires pairs dans $\mathbb{R}^n$ déjà introduit dans l'introduction. Il est avantageux de linéariser la construction ci-dessus en considérant l'application linéaire

$$\vartheta_g : \mathbb{C}[\mathrm{X}_n] \longrightarrow \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z})), \quad [L] \mapsto \vartheta_g(L).$$

De plus, on note $\vartheta_0 : \mathbb{C}[\mathrm{X}_n] \to \mathbb{C}$ l'application linéaire envoyant $[L]$ sur 1 pour tout L. Rappelons que l'espace $\mathbb{C}[\mathrm{X}_n]$ s'identifie canoniquement au dual de l'espace de formes modulaires algébriques $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ (§IV.4.4). Il est donc muni d'une action (à gauche) de l'anneau $\mathrm{H}(\mathrm{O}_n)$, par transposition.

Dans le but de comprendre le $\mathrm{H}(\mathrm{O}_n)^{\mathrm{opp}}$-module $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$, un fait important est que l'application ϑ_g entrelace l'action de $\mathrm{H}(\mathrm{O}_n)$ sur $\mathbb{C}[\mathrm{X}_n]$ et celle de $\mathrm{H}(\mathrm{Sp}_{2g}) \subset \mathrm{H}(\mathrm{PGSp}_{2g})$ (§IV.5.3), et ce selon des recettes bien précises. Ces relations ont été découvertes par Eichler dans des cas particuliers quand

$g = 1$ [Eic52, Satz 21.3] [Ral79] et sont appelées depuis *relations de commutation d'Eichler*. Elles entraînent en particulier que le noyau de ϑ_g est stable par l'action de $\mathrm{H}(\mathrm{O}_n)$. Le cas du genre g quelconque a été étudié sous divers aspects par de nombreux auteurs depuis Eichler, dont Rallis [Ral82], Freitag [Fre83, Ch. IV §5], Yoshida [Yo86] et Andrianov [And87, Ch. V]. Nous nous contenterons pour l'instant d'énoncer le cas particulier suivant, explicité par Walling dans [Walli06]. Nous renvoyons le lecteur au §V.5 pour une démonstration dans le cas du genre $g = 1$, ce qui constitue un exercice sans grande difficulté.

On rappelle que l'opérateur de Hecke $\mathrm{T}_p \in \mathrm{H}(\mathrm{O}_n)$ est l'opérateur $\mathrm{T}_{\mathbb{Z}/p\mathbb{Z}}$ des p-voisins (§IV.2.6,§IV.4.4). On définit un opérateur de Hecke

$$\mathrm{S}_p \in \mathrm{H}(\mathrm{Sp}_{2g})$$

en considérant les couples $(M, N) \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(\mathbb{Q}^{2g})$ tels que soit $M \cap N$ est d'indice p dans M et N, soit $M = N$ (§IV.2.6). Autrement dit, c'est l'opérateur $\mathrm{T}_{\mathbb{Z}/p\mathbb{Z}} + 1$ dans les notations *loc. cit.*

Proposition 1.1. *On suppose* $1 \leq g \leq \frac{n}{2}$. *Pour tout nombre premier* p, *le diagramme*

$$\begin{tikzcd}
\mathbb{C}[\mathrm{X}_n] \arrow[r, "\vartheta_g"] \arrow[d, "\mathrm{T}_p"'] & \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z})) \arrow[d, "p^{\frac{n}{2}-1-g}\,\mathrm{S}_p + p^g\,\frac{p^{n-2g-1}-1}{p-1}"] \\
\mathbb{C}[\mathrm{X}_n] \arrow[r, "\vartheta_g"] & \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))
\end{tikzcd}$$

est commutatif. En particulier, $\operatorname{Ker}\vartheta_g$ *est stable par* T_p.

Démonstration. C'est un cas particulier de [Walli06, Thm. 2.1], observant que notre opérateur S_p coïncide avec l'opérateur noté $\mathrm{T}_1(p^2)+1$ par Walling. □

Si l'on remplace T_p par un opérateur de Hecke $\mathrm{T}_A \in \mathrm{H}(\mathrm{O}_n)$ plus général, les relations analogues données par exemple par Andrianov et Freitag prennent une forme d'apparence assez absconse. Elles sont toutefois particulièrement limpides (notamment celle ci-dessus) dans la présentation de Rallis, qui requiert néanmoins les points de vue de Satake et Langlands sur les opérateurs de Hecke. Nous reviendrons sur cela au §VI.1.1.

Observons que si Φ_g est l'opérateur de Siegel rappelé au §IV.5.2, on a la relation évidente $\Phi_g(\vartheta_g(L)) = \vartheta_{g-1}(L)$ pour $g \geq 2$. Cette relation s'étend

à $g = 1$ si l'on pose $\Phi_1(\sum_{n\geq 0} a_n q^n) = a_0$. Il en découle que la suite des sous-espaces

$$\operatorname{Ker}\vartheta_g \subset \mathbb{C}[\mathrm{X}_n],$$

pour $g \geq 0$, est décroissante. De plus, si $g \geq 1$ alors ϑ_g induit une injection $\mathbb{C}$-linéaire

$$\operatorname{Ker}\vartheta_{g-1}/\operatorname{Ker}\vartheta_g \longrightarrow \mathrm{S}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z})).$$

Il est immédiat que l'on a $\operatorname{Ker}\vartheta_n = \{0\}$ et que $\operatorname{Ker}\vartheta_0$ est de codimension 1 dans $\mathbb{C}[\mathrm{X}_n]$. De plus, le vecteur $\sum_{L\in \mathrm{X}_n} \frac{1}{|\mathrm{O}(L)|}[L]$ est propre sous l'action de $\mathrm{H}(\mathrm{O}_n)$ de valeurs propres explicites (Proposition III.2.4 et §IV.4.7), la droite qu'il engendre étant un supplémentaire de $\operatorname{Ker}\vartheta_0$. La question de déterminer toute la filtration $\operatorname{Ker}\vartheta_g$, ainsi que la structure des $\mathrm{H}(\mathrm{O}_n)$-modules $\operatorname{Ker}\vartheta_{g-1}/\operatorname{Ker}\vartheta_g$ quand $g \geq 1$, est en revanche tout à fait non triviale dès que $n > 8$. C'est évidemment un problème plus fin que celui de comprendre le $\mathrm{H}(\mathrm{O}_n)$-module $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$, le but de ce mémoire... Quand $n = 16$ et $n = 24$, cette filtration a été étudiée en détail par plusieurs auteurs, dont nous allons rappeler les contributions ci-dessous. Cela conduira à une démonstration directe du théorème I.A (cas $n = 16$) ainsi qu'à point de départ pour notre démonstration du théorème I.E (cas $n = 24$).

2. Séries thêta de $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16}

On rappelle $\mathrm{X}_{16} = \{\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16}\}$ (Witt). L'espace $\mathrm{M}_8(\mathrm{SL}_2(\mathbb{Z}))$ étant de dimension 1, on a l'identité bien connue

$$\vartheta_1(\mathrm{E}_8 \oplus \mathrm{E}_8) = \vartheta_1(\mathrm{E}_{16}). \tag{2.1}$$

En particulier, l'élément $[\mathrm{E}_8 \oplus \mathrm{E}_8] - [\mathrm{E}_{16}]$ engendre $\operatorname{Ker}\vartheta_1 = \operatorname{Ker}\vartheta_0$, et c'est un vecteur propre des T_p. Un fait absolument remarquable, conjecturé par Witt dans [Wit41], est que l'identité (2.1) persiste jusqu'en genre 3 :

$$\vartheta_g(\mathrm{E}_8 \oplus \mathrm{E}_8) = \vartheta_g(\mathrm{E}_{16}) \ \text{ si } \ g = 1, 2, 3. \tag{2.2}$$

Cela a été démontré par Witt *loc. cit.* pour $g = 2$, et beaucoup plus tard par Igusa et Kneser, indépendamment, pour $g = 3$ [Igu67][Kn67]. Igusa démontre $\mathrm{S}_8(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ pour $g \leq 3$. Nous renvoyons à l'appendice A pour un exposition de la démonstration remarquable de Kneser, qui est très différente. Au final, $\operatorname{Ker}\vartheta_3 = \operatorname{Ker}\vartheta_0$, et si

$$F := \vartheta_4(\mathrm{E}_8 \oplus \mathrm{E}_8) - \vartheta_4(\mathrm{E}_{16}),$$

alors $F \in \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. Il est bien connu que l'on a $F \neq 0$; précisons ce fait.

Proposition 2.1. *Soit* c_Q *le coefficient de Fourier de* F *correspondant à une matrice de Gram d'une* $\mathbb{Z}$*-base d'un réseau pair* Q *de rang* 4 (*il ne dépend pas du choix d'une telle base*). *On a*

$$\frac{\mathrm{c}_{\mathrm{D}_4}}{|\mathrm{O}(\mathrm{D}_4)|} = 4480 \qquad \text{et} \qquad \frac{\mathrm{c}_{\mathrm{A}_4}}{|\mathrm{O}(\mathrm{A}_4)|} = -21504.$$

En particulier, $\mathrm{c}_{\mathrm{D}_4} = -\mathrm{c}_{\mathrm{A}_4}$.

Démonstration. En effet, un examen des systèmes de racines $\mathbf{D}_n$ et $\mathbf{A}_m$ montre que le nombre de sous-réseaux de D_n isométriques à D_4 (resp. A_m) est $\binom{n}{4}$ (resp. $2^m\binom{n}{m+1}$). D'autre part, il se trouve que si $R = \mathbf{D}_4$ ou $\mathbf{A}_4$, il existe exactement une orbite de sous-réseaux de E_8 isométriques à $\mathrm{Q}(R)$ sous l'action de $\mathrm{O}(\mathrm{E}_8)$, son cardinal étant $\frac{|\mathrm{O}(\mathrm{E}_8)|}{|\mathrm{W}(R)|\cdot|\mathrm{A}(R)|}$. Indiquons brièvement comment justifier cette dernière affirmation, dont la proposition découle alors par un simple calcul. On traite simultanément les deux cas $R = \mathbf{D}_4$ ou $\mathbf{A}_4$, et on pose $Q = \mathrm{Q}(R)$, $E = \operatorname{rés} Q$ et $\Gamma = \mathrm{A}(R)/\mathrm{W}(R)$ (la notation rés a été définie au §II.1).

On commence par observer qu'un réseau euclidien pair $L \subset \mathbb{R}^4$ tel que rés $L \simeq E$ est nécessairement isomorphe à Q. En effet, nous laissons au lecteur le soin de vérifier que cela se déduit du fait bien connu suivant : tout réseau entier et unimodulaire de $\mathbb{R}^d$ pour $d \in \{4, 5\}$ est isométrique au réseau carré I_d (§II.2). La proposition 2.2 de l'appendice B montre que si $L \subset \mathrm{E}_8$ est isométrique à Q, son orthogonal $L^\perp$, qui est pair de rang 4, admet un résidu isomorphe à $-E$. Mais dans les deux cas $E \simeq -E$, donc $L^\perp$ est isométrique à Q. On considère enfin les lagrangiens du résidu $E \oplus E$ de $Q \oplus Q$; par la proposition II.1.1, ils donnent chacun naissance à un q-module sur $\mathbb{Z}$ de rang 8 contenant $Q \oplus Q$, nécessairement isomorphe à E_8. Le qe-module E étant anisotrope, les lagrangiens de $E \oplus -E$ sont les graphes des automorphismes de E, et on constate dans les deux cas qu'ils sont permutés simplement transitivement par $1 \times \Gamma$, car l'homomorphisme naturel $\Gamma \to \mathrm{Aut}(E)$ est bijectif. Il suit de ces observations que l'ensemble des sous-réseaux de E_8 isométriques à Q forment une seule orbite sous l'action de $\mathrm{O}(\mathrm{E}_8)$, de stabilisateur isomorphe à $\mathrm{A}(R) \times \mathrm{W}(R)$. □

Ainsi, $\operatorname{Ker} \vartheta_4 = 0$. Cela termine la description de la filtration de $\mathbb{C}[\mathrm{X}_{16}]$ et nous ramène à comprendre l'action de $\mathrm{H}(\mathrm{Sp}_8)$ sur la forme propre $F \in \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. Cette forme est particulièrement intéressante. En effet, Igusa a démontré dans [IGU81] qu'elle est proportionnelle à la fameuse forme de Schottky. Poor et Yuen en ont obtenu dans [PY96] une seconde démonstration, en vérifiant

$$\dim \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})) = 1. \tag{2.3}$$

Nous renvoyons à [DI98] pour une seconde démonstration de cette égalité, ainsi qu'au Théorème IX.5.10 pour une troisième !

Soit $\tau(n)$ la fonction de Ramanjuan, définie par $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$. Un calcul élémentaire montre que le théorème A de l'introduction est conséquence immédiate du (i) du théorème suivant, l'apparition des termes 286 et 405 provenant de la relation $\frac{|\mathrm{O}(\mathrm{E}_{16})|}{|\mathrm{O}(\mathrm{E}_8\oplus\mathrm{E}_8)|} = \frac{286}{405}$. Rappelons que l'opérateur de Hecke $\mathrm{S}_p \in \mathrm{H}_p(\mathrm{Sp}_{2g})$ a été introduit au §V.1.

Théorème 2.2. *Soit p un nombre premier.*

(i) La valeur propre de T_p sur $[\mathrm{E}_8 \oplus \mathrm{E}_8] - [\mathrm{E}_{16}]$ est

$$p^4\,\frac{p^7-1}{p-1} + p^7 + \tau(p)\,\frac{p^4-1}{p-1}.$$

(ii) La valeur propre de S_p sur la droite $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ est

$$p^4 + \tau(p)\,p^{-3}\,\frac{p^4-1}{p-1}.$$

Nous avons vu ci-dessus que ϑ_4 induit un isomorphisme $\mathrm{Ker}\,\vartheta_0 \xrightarrow{\sim} \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. Les assertions (i) et (ii) sont alors équivalentes d'après la proposition 1.1 (relations de commutation d'Eichler). Il se trouve que l'assertion (ii) est une application immédiate des travaux d'Ikeda [Ike01] (preuve de la conjecture de Duke-Imamoğlu [BK00]). En effet, si k et g sont des entiers pairs tels que $k \equiv g \bmod 4$, Ikeda construit *loc. cit.* une application linéaire injective

$$\mathrm{I}_g : \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z})) \longrightarrow \mathrm{S}_{\frac{k+g}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$$

ayant la propriété de compatibilité suivante aux opérateurs de Hecke. Si $f = q + \sum_{n\geq 2} a_n q^n \in \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ est propre pour $\mathrm{H}(\mathrm{PGL}_2)$, alors pour tout nombre premier p, $\mathrm{I}_g(f)$ est propre pour S_p de valeur propre

$$p^g(1 + a_p\, p^{-\frac{k+g}{2}+1}\,\frac{p^g-1}{p-1}). \tag{2.4}$$

(Nous renvoyons le néophyte au §VII.2 pour une explication du passage de l'énoncé d'Ikeda à celui-là). Dans la littérature, la forme $\mathrm{I}_g(f)$ est souvent appelée *relèvement d'Ikeda* en genre g de f. Si $k = 12$, $g = 4$, et si f est la forme modulaire $\Delta \in \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, on constate que son relèvement d'Ikeda $\mathrm{I}_4(\Delta)$ est un élément (non nul) de $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$, ayant la valeur propre de l'énoncé (ii), ce qui conclut. $\square$

Mentionnons qu'il avait déjà été observé par Breulmann et Kuss [BK00, §3] que lorsque $p = 2$, la valeur propre de l'opérateur de Hecke S_p sur la forme de Schottky est bien donnée par la formule du (ii), conformément à la conjecture de Duke-Imamoğlu. Leur méthode consiste à réaliser F comme série thêta à coefficients harmoniques construite à partir de E_8 (ce que nous ferons d'ailleurs également un peu plus loin !). Observons qu'une vérification similaire, qui paraît plus économe, est fournie par le calcul de T_2 effectué au §III.3.1.

L'apparition de la forme Δ dans l'argument ci-dessus est très indirecte, conséquence du résultat profond d'Ikeda. Nous allons donner au §V.4 une autre démonstration du (ii) que nous avons découverte et qui est indépendante du travail d'Ikeda. Elle repose notamment sur la trialité pour le groupe $\mathrm{PGSO}_{\mathrm{E}_8}$ sur $\mathbb{Z}$. Nous obtiendrons également plus tard une troisième démonstration de l'assertion (ii) du théorème, nettement plus sophistiquée, reposant sur la théorie d'Arthur : c'est le cas particulier (particulièrement simple !) où $k = 8$ dans l'énoncé du théorème IX.5.10. Enfin, nous expliquerons aussi comment l'assertion (i) du théorème se déduit trivialement d'une conjecture très générale concernant la théorie d'Arthur, qui sera exposée au chapitre VIII : voir les exemples du §VIII.5.7.

3. Séries thêta des réseaux de Niemeier

Considérons maintenant le cas $n = 24$. D'après Erokhin [Ero79], les séries thêta de genre 12 des 24 réseaux de Niemeier sont linéairement indépendantes, i.e. $\operatorname{Ker} \vartheta_{12} = 0$. Cela ne vaut pas en genre 11. En effet, ainsi que l'ont observé Borcherds, Freitag et Weissauer [BFW98] par une construction ingénieuse, $\operatorname{Ker} \vartheta_{11}$ est de dimension 1. C'est un analogue spectaculaire en dimension 24 de la découverte de Witt étudiée au paragraphe précédent.

Une étude plus fine du $\mathrm{H}(\mathrm{O}_{24})$-module filtré $\mathbb{C}[\mathrm{X}_{24}]$ a été initiée par Nebe et Venkov dans leur délicieux article [NV01]. Leur point de départ est le calcul de T_2 rappelé au §III.3.3, qu'ils déduisent de la thèse de Borcherds [Bor84]. Ils observent que T_2 possède 24 valeurs propres entières distinctes, et disposent pour chacune d'entre elle d'un vecteur propre explicite, qui est nécessairement propre pour l'action de tout $\mathrm{H}(\mathrm{O}_n)$. Il sera commode, suivant ces auteurs, de numéroter ces vecteurs propres v_i, $i = 1, \ldots, 24$, de sorte que les valeurs propres λ_i de T_2 associées soient rangées par ordre décroissant (voir la table V.1). La détermination de la filtration de $\mathbb{C}[\mathrm{X}_{24}]$ équivaut alors à celle du *degré* de chaque v_i, c'est-à-dire du plus petit entier $\mathrm{g}_i \geq 0$ tel que $\vartheta_{\mathrm{g}_i}(\mathrm{v}_i) \neq 0$. Nebe et Venkov y parviennent pour 22 des 24 valeurs propres, et

proposent une conjecture pour les deux cas restants, que nous avons soulignés dans le tableau ci-dessous.

λ	8390655	4192830	2098332	1049832	533160	519120	268560	244800
degré	0	1	2	3	4	4	5	5
λ	145152	126000	99792	91152	89640	69552	51552	45792
degré	6	6	6	7	8	7	8	7
λ	35640	21600	17280	5040	-7920	-16128	-48528	-98280
degré	8	8	$\underline{9}$	9	$\underline{10}$	10	11	12

TABLE V.1 – La filtration de $\mathbb{C}[\mathrm{X}_{24}]$, d'après Nebe et Venkov.

Commentons un peu cette table. La valeur propre triviale

$$(2^{12}-1)(2^{11}+1) = 8390655 = \lambda_1$$

est bien entendu associée à l'unique vecteur propre degré 0. De plus, il est facile de vérifier que ϑ_1 induit une surjection $\ker \vartheta_0 \to \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, de sorte qu'un, et un seul, des vecteurs propres de T_2 est de degré 1. D'après le théorème 5.1, c'est celui de valeur propre

$$\tau(2)^2 - 2^{11} + 2\,(2^{21}-1) = 4192830 = \lambda_2.$$

Les autres valeurs propres sont nettement plus subtiles à comprendre. Par exemple, Nebe et Venkov mentionnent à la fin de leur article, que pour $i = 3, 5, 11, 13$ et 24 (auquel cas g_i vaut respectivement $2, 4, 6, 8, 12$), alors $\vartheta_{\mathrm{g}_i}(\mathrm{v}_i)$ est proportionnel au relèvement d'Ikeda

$$\mathrm{I}_{\mathrm{g}_i}(\Delta_{23-\mathrm{g}_i})$$

où Δ_w désigne un générateur de $\mathrm{S}_{w+1}(\mathrm{SL}_2(\mathbb{Z}))$ quand $w \in \{11, 15, 17, 19, 21\}$ (voir le corollaire §VI.3.4 pour une justification de ce fait). L'action de $\mathrm{H}(\mathrm{O}_{24})$ sur ces v_i est donc explicitement connue (modulo les relations d'Eichler) en fonction des coefficients de Fourier des 5 formes modulaires Δ_w ci-dessus. Quand $i = 24$, cela avait déjà été remarqué par Borcherds, Freitag et Weissauer, immédiatement après l'annonce de [IKE01] (voir également [BK00]). Par exemple,

$$\tau(2)(2^{12}-1) = -98280 = \lambda_{24};$$

plus généralement la valeur propre de T_p sur v_{24} est $\tau(p)\frac{p^{12}-1}{p-1}$.

Un pas supplémentaire spectaculaire a alors été obtenu à nouveau par Ikeda dans son article [IKE06], comme conséquence des résultats sus-cités de Nebe-Venkov, et de sa résolution partielle d'une conjecture de Miyawaki.

λ	126000	51552	17280	-7920
degré	6	8	$\underline{9}$	$\underline{10}$

TABLE V.2 – Les 4 vecteurs propres mystérieux

Ikeda parvient à exprimer l'action de $\mathrm{H}(\mathrm{O}_{24})$ sur tous les v_i, toujours en terme des Δ_w ci-dessus, excepté pour quatre d'entre elles, à savoir les suivantes :

Nous reviendrons sur l'énoncé exact démontré par Ikeda au §IX.2, dans lequel nous expliquerons également les valeurs popres manquantes ci-dessus.

Terminons ce paragraphe par une discussion de $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$. Nous avons déjà observé au paragraphe IV.1.6 que l'application naturelle $\widetilde{\mathrm{X}}_n \to \mathrm{X}_n$ est bijective pour $n < 24$, mais que pour $n = 24$ la classe du réseau de Leech (et seulement celle-ci) possède deux antécédents, que nous noterons $\mathrm{Leech}^{\pm}$. Il suit que $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$ est de dimension 1, constitué des fonctions nulles sur les 23 réseaux de Niemeier avec racines et prenant des valeurs opposées sur Leech^{+} et Leech^{-}.

Proposition 3.1. *La valeur propre de* T_p *sur la droite* $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$ *est*

$$\tau(p)\,\frac{p^{12}-1}{p-1}.$$

Nous démontrerons ce résultat au §VII.5, et plus précisément que l'anneau $\mathrm{H}(\mathrm{O}_{24})$ agit de la même manière sur les droites $\mathbb{C}\mathrm{v}_{24} \subset \mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24})$ et $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$. Cela répondra notamment à une question de Schulze-Pillot [SP99, Remark, §1].

Cette proposition admet une traduction frappante en terme de réseaux. Disons qu'un p-voisin M d'un réseau unimodulaire pair L de $\mathbb{R}^n$ est *propre* s'il existe $g \in \mathrm{SO}(\mathbb{R}^n)$ tel que $g(M) = L$. On note $\mathrm{N}_p^+(L, M)$ le nombre des p-voisins propres de L isométriques à M et on pose $\mathrm{N}_p^-(L, M) = \mathrm{N}_p(L, M) - \mathrm{N}_p^+(L, M)$. Si L possède une isométrie de déterminant -1, tous ses p-voisins sont propres. C'est bien entendu le cas de tous les réseaux de Niemeier avec racines. Le cas du réseau de Leech est en revanche plus intéressant, comme le montre le corollaire suivant immédiat de la proposition 3.1.

Corollaire 3.2. *Pour tout nombre premier p, on a la relation*

$$\mathrm{N}_p^+(\mathrm{Leech}, \mathrm{Leech}) - \mathrm{N}_p^-(\mathrm{Leech}, \mathrm{Leech}) = \tau(p)\frac{p^{12}-1}{p-1}.$$

Une conséquence amusante de ce corollaire est que la fameuse conjecture de Lehmer est équivalente à "$\mathrm{N}_p^+(\mathrm{Leech}, \mathrm{Leech}) \neq \mathrm{N}_p^-(\mathrm{Leech}, \mathrm{Leech})$ pour tout premier p" !

4. Une construction alternative de $\mathrm{I}_4(\Delta)$ par trialité

Comme promis au §V.2, nous allons donner ci-dessous une seconde démonstration du théorème 2.2 (et donc du théorème I.A), indépendante du théorème d'Ikeda [Ike01]. Cela nous permettra au passage de donner des exemples non triviaux de formes automorphes pour O_8 et d'illustrer les techniques du chapitre IV.

4.1. Séries thêta harmoniques

On se place dans l'espace euclidien $V = \mathbb{R}^n$. Soit $1 \leq g \leq \frac{n}{2}$ un entier. L'espace vectoriel $V^g = V \otimes \mathbb{R}^g$ est muni d'une représentation $\mathbb{R}$-linéaire naturelle de $\mathrm{O}(V) \times \mathrm{GL}_g(\mathbb{R})$. Pour tout entier $d \geq 0$, considérons l'espace $\mathrm{H}_{d,g}(V)$ des polynômes $P : V^g \to \mathbb{C}$ tels que :

(i) P est harmonique relativement au laplacien euclidien de V^g,

(ii) $P \circ h = \text{dét}(h)^d P$ pour tout $h \in \mathrm{GL}_g(\mathbb{R})$.

Cet espace est stable sous l'action de $\mathrm{O}(V)$. On en construit des éléments de la manière suivante. Soit $I \subset V \otimes \mathbb{C}$ un sous-espace isotrope de dimension g, et soit $e_1, \ldots, e_g$ une $\mathbb{C}$-base de I. Il n'est pas difficile de vérifier que

$$(v_1, \ldots, v_g) \mapsto \text{dét}[e_i \cdot v_j]^d_{1 \leq i,j \leq g} \tag{4.1}$$

est un élément de $\mathrm{H}_{d,g}(V)$. Il engendre une droite ne dépendant que de I. Ces droites sont permutées transitivement par $\mathrm{O}(V)$ et engendrent $\mathrm{H}_{d,g}(V)$, qui est une représentation irréductible de $\mathrm{O}(V)$ d'après [KV78, (0.9),(5.7)].

Si $L \subset V$ est un réseau unimodulaire pair, et si $P \in \mathrm{H}_{d,g}(V)$, on pose

$$\vartheta_g(L, P) = \sum_{v \in L^g} P(v) q^{\frac{v.v}{2}}.$$

L'équation fonctionnelle de la fonction ϑ de Jacobi permet de démontrer $\vartheta_g(L, P) \in \mathrm{M}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ [Fre83, Kap. III §3]. Observons que

$$\vartheta_g(L, P) = \vartheta_g(\gamma(L), \gamma(P)), \qquad \forall \gamma \in \mathrm{O}(V). \tag{4.2}$$

En particulier, $\vartheta_g(L, P) = 0$ pour tout P si $\mathrm{H}_{d,g}(V)^{\mathrm{O}(L)} = 0$. Commençons par donner un exemple, sans doute bien connu, où cet espace d'invariants n'est pas nul pour $n = 8$.

Lemme 4.2. *Soient $R \subset V$ un système de racines, $W \subset \mathrm{O}(V)$ son groupe de Weyl et $W^+ = W \cap \mathrm{SO}(V)$. Alors*

$$H_W(t) := \sum_{d \geq 0} (\dim \mathrm{H}_{d,1}(V)^W)\, t^d = (1-t^2) \prod_i (1-t^{m_i+1})^{-1},$$

où les m_i sont les exposants de W, et

$$\sum_{d \geq 0} (\dim \mathrm{H}_{d,1}(V)^{W^+})\, t^d = (1+t^{|R|/2)}) H_W(t).$$

Démonstration. Soient A et B les séries génératrices respectives des suites $\dim \mathrm{Pol}_d(V)^W$ et $\dim(\mathrm{Pol}_d(V) \otimes \text{dét})^W$ ("anti-invariants"), pour $d \geq 0$. D'après [Bou81b, Ch. V §6], on a $B = t^{|R|/2} A$ et $A = \prod_i (1-t^{m_i+1})^{-1}$. Soit $\mathrm{Pol}_d(V)$ l'espace des polynômes $V \to \mathbb{C}$ qui sont homogènes de degré d. Notons $\mathbf{\Delta} = \sum_{i=1}^n \frac{\partial^2}{\partial x_i^2}$ le laplacien standard de $\mathbb{R}^n$. On dispose pour tout $d \in \mathbb{Z}$ d'une suite exacte $\mathrm{O}(V)$-équivariante

$$0 \longrightarrow \mathrm{H}_{d,1}(V) \longrightarrow \mathrm{Pol}_d(V) \xrightarrow{\mathbf{\Delta}} \mathrm{Pol}_{d-2}(V) \longrightarrow 0,$$

la surjectivité de $\mathbf{\Delta}$ étant un résultat classique (voir par exemple [GW98, §5.2.3]). On en déduit (i) puis (ii). □

Considérons par exemple le réseau $\mathrm{E}_8 \subset \mathbb{R}^8$, dont le système de racines $\mathrm{R}(\mathrm{E}_8)$ est précisément de type $\mathbf{E}_8$. Ses exposants sont les 8 entiers $1 \leq m \leq 30$ premiers à 30. Comme $\mathrm{W}(\mathbf{E}_8) = \mathrm{O}(\mathrm{E}_8)$, on trouve

$$\sum_{d \geq 0} (\dim \mathrm{H}_{d,1}(V)^{\mathrm{O}(\mathrm{E}_8)})\, t^d = 1 + t^8 + t^{12} + t^{14} + t^{16} + t^{18} + 2\,t^{20} + \cdots. \tag{4.3}$$

Le plus petit invariant est donc pour $d = 8$.

Proposition 4.3. *Le polynôme $A(x) = -30\,(x \cdot x)^4 + \sum_{\alpha \in \mathrm{R}(\mathrm{E}_8)} (\alpha \cdot x)^8$ est dans $\mathrm{H}_{8,1}(V)^{\mathrm{O}(E_8)}$. Il satisfait $A(\alpha) = 144$ pour toute racine $\alpha \in \mathrm{R}(\mathrm{E}_8)$. En particulier, on a l'égalité $\vartheta_1(\mathrm{E}_8, A) = 240 \cdot 144\ \Delta$.*

Démonstration. L'invariance de A par $\mathrm{O}(\mathrm{E}_8)$ est évidente. Vérifions que A est harmonique. Avec les notations de la démonstration du lemme 4.2, le polynôme $\mathbf{\Delta} A \in \mathrm{Pol}_6(V)$ est invariant. Pour tout $d \geq 2$, on a la décomposition

$$\mathrm{Pol}_d(V) = (x \cdot x)\, \mathrm{Pol}_{d-2}(V) \oplus \mathrm{H}_{d,1}(V).$$

La série de Poincaré (4.3) montre donc que $\mathbf{\Delta} A$ est proportionnel à $(x\cdot x)^3$. Il ne reste qu'à voir que $\mathbf{\Delta} A$ s'annule sur les racines de E_8. C'est une vérification simple laissée au lecteur, utilisant d'une part les formules

$$\mathbf{\Delta}(\alpha\cdot x)^k = k(k-1)(\alpha\cdot\alpha)(\alpha\cdot x)^{k-2}, \quad \mathbf{\Delta}(x\cdot x)^k = 2k(\dim(V)+2k-2)(x\cdot x)^{k-1},$$

et d'autre part le fait que dans E_8, il y a exactement 114 racines non orthogonales à une racine α_0 donnée d'après [Bou81b, Chap. VI, §1.11, Prop. 32], leur produit scalaire avec α_0 étant ± 1 pour 112 d'entre elles. Cette même propriété entraîne aussi $A(\alpha) = 144$ pour tout $\alpha \in \mathrm{R}(\mathrm{E}_8)$, puis la dernière assertion. □

Il sera utile d'exprimer l'identité ci-dessus en terme de formes automorphes pour $\mathrm{O}_8 = \mathrm{O}_{\mathrm{E}_8}$ (§IV.4.4). Nous allons pour cela linéariser la définition des séries théta harmoniques, à la manière du §V.1. Rappelons que pour tout entier $n \equiv 0 \bmod 8$, le $\mathrm{O}_n(\mathbb{A}_f)$-ensemble $\mathcal{R}(\mathrm{O}_n)$ s'identifie naturellement à celui des réseaux unimodulaires pairs de $\mathbb{R}^n$ inclus dans $\mathrm{E}_n \otimes \mathbb{Q}$ (§IV.1.2).

Si $L \in \mathcal{R}(\mathrm{O}_n)$, l'application $P \mapsto \vartheta_g(L,P)$, $\mathrm{H}_{d,g}(V) \to \mathrm{M}_{\frac{n}{2}+d}(\mathrm{O}_n)$, est $\mathbb{C}$-linéaire. De plus, $\vartheta_g(\gamma L, \gamma P) = \vartheta_g(L,P)$ pour tout $\gamma \in \mathrm{O}_n(\mathbb{Q})$ (formule (4.2)). On dispose donc d'une unique application linéaire

$$(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)] \otimes \mathrm{H}_{d,g}(V))_{\mathrm{O}_n(\mathbb{Q})} \to \mathrm{M}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$$

envoyant la classe de $[L] \otimes P$ sur $\vartheta_g(L,P)$ pour tout $L \in \mathcal{R}(\mathrm{O}_n)$ et tout $P \in \mathrm{H}_{d,g}(V)$. D'après l'isomorphisme IV.(4.3), le $\mathrm{H}(\mathrm{O}_n)$-module de gauche s'identifie canoniquement à $\mathrm{M}_{\mathrm{H}_{d,g}(V)^*}(\mathrm{O}_n)^*$. Cette double dualité n'étant pas très heureuse, il est agréable de la supprimer en utilisant l'isomorphisme canonique entre les $\mathrm{H}(\mathrm{O}_n)$-modules $\mathrm{M}_{\mathrm{H}_{d,g}(V)^*}(\mathrm{O}_n)^*$ et $\mathrm{M}_{\mathrm{H}_{d,g}}(V)(\mathrm{O}_n)^{\mathrm{t}}$ (Corollaire IV.4.9). Rappelons que le t en exposant dans ce dernier espace signifie que l'action de $\mathrm{H}(\mathrm{O}_n)$ est tordue par $T \mapsto T^{\mathrm{t}}$, au sens de la remarque IV.2.4. Comme $T^{\mathrm{t}} = T$ pour tout $T \in \mathrm{H}(\mathrm{O}_n)$ (Proposition IV.2.8), cette torsion est sans effet ici, et sera allègrement ignorée par la suite.

Rappelons enfin que nous notons $[L,P]$ l'élément de $\mathrm{M}_{\mathrm{H}_{d,g}(V)}(\mathrm{O}_n)$ image de $[L] \otimes P$ par l'isomorphisme canonique composé $(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)] \otimes \mathrm{H}_{d,g}(V))_{\mathrm{O}_n(\mathbb{Q})} \xrightarrow{\sim} \mathrm{M}_{\mathrm{H}_{d,g}(V)}(\mathrm{O}_n)$ (voir la fin du §IV.4.7).

Proposition-Définition 4.4. *Il existe une unique application linéaire*

$$\vartheta_{d,g} : \mathrm{M}_{\mathrm{H}_{d,g}(V)}(\mathrm{O}_n) \to \mathrm{M}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$$

envoyant $[L,P]$ sur $\vartheta_g(L,P)$ pour tout $L \in \mathcal{R}(\mathrm{O}_n)$ et tout $P \in \mathrm{H}_{d,g}(V)$. Si $d > 0$ alors $\mathrm{Im}(\vartheta_{d,g}) \subset \mathrm{S}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$.

Démonstration. L'existence et l'unicité d'une telle application suivent de la discussion précédente. Concrètement, si $F \in \mathrm{M}_{\mathrm{H}_{d,g}(V)}(\mathrm{O}_n)$ on a

$$\vartheta_{d,g}(F) = \sum_i \frac{1}{|\mathrm{O}(L_i)|}\, \vartheta_g(L_i, P_i)$$

où les L_i forment un système de représentants des $\mathrm{O}_n(\mathbb{Q})$-orbites de $\mathcal{R}(\mathrm{O}_n)$, et où l'on a posé $P_i = F(L_i)$. □

Quand $d = 0$, on a un isomorphisme $\mathrm{H}_{d,g}(V) \simeq \mathbb{C}$ (représentation triviale), et l'application $\vartheta_{d,g}$ n'est autre que la composée de l'isomorphisme $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n) \xrightarrow{\sim} \mathbb{C}[\mathrm{X}_n]$ donné par le corollaire IV.4.9 et de l'application ϑ_g du §V.1.

Corollaire 4.5. *L'application* $\vartheta_{8,1} : \mathrm{M}_{\mathrm{H}_{8,1}(\mathbb{R}^8)}(\mathrm{O}_8) \to \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$ *est un isomorphisme entre espaces de dimension* 1.

Démonstration. Il est bien connu que $\dim \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z})) = 1$. Rappelons, d'après Mordell, que l'on a $\mathrm{X}_8 = \{\mathrm{E}_8\}$, de sorte que pour tout entier $d \geq 0$ on a $\dim \mathrm{M}_{\mathrm{H}_{d,1}(\mathbb{R}^8)}(\mathrm{O}_8) = \dim \mathrm{H}_{d,1}(\mathbb{R}^8)^{\mathrm{O}(\mathrm{E}_8)}$. Un examen de la série (4.3) montre que $\dim \mathrm{M}_{\mathrm{H}_{8,1}(\mathbb{R}^8)}(\mathrm{O}_8) = 1$. Il suffit donc de voir que $\vartheta_{8,1}$ est non nulle, mais cela résulte de la proposition 4.3. □

On dispose encore de relations de commutation d'Eichler pour l'application $\vartheta_{d,g} : \mathrm{M}_{\mathrm{H}_{d,g}(V)}(\mathrm{O}_n) \to \mathrm{M}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ (voir le §VI.1.1 pour une justification). En particulier, pour tout nombre premier p on a

$$\vartheta_{d,g} \circ \mathrm{T}_p = (p^{\frac{n}{2}-1-g}\, \mathrm{S}_p \,+\, p^g\, \frac{p^{n-2g-1}-1}{p-1}) \circ \vartheta_{d,g}. \tag{4.4}$$

Nous renvoyons au §V.5 pour une démonstration de cette formule pour $g = 1$. Combinée au corollaire 4.5, on obtient le corollaire suivant.

Corollaire 4.6. *La valeur propre de* T_p *sur la droite* $\mathrm{M}_{\mathrm{H}_{8,1}(\mathbb{R}^8)}(\mathrm{O}_8)$ *est*

$$p^{-8}(\tau(p)^2 - p^{11}) + p\,\frac{p^5-1}{p-1}.$$

4.7. L'opérateur de Hecke des perestroïkas

Rappelons que nous avons défini dans l'exemple IV.2.16 une injection naturelle

$$\mathrm{H}(\mu) : \mathrm{H}(\mathrm{O}_n) \to \mathrm{H}(\mathrm{PGO}_n)$$

associée au $\mathbb{Z}$-morphisme canonique $\mu : \mathrm{O}_n \to \mathrm{PGO}_n$. Nous noterons désormais $\mathrm{H}(\mu)$ comme une inclusion $\mathrm{H}(\mathrm{O}_n) \subset \mathrm{H}(\mathrm{PGO}_n)$ pour ne pas surcharger les notations. Soit W une représentation de $\mathrm{PGO}_n(\mathbb{R})$, et soit W' sa restriction à $\mathrm{O}_n(\mathbb{R})$. D'après la proposition §IV.4.3, la restriction des fonctions suivant $\mathcal{R}(\mathrm{O}_n) \to \mathcal{R}(\mathrm{PGO}_n)$ définit une application $\mathrm{H}(\mathrm{O}_n)$-équivariante

$$\mu^* : \mathrm{M}_W(\mathrm{PGO}_n) \to \mathrm{M}_{W'}(\mathrm{O}_n).$$

Lemme 4.8. *L'application μ^* est un isomorphisme.*

Démonstration. En effet, l'application $\mathrm{O}_n(\mathbb{Q})\backslash\mathcal{R}(\mathrm{O}_n) \to \mathrm{PGO}_n(\mathbb{Q})\backslash\mathcal{R}(\mathrm{PGO}_n)$ est bijective d'après la proposition IV.1.4 (c'est $\xi_2 \circ \xi_1$). On conclut car si $M \subset \mathbb{R}^n$ est un réseau euclidien, ou plus généralement un $\widetilde{\mathrm{b}}$-module sur $\mathbb{Z}$ défini positif, alors $\mathrm{O}(M) = \mathrm{GO}(M)$. $\square$

Une manière de voir ce lemme est de dire que l'action de $\mathrm{H}(\mathrm{O}_n)$ sur $\mathrm{M}_{W'}(\mathrm{O}_n)$ s'augmente en une action de l'anneau plus gros $\mathrm{H}(\mathrm{PGO}_n)$. Nous allons appliquer ceci aux $\mathrm{H}_{d,1}(\mathbb{R}^n)$. Ces espaces sont munis d'une représentation naturelle de $\mathrm{GO}(\mathbb{R}^n)$, sur laquelle l'homothétie de rapport λ agit par le scalaire λ^{-d}. En particulier, si d est pair alors

$$\mathrm{H}_{d,1}(\mathbb{R}^n) \otimes \nu^{d/2}$$

se factorise en une représentation de $\mathrm{PGO}_n(\mathbb{R})$ dont la restriction à $\mathrm{O}_n(\mathbb{R})$ est simplement $\mathrm{H}_{d,1}(\mathbb{R}^n)$. On rappelle que l'opérateur $\mathrm{K}_p \in \mathrm{H}_p(\mathrm{PGO}_n)$ des perestroïkas relativement à p a été défini au §IV.2.6 (et $\mathrm{K}_p = \mathrm{K}_p^{\mathrm{t}}$).

Lemme 4.9. *Soient $d \equiv 0 \bmod 2$, $W = \mathrm{H}_{d,1}(\mathbb{R}^n) \otimes \nu^{d/2}$, p un nombre premier, et $\ell_{2r}(p) = \prod_{i=0}^{r-1}(1+p^i)$* (i.e. *le nombre de lagrangiens de* $\mathrm{H}(\mathbb{F}_p^r)$). *Le diagramme suivant est commutatif :*

$$\begin{tikzcd}
\mathrm{M}_W(\mathrm{PGO}_n) \arrow[r, "\vartheta_{d,1}\circ\mu^*"] \arrow[d, "\mathrm{K}_p"'] & \mathrm{M}_{\frac{n}{2}+d}(\mathrm{SL}_2(\mathbb{Z})) \arrow[d, "\ell_{n-2}(p)\, p^{-d/2}\, \mathrm{T}(p)"] \\
\mathrm{M}_W(\mathrm{PGO}_n) \arrow[r, "\vartheta_{d,1}\circ\mu^*"] & \mathrm{M}_{\frac{n}{2}+d}(\mathrm{SL}_2(\mathbb{Z}))
\end{tikzcd}$$

Démonstration. C'est une variante harmonique du résultat d'Eichler [Eic52, Satz 21.3] (voir aussi [Ral79]). Nous redonnons l'argument.

On fixe un réseau unimodulaire M dans $\mathrm{E}_n \otimes \mathbb{Q}$ (ou, plus généralement, un réseau homodual de $\mathrm{E}_n \otimes \mathbb{Q}$), ainsi qu'un polynôme P dans l'espace $\mathrm{H}_{d,1}(\mathbb{R}^n) \otimes \nu^{d/2}$. Soit $\mathrm{Per}_p(M)$ l'ensemble des perestroïkas de M relativement à p.

Si $N \in \mathrm{Per}_p(M)$, alors $\mu^*([\underline{N}, P]) = [\gamma(N), p^{-d/2}\,\gamma(P)]$ où $\gamma \in \mathrm{GO}(\mathbb{Q})$ est un élément quelconque de facteur de similitude p^{-1}. Comme le réseau $p^{-1/2}N \subset \mathbb{R}^n$ est isométrique à $\gamma(N)$, la relation (4.2) entraîne

$$\vartheta_{d,1} \circ \mu^*([N, P]) = \vartheta_{d,1}(\frac{N}{\sqrt{p}}, P).$$

Si $m \geq 0$, le m-ième coefficient de Fourier de $\vartheta_{d,1} \circ \mu^* \circ \mathrm{K}_p([M, P])$ vaut donc

$$\sum_{(N,v)} P(\frac{v}{\sqrt{p}}) \tag{4.5}$$

la somme portant sur tous les couples (N, v) avec $N \in \mathrm{Per}_p(M)$ et $v \in N$ tels que $v \cdot v = 2mp$.

Supposons m premier à p. Observons qu'un élément $v \in M$ tel que $v \cdot v = 2mp$ est non nul modulo pM et isotrope. Il appartient donc à exactement $\ell_{n-2}(p)$ perestroïkas de M (i.e. le nombre de lagrangiens de $M \otimes \mathbb{F}_p$ contenant une droite isotrope donnée). La somme (4.5) vaut donc simplement

$$p^{-d/2}\ell_{n-2}(p)a_{mp},$$

où a_r désigne le r-ième coefficient de Fourier de $\vartheta_{d,1}(M, P)$. Pour conclure, on pourrait traiter le cas m multiple de p de manière similaire, ou simplement invoquer le lemme 5.2. □

Corollaire 4.10. *Pour tout nombre premier p, la valeur propre de K_p sur la droite $\mathrm{M}_{\mathrm{H}_{8,1}(\mathbb{R}^8)\otimes\nu^4}(\mathrm{PGO}_8)$ est $2\,p^{-4}\,\frac{p^4-1}{p-1}\tau(p)$.*

Démonstration. Cela suit en effet de l'identité $\ell_6(p) = 2(1+p)(1+p^2) = 2\frac{p^4-1}{p-1}$, des lemmes 4.8 et 4.9, et du corollaire 4.5. □

4.11. Passage de PGO_n à PGSO_n

L'application μ_3 de la proposition IV.1.7 étant bijective et $\mathrm{PGSO}_n(\mathbb{A}_f)$-équivariante, les arguments donnés aux §IV.2.11 et §IV.4.4 concernant la comparaison entre SO_n et O_n s'étendent *mutatis mutandis* au cas de PGSO_n et PGO_n. On dispose notamment d'une action du groupe

$$\mathrm{PGO}_n(\mathbb{A}_f)/\mathrm{PGSO}_n(\mathbb{A}_f) \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathrm{P}}$$

sur $\mathrm{H}(\mathrm{PGSO}_n)$ qui préserve chaque $\mathrm{H}_p(\mathrm{PGSO}_n)$, et dont les invariants sont exactement $\mathrm{H}(\mathrm{PGO}_n)$. En particulier, $\mathrm{H}(\mathrm{PGO}_n) \subset \mathrm{H}(\mathrm{PGSO}_n)$. Si U est une

représentation de $\mathrm{PGSO}_n(\mathbb{R})$, d'induite $\mathrm{Ind}\, U$ à $\mathrm{PGO}_n(\mathbb{R})$, on dispose d'un isomorphisme canonique $\mathrm{H}(\mathrm{PGO}_n)$-équivariant

$$\mathrm{ind} : \mathrm{M}_U(\mathrm{PGSO}_n) \to \mathrm{M}_{\mathrm{Ind}\, U}(\mathrm{PGO}_n).$$

Enfin, si W est une représentation de $\mathrm{PGO}_n(\mathbb{R})$, et si W' désigne sa restriction à $\mathrm{PGSO}_n(\mathbb{R})$, l'action par conjugaison de $\mathrm{PGO}_n(\mathbb{Q})/\mathrm{PGSO}_n(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ sur $\mathrm{M}_{W'}(\mathrm{PGSO}_n)$ muni ce dernier espace d'une symétrie naturelle que l'on notera s. La restriction des fonctions selon la bijection $\mathcal{R}(\mathrm{PGSO}_n) \to \mathcal{R}(\mathrm{PGO}_n)$ définit une injection $\mathrm{H}(\mathrm{PGO}_n)$-équivariante

$$\mathrm{res} : \mathrm{M}_W(\mathrm{PGO}_n) \longrightarrow \mathrm{M}_{W'}(\mathrm{PGSO}_n)$$

d'image $\mathrm{M}_{W'}(\mathrm{PGSO}_n)^{s=\mathrm{id}}$.

Soit W la représentation $\mathrm{H}_{d,1}(\mathbb{R}^n) \otimes \nu^{d/2}$ de $\mathrm{PGO}_n(\mathbb{R})$ définie au §IV.4.7 ($d \equiv 0 \bmod 2$). Si $n > 2$, sa restriction W' à $\mathrm{PGSO}_n(\mathbb{R})$ est irréductible [GW98, §5.2]. Pour des raisons générales, on a enfin $\mathrm{Ind}\, W' \simeq W \oplus W \otimes \epsilon$, où ε est le caractère d'ordre 2 de $\mathrm{PGO}_n(\mathbb{R})$ de noyau $\mathrm{PGSO}_n(\mathbb{R})$.

Lemme 4.12. *Soient* $W = \mathrm{H}_{8,1}(\mathbb{R}^8) \otimes \nu^4$ *et* $W' = W_{|\mathrm{PGSO}_8(\mathbb{R})}$. *L'application de restriction* $\mathrm{res} : \mathrm{M}_W(\mathrm{PGO}_8) \to \mathrm{M}_{W'}(\mathrm{PGSO}_8)$ *est bijective.*

Démonstration. Il s'agit de montrer que l'espace $\mathrm{M}_{W'}(\mathrm{PGSO}_8)^{s=-\mathrm{id}}$, qui est naturellement isomorphe à $\mathrm{M}_{W\otimes\varepsilon}(\mathrm{PGO}_8)$, est nul. D'après le lemme IV.4.8, il est équivalent de montrer que $\mathrm{M}_{\mathrm{H}_{8,1}(\mathbb{R}^8)\otimes\varepsilon}(\mathrm{O}_8) = 0$. Cela découle de ce que $\mathrm{X}_8 = \{\mathrm{E}_8\}$, $\mathrm{O}(\mathrm{E}_8) = W(\mathbf{E}_8)$, et du lemme 4.2, qui assure que les $W(\mathbf{E}_8)^+$-invariants de $\mathrm{H}_{8,1}(\mathbb{R}^8)$ sont en fait $W(\mathbf{E}_8)$-invariants (et de dimension 1). $\square$

Nous avons vu au §IV.2.11 que l'élément $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^{n/2}}$ de $\mathrm{H}_p(\mathrm{O}_n)$ se décompose de manière naturelle comme somme de deux éléments $\mathrm{T}^{\pm}_{(\mathbb{Z}/p\mathbb{Z})^{n/2}}$ de $\mathrm{H}_p(\mathrm{SO}_n)$. Un phénomène similaire se produit avec l'opérateur de Hecke $\mathrm{K}_p \in \mathrm{H}_p(\mathrm{PGO}_n)$ des perestroïkas, qui se raffine lorsqu'on le voit dans $\mathrm{H}_p(\mathrm{PGSO}_n)$.

En effet, observons que $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(\mathrm{E}_n \otimes \mathbb{Q})$ étant donné, l'ensemble Ω des $\underline{N} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(\mathrm{E}_n \otimes \mathbb{Q})$ tels que N est une perestroïka de M relativement à p est constitué d'exactement deux orbites sous l'action de $\mathrm{GSO}(M)$, et d'une seule sous $\mathrm{GO}(M)$. En effet, cela découle de la lissité de GO_M et GSO_M sur $\mathbb{Z}$, et de ce que l'action de $\mathrm{GO}(M \otimes \mathbb{F}_p)$ (resp. $\mathrm{GSO}(M \otimes \mathbb{F}_p)$) sur l'ensemble des lagrangiens de $M \otimes \mathbb{F}_p \simeq \mathrm{H}(\mathbb{F}_p^{n/2})$ est transitive d'après le théorème de Witt (resp. admet deux orbites). Ces deux orbites donnent donc naissance à deux opérateurs de Hecke $\mathrm{K}_p^{\pm} \in \mathrm{H}_p(\mathrm{PGSO}_n)$ tels que

$$\mathrm{K}_p = \mathrm{K}_p^+ + \mathrm{K}_p^-$$

et qui sont échangés sous l'action de $\mathrm{PGO}_n(\mathbb{Q}_p)/\mathrm{PGSO}_n(\mathbb{Q}_p) \simeq \mathbb{Z}/2\mathbb{Z}$.

Corollaire 4.13. *Soit* $W = (\mathrm{H}_{8,1}(\mathbb{R}^8) \otimes \nu^4)_{|\mathrm{PGSO}_8(\mathbb{R})}$. *Pour tout nombre premier* p, *la valeur propre de* $\mathrm{K}_p^{\pm}$ *sur la droite* $\mathrm{M}_W(\mathrm{PGSO}_8)$ *est* $p^{-4\frac{p^4-1}{p-1}}\,\tau(p)$.

Démonstration. Soit $s_0 \in \mathrm{PGO}(\mathrm{E}_8)$ l'image d'une réflexion par rapport à une racine. La conjugaison par cet élément définit un $\mathbb{Z}$-automorphisme de PGSO_8, et induit en particulier un isomorphisme $\mathrm{H}(s_0)$ de $\mathrm{H}(\mathrm{PGSO}_8)$. D'autre part, la démonstration du lemme 4.12 révèle que la symétrie s de $\mathrm{M}_W(\mathrm{PGSO}_8)$, également induite par s_0, est l'identité. Mais le lemme IV.4.3 assure que

$$T \circ s_0 = s_0 \circ \mathrm{H}(s_0)(T), \qquad \forall\, T \in \mathrm{H}(\mathrm{PGSO}_8).$$

Or on a $\mathrm{H}(s_0)(\mathrm{K}_p^+) = \mathrm{K}_p^-$ car l'image de s_0 dans $\mathrm{PGO}_8(\mathbb{Q}_p)/\mathrm{PGSO}_8(\mathbb{Z}_p)$ est non triviale pour tout nombre premier p. Il suit que K_p^+ et K_p^- ont même valeur propre sur la droite $\mathrm{M}_W(\mathrm{PGSO}_8)$, à savoir la moitié de celle de K_p. On conclut par le corollaire 4.10 et le lemme 4.12. □

4.14. Trialité pour PGSO_8

L'étape suivante repose sur la trialité pour le $\mathbb{Z}$-groupe PGSO_8. L'existence de la trialité dans ce contexte est brièvement discutée par Gross dans [Gro96, §4], qui considère plus précisément le cas du revêtement Spin_8 de G (on peut alors redescendre au groupe G par quotient). Étant donné son importance ici, il ne semble pas inutile de préciser un peu cette construction.

Nous suivrons l'approche de [BS60] dans le cas des corps, qui s'étend à tout anneau par les résultats de [KPS94]. On rappelle que si A est un anneau commutatif, une A-algèbre d'octonions [1] C est la donnée d'un q-module sur A de rang 8 muni d'une structure de A-algèbre unitaire $(x, y) \mapsto x \star y$, tels que $\mathrm{q}(x \star y) = \mathrm{q}(x)\mathrm{q}(y)$ pour tout $x, y \in C$. Le point de départ est d'enrichir le q-module E_8 d'une structure de $\mathbb{Z}$-algèbre d'octonions, de laquelle dépendra la construction d'une trialité sur PGSO_8. Ainsi que l'ont observé van der Blij et Springer [BS59, (4.5)], il existe une telle structure sur E_8, et même une seule modulo $\mathrm{O}(\mathrm{E}_8)$, à savoir l'anneau des octonions de Coxeter [Cox46].

Soit C une A-algèbre d'octonions. Considérons la propriété suivante portant sur C et $\gamma \in \mathrm{GSO}(C)$, notée $\mathcal{P}(C, \gamma)$ (*principe de trialité de Cartan*) :

$$\exists\, \gamma', \gamma'' \in \mathrm{GSO}(C),\ \gamma'(x \star y) = \gamma(x) \star \gamma''(y),\ \ \forall x, y \in C. \tag{4.6}$$

1. Dans [KPS94], les auteurs parlent aussi d'*algèbre de Cayley*, ou encore d'*algèbre de composition de rang* 8, cf. p. 51 et 56 *loc. cit.* Soulignons que l'on ne réclame pas l'associativité de $\star$, qui n'est de fait jamais satisfaite.

La proposition [KPS94, Prop. 4.5] affirme que :

(i) Si $\mathcal{P}(C,\gamma)$ est satisfaite, alors le couple (γ',γ'') est unique modulo action diagonale de $A^\times$.

(ii) Si $\mathrm{Pic}(A) = 0$ alors $\mathcal{P}(C,\gamma)$ est satisfaite pour tout $\gamma \in \mathrm{GSO}(C)$ (quand A est un corps, c'est [BS60, Thm. 1]).

(iii) Si $\gamma \in \mathrm{GSO}(C)$, alors il existe une partition de l'unité $1 = \sum_i f_i$ dans A, telle que pour tout i, $\mathcal{P}(\gamma \otimes A_{f_i}, C \otimes A_{f_i})$ est satisfaite.

On rappelle que PGSO_C est par définition le quotient de GSO_C par son sous-A-groupe central $\mathbb{G}_m$ constitué des homothéties (§II.1). Les propriétés (i) et (iii) justifient alors immédiatement la définition suivante.

Proposition-Définition 4.15. (Trialité) *Soit C une A-algèbre d'octonions et soit $\pi : \mathrm{GSO}_C \to \mathrm{PGSO}_C$ le morphisme naturel. Il existe un unique automorphisme τ du A-groupe PGSO_C ayant la propriété suivante : pour toute A-algèbre commutative B, et tout $\gamma \in \mathrm{GSO}_C(B)$ tel que $\mathcal{P}(C \otimes B, \gamma)$ est satisfaite, alors $\tau(\pi(\gamma)) = \pi(\gamma'')$.*

D'après [KPS94, Prop. 4.6] et [BS60, §1 Cor. 2], cet automorphisme τ satisfait $\tau^3 = 1$. On l'appelle *trialité du A-groupe* PGSO_C (qui ne dépend que du q-module sur A sous-jacent à C) *associée à la structure d'octonions* C. Il existe de nombreux points de vue sur la trialité dans la littérature. Une propriété géométrique fascinante, découverte par E. Study et développée par E. Cartan, est la suivante.

Lemme 4.16. *Soit C une algèbre d'octonions sur le corps k dont le* q*-module sous-jacent est hyperbolique. Soient Q_1, Q_2 et Q_3, les classes de conjugaison des sous-groupes de* $\mathrm{PGSO}(C)$ *stabilisant respectivement une droite isotrope de C ou l'un des deux types de lagrangiens de C. La trialité de* PGSO_C *permute transitivement les trois classes Q_i dans* $\mathrm{PGSO}(C)$.

Démonstration. C'est [BS60, Thm. 8]. Précisément, si $a \mapsto \overline{a} := -a + (a \cdot 1)$ désigne l'involution canonique de C, alors τ envoie le stabilisateur de la doite isotrope $k\overline{a} \subset C$ sur le stabilisateur du lagrangien $a \star C$, et ce dernier sur le stabilisateur du lagrangien $C \star a$ (qui est de type opposé). □

Soit $\tau \in \mathrm{Aut}(\mathrm{PGSO}_8)$ la trialité associée à une structure fixée d'octonions de Coxeter sur E_8. En tant qu'automorphisme du $\mathbb{Z}$-groupe PGSO_8, elle agit naturellement sur $\mathcal{R}(\mathrm{PGSO}_8)$, les $\mathcal{R}_p(\mathrm{PGSO}_8)$, et sur $\mathrm{H}(\mathrm{PGSO}_8)$ en préservant les $\mathrm{H}_p(\mathrm{PGSO}_8)$ (Lemme IV.4.3). Les inclusions naturelles $\mathrm{H}(\mathrm{O}_8) \subset \mathrm{H}(\mathrm{PGO}_8) \subset \mathrm{H}(\mathrm{PGSO}_8)$ permettent de voir l'opérateur de Hecke T_p comme un élément de $\mathrm{H}(\mathrm{PGSO}_8)$.

Corollaire 4.17. *Pour tout nombre premier p, l'application $T \mapsto \mathrm{H}(\tau)(T)$ induit un 3-cycle du sous-ensemble $\{\mathrm{T}_p, \mathrm{K}_p^+, \mathrm{K}_p^-\} \subset \mathrm{H}_p(\mathrm{PGSO}_8)$.*

Démonstration. Soient $G = \mathrm{PGSO}_8$, $M = \mathrm{E}_8$ et $V_0 = \mathrm{E}_8 \otimes \mathbb{Q}$. L'élément $\underline{M} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V_0) = \mathcal{R}(G)$ a bien sûr pour stabilisateur $G(\widehat{\mathbb{Z}})$ sous l'action de $G(\mathbb{A}_f)$, il est donc préservé par τ. Soient Ω_1, Ω_2 et Ω_3 les $G(\widehat{\mathbb{Z}})$-orbites dans $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V_0)$ constituées respectivement des classes d'isométrie de p-voisins de M, ou des deux types de perestroïkas de M relativement à p. Ces orbites se factorisent manifestement en des $G(\mathbb{F}_p)$-orbites, les classes de conjugaison de stabilisateurs de $G(\mathbb{F}_p)$-correspondantes étant exactement les classes Q_i du lemme précédent appliqué à $C = \mathrm{E}_8 \otimes \mathbb{F}_p$, ce qui conclut. □

Si $d \geq 0$, on a déjà dit que la représentation $\mathrm{H}_{d,r}(\mathbb{R}^{2r})$ est irréductible en tant que représentation de $\mathrm{GO}(\mathbb{R}^{2r})$. Cependant, il suit de [KV78, Thm. 6.13] que sa restriction à $\mathrm{GSO}(\mathbb{R}^{2r})$ se décompose en somme directe de deux représentations irréductibles non isomorphes

$$\mathrm{H}_{d,r}(\mathbb{R}^{2r}) = \mathrm{H}_{d,r}(\mathbb{R}^{2r})^+ \oplus \mathrm{H}_{d,r}(\mathbb{R}^{2r})^-$$

que nous ne chercherons pas à distinguer. Concrètement, si $e_1, \ldots, e_r$ est une base d'un lagrangien $I \subset \mathbb{C}^{2r}$, la fonction $(v_1, \ldots, v_r) \mapsto \text{dét}[e_i \cdot v_j]^d$ est dans $\mathrm{H}_{d,r}(\mathbb{R}^{2r})^{\pm}$ le signe $\pm$ étant uniquement déterminé par le type du lagrangien I. Observons que si $d = 0$, auquel cas $\mathrm{H}_{d,r}(\mathbb{R}^{2r}) \simeq \Lambda^r(\mathbb{R}^{2r})^*$, ce phénomène est bien connu !

Soient Γ un groupe, U un Γ-module et $\sigma \in \mathrm{Aut}(\Gamma)$. On note U^σ le Γ-module obtenu par restriction de U via $\sigma : \Gamma \to \Gamma$.

Corollaire 4.18. *Soient $d \equiv 0 \bmod 2$. L'application $U \mapsto U^\tau$ induit un 3-cycle de l'ensemble constitué des classes d'isomorphisme des trois représentations de* $\mathrm{PGSO}_8(\mathbb{R})$

$$\mathrm{H}_{d,1}(\mathbb{R}^8) \otimes \nu^{d/2} \text{ et } \mathrm{H}_{d/2,4}(\mathbb{R}^8)^{\pm} \otimes \nu^d.$$

Démonstration. Observons que les espaces $\mathrm{H}_{d,g}(\mathbb{R}^8)$ sont munis d'actions naturelles de $\mathrm{GO}_8(\mathbb{C})$ étendant les opérations de $\mathrm{GO}_8(\mathbb{R})$ considérées précédemment. En particulier, les trois représentations de l'énoncé se factorisent en des représentations de $\mathrm{PGSO}_8(\mathbb{C})$, qui sont bien sûr irréductibles. Rappelons que $V = \mathbb{R}^8$.

Soit $D \subset V \otimes \mathbb{C}$ une droite isotrope. Le stabilisateur $S_D \subset \mathrm{PGSO}_8(\mathbb{C})$ de la droite D est un sous-groupe parabolique isomorphe à $\mathrm{GSO}(\mathbb{C}^6) \ltimes \mathbb{C}^6$. Son action naturelle sur $V^{\otimes 2} \otimes \nu^{-1}$ préserve la droite $D^{\otimes 2}$, sur laquelle il

agit donc par multiplication par un caractère que nous noterons η_D. Soit $\ell(D) \subset \mathrm{H}_{d,1}(\mathbb{R}^8) \otimes \nu^{d/2}$ la droite de polynômes harmoniques associés à D (formule (4.1)). On constate que $\ell(D)$ est propre de caractère $\eta_D^{d/2}$ sous l'action de S_D.

De même, soit $I \subset V \otimes \mathbb{C}$ un lagrangien. Le stabilisateur $S_I \subset \mathrm{PGSO}_8(\mathbb{C})$ de I est un sous-groupe parabolique isomorphe à $\mathrm{GL}(\mathbb{C}^4)/\{\pm 1\} \ltimes \mathrm{Sym}^2(\mathbb{C}^4)$. Son action naturelle sur $\Lambda^4 V \otimes \nu^{-2}$ préserve la droite $\Lambda^4 I$, sur laquelle il agit donc par un caractère que nous noterons η_I. La doite $\ell(I) \subset \mathrm{H}^{\pm}_{d/2,4}(\mathbb{R}^8) \otimes \nu^d$ de polynômes harmoniques associés à I, le signe $\pm$ dépendant du type du lagrangien I, est manifestement propre de caractère $\eta_I^{d/2}$ sous l'action de S_I.

Rappelons que d'après la théorie du plus haut poids de Cartan-Weyl, étant donné un sous-groupe parabolique S du groupe semi-simple $G = \mathrm{PGSO}_8(\mathbb{C})$, et un caractère polynômial $\eta : S \to \mathbb{C}^\times$, il existe à isomorphisme près au plus une représentation polynômiale irréductible de G dont la restriction à S contienne le caractère η. De plus, si une telle représentation existe pour le couple (S, η) avec $\eta \neq 1$, elle n'existe pas pour le couple (S, η^{-1}) (propriété de dominance).

Les observations ci-dessus caractérisent donc uniquement les trois représentations de l'énoncé. Pour conclure, on observe que τ permute les trois types de sous-groupes paraboliques considérés ci-dessus d'après le lemme 4.16, et ce avec leur caractère distingué $S \to \mathbb{C}^\times$ noté η_* ci-dessus. En effet, cette dernière propriété est automatique car si S est un tel parabolique, on observe que le groupe des caractères polynômiaux $S \to \mathbb{C}^\times$ est isomorphe à $\mathbb{Z}$, le caractère η étant l'unique générateur dominant d'après le cas $d = 2$. $\square$

Soit d un entier pair. Quitte à échanger les signes $\pm$, on peut supposer que $(\mathrm{H}_{d,1}(\mathbb{R}^8) \otimes \nu^{d/2})^\tau \simeq \mathrm{H}_{d/2,4}(\mathbb{R}^8)^+ \otimes \nu^d$ d'après le corollaire ci-dessus. D'après le lemme IV.4.3, l'automorphisme τ induit un isomorphisme

$$\tau^* : \mathrm{M}_{\mathrm{H}_{d/2,4}(\mathbb{R}^8)^+ \otimes \nu^d}(\mathrm{PGSO}_8) \xrightarrow{\sim} \mathrm{M}_{\mathrm{H}_{d,1}(\mathbb{R}^8) \otimes \nu^{d/2}}(\mathrm{PGSO}_8)$$

tel que $T \circ \tau^* = \tau^* \circ \mathrm{H}(\tau)(T)$ pour tout $T \in \mathrm{H}(\mathrm{PGSO}_8)$.

Corollaire 4.19. *Soit d un entier pair. On a une suite d'isomorphismes :*

$$\begin{tikzcd}
\mathrm{M}_{\mathrm{H}_{d/2,4}(\mathbb{R}^8)^+ \otimes \nu^d}(\mathrm{PGSO}_8) \arrow[r, "\mathrm{ind}", "\sim"'] \arrow[d, "\tau^*"', "\wr"] & \mathrm{M}_{\mathrm{H}_{d/2,4}(\mathbb{R}^8) \otimes \nu^d}(\mathrm{PGO}_8) \arrow[r, "\mu^*", "\sim"'] & \mathrm{M}_{\mathrm{H}_{d/2,4}(\mathbb{R}^8)}(\mathrm{O}_8) \\
\mathrm{M}_{\mathrm{H}_{d,1}(\mathbb{R}^8) \otimes \nu^{d/2}}(\mathrm{PGSO}_8) \arrow[rr, "\mu^*", "\sim"'] & & \mathrm{M}_{\mathrm{H}_{d,1}(\mathbb{R}^8)}(\mathrm{SO}_8)
\end{tikzcd}$$

Démonstration. Tous ces isomorphismes ont déjà été décrits, à l'exception de celui de la ligne du bas, noté μ^*. C'est le morphisme définit par le restriction des fonctions par la bijection $\mathcal{R}(\mathrm{SO}_n) \to \mathcal{R}(\mathrm{PGSO}_n)$, qui est un isomorphisme pour des raisons identiques à celles évoquées dans la démonstration du lemme 4.8. □

Corollaire 4.20. *La valeur propre de* T_p *sur la droite* $\mathrm{M}_{\mathrm{H}_{4,4}(\mathbb{R}^8)}(\mathrm{O}_8)$ *est*

$$p^{-4}\,\frac{p^4-1}{p-1}\,\tau(p).$$

Démonstration. On applique le corollaire 4.19 à $d = 8$. Le corollaire 4.13 et le lemme 4.17 montrent que la valeur propre de l'opérateur de Hecke T_p sur la droite $\mathrm{M}_{\mathrm{H}_{4,4}(\mathbb{R}^8)^+\otimes\nu^8}(\mathrm{PGSO}_8)$ est celle de l'énoncé. On conclut car μ^* et ind sont $\mathrm{H}(\mathrm{O}_8)$-équivariants (Lemme 4.8, §4.11). □

4.21. Une dernière série thêta et fin de la démonstration

Considérons pour finir l'application

$$\vartheta_{4,4} : \mathrm{M}_{\mathrm{H}_{4,4}(\mathbb{R}^8)}(\mathrm{O}_8) \longrightarrow \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})).$$

Proposition 4.22. $\vartheta_{4,4}$ *est un isomorphisme.*

Démonstration. En effet, les deux espaces étant de dimension 1 (formule (2.3), Corollaire 4.20), il suffit de voir que cette application est non nulle, ce qui a déjà été vérifié par Breulmann et Kuss dans [BK00]. Expliquons rapidement comment on peut procéder.

Soient $e = (e_1, \ldots, e_4)$ un quadruplet d'éléments de $\mathrm{E}_8 \otimes \mathbb{C}$ engendrant un lagrangien, et $P_e(v_1, \ldots, v_4) = \text{dét}[e_i \cdot v_j]_{1\le i,j\le 4}$; pour tout entier $d \ge 0$ on a $P_e^d \in \mathrm{H}_{d,4}(\mathbb{R}^8)$. Soient $Q \subset \mathrm{E}_8$ un sous-réseau de rang 4, ainsi que $v_1, \ldots, v_4$ une $\mathbb{Z}$-base de Q. La relation $P_e(\gamma(v_1), \ldots, \gamma(v_4))) = \det(\gamma)P_e(v_1, \ldots, v_4)$ pour tout $\gamma \in \mathrm{GL}(Q)$ montre que $P_e(v_1, \ldots, v_4)^d$ ne dépend pas du choix des v_i lorsque d est pair ; il y a donc un sens à le noter $P_e(Q)^d$. En particulier, si d est pair le coefficient de Fourier de la série thêta $\vartheta_{d,4}(\mathrm{E}_8, P_e^d)$ correspondant à la matrice de Gram d'une $\mathbb{Z}$-base de Q est

$$\mathrm{c}_Q(P_e^d) = |\mathrm{O}(Q)| \sum_M P_e(M)^d,$$

la somme portant sur l'ensemble des sous-réseaux $M \subset \mathrm{E}_8$ isométriques à Q. Nous donnons quelques valeurs numériques dans la table V.3.

TABLE V.3 – Quelques valeurs de $\frac{c_Q(P_e^d)}{|O(Q)|}$ où $e = (\varepsilon_{2j-1} + i\varepsilon_{2j})_{1\leq j\leq 4}$

$Q \setminus d$	0	2	4	6	8	10
D_4	3150	0	4800	-4800	43200	-81600
A_4	24192	0	-23040	-46080	-69120	-92160
$A_1 \oplus A_3$	151200	0	115200	1267200	6566400	7718400
${A_2}^2$	67200	0	115200	-1382400	4492800	-43084800
${A_1}^2 \oplus A_2$	302400	0	-691200	2073600	85017600	214963200
${A_1}^4$	122850	0	576000	-6796800	191808000	-343641600
$\dim M_{H_{d,4}(\mathbb{R}^8)}(O_8)$	1	0	1	1	1	2

Dans cette table, $Q \simeq Q(R)$ où R est un système de racines (de type ADE) de rang 4 (§I.3) et $(\varepsilon_j)_{1\leq j\leq 8}$ désigne la base canonique de $\mathbb{R}^8$. Il n'est pas difficile d'énumerer à l'aide de l'ordinateur tous les sous-réseaux de E_8 isométriques à Q. Par exemple, si Φ désigne un système positif de $R(E_8)$, et si $<$ désigne un ordre total arbitraire fixé de Φ, les sous-réseaux de E_8 isométriques à D_4 sont en bijection avec les quadruplets (r_1, r_2, r_3, r_4) d'éléments de Φ tels que $r_1 < r_2 < r_3$, et tels que les éléments r_1, r_2 et r_3 soient deux à deux orthogonaux et de produit scalaire -1 avec r_4. Nous renvoyons à la feuille de calculs [CL `PARI`] pour une implémentation de cet algorithme sous `PARI` et pour une justification de la table V.3.

La proposition découle du fait que $c_{D_4}(P_e^4) \neq 0$. Constatons également, pour se rassurer, que l'on retrouve bien l'égalité $c_{D_4}(P_e^4) = -c_{A_4}(P_e^4)$, ce qui est en accord avec la proposition 2.1. □

Remarque 4.23. La dernière ligne de la table V.3 découle de l'isomorphisme $M_{H_{d,4}(\mathbb{R}^8)}(O_8) \simeq M_{H_{2d,1}(\mathbb{R}^8)}(SO_8)$ ($\simeq H_{2d,1}(\mathbb{R}^8)^{W(E_8)^+}$) donné par le corollaire 4.20, ainsi que du lemme 4.2. La nullité de ces espaces quand $d = 2$ explique celle de la colonne $d = 2$ de la table. La table montre donc que $\vartheta_{d,4}$ est injectif quand d est pair et ≤ 8. En faisant varier la base lagrangienne e, il est facile de vérifier que $\vartheta_{10,4}$ est également injective.

Cela conclut la démonstration du (ii) du théorème 2.2, en vertu du corollaire 4.20 et des relations de commutation d'Eichler (4.4). La suite d'iso-

morphismes suivante résume assez bien notre démonstration. On a posé $W = \mathrm{H}_{8,1}(\mathbb{R}^8)$, $U = \mathrm{H}_{4,4}(\mathbb{R}^8)$ et $U^+ = \mathrm{H}_{4,4}(\mathbb{R}^8)^+$.

$$\begin{tikzcd}
\mathrm{M}_{W\otimes\nu^4}(\mathrm{PGSO}_8) & \mathrm{M}_{W\otimes\nu^4}(\mathrm{PGO}_8) \arrow[l, "\mathrm{res}", "\sim"'] \arrow[r, "\mu^*", "\sim"'] & \mathrm{M}_W(\mathrm{O}_8) \arrow[r, "\vartheta_{8,1}", "\sim"'] & \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z})) \\
\mathrm{M}_{U^+\otimes\nu^8}(\mathrm{PGSO}_8) \arrow[u, "\tau^*", "\wr"'] \arrow[r, "\sim", "\mathrm{ind}"'] & \mathrm{M}_{U\otimes\nu^8}(\mathrm{PGO}_8) \arrow[r, "\sim", "\mu^*"'] & \mathrm{M}_U(\mathrm{O}_8) \arrow[r, "\sim", "\vartheta_{4,4}"'] & \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))
\end{tikzcd}$$

5. Appendice : un exemple simple de relation d'Eichler

On se propose de démontrer la formule IV.(4.4) pour $g = 1$. Soient L un réseau unimodulaire pair de rang r et $P : L \otimes \mathbb{R} \to \mathbb{C}$ un polynôme harmonique homogène de degré d. On rappelle que la série thêta associée $\vartheta(L, P) = \sum_{v\in L} P(v) q^{\frac{v\cdot v}{2}}$ est un élément de $\mathrm{M}_{d+r/2}(\mathrm{SL}_2(\mathbb{Z}))$.

Théorème 5.1. *Soient L un réseau unimodulaire pair de rang r, $P : L\otimes\mathbb{R} \to \mathbb{C}$ un polynôme harmonique homogène de degré d, et p un nombre premier. On a la relation*

$$\sum_{L'} \vartheta(L', P) = \left(p\,\frac{p^{r-3}-1}{p-1} \,+\, p^{-d}\,\mathrm{T}(p^2) \right) \vartheta(L, P),$$

où $L' \subset \frac{1}{p}L$ parcourt les p-voisins de L.

Démonstration. On notera $\mathrm{a}_n(g)$ le n-ième coefficient de Fourier de la forme modulaire $g \in \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}))$. On rappelle la relation [Ser70, p. 164]

$$\mathrm{a}_n(\mathrm{T}(p^2)(g)) = \sum_{d|(p^2,n)} d^{k-1} \mathrm{a}_{\frac{np^2}{d^2}}(g).$$

On pose $f = \sum_{L'} \vartheta(L', P)$ où $L' \subset \frac{1}{p}L$ parcourt les p-voisins de L.

Fixons $n \geq 1$ un entier, pour l'instant premier à p, et posons $\mathrm{q}(x) = \frac{x\cdot x}{2}$ pour tout $x \in L \otimes \mathbb{R}$. Considérons l'ensemble X des couples (L', w) où L' est un p-voisin de L et w est un élément de L' tel que $\mathrm{q}(w) = n$. Soit aussi $Y = \{v \in L, \mathrm{q}(v) = np^2\}$. On dispose d'une application évidente

$$\pi : X \to Y, \quad (L', w) \mapsto pw.$$

Nous allons voir que π est surjective et examiner ses fibres. Soit $v \in Y$, il y a deux cas :

(1) v est dans pL. Dans ce cas, $w = v/p$ est dans L et il y a donc autant de p-voisins L' de L contenant w que de sous-réseaux d'indice p de L contenant w et qui sont l'orthogonal d'une droite isotrope modulo p (les "M" du §III.1). Comme on a $(\mathrm{q}(w), p) = 1$, w est non isotrope mod pL : on trouve $|\pi^{-1}(\{v\})| = \frac{p^{r-2}-1}{p-1}$.

(2) v n'est pas dans pL. Dans ce cas, il engendre une droite isotrope dans L/pL. Si M est son orthogonal modulo p, c'est-à-dire l'ensemble des $x \in L$ tels que $x.v \in p\mathbb{Z}$, alors $L' = M + \mathbb{Z}\frac{v}{p}$ est un p-voisin de L car p^2 divise $\mathrm{q}(v)$. Mieux, c'est l'unique p-voisin de L contenant $w = v/p$. En effet, si K est un tel p-voisin, et si $N = L \cap K$, alors v est dans N et pour tout x dans K on a $x.\frac{v}{p} \in \mathbb{Z}$. En particulier, $N \subset M$, puis $N = M$ et $K = L'$. Ainsi, $|\pi^{-1}(\{v\})| = 1$.

Supposons d'abord $P = 1$ (et donc $h = 0$). Cette analyse montre

$$\mathrm{a}_n(f) = |X| = \frac{p^{r-2}-1}{p-1}\mathrm{a}_n(\vartheta(L,1)) + (\mathrm{a}_{np^2}(\vartheta(L,1)) - \mathrm{a}_n(\vartheta(L,1))),$$

qui est la formule cherchée du moins pour les coefficients d'indice premier à p. Quand P est quelconque, $\mathrm{a}_n(f)$ est la somme des $p^{-d}P(v)$ pour $(L', v/p)$ parcourant X, et donc

$$\mathrm{a}_n(f) = \frac{p^{r-2}-1}{p-1}\mathrm{a}_n(\vartheta(L,P)) + (p^{-d}\mathrm{a}_{np^2}(\vartheta(L,P)) - \mathrm{a}_n(\vartheta(L,P))),$$

On conclut par le lemme suivant :

Lemme 5.2. *Soient $g \in \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}))$, $k > 0$, et p premier. On suppose que $\mathrm{a}_n(g) = 0$ pour tout n premier à p. Alors $g = 0$.*

Démonstration. En effet, la fonction holomorphe $g(\tau)$ est alors invariante par $\tau \mapsto \tau + \frac{1}{p}$, et on conclut car le sous-groupe de $\mathrm{SL}_2(\mathbb{R})$ engendré par cette translation et $\mathrm{SL}_2(\mathbb{Z})$ n'est pas discret. □

On peut aussi vérifier la formule pour tous les coefficients, en introduisant encore $\pi : X \to Y$ comme précédemment. On constate que le décompte n'est pas modifié pour le cas (2), mais uniquement pour le (1).

Premier sous-cas : $\frac{n}{p} \in \mathbb{Z} - p\mathbb{Z}$. Soit v dans Y de la forme pw avec $w \in L$. Remarquons que $w \notin pL$ car p^2 ne divise pas $\mathrm{q}(w) = n$, par contre w est isotrope dans L/pL. Mais si $x \in L/pL$ est un vecteur isotrope, il existe

$$1 + p\,\mathrm{c}_{r-2}(p) = \frac{p^{r-2}-1}{p-1} + p^{r/2-1}$$

droites isotropes de L/pL orthogonales à x, c'est donc aussi $|\pi^{-1}(\{v\})|$. Ici, $\mathrm{c}_i(p) = \frac{p^{i-1}-1}{p-1} + p^{i/2-1}$ est le cardinal de la quadrique hyperbolique de rang i sur $\mathbb{Z}/p\mathbb{Z}$. On en déduit

$$\mathrm{a}_n(f) = (\frac{p^{r-2}-1}{p-1} + p^{r/2-1})\mathrm{a}_n(\vartheta(L,P)) + (p^{-d}\mathrm{a}_{np^2}(\vartheta(L,P)) - \mathrm{a}_n(\vartheta(L,P))),$$

ce qui conclut.

Second sous-cas : p^2 divise n. Soit v dans Y de la forme pw avec w dans L. Alors w est isotrope dans L/pL. Si il est nul, il est dans tous les p-voisins de L : $|\pi^{-1}(\{v\})| = \mathrm{c}_r(p)$. Sinon, on a comme ci-dessus $|\pi^{-1}(\{v\})| = \frac{p^{r-2}-1}{p-1} + p^{r/2-1}$. Mais

$$\mathrm{c}_r(p) - \frac{p^{r-2}-1}{p-1} - p^{r/2-1} = p^{r-2}$$

On en déduit l'identité

$$\mathrm{a}_n(f) = p^{d+r-2}\mathrm{a}_{n/p^2}(\vartheta(L,P)) + (\frac{p^{r-2}-1}{p-1} + p^{r/2-1})\mathrm{a}_n(\vartheta(L,P))$$

$$+(p^{-d}\mathrm{a}_{np^2}(\vartheta(L,P)) - \mathrm{a}_n(\vartheta(L,P))).$$

Ce qui conclut. $\square$

VI. Paramétrisation de Langlands

1. Rappels et notations sur les k-groupes réductifs

Soit k un corps algébriquement clos. Nous renvoyons aux traités de Springer [SPR81] et Borel [BOR91] pour la théorie des k-groupes réductifs. Notre convention est qu'un tel k-groupe est connexe. Si k est de caractéristique nulle, on rappelle qu'un k-groupe connexe G est dit réductif si la catégorie de ses k-représentations de dimension finie est semi-simple.

Si A est un anneau quelconque, un A-groupe G est dit réductif s'il est lisse sur A et si pour tout homomorphisme de A vers un corps algébriquement clos k, le groupe $G \times_A k$ est réductif : voir [SGA3] et [CON11]. Les A-groupes classiques étudiés au § II. 1 sont donc réductifs [BOR91, §23] [CON11, App. C], excepté le groupe orthogonal en dimension paire qui n'est pas connexe, ainsi que les groupes de similitudes et similitudes projectives associés pour la même raison. Un A-groupe est dit semi-simple s'il est réductif et si son centre est fini sur A. Le centre (schématique) d'un A-groupe réductif G sera noté $\mathrm{Z}(G)$. Une *isogénie centrale* $G \to G'$ entre deux A-groupes réductifs est un morphisme fini et plat de A-groupes qui est surjectif et de noyau (au sens schématique) inclus dans $\mathrm{Z}(G)$. Plus généralement, un morphisme de A-groupes $G \to G'$ sera dit *central* si le morphisme induit $G \times \mathrm{Z}(G') \to G'$ est plat, surjectif et de noyau inclus dans $\mathrm{Z}(G) \times \mathrm{Z}(G')$.

1.1. La donnée radicielle basée d'un k-groupe réductif

Soit k un corps algébriquement clos. La théorie des systèmes de racines des k-groupes réductifs, convenablement formulée, produit une équivalence de catégorie canonique

$$\Psi : \mathcal{C}_k \xrightarrow{\sim} \mathcal{D}$$

entre la catégorie $\mathcal{C}_k$ des k-groupes réductifs "à automorphismes intérieurs près" et la catégorie $\mathcal{D}$ des *données radicielles basées*. Cette classification est due à Chevalley dans le cas des groupes semi-simples et au séminaire Demazure-Grothendieck [SGA3, Exp. XXI] en général, où elle est même étudiée sur un anneau k quelconque. Nous nous contenterons ci-dessous de

préciser son énoncé, en renvoyant à [Spr81] pour un exposé détaillé, également résumé dans [Spr79] et [Jan03, II, Ch. 1], ainsi qu'à Kottwitz [Kot84, §1] pour la formulation intrinsèque adoptée ici.

Si G est un k-groupe réductif, on note $\mathrm{Int}(G)$ le groupe des automorphismes *intérieurs* de G, i.e. de la forme $\mathrm{int}_g : x \mapsto gxg^{-1}$, pour $g \in G(k)$. Si G et G' sont deux k-groupes réductifs on note également $\mathrm{Hom}_c(G, G')$ l'ensemble des morphismes centraux de G vers G'. Il est muni d'une action évidente de $\mathrm{Int}(G')$. On observe qu'il y a un sens à considérer la catégorie $\mathcal{C}_k$ dont les objets sont les k-groupes réductifs et ayant pour morphismes $G \to G'$ l'ensemble quotient $\mathrm{Hom}_c(G, G')/\mathrm{Int}(G')$, la composition des morphismes se déduisant de celle des morphismes centraux par passage au quotient.

Rappelons qu'une *donnée radicielle basée* est la donnée :

- de deux groupes abéliens libres de rang fini X et $X^\vee$ munis d'un accouplement parfait $\langle -, - \rangle : X \times X^\vee \to \mathbb{Z}$,
- de parties finies $\Phi \subset X$ et $\Phi^\vee \subset X^\vee$ munies d'une bijection $\Phi \to \Phi^\vee$ notée $\alpha \mapsto \alpha^\vee$,
- de sous-ensembles $\Delta \subset \Phi$ et $\Delta^\vee \subset \Phi^\vee$ tels que $\Delta^\vee = \{\alpha^\vee, \alpha \in \Delta\}$,

soumis aux conditions suivantes :

- pour tout $\alpha \in \Phi$, on a $\langle \alpha, \alpha^\vee \rangle = 2$,
- si $s_\alpha \in \mathrm{End}(X)$ désigne la reflexion $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$, et si $s_{\alpha^\vee} \in \mathrm{End}(X^\vee)$ est définie de manière similaire en échangeant α et $\alpha^\vee$, alors pour tout $\alpha \in \Phi$ on a $s_\alpha(\Phi) = \Phi$ et $s_{\alpha^\vee}(\Phi^\vee) = \Phi^\vee$.

Il résulte de ces axiomes que si $\mathrm{Q}(\Phi) \subset X$ désigne le groupe abélien engendré par les éléments de Φ, alors Φ est un système de racines dans $\mathrm{Q}(\Phi) \otimes \mathbb{Q}$ au sens de Bourbaki [Bou81b, Ch. VI]. On supposera enfin que

- Φ est réduit [1] et Δ en est une base.

Un morphisme $\psi_1 \to \psi_2$ entre deux données radicielles basées $\psi_i = (X_i, \Phi_i, \Delta_i, X_i^\vee, \Phi_i^\vee, \Delta_i^\vee)$ est la donnée d'une application linéaire $X_2 \to X_1$ induisant une bijection $\Phi_2 \to \Phi_1$ envoyant Δ_2 sur Δ_1, et dont la transposée $X_1^\vee \to X_2^\vee$ induit également une bijection $\Phi_1^\vee \to \Phi_2^\vee$ envoyant $\Delta_1^\vee$ sur $\Delta_2^\vee$. Cela définit la catégorie $\mathcal{D}$. Une *isogénie* $\psi_1 \to \psi_2$ est un morphisme comme ci-dessus induisant un isomorphisme $X_2 \otimes \mathbb{Q} \to X_1 \otimes \mathbb{Q}$. Il ne nous reste qu'à rappeler la définition du foncteur Ψ.

1. Soulignons que cette hypothèse ne fait pas partie des axiomes dans les références sus-citées, elle nous évitera quelques circonvolutions.

Si G est un k-groupe réductif, la donnée radicielle basée $\Psi(G)$ qui lui est associée s'obtient ainsi. On choisit un tore maximal T de G ainsi qu'un sous-groupe de Borel B contenant T. On note

$$\mathrm{X}^*(T) = \mathrm{Hom}(T, \mathbb{G}_m), \;\; \mathrm{X}_*(T) = \mathrm{Hom}(\mathbb{G}_m, T),$$

les groupes abéliens libres de rang fini respectivement constitués des caractères et des co-caractères du tore T. Ils sont munis d'une dualité parfaite évidente $\langle -, - \rangle : \mathrm{X}^*(T) \times \mathrm{X}_*(T) \longrightarrow \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$. On pose alors

$$\Psi(G, T, B) = (X^*(T), \Phi(G, T), \Delta(G, T, B), X_*(T), \Phi^\vee(G, T), \Delta^\vee(G, T, B)),$$

où $\Phi(G, T)$ (resp. $\Phi^\vee(G, T)$) désigne l'ensemble des racines (resp. coracines [2]) de G relativement à T, et où $\Delta(G, T, B)$ est la base de $\Phi(G, T)$ associée au système positif de $\Phi(G, T)$ intervenant dans $\mathrm{Lie}(B)$. C'est une donnée radicielle basée.

Si l'on change le couple (T, B) en (T', B'), il existe un élément $g \in G(k)$ unique modulo $T(k)$ tel que $gTg^{-1} = T'$ et $gBg^{-1} = B'$. L'automorphisme intérieur int_g induit un isomorphisme $\Psi(G, T, B) \xrightarrow{\sim} \Psi(G, T', B')$ dans $\mathcal{D}$ qui est indépendant du choix de g.

Suivant Kottwitz [Kot84, §1], on définit $\Psi(G)$ comme étant la limite inductive (ou projective !) des $\Psi(G, T, B)$, indexée par les couples (T, B), avec pour morphismes de transition les isomorphismes induits par des éléments de $\mathrm{Int}(G)$. La construction $G \mapsto \Psi(G)$ est fonctorielle en les morphismes centraux et fait correspondre à une isogénie centrale une isogénie de données radicielles. En particulier, le groupe $\mathrm{Aut}(G)$ des automorphismes du k-groupe G agit sur $\mathrm{Aut}_{\mathcal{D}}(\Psi(G))$, le sous-groupe $\mathrm{Int}(G)$ agissant trivialement.

Jusqu'ici k était un corps algébriquement clos. Mentionnons que la définition du foncteur Ψ s'étend verbatim au cas d'un anneau quelconque k si l'on se restreint à la sous-catégorie de $\mathcal{C}_k$ constituée des k-groupes réductifs *déployés* [SGA3, XXII Prop. 1.14], [Jan03, II Ch. 1]. Si k est un anneau intègre tel que $\mathrm{Pic}(k) = 0$ (par exemple un corps ou un anneau principal), ce sont les k-groupes réductifs possédant un tore maximal déployé, i.e. isomorphe à une puissance de $\mathbb{G}_m$. En particulier, il y a un sens à parler de la donnée radicielle basée $\Psi(G)$ d'un tel k-groupe. Elle s'identifie canoniquement dans $\mathcal{D}$ à celle de $G \times_k K$ pour tout homomorphisme de k vers un corps algébriquement clos K.

2. Soit $\alpha \in \Phi(G, T)$, soit $T_\alpha \subset T$ la composante neutre du noyau de $\alpha : T \to \mathbb{G}_m$, et soit Z_α le groupe dérivé du centralisateur dans G de T_α. C'est un k-groupe isomorphe à SL_2 ou PGL_2. On rappelle que la coracine $\alpha^\vee \in \mathrm{X}_*(T)$ est l'unique cocaractère d'image dans Z_α tel que $\langle \alpha, \alpha^\vee \rangle = 2$.

Vocabulaire

Lorsqu'un k-groupe réductif G a une donnée radicielle basée bien définie, on parlera librement du système de racines de G, des racines simples/positives de G, du groupe de Weyl de G, etc... pour désigner les objets analogues déduits de $\Psi(G)$. Par exemple, le groupe de Weyl de G est le sous-groupe $W \subset \mathrm{Aut}(X)$ engendré par l'ensemble des s_α avec $\alpha \in \Delta$, où $\Psi(G) = (X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$. Un élément de X est appelé *poids* de G, et le groupe abélien X le *réseau des poids* de G ; de même $X^\vee$ est le *réseau des co-poids* de G.

1.2. Dual de Langlands

Si $\psi = (X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$ est une donnée radicielle basée, alors

$$\psi^\vee = (X^\vee, \Phi^\vee, \Delta^\vee, X, \Phi, \Delta)$$

en est encore une de manière évidente, appelée *donnée duale* de ψ. L'association $\psi \mapsto \psi^\vee$ définit un endofoncteur contravariant involutif de $\mathcal{D}$. Lorsque k est algébriquement clos, il induit via l'équivalence de catégories Ψ une involution de $\mathcal{C}_k$: c'est le point de départ de la notion de dual de Langlands, à ceci près que l'on fait intervenir le corps de complexes.

Précisément, si G est un k-groupe réductif déployé, un *groupe dual* de G au sens de Langlands est la donnée d'un $\mathbb{C}$-groupe réductif $\widehat{G}$ et d'un isomorphisme $\Psi(\widehat{G}) \xrightarrow{\sim} \Psi(G)^\vee$ dans $\mathcal{D}$. Le $\mathbb{C}$-groupe $\widehat{G}$ est alors uniquement déterminé par G à isomorphismes intérieurs près. Par abus de language, on l'appelle le *dual de Langlands de G*.

1.3. Exemples

Nous laissons au lecteur le soin de vérifier que $\widehat{\mathrm{GL}}_n(\mathbb{C}) \simeq \mathrm{GL}_n(\mathbb{C})$ et $\widehat{\mathrm{PGL}}_n(\mathbb{C}) \simeq \mathrm{SL}_n(\mathbb{C})$. En revanche, il nous sera utile de détailler les cas (très classiques !) des groupes orthogonaux et symplectiques.

Nous utiliserons à plusieurs reprises la construction suivante. Soient $\psi = (X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$ une donnée radicielle basée et $Y \subset X \otimes \mathbb{Q}$ un sous-groupe de type fini contenant Φ. On suppose

$$\Phi^\vee \subset Y^\sharp := \{x \in X^\vee \otimes \mathbb{Q},\ \ \langle y, x\rangle \subset \mathbb{Z} \quad \forall y \in Y\}.$$

L'orthogonal $Y^\perp$ de Y dans $X^\vee \otimes \mathbb{Q}$ est alors d'intersection nulle avec $\mathrm{Q}(\Phi^\vee)$, et si $\pi : \mathrm{Q}(\Phi^\vee) \to Y^\sharp/Y^\perp$ désigne l'application canonique, on constate que

$$\psi' = (Y, \Phi, \Delta, Y^\sharp/Y^\perp, \pi(\Phi^\vee), \pi(\Delta^\vee))$$

est une donnée radicielle basée de manière évidente. Si l'on a une inclusion $Y \subset X$ (resp. $X \subset Y$), elle induit un morphisme $\psi \to \psi'$ (resp. une isogénie $\psi' \to \psi$). Cette construction appliquée à $\psi^\vee$ fournit par ailleurs une construction similaire dans laquelle caractères et co-caractères sont échangés.

Dans ce qui suit k est un anneau quelconque.

Groupe spécial orthogonal pair et ses variantes

Soient $r \geq 2$ un entier, $U = k^r$ et $V = \mathrm{H}(U) = U \oplus U^*$ le q-module hyperbolique sur U (§ II.1). Le k-groupe $\widetilde{G} = \mathrm{GSO_V}$ est réductif et déployé.

Si $(e_i)_{i=1}^r$ est une k-base de U, et si $e_i^* \in U^*$ désigne sa base duale, le k-sous-groupe $\widetilde{T}$ de $\widetilde{G}$ préservant chacune des droites ke_i et ke_j^* est un tore maximal déployé de $\widetilde{G}$. Le k-sous-groupe de $\widetilde{G}$ préservant le drapeau complet de U associé à $\{e_1\}$, $\{e_1, e_2\}$, ..., est un sous-groupe de Borel contenant $\widetilde{T}$.

Soit $\varepsilon_i \in \mathrm{X}^*(\widetilde{T})$ le caractère de $\widetilde{T}$ agissant sur ke_i, soit $\nu : \widetilde{G} \to \mathbb{G}_m$ le facteur de similitude, et soit ε_0 la restriction de ν à $\widetilde{T}$. On constate que $\widetilde{T}$ agit sur ke_j^* par multiplication par le caractère $-\varepsilon_j + \varepsilon_0$. Les ε_i, $i = 0, \ldots, r$ forment une $\mathbb{Z}$-base de $\mathrm{X}^*(\widetilde{T})$.

L'ensemble $\Phi(\widetilde{G}, \widetilde{T})$ est constitué des $\pm(\varepsilon_i - \varepsilon_j)$ et $\pm(\varepsilon_i + \varepsilon_j - \varepsilon_0)$ pour $1 \leq i < j \leq r$. De plus, $\Delta(\widetilde{G}, \widetilde{T}, \widetilde{B})$ est réunion des $\varepsilon_i - \varepsilon_{i+1}$, $i = 1, \ldots, r-1$ et de $\varepsilon_{r-1} + \varepsilon_r - \varepsilon_0$. Soit $\varepsilon_i^* \in \mathrm{X}_*(\widetilde{T})$ la $\mathbb{Z}$-base duale de la base de $\mathrm{X}^*(\widetilde{T})$ constituée des ε_i, $i = 0, \ldots, r$. On constate que pour $1 \leq i < j$, alors $(\varepsilon_i - \varepsilon_j)^\vee = \varepsilon_i^* - \varepsilon_j^*$ et $(\varepsilon_i + \varepsilon_j - \varepsilon_0)^\vee = \varepsilon_i^* + \varepsilon_j^*$.

Soit $s \in \mathrm{O}_V(k)$ l'élément fixant e_i et e_i^* pour $i < r$, et échangeant e_r et e_r^*. La conjugaison par s induit un automorphisme de $\widetilde{G}$ préservant $\widetilde{T}$ et $\widetilde{B}$. Soit $\Psi(s)$ l'automorphisme induit de $\Psi(\widetilde{G})$: il fixe ε_i pour $i = 0, \cdots, r-1$ et envoie ε_r sur $\varepsilon_0 - \varepsilon_r$. Si $r \neq 4$, c'est l'unique involution non triviale du "diagramme de Dynkin" de $\Delta(\widetilde{G}, \widetilde{T}, \widetilde{B})$.

Considérons maintenant le k-groupe $G = \mathrm{SO}_V$. Sa donnée radicielle basée relative à $T := \widetilde{T} \cap G$ et $B = \widetilde{B} \cap G$ se déduit de celle de $\widetilde{G}$ par les recettes rappellées plus haut, en considérant le sous-groupe de cocaractères $\mathrm{X}_*(T) = \varepsilon_0^\perp = \oplus_{i=1}^r \mathbb{Z}\varepsilon_i^* \subset \mathrm{X}_*(\widetilde{T})$ et le groupe de caractères $\mathrm{X}^*(T) = \mathrm{X}^*(\widetilde{T})/\mathbb{Z}\varepsilon_0$. Autrement dit, "on impose $\varepsilon_0 = 0$ dans $\Psi(\widetilde{G}, \widetilde{T}, \widetilde{B})$".

Soit $\underline{\varepsilon_i}$ l'image de ε_i dans $\mathrm{X}^*(T)$, de sorte que $\mathrm{X}^*(T) = \oplus_{i=1}^r \mathbb{Z}\underline{\varepsilon_i}$. On constate que l'application linéaire $\mathrm{X}_*(T) \to \mathrm{X}^*(T)$ envoyant ε_i^* sur $\underline{\varepsilon_i}$ induit un isomorphisme $\Psi(\mathrm{SO}_V) \xrightarrow{\sim} \Psi(\mathrm{SO}_V)^\vee$; en particulier

$$\widehat{\mathrm{SO}}_V(\mathbb{C}) \simeq \mathrm{SO}_{2\mathrm{r}}(\mathbb{C})$$

où SO_{2r} désigne le $\mathbb{C}$-groupe spécial orthogonal du q-module standard sur $\mathbb{C}^{2r}$.

De même, la donnée radicielle de $\mathrm{P}\widetilde{G} = \mathrm{PGSO}_V$ relative aux images respectives $\mathrm{P}\widetilde{T}$ et $\mathrm{P}\widetilde{B}$ de $\widetilde{T}$ et $\widetilde{B}$ dans $\mathrm{P}\widetilde{G}$ s'obtient en considérant le sous-groupe de caractères $\mathrm{X}^*(\mathrm{P}\widetilde{T}) = \zeta^\perp \subset \mathrm{X}^*(\widetilde{T})$, où ζ désigne le co-caractère central $\varepsilon_0^* + \sum_{i=1}^r \varepsilon_i^*$, et le groupe de co-caractères $\mathrm{X}_*(\mathrm{P}\widetilde{T}) = \mathrm{X}_*(\widetilde{T})/\mathbb{Z}\zeta$. Autrement dit, on impose $-2\varepsilon_0^* = \sum_{i=1}^r \varepsilon_i^*$ dans la donnée de $\widetilde{G}$. Le groupe $\widehat{\mathrm{PGSO}_V}(\mathbb{C})$ est isomorphe au groupe des spineurs $\mathrm{Spin}_{2r}(\mathbb{C})$ du q-module standard sur $\mathbb{C}^{2r}$.

Groupe spécial orthogonal impair

Soient $r \geq 1$ un entier, $U = k^r$ et soit V le k-module $\mathrm{H}(U) \oplus k$ muni de la forme quadratique somme orthogonale du q-module $\mathrm{H}(U)$ et de $x \mapsto x^2$. Le k-groupe $G = \mathrm{SO_V}$ est alors semi-simple et déployé (§B.1).

On définit un tore maximal déployé T à partir d'une k-base (e_i) de U, un sous-groupe de Borel B contenant T, ainsi qu'une $\mathbb{Z}$-base ε_i de $\mathrm{X}^*(T)$, comme précédemment. On constate cette fois-ci que $\Phi(G,T)$ est réunion des $\pm\varepsilon_i \pm \varepsilon_j$ pour $1 \leq i < j \leq r$ et des $\pm\varepsilon_i$ pour $i = 1, \ldots, r$. De plus, $\Delta(G,T,B)$ est réunion des $\varepsilon_i - \varepsilon_{i+1}$ pour $i < r$ et de ε_r.

Les groupes de similitudes et similitudes projectives associés à V sont peu différents de G dans ce cadre, nous ne les considèrerons pas. En revanche, le groupe des spineurs de V jouera un rôle. On peut le définir suivant Chevalley au moyen de l'algèbre de Clifford de V. Sur un corps algébriquement clos, on peut se contenter de décrire sa donnée radicielle basée : c'est la donnée associée au sous-groupe $Y = \mathrm{X}^*(T) + \mathbb{Z}\,\frac{1}{2}(\sum_{i=1}^r \varepsilon_i) \subset \mathrm{X}^*(T) \otimes \mathbb{Q}$.

Groupe symplectique et ses variantes

Enfin, les k-groupes de la série symplectique sont aussi réductifs déployés. Considérons d'abord le k-groupe $\widetilde{G} = \mathrm{GSp}_{2g}$ des similitudes symplectiques de la forme alternée hyperbolique sur $U = k^g$.

On définit $\widetilde{T}$, $\widetilde{B}$, les ε_i et les ε_i^*, pour $i = 0, \cdots, g$, comme dans le cas orthogonal pair. L'ensemble $\Phi(\widetilde{G}, \widetilde{T})$ est cette fois-ci constitué des $\pm(\varepsilon_i - \varepsilon_j)$ pour $1 \leq i < j \leq g$, et des $\pm(\varepsilon_i + \varepsilon_j - \varepsilon_0)$ pour $1 \leq i \leq j \leq g$. De plus, $\Delta(\widetilde{G}, \widetilde{T}, \widetilde{B})$ est réunion des $\varepsilon_i - \varepsilon_{i+1}$ pour $1 \leq i < g$ et de $2\varepsilon_g - \varepsilon_0$. Enfin, $(\varepsilon_i - \varepsilon_j)^\vee = \varepsilon_i^* - \varepsilon_j^*$, $(\varepsilon_i + \varepsilon_j - \varepsilon_0)^\vee = \varepsilon_i^* + \varepsilon_j^*$ pour $i < j$, et $(2\varepsilon_i - \varepsilon_0)^\vee = \varepsilon_i^*$.

Les données radicielles des k-groupes $G = \mathrm{Sp}_{2g}$ et $\mathrm{P}\widetilde{G} = \mathrm{PGSp}_{2g}$ se déduisent verbatim de celle de $\widetilde{G}$ comme dans le cas orthogonal pair. Au final, on constate $\widehat{\mathrm{Sp}_{2g}}(\mathbb{C}) \simeq \mathrm{SO}_{2g+1}(\mathbb{C})$ et $\widehat{\mathrm{PGSp}_{2g}}(\mathbb{C}) \simeq \mathrm{Spin}_{2g+1}(\mathbb{C})$.

1.4. Représentations des groupes réductifs déployés en caractéristique nulle

Soit k un corps algébriquement clos de caractéristique nulle, soit G un k-groupe réductif, et soit $\Psi(G) = (X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$ sa donnée radicielle basée. Soit

$$X_+ = \{\lambda \in X, \langle \lambda, \alpha^\vee \rangle \geq 0 \ \ \forall \alpha \in \Delta\}$$

le sous-monoïde additif de X constitué des *poids dominants* de G. C'est un domaine fondamental de X sous l'action du groupe de Weyl W de G.

On munit X d'un ordre partiel pour la relation dite de *dominance* : $\lambda \leq \mu \Leftrightarrow \mu - \lambda$ est une somme finie d'éléments de Δ [ST98]. Une propriété notable de cette relation est que si $\lambda, \mu \in X_+$ sont tels que $\lambda < \mu$, il existe une racine $\alpha \in \Phi$ positive relativement à Δ telle que $\mu - \alpha \in X_+$ et $\lambda \leq \mu - \alpha$ [ST98, Cor. 2.7]. Par exemple, un élément $\lambda \in X_+$ est minimal si et seulement si $\lambda - \alpha \notin X_+$ pour toute racine positive $\alpha \in \Phi$.

Une k-représentation de G est la donnée d'un k-espace vectoriel V de dimension finie et d'un morphisme de k-groupes $G \to \mathrm{GL}_V$. Elles forment une catégorie abélienne de manière évidente, qui est semi-simple car G est réductif. Le produit tensoriel des représentations définit une structure d'anneau commutatif $\mathrm{Rep}(G)$ sur le groupe de Grothendieck de cette catégorie, que l'on notera $\mathrm{Rep}(G)$. L'association $G \mapsto \mathrm{Rep}(G)$ définit de manière naturelle un foncteur de la catégorie $\mathcal{C}_k$ dans les anneaux commutatifs (§1.1).

Si $\lambda \in X_+$, la théorie du plus haut poids de Cartan-Weyl démontre qu'il existe une k-représentation irréductible V_λ de G, unique à isomorphisme près, dont c'est le plus haut poids. De plus, toute irréductible s'obtient ainsi. Rappelons brièvement de quoi il s'agit. Soit T un tore maximal de G et soit B un sous-groupe de Borel contenant T, de sorte que $\Psi(G)$ s'identifie canoniquement à $\Psi(G, T, B)$. L'action de T sur toute k-représentation V de G est diagonalisable, et l'on note $\mathrm{Poids}(V) \subset X$ l'ensemble des caractères de T intervenant dans V. Il est stable pour l'action de W. Si V est irréductible, on démontre que l'espace des invariants $V^{B(k)}$ est de dimension 1 et que T y agit par un élément de X_+ : c'est le *plus haut poids* de V. Le plus haut poids λ de V a alors la propriété suivante : pour tout $\mu \in \mathrm{Poids}(V)$ alors $\mu \leq \lambda$. De plus, on a

$$\mathrm{Poids}(V) \cap X_+ = \{\mu \in X_+, \mu \leq \lambda\}$$

(voir par exemple [HU72, §13.2 et §21.3]).

2. Paramétrisation de Satake

2.1. L'isomorphisme de Satake

Soit G un $\mathbb{Z}_p$-groupe. À la manière du §IV.2.5, notons $\mathcal{R}_p(G)$ le $G(\mathbb{Q}_p)$-ensemble $G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$ et $\mathrm{H}_p(G)$ l'anneau de Hecke de $\mathcal{R}_p(G)$ (§IV.2).

On suppose que G est réductif déployé (§1.1). Ainsi que l'a observé Gross [Gro96, Prop. 1.1], cette dernière hypothèse est satisfaite si G provient par extension des scalaires à $\mathbb{Z}_p$ d'un $\mathbb{Z}$-groupe réductif, ce qui sera toujours le cas dans nos applications. Soit $\widehat{G}$ le dual de Langlands de G, c'est-à-dire un $\mathbb{C}$-groupe réductif $\widehat{G}$ muni d'un isomorphisme $\Psi(\widehat{G}) \xrightarrow{\sim} \Psi(G)^\vee$ (§1.2). Son anneau de Grothendieck $\mathrm{Rep}(\widehat{G})$ est alors canoniquement défini (§1.4). L'isomorphisme de Satake [Sat63], revisité par Langlands [Lan71, §2], est un isomorphisme d'anneaux canonique [3]

$$\mathrm{Sat} : \mathrm{H}_p(G) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,] \xrightarrow{\sim} \mathrm{Rep}(\widehat{G}) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,]$$

Nous renvoyons à l'article de Satake [Sat63], ainsi qu'aux articles de *survey* de Cartier [Car79, §IV] et de Gross [Gro98], pour des détails sur sa définition et ses propriétés générales, que nous ne rediscutons que brièvement ci-dessous. La construction originale de Satake suppose satisfaites certaines propriétés axiomatiques du couple de groupes $(G(\mathbb{Z}_p), G(\mathbb{Q}_p))$, qu'il vérifie pour les groupes classiques, et qui ont été démontrées par Tits en général [Tit79]. Le point de vue utilisé ici, consistant à faire apparaître la "struture entière" $\mathrm{Rep}(\widehat{G})$ plutôt que les fonctions centrales sur $\widehat{G}$, est emprunté à l'article de Gross sus-cité. Ainsi que l'observe Gross, on peut remplacer $\mathbb{Z}[\,p^{-\frac{1}{2}}\,]$ par $\mathbb{Z}[\,p^{-1}\,]$ dans l'isomorphisme de Satake lorsque la demi-somme des racines positives de G est un poids de G.

Définition de l'homomorphisme de Satake : Soient T un $\mathbb{Z}_p$-tore maximal déployé de G, B un $\mathbb{Z}_p$-groupe de Borel de G contenant T et N le radical unipotent de B. Si V est un $G(\mathbb{Q}_p)$-module, le groupe abélien $V_{N(\mathbb{Q}_p)}$ des co-invariants de V sous l'action de $N(\mathbb{Q}_p)$ est muni d'une structure de $T(\mathbb{Q}_p)$-module car $T(\mathbb{Q}_p)$ normalise $N(\mathbb{Q}_p)$; cela définit un foncteur des $G(\mathbb{Q}_p)$-modules vers les $T(\mathbb{Q}_p)$-modules appelé *foncteur de Jacquet*. Les décompositions ensemblistes $G(\mathbb{Q}_p) = B(\mathbb{Q}_p)G(\mathbb{Z}_p)$ et $B(\mathbb{Q}_p) = T(\mathbb{Q}_p) \times N(\mathbb{Q}_p)$ assurent que l'inclusion évidente $\mathcal{R}_p(T) \to \mathcal{R}_p(G)$ induit une bijection ("projection horocyclique")

$$\mathcal{R}_p(T) \xrightarrow{\sim} N(\mathbb{Q}_p)\backslash\mathcal{R}_p(G).$$

3. Au sens strict, il faudrait remplacer $\mathrm{H}_p(G)$ par l'anneau opposé $\mathrm{H}_p(G)^{\mathrm{opp}}$ dans cet isomorphisme. Comme l'existence de ce dernier entraîne la commutativité de $\mathrm{H}_p(G)$, nous ne nous embarrasserons pas de cette décoration.

Il en résulte que si l'on prend $V = \mathbb{Z}[\mathcal{R}_p(G)]$ alors $V_{N(\mathbb{Q}_p)}$ s'identifie canoniquement à $\mathbb{Z}[\mathcal{R}_p(T)]$, d'où l'on tire un homomorphisme d'anneaux

$$\mathrm{s}_1 : \mathrm{H}_p(G) \to \mathrm{H}_p(T).$$

Soit $\mathrm{X}_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$ le groupe des co-caractères de T. L'application naturelle $\mathrm{X}_*(T) \to T(\mathbb{Q}_p)$, $\lambda \mapsto \lambda(p)$, induit une bijection $\mathrm{X}_*(T) \xrightarrow{\sim} \mathcal{R}_p(T)$ puis un isomorphisme d'anneaux $\eta : \mathbb{Z}[\mathrm{X}_*(T)] \xrightarrow{\sim} \mathrm{H}_p(T)$ par commutativité de T. On considère alors l'homomorphisme

$$s_2 : \mathrm{H}_p(G) \to \mathbb{Z}[\mathrm{X}_*(T)][\,p^{-\frac{1}{2}}\,]$$

défini comme le composé de $(\eta^{-1} \circ s_1) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}]$ par l'automorphisme de $\mathbb{Z}[\mathrm{X}_*(T)][\,p^{-\frac{1}{2}}\,]$ envoyant un co-caractère λ sur $p^{-\langle\lambda,\rho\rangle}\,\lambda$, où ρ est la demi-somme des racines positives de G relativement à (T, B). Satake démontre que s_2 est un isomorphisme sur l'anneau des invariants $\mathbb{Z}[\mathrm{X}_*(T)]^W[\,p^{-\frac{1}{2}}]$, où W désigne le groupe de Weyl de G. Mais d'après la définition du groupe dual $\widehat{G}$, l'anneau $\mathbb{Z}[\mathrm{X}_*(T)]^W$ s'identifie canoniquement à $\mathbb{Z}[\mathrm{X}^*(\widehat{T})]^W$, soit encore à $\mathrm{Rep}(\widehat{G})$ d'après Chevalley : cela définit l'isomorphisme Sat. $\square$

Désignons par $\widehat{G}(\mathbb{C})_{\mathrm{ss}}$ l'ensemble (bien défini !) des classes de conjugaison d'éléments semi-simples de $\widehat{G}(\mathbb{C})$. Soit $c \in \widehat{G}(\mathbb{C})_{\mathrm{ss}}$. L'application $V \mapsto \mathrm{trace}(c\,|\,V)$, associant à une $\mathbb{C}$-représentation de dimension finie V de $\widehat{G}$ la trace de c dans V, s'étend en un homomorphisme d'anneaux $\mathrm{tr}(c) : \mathrm{Rep}(\widehat{G}) \to \mathbb{C}$. D'après un résultat classique dû à Chevalley, l'application ainsi définie

$$\mathrm{tr} : \widehat{G}(\mathbb{C})_{\mathrm{ss}} \to \mathrm{Hom}_{\mathrm{anneaux}}(\mathrm{Rep}(\widehat{G}), \mathbb{C})$$

est une bijection. Le scholie suivant, l'un des points de départ des travaux de Langlands, en résulte immédiatement.

Scholie 2.2. *L'application* $c \mapsto \mathrm{tr}(c) \circ \mathrm{Sat}$ *définit une bijection*

$$\widehat{G}(\mathbb{C})_{\mathrm{ss}} \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{anneaux}}(\mathrm{H}_p(G), \mathbb{C}).$$

Mentionnons enfin que l'involution $T \mapsto T^{\mathrm{t}}$ de $\mathrm{H}_p(G)$ correspond par l'homomorphisme de Satake à l'involution de $\mathrm{Rep}(\widehat{G})$ induite par la dualité sur les représentations, ou encore à l'inversion sur $\widehat{G}(\mathbb{C})_{\mathrm{ss}}$.

Exemple 2.3. Replaçons-nous tout d'abord dans le cadre général du chapitre IV §2.1 & §2.2, où X désigne un Γ-ensemble transitif quelconque. Regardons $\mathbb{Z}$ comme Γ-module pour l'action triviale. Le $\mathrm{H}(X)^{\mathrm{opp}}$-module $\mathbb{Z}_X$ est libre de rang 1 sur $\mathbb{Z}$, et définit donc un morphisme d'anneaux

$$\deg : \mathrm{H}(X) \to \mathbb{Z},$$

appelé *degré*, qui n'est autre que $\deg(h) = \sum_{x \in X} h_{x,y}$, où $y \in X$ est un élément quelconque. Si $X = \mathcal{R}_p(G)$, on peut se demander quel est l'élément $s \in \widehat{G}(\mathbb{C})_{\mathrm{ss}}$ correspondant à l'homomorphisme deg par le scholie ci-dessus. Comme le foncteur de Jacquet du $G(\mathbb{Q}_p)$-module trivial $\mathbb{Z}$ est le $T(\mathbb{Q}_p)$-module trivial $\mathbb{Z}$, il découle[4] de la définition de l'homomorphisme de Satake rappelée ci-dessus que s est la classe de conjugaison de $\rho(p) = (2\rho)(p^{\frac{1}{2}})$, où 2ρ est vu comme un co-caractère de $\widehat{G}$.

Isogénies

Soient G et G' deux $\mathbb{Z}_p$-groupes réductifs déployés et soit $f : G \to G'$ un morphisme central. Ce morphisme induit d'une part un homomorphisme d'anneaux $\mathrm{Rep}(f) : \mathrm{Rep}(\widehat{G}) \to \mathrm{Rep}(\widehat{G'})$ par l'équivalence Ψ et la dualité sur les données radicielles. D'autre part, Satake a défini dans [Sat63, §7] un homomorphisme d'anneaux canonique $\mathrm{H}(f) : \mathrm{H}_p(G) \longrightarrow \mathrm{H}_p(G')$.

Lorsque f est une isogénie centrale, $\mathrm{H}(f)$ coïncide avec l'homomorphisme $\mathrm{H}_p(G) \to \mathrm{H}_p(G')$ associé par la proposition-définition §2.14 au morphisme évident $\mathcal{R}_p(G) \to \mathcal{R}_p(G')$ défini par f. En effet, vérifions que ce dernier satisfait les hypothèses du §2.12. D'une part, un argument galoisien direct assure que $f(G(\mathbb{Q}_p))$ contient le groupe dérivé de $G'(\mathbb{Q}_p)$. De plus, la décomposition de Cartan-Tits (§2.5) montre que $G(\mathbb{Z}_p)$ est un sous-groupe compact maximal de G, égal à $f^{-1}(G'(\mathbb{Z}_p))$, d'où l'injectivité de $\mathcal{R}_p(G) \to \mathcal{R}_p(G')$. Mieux, cette décomposition entraîne l'injectivité de $G(\mathbb{Z}_p)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p) \to G'(\mathbb{Z}_p)\backslash G'(\mathbb{Q}_p)/G'(\mathbb{Z}_p)$, et donc que l'action sur $\mathrm{H}_p(G)$ de $G'(\mathbb{Z}_p)$, puis du groupe S *loc. cit.*, est triviale.

Le second théorème de Satake [Sat63, §7 Thm. 4] est la commutativité

4. Soient V un $G(\mathbb{Q}_p)$-module et $\pi : V^{G(\mathbb{Z}_p)} \to V_{N(\mathbb{Q}_p)}$ la projection canonique. L'anneau $\mathrm{H}(G)$ opère sur $V^{G(\mathbb{Z}_p)}$ (§IV.2.2). On observera que par construction de s_2, on a $\pi \circ T = s_2(T) \circ \pi$ pour tout $T \in \mathrm{H}_p(G)$. L'assertion s'en déduit en considérant $V = \mathbb{Z}$ et en se rappelant du décalage par ρ intervenant dans la définition de l'homomorphisme de Satake.

du diagramme

$$\begin{tikzcd} \mathrm{H}_p(G) \arrow[r, "\mathrm{H}(f)"] \arrow[d, "\mathrm{Sat}"'] & \mathrm{H}_p(G') \arrow[d, "\mathrm{Sat}"] \\ \mathrm{Rep}(\widehat{G}) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,] \arrow[r, "\mathrm{Rep}(f)"'] & \mathrm{Rep}(\widehat{G'}) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,] \end{tikzcd} \tag{2.1}$$

auquel on réfèrera comme la "compatibilité de l'isomorphisme de Satake aux isogénies".

Exemple du groupe spécial orthogonal pair

Donnons un exemple d'application de la discussion précédente dans le cas d'un automorphisme de G. Soit $r \geq 1$ un entier, soit V le q-module hyperbolique sur $\mathbb{Z}_p^r$, et soit $G = \mathrm{SO}_V$, de sorte que $\widehat{G}$ est le $\mathbb{C}$-groupe SO_{2r} (§1.3). Le groupe $\mathrm{O}(V)$ agit par $\mathbb{Z}_p$-automorphismes sur G (par conjugaison), ainsi donc sur $\Psi(G)$. L'homomorphisme induit $\mathrm{O}(V)/\mathrm{SO}(V) \to \mathrm{Aut}_{\mathfrak{D}}(\Psi(G))$ est bijectif, et l'élément non-trivial est induit par l'élément $\Psi(s)$ défini loc.cit. Ce groupe agit également sur $\mathrm{Rep}(\widehat{G})$ par fonctorialité, et cette action coïncide avec l'action naturelle de $\mathrm{O}_{2r}(\mathbb{C})/\mathrm{SO}_{2r}(\mathbb{C})$ pour la même raison. Désignons par $\mathrm{H}_p(\mathrm{O}_V)$ et $\mathrm{H}_p(\mathrm{SO}_V)$ les anneaux de Hecke respectifs des $\mathbb{Z}_p$-groupes O_V et SO_V. Nous avons défini au §2.11 un homomorphisme canonique $\mathrm{H}_p(\mathrm{O}_V) \to \mathrm{H}_p(\mathrm{SO}_V)$ identifiant $\mathrm{H}_p(\mathrm{O}_V)$ à l'anneau des invariants $\mathrm{H}_p(\mathrm{SO}_V)^{\mathrm{O}(V)}$. On en déduit par composition avec l'isomorphisme de Satake de SO_V un isomorphisme canonique

$$\mathrm{H}_p(\mathrm{O}_V) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,] \xrightarrow{\sim} (\mathrm{Rep}(\mathrm{SO}_{2r}(\mathbb{C})) \otimes \mathbb{Z}[\,p^{-\frac{1}{2}}\,])^{\mathrm{O}_{2r}(\mathbb{C})}. \tag{2.2}$$

Scholie 2.4. *L'isomorphisme de Satake de* SO_V *induit une bijection entre* $\mathrm{Hom}_{\mathrm{anneaux}}(\mathrm{H}_p(\mathrm{O}_V), \mathbb{C})$ *et l'ensemble des classes de* $\mathrm{O}_{2r}(\mathbb{C})$*-conjugaison d'éléments semi-simples de* $\mathrm{SO}_{2r}(\mathbb{C})$.

2.5. Les deux bases naturelles de l'anneau de Hecke de G

Soit G un $\mathbb{Z}_p$-groupe réductif déployé, de dual de Langlands $\widehat{G}$. Écrivons $\Psi(\widehat{G}) = (X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$ et désignons par $X_+ \subset X$ l'ensemble ordonné des poids dominants de $\widehat{G}$ comme au §1.4. Nous allons rappeler les deux $\mathbb{Z}$-bases naturelles de $\mathrm{H}_p(G)$ et $\mathrm{Rep}(\widehat{G})$ indexées par X_+, et indiquer quelques liens entre ces dernières dont nous aurons besoin, suivant Gross [Gro98].

Une conséquence de la réductivité de G sur $\mathbb{Z}_p$ est l'existence d'une *décomposition de Cartan*, due à Tits dans cette généralité mais classique dans nos exemples (théorie des "diviseurs élémentaires"). Soit T un tore maximal déployé de G et B un sous-groupe de Borel de G contenant T, ce qui identifie canoniquement $\Psi(\widehat{G})$ à $\Psi(G,T,B)^\vee$, et en particulier X au groupe des cocaractères $\mathrm{X}_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$. La décomposition en question s'écrit [5]

$$G(\mathbb{Q}_p) = \coprod_{\lambda \in X_+} G(\mathbb{Z}_p)\, \lambda(p)\, G(\mathbb{Z}_p).$$

Si $\lambda \in X$ on désignera par $\mathrm{c}_\lambda \in \mathrm{H}_p(G)$ la fonction caractéristique de la double classe $G(\mathbb{Z}_p)\lambda(p)G(\mathbb{Z}_p)$, ou selon le point de vue, des couples (x,y) dans $G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$ tels que $y^{-1}x \in G(\mathbb{Z}_p)\lambda(p)G(\mathbb{Z}_p)$ (§IV.2.1). L'élément $\mathrm{c}_\lambda \in \mathrm{H}_p(G)$ ne dépend pas du choix de (T,B). Il est clair que $\mathrm{c}_\lambda^{\mathrm{t}} = \mathrm{c}_{-\lambda}$ (§2.1) et $\mathrm{c}_{w(\lambda)} = \mathrm{c}_\lambda$ pour tout $\lambda \in X$ et $w \in W$ (le groupe de Weyl de G). D'après la décomposition de Cartan-Tits, les c_λ avec $\lambda \in X_+$ forment une $\mathbb{Z}$-base de $\mathrm{H}_p(G)$. Si $\lambda, \mu \in X_+$, on a

$$\mathrm{c}_\lambda \cdot \mathrm{c}_\mu = \mathrm{c}_{\lambda+\mu} + \sum_{\nu < \lambda+\mu} n_{\lambda,\mu,\nu} \mathrm{c}_\nu \tag{2.3}$$

pour certains entiers $n_{\lambda,\mu,\nu}$ [Gro98, (2.9)]. L'anneau $\mathrm{H}_p(G)$ admet donc une filtration évidente indéxée par le monoïde ordonné X_+, d'anneau gradué associé $\mathbb{Z}[X_+]$. En particulier, si l'on désigne par $\Omega \subset X_+$ une famille génératrice de X_+, l'homomorphisme d'anneaux $\mathbb{Z}[\{x_\omega\}_{\omega\in\Omega}] \to \mathrm{H}_p(G)$ envoyant x_ω sur c_ω est surjectif. Si $X^\vee = \mathrm{Q}(\Phi^\vee)$, auquel cas $X_+ \simeq \mathbb{N}^r$, et si Ω est la base de X_+ (co-poids fondamentaux), cet homomorphisme est un isomorphisme.

De même, les classes $[V_\lambda] \in \mathrm{Rep}(\widehat{G})$ des représentations irréductibles V_λ pour $\lambda \in X_+$ fournissent une $\mathbb{Z}$-base de $\mathrm{Rep}(\widehat{G})$ d'après la théorie du plus haut poids rappelée au §1.4. Bien qu'elles soient toutes deux indexées par X_+, le lien entre les $\mathrm{Sat}(\mathrm{c}_\lambda)$ et les $[V_\lambda]$ est non trivial. Nous renvoyons à l'article de Gross *loc. cit.* pour une discussion détaillée de cette question, dans laquelle des travaux de Lustig [Lus83] jouent un rôle essentiel.

Soient $\widehat{T} \subset \widehat{G}$ un tore maximal et $\widehat{B} \subset \widehat{G}$ un sous-groupe de Borel contenant $\widehat{T}$, de sorte que $\Psi(\widehat{G})$ s'identifie à $\Psi(\widehat{G}, \widehat{T}, \widehat{B})$. Si V est une $\mathbb{C}$-représentation de $\widehat{G}$ et si $\mu \in X$ on note $V(\mu) \subset V$ l'espace propre pour le caractère μ sous l'action de $\widehat{T}$.

5. La notation $\lambda(p)$ désigne l'image de p dans $T(\mathbb{Q}_p)$ par le morphisme $\mathbb{Q}_p^\times \to T(\mathbb{Q}_p)$ induit par λ.

Proposition 2.6. (Gross) *Soient G un $\mathbb{Z}_p$-groupe semi-simple déployé et X_+ l'ensemble ordonné des poids dominants de $\widehat{G}$. Soit $\lambda \in X_+$.*

(i) Si λ est un élément minimal alors $p^{\langle\lambda,\rho\rangle}[V_\lambda] = \mathrm{Sat}(\mathrm{c}_\lambda)$, où 2ρ est la somme des racines positives de G.

(ii) Si $\mu \in X_+$ et $\dim(V_\lambda(\mu)) = 1$, alors $d_\lambda(\mu) = 1$.

(iii) (Lusztig) *Si $V_\lambda = \mathrm{Lie}(G)$ est la représentation adjointe, alors $d_\lambda(0) = \sum_i p^{m_i - 1}$ où les m_i sont les exposants du groupe de Weyl de G.*

En effet, ainsi que l'explique Gross [Gro98, §3], on dispose pour tout $\lambda \in X_+$ d'une identité de la forme

$$p^{\langle\lambda,\rho\rangle}[V_\lambda] = \mathrm{Sat}(\mathrm{c}_\lambda) + \sum_{\{\mu\in \mathrm{P}^+,\, \mu<\lambda\}} d_\lambda(\mu)\,\mathrm{Sat}(\mathrm{c}_\mu), \tag{2.4}$$

pour certains entiers $d_\lambda(\mu)$ dépendant de p. Le (i) en résulte. Suivant Lusztig et S. Kato, Gross donne également une formule explicite (bien que difficilement praticable) pour $d_\lambda(\mu)$ sous l'hypothèse que G est adjoint, i.e. de centre trivial. Il en déduit (ii) et (iii) dans le cas adjoint (formules (4.5) et (4.6) §4 *loc. cit.*). Pour achever la démonstration de la proposition, il ne reste qu'à expliquer comment nous ramener à ce cas pour un G semi-simple général. Le lemme suivant est conséquence immédiate des définitions (voir [Sat63, (7.4)]).

Lemme 2.7. *Soit $f : G \to G'$ un morphisme central entre $\mathbb{Z}_p$-groupes réductifs déployés, X (resp. X') le réseau des poids de $\widehat{G}$ (resp. $\widehat{G'}$). Pour tout poids dominant $\mu \in X$, on a $\mathrm{H}(f)(\mathrm{c}_\mu) = \mathrm{c}_{\mu'}$ et $\mathrm{Rep}(f)([V_\mu]) = [V_{\mu'}]$, où μ' est l'image de μ par l'application $\Psi(f)^\vee : X \to X'$.*

Dans les notations de ce lemme, et si de plus f est une isogénie centrale de sorte que l'application $\mathrm{H}(f)$ soit injective, l'indépendance linéaire des $\mathrm{c}_{\mu'}$ dans $\mathrm{H}_p(G')$ entraîne donc que $d_\lambda(\mu) = d_{\lambda'}(\mu')$ pour tout $\lambda, \mu \in X_+$. On conclut la démonstration de la proposition en considérant l'isogénie canonique $G \to G/\mathrm{Z}(G)$. Cet argument montre également que la formule de Kato et Lusztig susmentionnée vaut pour tout $\mathbb{Z}_p$-groupe semi-simple G, par réduction au cas adjoint. □

2.8. Cas des groupes classiques : un formulaire

Groupe orthogonal pair et ses variantes

Soient $r \geq 2$ un entier et L le q-module hyperbolique sur $\mathbb{Z}_p^r$. On dispose d'un carré commutatif d'injections naturelles (§IV.2.11, Exemple IV.2.16, §2.1)

$$\begin{tikzcd} \mathrm{H}_p(\mathrm{SO}_L) \arrow[r, hook] & \mathrm{H}_p(\mathrm{PGSO}_L) \\ \mathrm{H}_p(\mathrm{O}_L) \arrow[u, hook] \arrow[r, hook] & \mathrm{H}_p(\mathrm{PGO}_L) \arrow[u, hook] \end{tikzcd}$$

L'injection du haut commute aux actions naturelles du groupe à deux éléments $\mathrm{O}_L(\mathbb{Z}_p)/\mathrm{SO}_L(\mathbb{Z}_p)$, celle du bas étant alors l'injection qui s'en déduit sur les invariants. Pour alléger les notations ces injections seront vues comme des inclusions. Il sera utile de décrire d'abord $\mathrm{H}_p(\mathrm{PGSO}_L)$.

Nous reprenons les notations du §1.3 relatives au $\mathbb{Z}_p$-groupes GSO_L, SO_L et PGSO_L. Soit $\lambda \in \mathrm{X}_*(\mathrm{P}\widetilde{T})$. Il admet un unique antécédent par l'application canonique $\mathrm{X}_*(\widetilde{T}) \to \mathrm{X}_*(\mathrm{P}\widetilde{T})$, disons

$$\widetilde{\lambda} = \sum_{i=0}^{r} m_i \varepsilon_i^*,$$

tel que $m_0 = \langle \varepsilon_0, \widetilde{\lambda} \rangle \in \{0, 1\}$. Le réseau homo-dual $M = \widetilde{\lambda}(p)L$ a pour $\mathbb{Z}_p$-base l'ensemble des $p^{m_i} e_i$ et des $p^{m_0 - m_i} e_i^*$ pour $1 \leq i \leq r$. Il vérifie donc

$$M/M \cap L \simeq \prod_{i=1}^{r} (\mathbb{Z}/p^{d_i}\mathbb{Z}),$$

où $d_i = \mathrm{Max}(m_i - m_0, -m_i) = |m_i - \frac{m_0}{2}| - \frac{m_0}{2}$ si $i \in \{1, \cdots r\}$, et $M^\sharp = p^{-m_0} M$. Notons $A_\lambda \in \mathrm{AF}$ la classe d'isomorphisme du groupe abélien ci-dessus et posons $v_\lambda = \langle \varepsilon_0, \widetilde{\lambda} \rangle = v_\lambda = m_0$. L'application

$$\eta : \lambda \mapsto (A_\lambda, v_\lambda)$$

induit manifestement une surjection de $\mathrm{X}_*(\mathrm{P}\widetilde{T})$ sur l'ensemble des couples (A, v) où A est un p-groupe abélien fini engendré par r éléments, et $v \in \{0, 1\}$. Il n'est pas difficile de vérifier que η est constante sur les orbites du sous-groupe de $\mathrm{Aut}(\mathrm{X}_*(\mathrm{P}\widetilde{T}))$ engendré par W et l'automorphisme $\tau := \Psi(s)$ introduit au §1.3. De plus, le co-poids λ est dominant si et seulement si $m_1 \geq m_2 \geq \cdots \geq m_{r-1} \geq d_r$. Deux co-poids dominants λ, λ' ont donc même image par η si, et seulement si, $\lambda' \in \{\lambda, \tau(\lambda)\}$. Si l'on compare ces considérations avec celles du § IV.2.6, on en déduit le :

Scholie 2.9. *Si λ est un co-poids de PGSO_L, on a l'égalité $\mathrm{T}_{(A_\lambda, v_\lambda)} = \sum_{\mu \in \{\lambda, \tau(\lambda)\}} \mathrm{c}_\mu$. De plus, on a $T^{\mathrm{t}} = T$ pour tout $T \in \mathrm{H}_p(\mathrm{PGO}_L)$.*

L'injection naturelle $\mathrm{X}_*(T) \to \mathrm{X}_*(\mathrm{P}\widetilde{T})$ identifie les co-poids de SO_L avec ceux de PGSO_L tels que $v_\lambda = 0$. Si λ est un co-poids de SO_L, on en déduit l'égalité $\mathrm{T}_{A_\lambda} = \sum_{\mu \in \{\lambda, \tau(\lambda)\}} \mathrm{c}_\mu$ dans $\mathrm{H}_p(\mathrm{O}_L)$.

Étant donné que $\mathrm{H}_p(\mathrm{PGO}_L)$ s'identifie aux invariants de $\mathrm{H}_p(\mathrm{PGSO}_L)$ sous l'action de conjugaison de $\mathrm{O}_L(\mathbb{Q}_p)/\mathrm{SO}_L(\mathbb{Q}_p)$, la proposition IV.2.9 est conséquence du fait que les c_λ, avec λ dominant, forment une $\mathbb{Z}$-base de $\mathrm{H}_p(\mathrm{PGSO}_L)$. Si $1 \leq i \leq r$, notons $\lambda_i \in \mathrm{X}_*(\mathrm{P}\widetilde{T})$ l'image de $\varepsilon_1^* + \cdots + \varepsilon_i^* \in \mathrm{X}_*(\widetilde{T})$, et notons également $\lambda_{r+1} \in \mathrm{X}_*(\mathrm{P}\widetilde{T})$ l'image de $-\varepsilon_0^*$. En particulier, on a $2\lambda_{r+1} = \lambda_r$. D'après le scholie, on a les relation $\mathrm{c}_{\lambda_i} = \mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ dans $\mathrm{H}_p(\mathrm{O}_L)$ pour $i < r$, $\mathrm{c}_{\lambda_r} + \mathrm{c}_{\tau(\lambda_r)} = \mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^r}$, et $\mathrm{c}_{\lambda_{r+1}} + \mathrm{c}_{\tau(\lambda_{r+1})} = \mathrm{K}_p$ dans $\mathrm{H}_p(\mathrm{PGO}_L)$. L'énoncé suivant est bien connu [Sat63] [Ral79, §4].

Corollaire 2.10. *(i) L'homomorphisme $\mathbb{Z}[X_1, \cdots, X_r] \to \mathrm{H}_p(\mathrm{PGO}_L)$ envoyant X_i sur $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ pour $1 \leq i \leq r-1$, et X_r sur K_p, est un isomorphisme d'anneaux.*

(ii) L'homomorphisme $\mathbb{Z}[Y_1, \cdots, Y_r] \to \mathrm{H}_p(\mathrm{O}_L)$ envoyant Y_i sur $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ pour $1 \leq i \leq r$, est un isomorphisme d'anneaux.

Démonstration. Le groupe PGSO_L étant adjoint, la discussion du §2.5 entraîne que $\mathrm{H}_p(\mathrm{PGSO}_L)$ est l'anneau de polynômes sur les c_ω, où ω parcourt les co-poids fondamentaux de PGSO_L. Ce sont les éléments $\lambda_{r+1}, \tau(\lambda_{r+1})$ et les λ_i pour $i = 1, \cdots, r-2$ d'après [Bou81b, Planche IV]. Les $r-2$ derniers sont invariants par τ, et les deux premiers sont échangés. Rappelons que si A est un anneau commutatif, le sous-anneau de $A[U,V]$ constitué des $P(U,V)$ tels que $P(U,V) = P(V,U)$ est $A[UV, U+V]$. Ainsi, $\mathrm{H}_p(\mathrm{PGO}_L)$ est l'anneau de polynômes sur les c_{λ_i}, $1 \leq i < r-1$, K_p et $\mathrm{c}_{\lambda_{r+1}}\mathrm{c}_{\tau(\lambda_{r+1})}$. Mais les seuls co-poids dominants de PGSO_L qui sont strictement inférieurs à $\lambda_{r+1} + \tau(\lambda_{r+1}) = \lambda_{r-1}$ sont les λ_i avec $0 \leq i < r-1$ et $i \equiv r-1 \bmod 2$, avec la convention $\lambda_0 = 0$. Il existe donc des entiers $a_j \in \mathbb{Z}$ et une identité de la forme

$$\mathrm{c}_{\lambda_{r+1}}\mathrm{c}_{\tau(\lambda_{r+1})} = \mathrm{c}_{\lambda_{r-1}} + \sum_{0 \leq j < r-1} a_j \mathrm{c}_{\lambda_j}.$$

Cela démontre le (i). Le (ii) se démontre par des arguments similaires. Le monoïde des co-poids dominants de SO_L est engendré par les λ_i pour $i \leq r-1$, λ_r et $\tau(\lambda_r)$. Le sous-anneau $\mathrm{H}_p(\mathrm{SO}_L) \subset \mathrm{H}_p(\mathrm{PGSO}_L)$ est donc engendré par les c_λ où λ parcourt cette liste. Mais si $S = \{\lambda_{r+1}, \tau(\lambda_{r+1})\}$ et si $s, t \in S$, on observe comme plus haut que $\mathrm{c}_s\mathrm{c}_t - \mathrm{c}_{s+t}$ est une combinaison linéaire à coefficients entiers des c_{λ_i} pour $0 \leq i \leq r-2$. Cela entraîne que $\mathrm{H}_p(\mathrm{SO}_L)$ est également engendré par l'anneau $\mathbb{Z}[\mathrm{c}_{\lambda_1}, \cdots, \mathrm{c}_{\lambda_{r-2}}]$ et les trois éléments $\mathrm{c}_s\mathrm{c}_t$ où

$s, t \in S$. On conclut en observant que si A est un anneau commutatif, le sous-anneau de $A[U^2, V^2, UV] \subset A[U, V]$ constitué des polynômes symétriques en U et V est $A[UV, (U+V)^2]$.

$\square$

D'après le scholie ci-dessus, pour $m \geq 0$ l'opérateur $\mathrm{T}_{p^m} \in \mathrm{H}_p(\mathrm{O}_L)$ des p^m-voisins coïncide avec $\mathrm{c}_{m\lambda_1}$. L'opérateur $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^2}$ interviendra à plusieurs reprises par la suite, et sera également noté $\mathrm{T}_{p,p}$.

Exemple 2.11. Dans $\mathrm{H}_p(\mathrm{O}_L)$, on a la relation

$$(\mathrm{T}_p)^2 = \mathrm{T}_{p^2} + (p+1)\ \mathrm{T}_{p,p} + \frac{(p^r-1)(p^{r-1}+1)}{p-1}.$$

Démonstration. Les co-poids dominants de SO_L strictement inférieurs à $2\lambda_1$ sont λ_2 et 0, d'où l'existence de $a, b \in \mathbb{Z}$ tels que $(\mathrm{T}_p^2) = \mathrm{T}_{p^2} + a\,\mathrm{T}_{p,p} + b$ (formule (2.3)). Comme L est un p-voisin de chacun de ses p-voisins (III. Déf. 1.2), l'entier b est simplement le nombre $b = \mathrm{c}_{2r}(p)$ de p-voisins d'un réseau autodual (III. Déf. 2.1). Calculons a à l'aide de l'homomorphisme *degré*, $\deg : \mathrm{H}(\mathrm{SO}_L) \to \mathbb{Z}$, introduit dans l'exemple 2.3.

Le degré de T_A est le nombre de A-voisins de L, en particulier $\deg(\mathrm{T}_p) = \mathrm{c}_{2r}(p)$ et $\deg(\mathrm{T}_{p^2}) = p^{2r-2}\mathrm{c}_{2r}(p)$ d'après la proposition III. 1.4. Dans le même esprit que le §III. 1, on vérifierait aisément que si $1 \leq i \leq r$, le nombre de $(\mathbb{Z}/p\mathbb{Z})^i$-voisins de L est le produit du nombre de sous-espaces isotropes de rang i de $L \otimes \mathbb{F}_p$ par le nombre de lagrangiens du q-module hyperbolique sur $(\mathbb{Z}/p\mathbb{Z})^i$ qui sont transverses à $(\mathbb{Z}/p\mathbb{Z})^i$ (i.e. $p^{\frac{i(i-1)}{2}}$ d'après la proposition-définition I. 1.3 (b)). Pour $i = 2$, on en trouve donc $\frac{\mathrm{c}_{2r}(p)\mathrm{c}_{2r-2}(p)}{(p+1)} \cdot p$. Un petit calcul conduit à $a = p+1$. $\square$

Remarque 2.12. Il serait intéressant de savoir si les T_{p^i}, $i = 1, \cdots, r$, engendrent la $\mathbb{Q}$-algèbre $\mathrm{H}_p(\mathrm{O}_L) \otimes \mathbb{Q}$.

Terminons ce formulaire sur les groupes orthogonaux pairs par certaines propriétés de l'isomorphisme de Satake. La demi-somme des racines positives de GSO_L est $\rho = (r-1)\varepsilon_1 + (r-2)\varepsilon_2 + \cdots + \varepsilon_{r-1} - \frac{r(r+1)}{4}\varepsilon_0$. Le seul co-poids dominant minimal de SO_L est λ_1, et PGSO_L en admet deux autres qui sont λ_{r+1} et $\tau(\lambda_{r+1})$. Le premier est le poids dominant de la représentation standard V_{St} (de dimension $2r$) de $\widehat{\mathrm{SO}_L}(\mathbb{C}) = \mathrm{SO}_{2r}(\mathbb{C})$, et le deux autres sont les poids dominants des deux représentations Spin $V_{\mathrm{Spin}}^{\pm}$ de $\widehat{\mathrm{PGSO}_L}(\mathbb{C}) = \mathrm{Spin}_{2r}(\mathbb{C})$. La proposition 2.6 (i) et le scholie entraînent les identités :

$$p^{r-1}[V_{\mathrm{St}}] = \mathrm{Sat}(\mathrm{T}_p) \quad \text{et} \quad p^{\frac{r(r-1)}{4}}([V_{\mathrm{Spin}}^+] + [V_{\mathrm{Spin}}^-]) = \mathrm{Sat}(\mathrm{K}_p). \tag{2.5}$$

Considérons maintenant la représentation $\Lambda^2 V_{\mathrm{St}}$, qui n'est autre que la représentation adjointe de $\mathrm{SO}_{2r}(\mathbb{C})$. Son plus haut poids est λ_2 ; l'unique poids dominant inférieur à ce dernier est le poids 0. Les points (i) et (iii) de la proposition 2.6 entraînent donc

$$p^{2r-3}[\Lambda^2 V_{\mathrm{St}}] = \mathrm{Sat}(\mathrm{T}_{p,p}) + p^{r-2} + \sum_{i=0}^{r-2} p^{2i}. \tag{2.6}$$

(Nous pourrions également invoquer l'exemple 2.3 à la place du (iii) de la proposition 2.6.)

Groupe symplectique et ses variantes

Soient $g \geq 1$ un entier et L le a-module hyperbolique sur $\mathbb{Z}_p^g$. Nous reprenons les notations du §1.3 relatives au $\mathbb{Z}_p$-groupes GSp_{2g}, Sp_{2g} et PGSp_{2g}. On constate de même que plus haut que si A est un p-groupe abélien fini engendré par g éléments, disons $A \simeq \prod_{i=1}^g \mathbb{Z}/p^{m_i}\mathbb{Z}$ avec $m_1 \geq \cdots \geq m_g \geq 0$, alors

$$\mathrm{T}_A = \mathrm{c}_{\sum_{i=1}^g m_i \varepsilon_i^*}, \ \text{ et } \ \mathrm{T}_{(A,1)} = \mathrm{c}_{\varepsilon_0^* + \sum_{i=1}^g (m_i+1)\varepsilon_i^*}. \tag{2.7}$$

D'après Shimura [Shi63], l'anneau $\mathrm{H}_p(\mathrm{PGSp}_{2g})$ est l'anneau de polynômes sur K_p et les $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ pour $i < g$, le sous-anneau $\mathrm{H}_p(\mathrm{Sp}_{2g})$ étant engendré par les $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ pour $i \leq g$ (la situation est en fait plus simple que celle du corollaire 2.10, les monoïdes des co-poids dominants de Sp_{2g} et PGSp_{2g} étant libres).

La demi-somme des racines positives ρ de GSp_{2g} est $-\frac{g(g+1)}{4}\,\varepsilon_0^* + g\,\varepsilon_1^* + (g-1)\,\varepsilon_2^* + \cdots + \varepsilon_g^*$. Soit V_{St} la représentation standard (de dimension $2g+1$) de $\widehat{\mathrm{Sp}_{2g}}(\mathbb{C}) = \mathrm{SO}_{2g+1}(\mathbb{C})$, et soit V_{Spin} la représentation Spin de $\mathrm{Spin}_{2g+1}(\mathbb{C})$. Le plus haut poids de V_{St} est ε_1^*, qui a pour unique poids dominant strictement inférieur 0. Le plus haut poids de V_{Spin} est $-\varepsilon_0^*$ qui est minimal. La proposition 2.6 entraîne donc

$$p^g[V_{\mathrm{St}}] = \mathrm{Sat}(\mathrm{T}_p) + 1, \ \text{ et } \ p^{\frac{g(g+1)}{4}}[V_{\mathrm{Spin}}] = \mathrm{Sat}(\mathrm{K}_p). \tag{2.8}$$

Groupe spécial orthogonal impair

Nous n'insisterons que sur les différences avec les autres cas, qui sont minimes. Soient $r \geq 1$ un entier, L le $\mathbb{Z}_p$-module $\mathbb{Z}_p^r \oplus (\mathbb{Z}_p^r)^* \oplus \mathbb{Z}_p$ muni de la forme quadratique somme orthogonale du q-module hyperbolique sur $\mathbb{Z}_p^r$ et de $x \mapsto x^2$, $V = L \otimes \mathbb{Q}_p$ et G le $\mathbb{Z}_p$-groupe SO_L (§B.1). C'est un exercice de vérifier que l'application $g \mapsto g(L)$ identifie $G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$ au sous-ensemble

$\mathcal{R}^{\mathrm{b}}_{\mathbb{Z}_p}(V) \subset \mathcal{R}_{\mathbb{Z}_p}(V)$ des réseaux $M \subset V$ tels que $M^\sharp = M$ si $p > 2$, ou tels que M est un sous-réseau d'indice 2 de $M^\sharp$ si $p = 2$ (§IV.2.6).

Soit V_{St} la représentation standard de $\widehat{\mathrm{SO}_L}(\mathbb{C}) = \mathrm{Sp}_{2r}(\mathbb{C})$ (de dimension $2r$) ; son plus haut poids est ε_1^* qui est minimal (nous reprenons les notations du §1.3 relatives au $\mathbb{Z}_p$-groupe G). On constate que l'opérateur de Hecke $\mathrm{c}_{\varepsilon_1^*}$ est associé aux couples $(N, M) \in \mathcal{R}^{\mathrm{b}}_{\mathbb{Z}_p}(V)^2$ tels que $M \cap N$ est d'indice p dans M : c'est l'opérateur T_p des p-voisins au sens de l'appendice B.3. La demi-somme des racines positives de SO_L étant $\frac{2r-1}{2}\,\varepsilon_1 + \frac{2r-3}{2}\,\varepsilon_2 + \cdots + \frac{1}{2}\,\varepsilon_r$, on a donc

$$p^{\frac{2r-1}{2}}[V_{\mathrm{St}}] = \mathrm{T}_p.$$

3. L'isomorphisme de Harish-Chandra

3.1. Le centre de l'algèbre enveloppante d'un $\mathbb{C}$-groupe réductif

Soient G un $\mathbb{C}$-groupe réductif, $\mathfrak{g}$ la $\mathbb{C}$-algèbre de Lie de G, $\mathrm{U}(\mathfrak{g})$ son algèbre enveloppante, et $\mathrm{Z}(\mathrm{U}(\mathfrak{g}))$ le centre de $\mathrm{U}(\mathfrak{g})$ [Dix74, Ch. 2]. Soit V un $\mathrm{U}(\mathfrak{g})$-module. On dit que V admet un caractère central s'il existe un homomorphisme de $\mathbb{C}$-algèbres

$$\mathrm{c}_V : \mathrm{Z}(\mathrm{U}(\mathfrak{g})) \to \mathbb{C}$$

tel que $z \cdot v = \mathrm{c}_V(z)v$ pour tout $v \in V$ et tout $z \in \mathrm{Z}(\mathrm{U}(\mathfrak{g}))$; on appelle alors c_V le *caractère central* de V. D'après [Dix74, Prop. 2.6.8], tout $\mathrm{U}(\mathfrak{g})$-module simple admet un caractère central. Suivant Harish-Chandra et Langlands, nous allons rappeler dans ce paragraphe comment voir ces caractères centraux comme des classes de conjugaison semi-simples dans la $\mathbb{C}$-algèbre de Lie $\widehat{\mathfrak{g}}$ du $\mathbb{C}$-groupe réductif dual $\widehat{G}$ de G.

Soit $\mathrm{Pol}(\widehat{\mathfrak{g}}) = \mathrm{Sym}(\widehat{\mathfrak{g}}^*)$ la $\mathbb{C}$-algèbre des fonctions polynomiales sur $\widehat{\mathfrak{g}}$. Elle est munie d'une action naturelle de $\widehat{G}(\mathbb{C})$ issue de l'action adjointe sur $\widehat{\mathfrak{g}}$, dont nous notons $\mathrm{Pol}(\widehat{\mathfrak{g}})^{\widehat{G}}$ l'algèbre des invariants. L'isomorphisme de Harish-Chandra est un isomorphisme canonique

$$\mathrm{HC} : \mathrm{Z}(\mathrm{U}(\mathfrak{g})) \xrightarrow{\sim} \mathrm{Pol}(\widehat{\mathfrak{g}})^{\widehat{G}}$$

[Dix74, Thm. 7.4.5 & 7.3.5] [Lan71, §2]. Soit $\widehat{\mathfrak{g}}_{\mathrm{ss}}$ l'ensemble des classes de conjugaison d'éléments semi-simples de $\widehat{\mathfrak{g}}$. Chaque telle classe $X \in \widehat{\mathfrak{g}}_{\mathrm{ss}}$ définit par évaluation un homomorphisme de $\mathbb{C}$-algèbres $\mathrm{Pol}(\widehat{\mathfrak{g}})^{\widehat{G}} \to \mathbb{C}$, $P \mapsto P(X)$. Un résultat classique de Chevalley assure que l'application $\widehat{\mathfrak{g}}_{\mathrm{ss}} \to \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathrm{Pol}(\widehat{\mathfrak{g}})^{\widehat{G}}, \mathbb{C})$ ainsi définie est bijective.

Scholie 3.2. *L'isomorphisme de Harish-Chandra induit une bijection canonique* $\mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathrm{Z}(\mathrm{U}(\mathfrak{g})), \mathbb{C}) \xrightarrow{\sim} \widehat{\mathfrak{g}}_{\mathrm{ss}}$.

Si X est le réseau des poids de G, les éléments de $X \otimes \mathbb{C}$ peuvent être vus comme des éléments de $\widehat{\mathfrak{g}_{\mathrm{ss}}}$. En effet, soient $\widehat{T}$ un tore maximal de $\widehat{G}$ et $\widehat{B} \subset \widehat{G}$ un sous-groupe de Borel contenant $\widehat{T}$. La donnée $\Psi(G)^\vee$ s'identifie à $\Psi(\widehat{G}, \widehat{T}, \widehat{B})$; en particulier X s'identifie à $\mathrm{X}_*(\widehat{T})$. L'application exponentielle définit un isomorphisme naturel entre $\mathrm{X} \otimes \mathbb{C}$ et l'algèbre de Lie complexe $\widehat{\mathfrak{t}}$ de $\widehat{T}$. Si W est le groupe de Weyl de G, on en déduit un bijection canonique

$$(X \otimes \mathbb{C})/W \xrightarrow{\sim} \widehat{\mathfrak{g}}_{\mathrm{ss}}. \tag{3.1}$$

Exemple 3.3. Soient $\lambda \in X_+$ un poids dominant de G et V_λ la $\mathbb{C}$-représentation irréductible de G de plus haut poids λ (§1.4). Cette représentation munit V_λ d'une structure de $\mathrm{U}(\mathfrak{g})$-module. Ce module est simple et son caractère central correspond à la classe de conjugaison de $\lambda + \rho$, où ρ est la demi-somme des racines positives de G.

Plus généralement, fixons une paire $T \subset B$ dans G identifiant $\Psi(G)$ à $\Psi(G, T, B)$. Soient $\mathfrak{t} \subset \mathfrak{b}$ leurs $\mathbb{C}$-algèbres de Lie respectives, et V un $\mathrm{U}(\mathfrak{g})$-module engendré par un élément $e \in V$ tel que $\mathfrak{b}\, e \subset \mathbb{C}e$ (*module de plus haut poids*). Soit $\lambda \in \mathfrak{t}^*$ la forme linéaire définie par $he = \lambda(h)e$ pour tout $h \in \mathfrak{t}$ (on peut également la voir de manière duale comme un élément de $\widehat{\mathfrak{t}}$). Alors V admet un caractère central d'après [Dix74, Prop. 7.1.8], et il résulte assez directement de la définition de l'homomorphisme de Harish-Chandra que la classe de conjugaison qui lui correspond est celle de $\lambda + \rho$ [Dix74, §7.4.6].

3.4. Caractère infinitésimal d'une représentation unitaire

Soit G un $\mathbb{R}$-groupe réductif. On applique les considérations et notations du paragraphe précédent au $\mathbb{C}$-groupe $G_{\mathbb{C}} := G \times_{\mathbb{R}} \mathbb{C}$. Nous renvoyons à [Kna86] et [Wall88] pour un exposé général de la théorie des représentations unitaires des groupes de Lie réductifs.

Soit V un espace de Hilbert muni d'une représentation unitaire du groupe de Lie $G(\mathbb{R})$. Soit $V^\infty \subset V$ le sous-espace des vecteurs $\mathcal{C}^\infty$, c'est-à-dire des $v \in V$ tels que l'application $g \mapsto gv, G(\mathbb{R}) \to V$, soit de classe $\mathcal{C}^\infty$; il est dense dans V (Gårding) et stable par $G(\mathbb{R})$. Si la représentation unitaire V est irréductible alors le $\mathrm{U}(\mathfrak{g})$-module V^∞ admet un caractère central [Wall88, §1.6.5], appelé *caractère infinitésimal* de V, nous le notons inf_V. Ainsi que l'a démontré Harish-Chandra, c'est un invariant assez fin de la représentation V : à isomorphisme près il n'y a qu'un nombre fini (éventuellement nul) de représentations unitaires irréductibles de G ayant un caractère infinitésimal

donné (c'est un résultat difficile, voir [Kna86, Cor. 10.37]). L'isomorphisme d'Harish-Chandra permet de voir $\inf_V$ comme une classe de conjugaison semi-simple dans $\widehat{\mathfrak{g}}$. Nous allons donner deux exemples.

Supposons d'abord que $G(\mathbb{R})$ est un groupe compact, auquel cas il est nécessairement connexe d'après Chevalley [Bor91, V. 24.6 (c) (ii)]. Toute $\mathbb{C}$-représentation V de $G_{\mathbb{C}}$ définit par restriction une représentation $V_{|G(\mathbb{R})}$ de $G(\mathbb{R})$. Le foncteur $V \mapsto V_{|G(\mathbb{R})}$ est une équivalence de catégories entre $\mathbb{C}$-représentations de $G_{\mathbb{C}}$ et représentations complexes, continues, de dimension finie, de $G(\mathbb{R})$. En particulier, toute représentation irréductible de $G(\mathbb{R})$ est isomorphe à $(V_\lambda)_{|G(\mathbb{R})}$ pour un unique poids dominant λ de $G_{\mathbb{C}}$; on la notera en général V_λ pour allèger les notations. D'après l'exemple 3.3, son caractère infinitésimal est la classe de conjugaison de $\lambda + \rho$ dans $\widehat{\mathfrak{g}}$. Il détermine en particulier uniquement V_λ.

Supposons maintenant que G est le $\mathbb{R}$-groupe Sp_{2g}. Reprenons quelques notations du §5.3 à ceci près que nous notons ici $\mathfrak{g}$ l'algèbre de Lie *complexifiée* de $G(\mathbb{R})$. On choisit pour sous-groupe compact maximal $K \subset G(\mathbb{R})$ le fixateur de $i1_g$ dans $\mathbb{H}_g$, d'algèbre de Lie $\mathfrak{k}$. C'est un groupe unitaire à g variables : l'homomorphisme $k \mapsto \mathrm{j}(k, i1_g)$, $K \to \mathrm{GL}_g(\mathbb{C})$, identifie $\mathrm{GL}_g(\mathbb{C})$ au complexifié de K, puis (par différentiation) $\mathfrak{k}_{\mathbb{C}}$ à l'algèbre de Lie $\mathfrak{gl}_g(\mathbb{C})$. La décomposition de Cartan complexifiée s'écrit

$$\mathfrak{g} = \mathfrak{k}_{\mathbb{C}} \oplus \mathfrak{p}^+ \oplus \mathfrak{p}^-,$$

où $\mathfrak{p}^\pm$ sont des sous-algèbres de Lie *abéliennes* stables par $\mathrm{ad}(K)$. Le point clef est que l'action adjointe sur $\mathfrak{p}$ de l'élément $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ du centre de K (qui est isomorphe à $\mathrm{U}(1)$) induit la structure complexe naturelle du $\mathbb{R}$-espace vectoriel $\mathfrak{p} \simeq \mathrm{Sym}_g(\mathbb{C})$.

Soit T un tore maximal de GL_g, B un sous-groupe de Borel contenant T, d'algèbres de Lie complexes respectives $\mathfrak{t} \subset \mathfrak{b} \subset \mathfrak{gl}_g(\mathbb{C}) = \mathfrak{k}_{\mathbb{C}}$. Les propriétés sus-mentionnées de $\mathfrak{p}^-$ assurent que $\mathfrak{t}$ est une sous-algèbre de Cartan de $\mathfrak{g}$ et que $\mathfrak{b} \oplus \mathfrak{p}^-$ en est une sous-algèbre de Borel.

Proposition 3.5. (Harish-Chandra) *Soient V une représentation unitaire de $\mathrm{Sp}_{2g}(\mathbb{R})$, e un élément de V^∞ et U une $\mathbb{C}$-représentation irréductible de GL_g tels que :*

(i) $\mathfrak{p}^- e = 0$,

(ii) la représentation de K engendrée par e est isomorphe à $U_{|K}$.

Alors :

(a) Le $\mathrm{U}(\mathfrak{g})$*-module* $\mathrm{U}(\mathfrak{g})e \subset V^\infty$ *admet un caractère central. Sa classe de conjugaison semi-simple associée est* $\lambda + \rho$ *où* $\lambda \in \mathfrak{t}^*$ *est le plus haut poids de* U *relativement à* B*, et* ρ *est la demi-somme des racines de* $\mathfrak{t}$ *dans* $\mathfrak{b} \oplus \mathfrak{p}^-$*.*

(b) La sous-représentation fermée $V' \subset V$ *engendrée par* e *sous l'action de* $\mathrm{Sp}_{2g}(\mathbb{R})$ *est irréductible. De plus, si* $f \in (V')^\infty$ *satisfait (i) et (ii) alors* $f \in \mathbb{C}[K].e$*.*

À isomorphisme près, il existe au plus une représentation unitaire irréductible du groupe $\mathrm{Sp}_{2g}(\mathbb{R})$ *possédant un vecteur* e *qui est* $\mathcal{C}^\infty$ *et satisfait les propriétés (i) et (ii).*

Ce résultat est bien connu des spécialistes de la théorie des représentations unitaires des groupes de Lie, nous en donnons une démonstrations pour le confort du lecteur.

Démonstration. D'après le (ii), l'espace $E = \mathbb{C}[K].e \subset V^\infty$ est une représentation de K isomorphe à $U_{|K}$. Il est stable par $\mathfrak{k}_\mathbb{C}$ et annulé par $\mathfrak{p}^-$ puisque $\mathrm{ad}(K)\mathfrak{p}^- \subset \mathfrak{p}^-$. Il est donc également stable par la sous-algèbre parabolique $\mathfrak{q} = \mathfrak{k}_\mathbb{C} \oplus \mathfrak{p}^-$ de $\mathfrak{g}$. Soit Y le $\mathrm{U}(\mathfrak{g})$-module induit $\mathrm{U}(\mathfrak{g}) \otimes_{\mathrm{U}(\mathfrak{q})} E$. L'inclusion de E dans V^∞ induit donc un morphisme $\mathrm{U}(\mathfrak{g})$-équivariant

$$u : Y \longrightarrow V^\infty,$$

dont on notera l'image $X = u(Y)$. Comme K est connexe, E est irréductible comme $\mathrm{U}(\mathfrak{k}_\mathbb{C})$-module. Quitte à remplacer e par un élément bien choisi de E on peut supposer que $\mathfrak{b}e \subset \mathbb{C}e$ et que $he = \lambda(h)e$ pour tout $h \in \mathfrak{t}$ (théorie du plus haut poids de Cartan-Weyl). L'élément $1 \otimes e$ engendre donc Y et satisfait $(\mathfrak{b} \oplus \mathfrak{p}^-)(1 \otimes e) \subset \mathbb{C}(1 \otimes e)$ d'après (i), on en déduit que Y, et donc $X = \mathrm{U}(\mathfrak{g})e$, admet un caractère infinitésimal satisfaisant l'assertion (a), d'après le second paragraphe de l'exemple 3.3.

Observons également que X est stable par K. De plus, l'action adjointe de K sur $\mathrm{U}(\mathfrak{g})$, ainsi que son action naturelle sur E, définissent une structure de K-module sur Y telle que u soit K-équivariant. Ces structures font de Y et X des $(\mathfrak{g}, K)$-modules, que nous noterons Y' et X', et de u un morphisme de $(\mathfrak{g}, K)$-modules (nous renvoyons à [Wall88, §3.3] pour ces notions). Nous avons déjà vu que Y est un $\mathrm{U}(\mathfrak{g})$-module de plus haut poids. D'après [Dix74, Prop. 7.1.8], cela entraîne d'une part que Y' admet un unique quotient simple, et également que Y' est admissible (cela signifie que chaque représentation irréductible de K apparaît avec une multiplicité finie, et se déduit de ce que chaque poids de Y a une multiplicité finie, voir *loc. cit.*). Mais X' admet un produit hermitien invariant (il est unitaire au sens de [Wall88, §9.3.3]),

car la représentation V est unitaire par hypothèse. Étant admissible comme quotient de Y', X' est irréductible, c'est donc l'unique quotient irréductible de Y'. Comme X' admet un caractère central, un résultat de Harish-Chandra assure que tous ses vecteurs sont en fait analytiques [WALL88, §1.6, §3.4.9], [KNA86, VIII 8.7], et donc que l'adhérence $\overline{X}$ de X dans V est stable par $G(\mathbb{R})$ [WALL88, §1.6.6]. Elle admet X' pour $(\mathfrak{g}, K)$-module : c'est donc l'unique représentation irréductible unitaire de $G(\mathbb{R})$ de $(\mathfrak{g}, K)$-module X' [WALL88, §3.4.11]. Cela démontre le premier point du (b). Les deux assertions restantes suivent du fait déjà vu que X' est l'unique quotient irréductible de Y'. $\square$

Soit $(X, \Phi, \Delta, X^\vee, \Phi^\vee, \Delta^\vee)$ la donnée radicielle basée associée à (GL_g, T, B). On écrit de manière standard $X = \oplus_{i=1}^g \mathbb{Z}\varepsilon_i$, $\Phi = \{\pm(\varepsilon_i - \varepsilon_j), 1 \leq i < j \leq g\}$, $\Delta = \{\varepsilon_i - \varepsilon_{i+1}, 1 \leq i < g\}$, $X^\vee = \oplus_{i=1}^g \mathbb{Z}\varepsilon_i^*$ et $(\varepsilon_i - \varepsilon_j)^\vee = \varepsilon_i^* - \varepsilon_j^*$ pour $i < j$. Les poids dominants de GL_g sont donc les $\lambda \in X$ tels que $\lambda = \sum_{i=1}^g m_i \varepsilon_i$ avec $m_1 \geq m_2 \geq \cdots \geq m_g$.

Corollaire 3.6. *Soit W la $\mathbb{C}$-représentation irréductible de GL_g de plus haut poids $\sum_{i=1}^g m_i\varepsilon_i$. Supposons qu'il existe une représentation unitaire irréductible π'_W de $\mathrm{Sp}_{2g}(\mathbb{R})$ satisfaisant les conditions de la proposition 3.5 pour $U = W^*$. La classe de conjugaison semi-simple de $\mathfrak{so}_{2g+1}(\mathbb{C})$ qui correspond à $\inf_{\pi'_W}$ a pour valeurs propres les $2g+1$ entiers*

$$\pm(m_i - i), \quad i = 1, \cdots, g, \quad \text{et} \quad 0.$$

Démonstration. En effet, un calcul sans difficultés montre que la représentation adjointe de K sur $\mathfrak{p}^-$ est isomorphe à la restriction par l'homomorphisme j de la représentation $(g, X) \mapsto g\,X\,{}^{\mathrm{t}}g$ de $\mathrm{GL}_g(\mathbb{C})$ sur $\mathrm{Sym}_g(\mathbb{C})$ (carré symétrique de la représentation standard). L'ensemble de ses poids est donc

$$\{\varepsilon_i + \varepsilon_j, 1 \leq i \leq j \leq g\}.$$

Cette description montre que la base correspondant à $\mathfrak{b} \oplus \mathfrak{p}^-$ du système de racines de $G_\mathbb{C}$ associé à T n'est autre que la base standard introduite au §1.3. En particulier, l'élément ρ de la proposition 3.5 (a) n'est autre que $g\varepsilon_1 + (g-1)\varepsilon_2 + \cdots + \varepsilon_g$. Le poids dominant λ de W^* relativement à B est $\sum_{i=1}^g -m_{g+1-i}\varepsilon_i$, et donc

$$\lambda + \rho = \sum_{i=1}^g (i - m_i)\varepsilon_{g+1-i}.$$

Les poids de $\widehat{\mathrm{Sp}_{2g}}(\mathbb{C}) = \mathrm{SO}_{2g+1}(\mathbb{C})$ dans sa représentation standard sur $\mathbb{C}^{2g+1}$ étant 0 et les $\pm\varepsilon_i^*$ d'après le §1.3, cela conclut. $\square$

Soit W une $\mathbb{C}$-représentation irréductible de GL_g dans laquelle -1_g agit trivialement. Soit $f \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme modulaire de Siegel parabolique non nulle et de poids W. La proposition ci-dessus s'applique à $U = \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$, tout élément e dans l'image de $W^* \otimes f$ (Prop. IV.5.4) et $U = W^*$. Elle démontre que si $w \in W^*$ est non nul, la fonction $\varphi_{w,f} \in \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$ définie au §IV.5.3 engendre topologiquement, sous l'action de $\mathrm{Sp}_{2g}(\mathbb{R})$, une sous-représentation irréductible de $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$, nécessairement isomorphe à la représentation π'_W de l'énoncé précédent. Cela démontre l'existence de π'_W dès que $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \neq 0$. En fait, Harish-Chandra a démontré l'existence de π'_W pour toute W dont le plus haut poids satisfait $m_g > g$ (c'est la *série discrète holomorphe*, voir [Kna86, Ch. VI, §4 Thm. 6.6]). Si cette hypothèse sur W est satisfaite nous dirons que W est *positive* ; c'est le seul cas qui nous intéressera dans ce mémoire. Observons que si W est positive, les $2g+1$ entiers de l'énoncé ci-dessus sont distincts.

Supposons que W est positive et que -1_g agit trivialement dans W (i.e. $\sum_i m_i \equiv 0 \bmod 2$), de sorte que π'_W se factorise par $\mathrm{Sp}_{2g}(\mathbb{R})/\{\pm 1_{2g}\}$. Il n'est pas difficile de vérifier que π'_W n'est pas isomorphe à sa conjuguée extérieure [6] par un élément de $\mathrm{PGSp}_{2g}(\mathbb{R})\backslash\mathrm{Sp}_{2g}(\mathbb{R})$. Autrement dit, la représentation unitaire de $\mathrm{PSGp}_{2g}(\mathbb{R})$

$$\pi_W = \mathrm{Ind}_{\mathrm{Sp}_{2g}(\mathbb{R})}^{\mathrm{PGSp}_{2g}(\mathbb{R})} \pi'_W,$$

induite d'un sous-groupe d'indice 2, est irréductible. Bien entendu, π_W et π'_W ont même caractère infinitésimal, car $\mathrm{Sp}_{2g}(\mathbb{R})$ et $\mathrm{PGSp}_{2g}(\mathbb{R})$ ont même algèbre de Lie.

Fixons $v_W \in \pi_W$ un vecteur $\mathcal{C}^\infty$ non nul, annulé par $\mathfrak{p}^-$, engendrant W^* sous l'action de K, et propre pour l'action de $\mathfrak{b}$. Un tel vecteur est unique à multiplication par un élément de $\mathbb{C}^*$ près d'après la proposition 3.5. On fixe de même $e_W \in W^*$ non nul et de plus haut poids relativement à B.

Corollaire 3.7. *Supposons W positive. Si $F \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, il existe un unique $u_F \in \mathcal{A}_{\pi_W}(\mathrm{PGSp}_{2g})$ tel que $u_F(v_W) = \varphi_{e_W,F}$. L'application $F \mapsto u_F$ définit un isomorphisme $\mathrm{H}^{\mathrm{opp}}(\mathrm{PGSp}_{2g})$-équivariant*

$$\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \xrightarrow{\sim} \mathcal{A}_{\pi_W}(\mathrm{PGSp}_{2g}).$$

6. Cela vient de ce que cette conjuguée extérieure admet un vecteur $\mathcal{C}^\infty$ annulé par $\mathfrak{p}^+$ et engendrant W sous l'action de K (*plus bas poids*). Son $(\mathfrak{g}, K)$-module s'étudie de manière tout-à-fait similaire à celui de π'_W : il ne peut être isomorphe à celui de π'_W que s'il est de dimension finie, i.e. si π'_W (et donc W) est triviale. Cela ne se produit pas car la représentation triviale de $\mathrm{Sp}_{2g}(\mathbb{R})$ n'apparaît pas dans $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$.

Démonstration. Les propositions IV.5.4 et 3.5 montrent que l'application de l'énoncé induit un isomorphisme $\mathrm{H}^{\mathrm{opp}}(\mathrm{PGSp}_{2g})$-équivariant entre $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ et le sous-espace $\mathrm{Hom}_{G(\mathbb{R})}(\pi_W, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})) \subset \mathcal{A}_{\pi_W}(\mathrm{PGSp}_{2g})$. On conclut par le fait général suivant : si G est un $\mathbb{Z}$-groupe tel que $G_{\mathbb{Q}}$ est semi-simple, et si U est une série discrète de $G(\mathbb{R})$, alors l'inclusion $\mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}_{\mathrm{cusp}}(G)) \subset \mathcal{A}_U(G)$ est une égalité [Wall84, Thm. 4.3]. □

Ainsi, si $F \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est non nulle et vecteur propre de tous les opérateurs de Hecke dans $\mathrm{H}(\mathrm{PGSp}_{2g})$ il y a un sens à parler de la représentation $\pi_F \in \Pi_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$ engendrée par F, suivant la définition générale du §3.2. Elle satisfait $(\pi_F)_\infty = \pi_W$.

Le discours précédent peut également être tenu pour Sp_{2g} plutôt que PGSp_{2g} et démontre l'existence d'un isomorphisme $\mathrm{H}^{\mathrm{opp}}(\mathrm{Sp}_{2g})$-équivariant entre $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ et $\mathcal{A}_{\pi'_W}(\mathrm{Sp}_{2g})$; son contenu n'en est que moins fin, d'après la proposition 5.7.

Isomorphismes exceptionnels en genre 1 et 2

Dans ce qui suit, on suppose W positive, de plus haut poids $\sum_i m_i \varepsilon_i$, et telle que -1_g agit trivialement dans W.

Supposons $g = 1$. Dans ce cas, W est la représentation dét^k avec $k = m_1 > 1$ et $k \equiv 0 \bmod 2$. L'isomorphisme $\mathfrak{sl}_2(\mathbb{C}) \simeq \mathfrak{so}_3(\mathbb{C})$ (carré symétrique) permet de voir le caractère infinitésimal de π_W comme la classe de conjugaison semi-simple dans $\mathfrak{sl}_2(\mathbb{C})$ de valeurs propres $\pm\frac{k-1}{2}$. En fait, la classification bien connue du dual unitaire de $\mathrm{SL}_2(\mathbb{R})$ (Bargmann [Bar47]) montre qu'à isomorphisme près, l'unique représentation unitaire irréductible de $\mathrm{PGL}_2(\mathbb{R})$ ayant un caractère infinitésimal de valeurs propres $\pm\frac{k-1}{2}$, avec $k > 3$ entier pair, est la représentation $\pi_{\text{dét}^k}$. Quand $k = 2$, il faut lui rajouter les deux représentations de dimension 1.

Supposons $g = 2$. Dans ce cas, conformément aux notations de [vdG08], W est la représentation $\mathrm{Sym}^j(\mathbb{C}^2) \otimes \text{dét}^k$ avec $j = m_1 - m_2$ et $k = m_2$, de plus $k > 2$ et $j \equiv 0 \bmod 2$. L'isomorphisme exceptionnel $\mathfrak{sp}_4(\mathbb{C}) \simeq \mathfrak{so}_5(\mathbb{C})$ permet de voir le caractère infinitésimal de π_W comme la classe de conjugaison semi-simple dans $\mathfrak{sp}_4(\mathbb{C})$ de valeurs propres pour son action sur $\mathbb{C}^4$:

$$\pm\frac{w_1}{2}, \quad \pm\frac{w_2}{2}$$

où $w_1 = m_1 + m_2 - 3 = 2k + j - 3$ et $w_2 = m_1 - m_2 + 1 = j + 1$.

4. La conjecture d'Arthur-Langlands

4.1. Paramétrisation de Langlands de $\Pi(G)$ pour G semi-simple sur $\mathbb{Z}$

Soit H un $\mathbb{C}$-groupe, de composante neutre H^0 et d'algèbre de Lie complexe $\mathfrak{h}$. Notons $H(\mathbb{C})_{\mathrm{ss}}$ (resp. $\mathfrak{h}_{\mathrm{ss}}$) l'ensemble des classes de $H(\mathbb{C})$-conjugaison d'éléments semi-simples de $H^0(\mathbb{C})$ (resp. de $\mathfrak{h}$), et considérons l'ensemble

$$\mathcal{X}(H)$$

des familles $(c_v)_{v\in \mathrm{P}\cup\{\infty\}}$, où $c_\infty \in \mathfrak{h}_{\mathrm{ss}}$ et $c_p \in H(\mathbb{C})_{\mathrm{ss}}$ pour tout $p \in \mathrm{P}$. Dans la discussion qui va suivre, H sera connexe (et même semi-simple), mais des exemples non connexes associés aux groupes orthogonaux pairs apparaîtront par la suite. Tout morphisme de $\mathbb{C}$-groupes $r : H \to H'$ définit une application encore notée $r : \mathcal{X}(H) \to \mathcal{X}(H')$, envoyant (c_v) sur $(r(c_v))$.

Soit G un $\mathbb{Z}$-groupe semi-simple. Comme nous l'avons déjà dit, pour tout nombre premier p le $\mathbb{Z}_p$-groupe $G_{\mathbb{Z}_p}$ est réductif et déployé [Gro96, Prop. 1.1] ; il admet donc une donnée radicielle basée $\Psi(G_{\mathbb{Z}_p})$. De plus, si $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}_p}$) est une clôture algébrique de $\mathbb{Q}$ (resp. $\mathbb{Q}_p$), et si $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ et $\overline{\mathbb{Q}} \to \mathbb{C}$ sont deux plongements, les isomorphismes associés de données radicielles basées

$$\Psi(G_{\mathbb{Z}_p}) \xrightarrow{\sim} \Psi(G_{\overline{\mathbb{Q}_p}}) \xleftarrow{\sim} \Psi(G_{\overline{\mathbb{Q}}}) \xrightarrow{\sim} \Psi(G_{\mathbb{C}})$$

ne dépendent d'aucun de ces choix de plongements effectués [7]. Le dual de Langlands de $G_{\overline{\mathbb{Q}}}$ est donc canoniquement le dual de Langlands des $G_{\mathbb{Z}_p}$ pour tout p et de $G_{\mathbb{C}}$: nous le noterons $\widehat{G}$.

Suivant Langlands [Lan71], on dispose d'une application canonique

$$\mathrm{c} : \Pi(G) \longrightarrow \mathcal{X}(\widehat{G}), \pi \mapsto (\mathrm{c}_v(\pi)),$$

définie comme suit. Soit $\pi = \pi_\infty \otimes \pi_f \in \Pi(G)$. On note $\mathrm{c}_\infty(\pi)$ le caractère infinitésimal de π_∞ (§3.4). L'isomorphisme de Satake entraîne que $\mathrm{H}(G) = \bigotimes_p \mathrm{H}_p(G)$ est commutative, de sorte que π_f est de dimension 1 et peut être vue comme un homomorphisme d'anneaux de $\mathrm{H}(G)^{\mathrm{opp}} = \mathrm{H}(G)$ dans $\mathbb{C}$, ou ce qui revient au même comme une collection de morphismes d'anneaux

$$\pi_p : \mathrm{H}_p(G) \to \mathbb{C},$$

7. L'argument de Gross est le suivant. C'est un fait général que l'action naturelle de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $\Psi(G_{\overline{\mathbb{Q}}})$ se factorise en une action fidèle du groupe de Galois d'un corps de nombres K galoisien sur $\mathbb{Q}$. Le fait que G est réductif sur $\mathbb{Z}_p$ entraîne que K est non ramifié en p, et donc $K = \mathbb{Q}$ d'après un résultat fameux de Minkowski. Cela entraîne que G est déployé sur $\mathbb{Z}_p$ et le reste des assertions ci-dessus.

où π_p est la restriction de π_f à $\mathrm{H}_p(G)$ au sens du §IV.2.5. Le scholie 2.2 associe donc à chaque π_p un unique élément $\mathrm{c}_p(\pi) \in \widehat{G}(\mathbb{C})_{\mathrm{ss}}$. Par définition, $\mathrm{c}(\pi)$ détermine π_f et le caractère infinitésimal de π_∞, l'application c est donc à fibres finies (Harish-Chandra §3.4).

Exemple 4.2. (La représentation triviale) Soit $\pi = 1_G \in \Pi_{\mathrm{disc}}(G)$ la représentation triviale de G (§IV.3.2). D'après l'exemple 3.3, $2\mathrm{c}_\infty(\pi)$ est la classe de conjugaison du co-poids 2ρ de $\widehat{G}$. De même, d'après l'exemple 2.3, la classe de conjugaison $\mathrm{c}_p(\pi)$ est celle de $\rho(p) = (2\rho)(p^{\frac{1}{2}})$.

4.3. Quelques exemples

Considérons d'abord le $\mathbb{Z}$-groupe PGL_2, de groupe dual SL_2. Soit $k > 0$ un entier pair, $F = \sum_{n\geq 1} a_n q^n \in \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ une forme modulaire propre pour tous les opérateurs de Hecke de $\mathrm{H}(\mathrm{PGL}_2)$ telle que $a_1 = 1$ (elles forment une base de $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ [Ser70, VII §5.4]). Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par F (voir §IV.3.2, §V.3.4). On a déjà déterminé $\mathrm{c}_\infty(\pi)$, c'est-à-dire $\inf_{\pi_W}$, en fonction de k *loc. cit.* Un $\mathbb{Z}$-isomorphisme $\mathrm{PGL}_2 \simeq \mathrm{PGSp}_2$ induit un isomorphisme $\mathrm{H}_p(\mathrm{PGSp}_2) \xrightarrow{\sim} \mathrm{H}_p(\mathrm{PGL}_2)$ envoyant K_p sur $\mathrm{T}_{\mathbb{Z}/p\mathbb{Z}}$, les relations (2.8) et (5.5), ainsi que [Ser70, VII Thm. 7], montrent donc que pour tout p premier

$$p^{\frac{k-1}{2}} \operatorname{Trace}(\mathrm{c}_p(\pi)) = a_p.$$

Considérons maintenant le $\mathbb{Z}$-groupe PGSp_4, de groupe dual le $\mathbb{C}$-groupe Sp_4 (qui est aussi Spin_5). Soit W la représentation $\mathrm{Sym}^j(\mathbb{C}^2)\otimes \mathrm{dét}^k$ de $\mathrm{GL}_2(\mathbb{C})$ avec $k \geq 3$, soit $F \in \mathrm{S}_W(\mathrm{Sp}_4(\mathbb{Z}))$ une forme propre (non nulle), et soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGSp}_4)$ la représentation engendrée par F. On a déjà déterminé $\mathrm{c}_\infty(\pi)$ (i.e. $\inf_{\pi_W}$) en fonction de j et k au §3.4. Si p est premier, l'élément $\mathrm{c}_p(\pi) \in \mathrm{Sp}_4(\mathbb{C})_{\mathrm{ss}}$ est uniquement caractérisé par sa trace et celle de son carré alterné dans la représentation tautologique $V_{\mathrm{Spin}} \simeq \mathbb{C}^4$ de $\mathrm{Sp}_4(\mathbb{C})$. Si $\mathrm{K}_p(F) = a_p F$ et $\mathrm{T}_p(F) = b_p F$, les relations (2.8) montrent que

$$p^{3/2} \operatorname{Trace}(\mathrm{c}_p(\pi) \,|\, V_{\mathrm{Spin}}) = a_p \quad \text{et} \quad p^2 \operatorname{Trace}(\mathrm{c}_p(\pi) \,|\, \Lambda^2 V_{\mathrm{Spin}}) = b_p + p^2 + 1.$$

Pour un $g \geq 1$ général, considérons une forme propre $F \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ telle que $\mathrm{T}_p(F) = b_p F$. Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ désigne la représentation engendrée par F, alors $\mathrm{c}_\infty(\pi) \subset \mathrm{so}_{2g+1}(\mathbb{C})_{\mathrm{ss}}$ est donné en fonction de W par la proposition 3.6. Si $V_{\mathrm{St}} \simeq \mathbb{C}^{2g+1}$ désigne la représentation tautologique de $\mathrm{SO}_{2g+1}(\mathbb{C})$, alors pour tout premier p,

$$p^g \operatorname{Trace}(\mathrm{c}_p(\pi) \,|\, V_{\mathrm{st}}) = b_p + 1.$$

Soit maintenant $n \equiv 0 \bmod 8$ et $G = \mathrm{SO}_n$ le groupe spécial orthogonal de E_n (§IV.4.4), de sorte que $\widehat{G}(\mathbb{C}) = \mathrm{SO}_n(\mathbb{C})$ Soit W la représentation irréductible de plus haut poids $\sum_{i=1}^{n/2} m_i\varepsilon_i$ avec $m_1 \geq \cdots m_{n/2-1} \geq |m_{n/2}|$ dans les notations du §1.3. Soit $F \in \mathrm{M}_W(\mathrm{SO}_n)$ une forme propre et $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ la représentation engendrée. Par définition, on a $\pi_\infty \simeq W^*$, mais $W^* \simeq W$ car $n \equiv 0 \bmod 4$, de sorte que les n valeurs propres de $\mathrm{c}_\infty(\pi) \in \mathfrak{so}_n(\mathbb{C})_{\mathrm{ss}}$ sont

$$\pm(m_i + \frac{n}{2} - i), \;\; i = 1, \cdots, \frac{n}{2}$$

d'après le §3.4. Soit p un nombre premier. Supposons que $\mathrm{T}_p(F) = \lambda_p F$, $\mathrm{T}_{p^2}(F) = \lambda_{p^2} F$ et $\mathrm{T}_{p,p}(F) = \lambda_{p,p} F$ (§2.8). Les relations (2.5),(2.6), ainsi que l'exemple 2.11, s'écrivent

$$p^{\frac{n}{2}-1}\,\mathrm{Trace}(\mathrm{c}_p(\pi) \,|\, V_{\mathrm{St}}) = \lambda_p,$$

$$p^{n-3}\,\mathrm{Trace}(\mathrm{c}_p(\pi) \,|\, \Lambda^2 V_{\mathrm{St}}) = \lambda_{p,p} + p^{\frac{n}{2}-2} + \frac{p^{n-2}-1}{p^2-1},$$

et $(p+1)\lambda_{p,p} = \lambda_p^2 - \lambda_{p^2} - \frac{(p^{\frac{n}{2}}-1)(p^{\frac{n}{2}-1}+1)}{p-1}$.

4.4. La conjecture d'Arthur-Langlands

Soient G un $\mathbb{Z}$-groupe semi-simple et $r : \widehat{G} \to \mathrm{SL}_n$ une $\mathbb{C}$-représentation. Cette représentation induit une application $\mathcal{X}(\widehat{G}) \to \mathcal{X}(\mathrm{SL}_n), (c_v) \mapsto (r(c_v))$ que nous notons encore r. Si $\pi \in \Pi(G)$, on peut lui associer l'élément

$$\psi(\pi, r) := r(\mathrm{c}(\pi)) \in \mathcal{X}(\mathrm{SL}_n).$$

Cet élément est appelé *paramètre de Langlands du couple* (π, r). Si $\pi \in \Pi_{\mathrm{disc}}(G)$, les conjectures de Langlands [Lan70], précisées par Arthur [Art89], affirment que $\psi(\pi, r)$ s'exprime en terme des $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$ pour $m \geq 1$. Avant de rappeler comment, nous devons introduire quelques notations.

– Notons St_m la $\mathbb{C}$-représentation tautologique de SL_m sur $\mathbb{C}^m$. Si a et b sont des entiers, la somme directe et le produit tensoriel des représentations St_a et St_b définissent des $\mathbb{C}$-représentations de $\mathrm{SL}_a \times \mathrm{SL}_b$ de dimensions respectives $a+b$ et ab, ainsi donc que des applications naturelles

$$\mathcal{X}(\mathrm{SL}_a) \times \mathcal{X}(\mathrm{SL}_b) \to \mathcal{X}(\mathrm{SL}_{a+b}) \;\text{ et }\; \mathcal{X}(\mathrm{SL}_a) \times \mathcal{X}(\mathrm{SL}_b) \to \mathcal{X}(\mathrm{SL}_{ab}).$$

Nous les noterons respectivement $(c, c') \mapsto c \oplus c'$ et $(c, c') \mapsto c \otimes c'$. Ces opérations sont commutatives, associatives et distributives en un sens évident.

– Suivant Arthur [ART89], considérons l'élément $e \in \mathcal{X}(\mathrm{SL}_2)$ défini par

$$e_p = \begin{bmatrix} p^{-\frac{1}{2}} & 0 \\ 0 & p^{\frac{1}{2}} \end{bmatrix} \ \forall p \in \mathrm{P}, \quad \text{et} \quad e_\infty = \begin{bmatrix} -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}.$$

Il donne naissance pour tout entier $d \geq 1$ à l'élément $\mathrm{Sym}^{d-1}(e) \in \mathcal{X}(\mathrm{SL}_d)$, où Sym^{d-1} désigne la représentation $\mathrm{Sym}^{d-1}\mathrm{St}_2$ de SL_2. Nous le noterons $[d]$; par exemple $[2] = e$. Ces éléments joueront par la suite un rôle particulièrement important. Observons d'ores et déjà que $[d] = \mathrm{c}(1_{\mathrm{PGL}_d})$, d'après l'exemple 4.2. On pose plus généralement, pour $m, d \geq 1$ entiers et $c \in \mathcal{X}(\mathrm{SL}_m)$,

$$c[d] := c \otimes [d].$$

– Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$, l'élément $\mathrm{c}(\pi) \in \mathcal{X}(\mathrm{SL}_m)$ sera simplement noté π. Cet abus de langage sera en général innocent, car $\mathrm{c}(\pi)$ détermine π d'après le *théorème de multiplicité* 1 *forte* de Piatetski-Shapiro, Jacquet et Shalika [JS81a]. (On prendra garde que l'injectivité de l'application de paramétrisation c est très spécifique des $\mathbb{Z}$-groupes PGL_m).

Ainsi, si $n_1, \ldots, n_k$, $d_1, \ldots, d_k$ sont des entiers ≥ 1, si $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour tout $i = 1, \ldots, k$, et si $n = \sum_{i=1}^k n_i d_i$, on dispose d'un élément bien défini

$$\pi_1[d_1] \oplus \pi_2[d_2] \oplus \cdots \oplus \pi_k[d_k] \ \in \ \mathcal{X}(\mathrm{SL}_n).$$

Il ne dépend que du multi-ensemble $\{(\pi_i, d_i), i = 1, \ldots, k\}$. Le sous-ensemble de $\mathcal{X}(\mathrm{SL}_n)$ formé des éléments qui sont de cette forme, pour un quadruple $(k, (n_i), (d_i), (\pi_i))$ quelconque tel que $n = \sum_{i=1}^k n_i d_i$, sera noté

$$\mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n).$$

On dispose d'un résultat d'unicité remarquable, dû à Jacquet-Shalika [JS81b] (voir aussi [LAN79]) :

Proposition 4.5. *Soient $k, l \geq 1$ des entiers, ainsi que, pour $1 \leq i \leq k$ (resp. $1 \leq j \leq l$), des entiers $n_i, d_i \geq 1$ (resp. $n'_j, d'_j \geq 1$) et une représentation π_i (resp. π'_j) dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ (resp. $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n'_j})$). Supposons que l'on ait $n := \sum_i n_i d_i = \sum_j n'_j d'_j$ et*

$$\oplus_{i=1}^k \pi_i[d_i] = \oplus_{j=1}^l \pi'_j[d'_j]$$

dans $\mathcal{X}(\mathrm{SL}_n)$. Alors on a $k = l$ et il existe $\sigma \in \mathfrak{S}_k$ tel que pour tout $1 \leq i \leq k$, $(n'_i, \pi'_i, d'_i) = (n_{\sigma(i)}, \pi_{\sigma(i)}, d_{\sigma(i)})$.

Le cas particulier des conjectures d'Arthur et Langlands que nous souhaitons mettre en évidence est le suivant.

Conjecture 4.6. (Langlands [LAN70], Arthur [ART89]) *Soient G un $\mathbb{Z}$-groupe semi-simple et $r : \widehat{G} \to \mathrm{SL}_n$ une $\mathbb{C}$-représentation. Si $\pi \in \Pi_{\mathrm{disc}}(G)$ alors $\psi(\pi, r) \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$.*

Autrement dit, pour tout $\pi \in \Pi_{\mathrm{disc}}(G)$, il existe un entier $k \geq 1$, des entiers $n_1, \ldots, n_k$, $d_1, \ldots, d_k$ et des représentations $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour tout $1 \leq i \leq k$, tels que $\psi(\pi, r) = \oplus_{i=1}^k \pi_i[d_i]$ (et cette écriture est unique à permutation des facteurs près d'après la proposition 4.5). Concrètement, cela dit que pour tout $v \in \mathrm{P} \cup \{\infty\}$, les n valeurs propres de la classe de conjugaison semi-simple $\rho(\mathrm{c}_v(\pi))$ sont les $\lambda\, p^\mu$ pour $v \in \mathrm{P}$ (resp. $\lambda + \mu$ pour $v = \infty$) où i parcourt $\{1, \ldots, k\}$, et où pour tout $i \in \{1, \ldots, k\}$:

- λ parcourt les valeurs propres de $\mathrm{St}_{r_i}(\mathrm{c}_v(\pi_i))$ comptées avec multiplicités,
- μ parcourt $\frac{1-d_i}{2}, \frac{3-d_i}{2}, \cdots, \frac{d_i-3}{2}, \frac{d_i-1}{2}$.

Nous renvoyons à la préface pour un autre point de vue sur cette conjecture, où elle est motivée par l'existence d'un groupe conjectural ayant des propriétés mirifiques (le *groupe de Langlands* de $\mathbb{Z}$). Ajoutons que le groupe G et r étant donnés, la philosophie de Langlands et Arthur suggère aussi une description de l'image de $\pi \mapsto \psi(\pi, r)$, nettement plus difficile à formuler en général, dont un ingrédient est la *formule de multiplicité d'Arthur-Langlands* déjà entrevue dans la préface. Dans les exemples qui suivent, nous ne discutons que de cas, nettement plus simples, où G est soit PGL_n soit un groupe classique, et où r est sa représentation "tautologique".

4.7. Quelques exemples

Le cas de PGL_n

Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$, on a tautologiquement $\mathrm{c}(\pi) = \psi(\pi, \mathrm{St}_n) = \pi$. Si d est un diviseur de n et si $\varpi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n/d})$, Speh a construit à l'aide de résidus de séries d'Eisenstein un $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGL}_n)$ tel que $\psi(\pi, \mathrm{St}_n) = \varpi[d]$. La conjecture de Jacquet, démontrée par Moeglin et Waldspurger [MW89], affirme que tout $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGL}_n)$ est de cette forme. Cela démontre la conjecture 4.6 quand $G = \mathrm{PGL}_n$ et $r = \mathrm{St}_n$.

Un autre cas fameux et connu de la conjecture 4.6 concerne la représentation carré symétrique $\mathrm{Sym}^2 : \widehat{\mathrm{PGL}_2} = \mathrm{SL}_2 \to \mathrm{SL}_3$. Plus précisément, Gelbart et Jacquet ont démontré que si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$, il existe une unique $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_3)$ telle que $\psi(\pi, \mathrm{Sym}^2) = \pi'$ [GJ78]. On note par abus $\pi' = \mathrm{Sym}^2 \pi$. Par exemple, si π est engendrée par une forme propre

$F \in \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ comme au §4.1, alors $\mathrm{c}_\infty(\mathrm{Sym}^2\,\pi)$ admet pour valeurs propres 0 et $\pm(k-1)$, et $\mathrm{c}_p(\mathrm{Sym}^2\,\pi) \in \mathrm{SL}_3(\mathbb{C})_{\mathrm{ss}}$ admet pour polynôme caractéristique

$$X^3 - (p^{1-k}a_p^2 - 1)(X^2 - X) + 1.$$

Groupes classiques

La *classification d'Arthur* [Art13], sur laquelle nous reviendrons au chapitre suivant, démontre la conjecture 4.6 quand G est un *groupe classique* (au sens légèrement restrictif précisé ci-dessous) et r la *représentation standard* de $\widehat{G}$; Arthur décrit aussi l'image de $\pi \mapsto \psi(\pi, r)$. Contentons-nous ici de préciser les terminologies en italique.

Notons $\mathrm{Class}_{\mathbb{C}}$ l'ensemble constitué des $\mathbb{C}$-groupes Sp_{2g} pour un entier $g \geq 1$ et des $\mathbb{C}$-groupes SO_m pour un entier $m \neq 2$. Par exemple, PGSp_{2g} n'est pas isomorphe à un groupe appartenant à $\mathrm{Class}_{\mathbb{C}}$ si $g > 2$. Le lecteur observera que les $\mathbb{C}$-groupes des deux familles sus-mentionnées sont deux à deux non isomorphes. Tout $\mathbb{C}$-groupe dans $\mathrm{Class}_{\mathbb{C}}$ possède une $\mathbb{C}$-repésentation distinguée tautologique, sur $\mathbb{C}^{2g}$ pour Sp_{2g}, sur $\mathbb{C}^m$ pour SO_m, appelée représentation *standard*, et notée St. Elle est irréductible et fidèle, et de dimension minimale pour ces propriétés.

Les $\mathbb{Z}$-groupes semi-simples G auxquels s'appliquent les travaux d'Arthur sus-cités sont ceux tels que $G_{\mathbb{C}}$ est isomorphe à un élément de $\mathrm{Class}_{\mathbb{C}}$, auquel cas $\widehat{G}$ l'est aussi (§1.3). C'est le cas du $\mathbb{Z}$-groupe Sp_{2g} et du $\mathbb{Z}$-groupe SO_L où L est un q-module sur $\mathbb{Z}$ de dimension > 2 (§II.1). C'est également le cas des $\mathbb{Z}$-groupes spéciaux orthogonaux de rang impair étudiés dans l'appendice B (voir la proposition 1.7 de cet appendice). On peut démontrer qu'il n'y en a pas d'autre à isomorphismes près [Gro96].

Cas des $\mathbb{Z}$-groupes O_n et PGO_n

Considérons le $\mathbb{Z}$-groupe orthogonal $G' = \mathrm{O}_n$ du q-module E_n (§IV.4.4). N'étant pas connexe, on ne peut lui appliquer verbatim les considérations du §4.1. Néanmoins, nous avons déjà observé au corollaire 2.4 que pour tout nombre premier p, l'isomorphisme de Satake de $G = \mathrm{SO}_n$ induit une bijection

$$\mathrm{Hom}_{\mathrm{anneaux}}(\mathrm{H}_p(\mathrm{O}_n), \mathbb{C}) \xrightarrow{\sim} \mathrm{O}_n(\mathbb{C})_{\mathrm{ss}};$$

on prendra garde que le terme de droite désigne l'ensemble des classes de $\mathrm{O}_n(\mathbb{C})$-conjugaison d'éléments semi-simples de $\mathrm{SO}_n(\mathbb{C})$ (§4.1). De même, il est facile de vérifier que si V' est une représentation irréductible de $G'(\mathbb{R})$, sa restriction V à $G(\mathbb{R})$ est soit irréductible, soit somme de deux représentations non isomorphes mais conjuguées extérieures sous l'action de $\mathrm{O}_n(\mathbb{R})$;

la $\mathrm{O}_n(\mathbb{C})$-orbite de l'élément de $(\mathfrak{so}_n)_{\mathrm{ss}}$ associé au caractère infinitésimal de chacun des constituants de V est donc indépendante du constituant choisi, et nous dirons par abus que c'est le caractère infinitésimal de V'. Nous avons donc défini une application de paramétrisation

$$\Pi(\mathrm{O}_n) \longrightarrow \mathcal{X}(\mathrm{O}_n(\mathbb{C}))$$

que nous noterons encore $\mathrm{c} : \pi \mapsto (\mathrm{c}_v(\pi))$. Il est donc naturel de poser

$$\mathcal{X}(\widehat{\mathrm{O}_n}) := \mathcal{X}(\mathrm{O}_n(\mathbb{C})).$$

Suivant le §4.1, toute $\mathbb{C}$-représentation $r : \mathrm{O}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ induit une application

$$r : \mathcal{X}(\widehat{\mathrm{O}_n}) \to \mathcal{X}(\mathrm{GL}_n)$$

de sorte qu'il y a encore un sens à poser $\psi(\pi, r) = r(\mathrm{c}(\pi))$ quand r est comme ci-dessus et $\pi \in \Pi(\mathrm{O}_n)$.

On dispose pour O_n d'une conjecture analogue à la conjecture 4.6 ; elle se déduit en fait de cette conjecture appliquée au $\mathbb{Z}$-groupe SO_n, expliquons comment. Soient $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$, $V' = (\pi')^*_\infty$ et $V = V'_{|\mathrm{SO}_n(\mathbb{R})}$. D'après le §IV.4.4, on dispose d'une injection naturelle $\mathrm{H}(\mathrm{O}_n)$-équivariante

$$\mathrm{res} : \mathrm{M}_{V'}(\mathrm{O}_n) \longrightarrow \mathrm{M}_V(\mathrm{SO}_n).$$

Soit $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ la représentation engendrée par l'une quelconque des formes propres appartenant au $\mathrm{H}(\mathrm{SO}_n)$-module engendré par $\mathrm{res}(F)$, où $F \in \mathrm{M}_{V'}(\mathrm{O}_n)$ désigne une forme propre quelconque engendrant π' (§IV.3.2). Les représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ obtenues ainsi seront appelées *les constituants de la restriction de π' à SO_n* ; elles forment un ensemble fini non vide. Si π est un tel constituant, $\mathrm{c}(\pi')$ est par définition l'image de $\mathrm{c}(\pi)$ par l'homomorphisme canonique $\mathcal{X}(\widehat{\mathrm{SO}_n}) \to \mathcal{X}(\widehat{\mathrm{O}_n})$. La proposition qui suit est donc évidente.

Proposition 4.8. *Soient $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$, $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ un constituant de la restriction de π' à SO_n, $r' : \mathrm{O}_n(\mathbb{C}) \to \mathrm{GL}_m(\mathbb{C})$ une $\mathbb{C}$-représentation, et r la restriction r' à $\mathrm{SO}_n(\mathbb{C})$. Alors $\psi(\pi', r') = \psi(\pi, r)$. En particulier, la conjecture d'Arthur-Langlands est satisfaite pour (π, r) si et seulement si elle l'est pour (π', r).*

Cette proposition est particulièrement utile dans le cas de la représentation tautologique St de $\mathrm{O}_n(\mathbb{C})$ sur $\mathbb{C}^n$, dont la restriction à $\mathrm{SO}_n(\mathbb{C})$ est sa représentation standard.

La discussion de ce paragraphe admet enfin un analogue naturel au cas du $\mathbb{Z}$-groupe PGO_n, pour lequel on dispose d'une application de paramétrisation

$$\mathrm{c} : \Pi(\mathrm{PGO}_n) \to \mathcal{X}(\widehat{\mathrm{PGO}_n}) := \mathcal{X}(\mathrm{Pin}_n)$$

où Pin_n désigne le $\mathbb{C}$-groupe Pin du q-module standard V_n de dimension n sur $\mathbb{C}$. Suivant [ABS64], on rappelle qu'il s'agit du sous-groupe des éléments x de l'algèbre de Clifford $\mathrm{C}(V_n)$ de V_n tels que $xx^t = 1$ et $\alpha(x)V_n x^{-1} \subset V_n$, $x \mapsto \alpha(x)$ et $x \mapsto x^t$ désignant respectivement l'involution et l'anti-involution canonique de $\mathrm{C}(V_n)$. Sa composante neutre, définie part $\alpha = \mathrm{id}$, est le $\mathbb{C}$-groupe Spin_n ; elle est d'indice 2. Tout élément $e \in V_n$ tel que $\mathrm{q}(e) = 1$ (i.e. $e^2 = 1$) appartient à $\mathrm{Pin}(V_n) = \mathrm{Pin}_n(\mathbb{C})$ et définit une section du morphisme canonique $\mathrm{Pin}_n \to \mathbb{Z}/2\mathbb{Z}$. Enfin, on dispose d'un morphisme surjectif naturel $\mathrm{Pin}_n \to \mathrm{O}_{V_n}, x \mapsto (v \mapsto \alpha(x)vx^{-1})$. Son noyau est ± 1 et l'image de tout élément $e \in V_n$ tel que $\mathrm{q}(e) = 1$ est la symétrie orthogonale par rapport à e.

Le cas de la représentation triviale

Supposons maintenant que G est un $\mathbb{Z}$-groupe semi-simple quelconque et considérons la représentation triviale $1 \in \Pi_{\mathrm{disc}}(G)$. Soit $\mu : \mathrm{SL}_2 \to \widehat{G}$ un $\mathbb{C}$-morphisme principal au sens de Kostant. Une formulation équivalente de la description de $\mathrm{c}(1)$ donnée dans l'exemple 4.2 est

$$\mu(e) = \mathrm{c}(1)$$

(cette observation est explicitement donnée dans [Gro98, §7], mais elle est sans doute plus ancienne). En particulier, si $r : \widehat{G} \to \mathrm{SL}_n$ désigne un $\mathbb{C}$-morphisme arbitraire, et s'il on décompose la représentation $r \circ \mu$ de SL_2 sous la forme $\oplus_{i=1}^k \mathrm{Sym}^{d_i - 1}\mathbb{C}^2$ avec $d_1, \ldots, d_k$ des entiers ≥ 1, on a donc

$$\psi(1, r) = \oplus_{i=1}^k [d_i].$$

Ceci est bien en accord avec la conjecture d'Arthur-Langlands (en l'occurence, avec les conjectures d'Arthur [Art89]), qui vaut donc pour le couple $(1, r)$ quelque soit la représentation r.

Supposons par exemple $G = \mathrm{SO}_n$ avec $n \equiv 0 \bmod 8$. On a alors $\mathrm{St} \circ \mu = \mathrm{Sym}^{n-2}\mathbb{C}^2 \oplus 1$, autrement dit $\psi(1, \mathrm{St}) = [n-1] \oplus [1]$. Cette relation vaut également si $G = \mathrm{O}_n$, car la représentation triviale de SO_n est évidemment la restriction à SO_n de la représentation triviale de O_n, elles ont donc même paramètre standard d'après la proposition 4.8.

4.9. Liens avec les fonctions L

Soient G un $\mathbb{Z}$-groupe semi-simple, $r : \widehat{G} \to \mathrm{GL}_n$ une $\mathbb{C}$-représentation et $\pi \in \Pi_{\mathrm{disc}}(G)$. D'après Langlands [LAN71, §3], le produit eulérien

$$\mathrm{L}(s, \pi, r) = \prod_{p \in \mathrm{P}} \text{dét}(1 - p^{-s} r(\mathrm{c}_p(\pi)))^{-1}$$

est absolument convergent pour $\mathrm{Re}(s)$ assez grand (voir aussi [SHA10, §2.5]).

Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ on pose $\mathrm{L}(s, \pi) = \mathrm{L}(s, \pi, \mathrm{St}_n)$ (on rappelle que St_n désigne la représentation tautologique de SL_n, §4.4). On sait depuis Godement et Jacquet que $\mathrm{L}(s, \pi)$ admet un prolongement holomorphe à $\mathbb{C}$ tout entier, à moins que $n = 1$ auquel cas $\pi = 1_{\mathrm{PGL}_1}$ et cette fonction $\mathrm{L}(s, \pi)$ n'est autre que la fonction $\zeta(s)$ de Riemann. D'après Jacquet et Shalika [JS81a], le produit eulérien $\mathrm{L}(s, \pi)$ est même absolument convergent pour $\mathrm{Re}(s) > 1$. Si $\psi(\pi, r) = \oplus_{i=1}^{k} \pi_i[d_i]$ il découle des définitions que l'on a

$$\mathrm{L}(s, \pi, r) = \prod_{i \in I} \prod_{j=0}^{d_i - 1} \mathrm{L}(s + j + \frac{1 - d_i}{2}, \pi_i),$$

et donc $\mathrm{L}(s, \pi, r)$ admet également un prolongement méromorphe à $\mathbb{C}$ tout entier, dont tous les pôles sont expliqués par les occurences de la représentation triviale dans $\psi(\pi, r)$.

Le lecteur prendra garde que les normalisations employées ici font de $s = \frac{1}{2}$ le centre naturel des équations fonctionnelles en jeu. Supposons par exemple que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ désigne la représentation associée à une forme propre normalisée $F = \sum_{n \geq 0} a_n q^n$, de poids k, comme au §4.3. On a alors $\mathrm{L}(s - \frac{k-1}{2}, \pi) = \sum_{n \geq 1} \frac{a_n}{n^s}$ pour $\mathrm{Re}(s) > 1$, ainsi que la relation de Hecke

$$(2\pi)^{-s} \Gamma(s) \mathrm{L}(s - \frac{k-1}{2}, \pi) = \int_0^\infty F(it) t^s \frac{dt}{t}, \quad \forall s \in \mathbb{C}. \tag{4.1}$$

4.10. La conjecture de Ramanujan généralisée

Soit G un $\mathbb{Z}$-groupe semi-simple et soit $\pi \in \Pi(G)$. On dit que π satisfait la conjecture de Ramanujan, ou qu'elle est *tempérée*, si [8] pour tout $p \in \mathrm{P}$, les valeurs propres de $\mathrm{c}_p(\pi)$ dans une (et donc toute) $\mathbb{C}$-représentation fidèle de $\widehat{G}$ sont toutes de module 1.

8. On ajoute en général une condition sur π_∞, conjecturalement automatique, que nous omettons ici.

La *conjecture de Ramanujan généralisée* affirme que si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ alors π est tempérée. L'exemple typique de représentation qui n'est pas tempérée est la représentation triviale $1 \in \Pi_{\mathrm{disc}}(\mathrm{PGL}_2)$, les valeurs propres de $\mathrm{c}_p(1) = e_p$ étant $p^{\pm 1/2}$. Plus généralement, la représentation triviale 1_G de G n'est pas tempérée si $G \neq 1$ (exemple 4.2). La conjecture 4.6 exprime donc notamment le défaut de la conjecture de Ramanujan en général.

La conjecture de Ramanujan généralisée est toujours ouverte, même pour $G = \mathrm{PGL}_2$. Par des travaux de nombreux auteurs, elle est cependant connue pour la classe importante des représentations $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ dites *algébriques régulières polarisées* (voir §VIII.2.16). En général, on dispose toutefois de l'estimée de Jacquet-Shalika [JS81a] : pour tout $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$, tout $p \in \mathrm{P}$ et toute valeur propre λ de $\mathrm{c}_p(\pi)$, alors $p^{-1/2} < |\lambda| < p^{1/2}$.

VII. Quelques cas de la conjecture d'Arthur-Langlands

1. Retour sur les relations d'Eichler

Dans toute cette partie, g et n sont des entiers ≥ 1 fixés tels que $n \equiv 0 \bmod 8$. On considère les $\mathbb{Z}$-groupes Sp_{2g} et O_n (rappelons que ce dernier est le $\mathbb{Z}$-groupe orthogonal du réseau E_n).

1.1. Le point de vue de Rallis

La série théta de Jacobi permet de construire une application $\mathbb{C}$-linéaire naturelle, unique à multiplication par un scalaire non nul près,

$$\vartheta : \mathrm{M}_U(\mathrm{O}_n) \longrightarrow \mathrm{M}_V(\mathrm{Sp}_{2g})$$

pour certains couples (U, V) où U est une $\mathbb{C}$-représentation irréductible de $\mathrm{O}_n(\mathbb{C})$ et V une $\mathbb{C}$-représentation irréductible de $\mathrm{GL}_g(\mathbb{C})$ [KV78] [FRE80]. Les couples (U, V) permis seront dit *compatibles* et seront décrits plus bas. Deux cas particuliers de cette construction ont d'ailleurs déjà joué un rôle dans ce mémoire : le couple $(1,\ \text{dét}^{n/2})$ au §V.1 et le couple $(\mathrm{H}_{d,g}, \text{dét}^{n/2+d})$ au §V.4 pour $2g \leq n$. Une propriété importante de l'application ϑ, déjà discutée dans divers cas *loc. cit.*, est qu'elle entrelace certains opérateurs de Hecke de O_n et Sp_{2g} ("relations de commutations d'Eichler"). Le but de ce paragraphe est de rappeler le point de vue de Rallis [RAL82] sur ces formules.

Posons $\mathfrak{z}_{\mathrm{Sp}_{2g}} = \mathrm{Z}(\mathrm{U}(\mathfrak{sp}_{2g}(\mathbb{C})))$ et $\mathfrak{z}_{\mathrm{O}_n} = \mathrm{Z}(\mathrm{U}(\mathfrak{so}_n(\mathbb{C})))^{\mathrm{O}_n(\mathbb{C})}$. Rallis construit dans [RAL82] un morphisme surjectif de $\mathbb{C}$-algèbres

$$\mathrm{Ral} : \begin{cases} \mathrm{H}(\mathrm{O}_n) \otimes \mathfrak{z}_{\mathrm{O}_n} \to \mathrm{H}(\mathrm{Sp}_{2g}) \otimes \mathfrak{z}_{\mathrm{Sp}_{2g}} & \text{si } n > 2g, \\ \mathrm{H}(\mathrm{Sp}_{2g}) \otimes \mathfrak{z}_{\mathrm{Sp}_{2g}} \to \mathrm{H}(\mathrm{O}_n) \otimes \mathfrak{z}_{\mathrm{O}_n}, & \text{si } n \leq 2g. \end{cases}$$

respectant les sous-anneaux $\mathrm{H}_p(*) \otimes \mathbb{C}$ (p premier) et $\mathfrak{z}_*$ de part et d'autre. Il a les propriétés suivantes :

(i) Si (U, V) est compatible alors : $\mathrm{Inf}_V \circ \mathrm{Ral}_{|\mathfrak{z}_{\mathrm{O}_n}} = \mathrm{Inf}_U$ si $n > 2g$, et $\mathrm{Inf}_U \circ \mathrm{Ral}_{|\mathfrak{z}_{\mathrm{Sp}_{2g}}} = \mathrm{Inf}_V$ sinon.

(ii) (La relation de commutation d'Eichler-Rallis) $\vartheta \circ T = \mathrm{Ral}(T) \circ \vartheta$ pour tout $T \in \mathrm{H}(\mathrm{O}_n)$ si $n > 2g$, et $\vartheta \circ \mathrm{Ral}(T) = T \circ \vartheta$ pour tout $T \in \mathrm{H}(\mathrm{Sp}_{2g})$ sinon.

Rajoutons que la condition nécessaire d'admissibilité d'un couple (U, V) donnée au (i), portant sur leurs caractères infinitésimaux, est suffisante si de plus la restriction de U à $\mathrm{SO}_n(\mathbb{C})$ n'est pas irréductible. Si cette restriction est irréductible, un et un seul des couples (U, V) et $(U \otimes \text{dét}, V)$ est admissible : voir [KV78] pour une description détaillée.

Rallis donne enfin une interprétation du morphisme Ral en terme des isomorphismes de Satake et Harish-Chandra de O_n et Sp_{2g}, que nous allons également rappeler. Si $a \geq 1$, notons O_a (resp. SO_a) le $\mathbb{C}$-groupe orthogonal (resp. spécial orthogonal) complexe standard à a variables. Cette notation est à priori en conflit avec celle des $\mathbb{Z}$-groupes O_n et SO_n, uniquement définis pour $n \equiv 0 \bmod 8$, mais c'est sans incidence puisque lorsque les deux notations coïncident elles désignent sur $\mathbb{C}$ le même objet. Le groupe $\mathrm{O}_a(\mathbb{C})$ agit par conjugaison sur $\mathcal{X}(\mathrm{SO}_a)$, et cette action est non triviale si a est pair. Si $a < b$ sont des entiers ≥ 1 tels que $a \not\equiv b \bmod 2$, il existe un $\mathbb{C}$-morphisme

$$\rho_{a,b} : \mathrm{O}_a \times \mathrm{SL}_2 \longrightarrow \mathrm{O}_b,$$

uniquement déterminé modulo conjugaison à l'arrivée par $\mathrm{O}_b(\mathbb{C})$, tel que la représentation $\mathrm{St} \circ \rho_{a,b}$ soit isomorphe à la somme directe de la représentation standard du facteur O_a et de la représentation $\mathrm{Sym}^{b-a-1}\mathrm{St}_2$ de SL_2. Les duaux de Langlands respectifs de SO_n et Sp_{2g} sont les $\mathbb{C}$-groupes SO_n et SO_{2g+1}. La discussion de [RAL82, §6] se traduit en l'énoncé suivant (on rappelle que $e \in \mathcal{X}(\mathrm{SL}_2)$ désigne l'élément d'Arthur, défini au §VI.4.4) :

Proposition 1.2. *(i) Si $n > 2g$, l'application $\mathcal{X}(\widehat{\mathrm{Sp}_{2g}}) \to \mathcal{X}(\widehat{\mathrm{O}}_n)$ induite par* Ral *est $x \mapsto \rho_{2g+1,n}(x, e)$.*

(ii) Si $n \leq 2g$, l'application $\mathcal{X}(\widehat{\mathrm{O}_n}) \to \mathcal{X}(\widehat{\mathrm{Sp}_{2g}})$ induite par Ral *est $x \mapsto \rho_{n,2g+1}(x, e)$.*

Ce résultat, combiné à la diagonalisabilité de $\mathrm{H}(\mathrm{O}_n)$ sur les $\mathrm{M}_U(\mathrm{O}_n)$, ramène l'étude des relations de commutations d'Eichler à des propriétés des isomorphismes de Satake de SO_n et Sp_{2g}. Par exemple, on observe que la proposition V.1.1 et la relation V.(4.4) se déduisent immédiatement des formules VI.(2.5) et VI.(2.8).

De même, la partie archimédienne de la proposition 1.2 éclaircit substantiellement la numérologie concernant les caractères infinitésimaux des couples compatibles (U, V). Illustrons ceci sur le couple $(\mathrm{H}_{d,g}, \text{dét}^{n/2+d})$. Pour

$g < \frac{n}{2}$ le plus haut poids de $\mathrm{H}_{d,g}(\mathbb{R}^n)$ est manifestement $d \sum_{i=1}^{g} \varepsilon_i$, et celui de $\mathrm{H}_{d,\frac{n}{2}}(\mathbb{R}^n)^{\pm}$ est $d(\pm\varepsilon_{\frac{n}{2}} + \sum_{i=1}^{\frac{n}{2}-1} \varepsilon_i)$ (voir §IV.4.14, §4.3), ce qui donne un caractère infinitésimal dans $\mathfrak{so}_n(\mathbb{C})$ avec pour valeurs propres les $\pm(d+\frac{n}{2}-i)$, pour $i = 1, \ldots, g$, et $\pm(\frac{n}{2}-i)$ pour $i = g+1, \ldots, \frac{n}{2}$ si $g < \frac{n}{2}$. D'un autre côté, la représentation $\pi'_{\det^k}$ (§VI.3.4) a un caractère infinitésimal dans $\mathfrak{so}_{2g+1}(\mathbb{C})$ avec pour valeurs propres 0 et les $\pm(k-i)$ pour $i = 1, \ldots, g$, ce qui est bien compatible avec la proposition 1.2.

Disons que les représentations $\pi_{\mathrm{O}} \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$ et $\pi_{\mathrm{Sp}} \in \Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ sont ϑ-correspondantes s'il existe un couple compatible (U, V) et des formes propres $F \in \mathrm{M}_U(\mathrm{O}_n)$ et $G \in \mathrm{S}_V(\mathrm{Sp}_{2g})$, engendrant respectivement π_{O} et π_{Sp}, telles que $\vartheta(F) = G$.

Corollaire 1.3. *Supposons que $\pi_{\mathrm{O}} \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$ et $\pi_{\mathrm{Sp}} \in \Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ sont ϑ-correspondantes. Alors $\psi(\pi_{\mathrm{O}}, \mathrm{St}) = \psi(\pi_{\mathrm{Sp}}, \mathrm{St}) \oplus [n-2g-1]$ si $n > 2g$, et $\psi(\pi_{\mathrm{Sp}}, \mathrm{St}) = \psi(\pi_{\mathrm{O}}, \mathrm{St}) \oplus [2g+1-n]$ sinon.*

1.4. Un raffinement : passage aux groupes Spin

Dans ce paragraphe, nous discutons d'un raffinement de la proposition 1.2 probablement bien connu des spécialistes, mais pour lequel nous n'avons pas trouvé de référence dans la littérature (il est cependant implicite dans [Ral79] dans le cas $g = 1$). Supposons le couple (U, V) compatible. Observons que si $\mathrm{M}_U(\mathrm{O}_n) \neq 0$ alors $-1 \in \mathrm{O}_n(\mathbb{Z})$ agit trivialement dans U, ce que nous supposons dès à présent. Cela entraîne que U se factorise en une représentation U' de $\mathrm{PGO}_n(\mathbb{C})$, et le lemme IV.4.8 fournit un isomorphisme naturel $\mathrm{H}(\mathrm{O}_n)$-équivariant

$$\mathrm{M}_{U'}(\mathrm{PGO}_n) \xrightarrow{\sim} \mathrm{M}_U(\mathrm{O}_n).$$

Autrement dit, $\mathrm{M}_U(\mathrm{O}_n)$ est naturellement muni d'une action de l'anneau de Hecke plus gros $\mathrm{H}(\mathrm{PGO}_n)$. De même, $\mathrm{M}_V(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est muni d'une action de $\mathrm{H}(\mathrm{PGSp}_{2g})$, et on peut se demander comment l'énoncé de Rallis s'étend à ces opérateurs.

Précisément, soit $F \in \mathrm{M}_U(\mathrm{PGO}_n)$ propre pour $\mathrm{H}(\mathrm{PGO}_n)$ et telle que $\vartheta(F) \neq 0$. Les relations de Rallis assurent que $\vartheta(F)$ est propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$. D'après le §VI.2.8, pour tout nombre premier p l'anneau $\mathrm{H}_p(\mathrm{PGSp}_{2g})$ (resp. $\mathrm{H}_p(\mathrm{PGO}_n)$) est engendré par $\mathrm{H}(\mathrm{Sp}_{2g})$ (resp. $\mathrm{H}(\mathrm{O}_n)$) et l'opérateur des perestroïkas K_p correspondant. Or on dispose d'une relation d'Eichler supplémentaire, en fait la plus simple de toutes [Fre82, Thm. 4.5], qui prend la forme

suivante quand $n > 2g$:

$$\vartheta \circ \mathrm{K}_p = p^{\frac{g(\frac{n}{2}-g-1)}{2}} \left[\prod_{i=0}^{\frac{n}{2}-g+1} (p^i + 1) \right] \mathrm{K}_p \circ \vartheta. \tag{1.1}$$

Le cas de cette formule dont nous aurons réellement besoin dans l'application au théorème 2.1 est celui de la proposition IV.4.9 (à comparer avec la formule IV.5.5). Cela montre que $\vartheta(F)$ est propre pour $\mathrm{H}(\mathrm{PGSp}_{2g})$. Nous dirons que $\pi_{\mathrm{PGO}} \in \Pi_{\mathrm{disc}}(\mathrm{PGO}_n)$ et $\pi_{\mathrm{PGSp}} \in \Pi_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$ sont ϑ-correspondantes s'il existe un couple compatible (U, V) et des formes propres $F \in \mathrm{M}_U(\mathrm{PGO}_n)$ et $G \in \mathrm{S}_V(\mathrm{Sp}_{2g}(\mathbb{Z}))$, engendrant respectivement π_{PGO} et π_{PGSp}, telles que $\vartheta(F) = G$.

Si $n > 2g$, le $\mathbb{C}$-morphisme $\rho_{2g+1,n} : \mathrm{SO}_{2g+1} \times \mathrm{SL}_2 \to \mathrm{SO}_n$ se relève en un $\mathbb{C}$-morphisme $\widetilde{\rho}_{2g+1,n} : \mathrm{Spin}_{2g+1} \times \mathrm{SL}_2 \to \mathrm{Spin}_n$. De même, si $n \leq 2g$ le $\mathbb{C}$-morphisme $\rho_{n,2g+1}$ se relève en un morphisme $\widetilde{\rho}_{n,2g+1} : \mathrm{Pin}_n \times \mathrm{SL}_2 \to \mathrm{Pin}_{2g+1}$ (voir le §VI.4.7 pour des rappels concernant Pin).

Proposition 1.5. *Supposons que les représentations* $\pi_{\mathrm{PGO}} \in \Pi_{\mathrm{disc}}(\mathrm{PGO}_n)$ *et* $\pi_{\mathrm{PGSp}} \in \Pi_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$ *sont* ϑ*-correspondantes.*

(i) Si $n > 2g$*, alors* $\mathrm{c}(\pi_{\mathrm{PGO}})$ *est l'image de* $\widetilde{\rho}_{2g+1,n}(\mathrm{c}(\pi_{\mathrm{PGSp}}), e)$ *par l'application naturelle* $\mathcal{X}(\mathrm{Spin}_n) \to \mathcal{X}(\mathrm{Pin}_n)$.

(ii) Si $n \leq 2g$*, alors* $\mathrm{c}(\pi_{\mathrm{PGSp}}) = \widetilde{\rho}_{n,2g+1}(\mathrm{c}(\pi_{\mathrm{PGO}}), e)$.

Démonstration. Supposons $n > 2g$. L'égalité à démontrer vaut après projection dans $\mathcal{X}(\widehat{\mathrm{O}_n})$ d'après Rallis Prop. 1.2 (i). D'après une observation déjà donnée ci-dessus, il ne reste qu'à la vérifier après application de l'opérateur de Hecke $\mathrm{K}_p \in \mathrm{H}(\mathrm{PGO}_n)$, vu par l'isomorphisme de Satake comme une fonction sur $\mathrm{Spin}_n(\mathbb{C})_{\mathrm{ss}}$ invariante sous l'action de $\mathrm{Pin}_n(\mathbb{C})$. D'après la formule VI.(2.5),

$$\mathrm{Sat}(\mathrm{K}_p) = p^{\frac{\frac{n}{2}(\frac{n}{2}-1)}{4}} ([V^+_{\mathrm{Spin}}] + [V^-_{\mathrm{Spin}}])$$

où $V_{\mathrm{Spin}^\pm}$ sont les deux représentations Spin de $\mathrm{Spin}_n(\mathbb{C})$ (conjuguées l'une de l'autre sous $\mathrm{Pin}_n(\mathbb{C})$). Mais il est bien connu que la restriction de chacune d'elle à $\mathrm{Spin}_{2g+1}(\mathbb{C}) \times \mathrm{Spin}_{n-2g-1}(\mathbb{C})$ est isomorphe au produit tensoriel des représentations Spin de chacun des deux facteurs. Soit $r_a : \mathrm{SL}_2 \to \mathrm{SL}_{2^a}$ la $\mathbb{C}$-représentation obtenue en relevant la représentation irréductible de dimension impaire $2a + 1$ dans Spin_{2a+1} puis en composant par la représentation Spin de ce dernier. C'est un exercice de vérifier que

$$\mathrm{trace}(\, r_a(e_p)\,) \;=\; \prod_{i=1}^{a} (p^{-\frac{i}{2}} + p^{\frac{i}{2}}).$$

On conclut par un calcul immédiat à partir des formules VI.(2.5), VI.(2.8) et (1.1). Le cas $n \leq 2g$ est similaire. La relation d'Eichler montrée par Freitag [Fre82, Thm. 4.5] est

$$\mathrm{K}_p \circ \vartheta = p^{-\frac{g(\frac{n}{2}-g-1)}{2}} \left[\prod_{i=1}^{g-\frac{n}{2}} (p^{-i}+1) \right] \vartheta \circ \mathrm{K}_p. \tag{1.2}$$

On conclut comme précédemment en utilisant que la restriction à $\mathrm{Spin}_n(\mathbb{C}) \times \mathrm{Spin}_{2g+1-n}(\mathbb{C})$ de la représentation Spin de $\mathrm{Spin}_{2g+1}(\mathbb{C})$ est le produit tensoriel de la représentation $V^+_{\mathrm{Spin}} \oplus V^-_{\mathrm{Spin}}$ de $\mathrm{Spin}_n(\mathbb{C})$, et de la représentation Spin de $\mathrm{Spin}_{2g+1-n}(\mathbb{C})$. □

Remarque 1.6. Observons pour terminer que si $n > 2g$, un élément (c_v) dans l'image de la composée $\mathcal{X}(\mathrm{Spin}_{2g+1}) \times \mathcal{X}(\mathrm{SL}_2) \to \mathcal{X}(\mathrm{Spin}_n) \to \mathcal{X}(\mathrm{Pin}_n)$ a la prioriété que pour tout v, la classe de $\mathrm{Pin}_n(\mathbb{C})$-conjugaison c_v est en fait une simple classe de $\mathrm{Spin}_n(\mathbb{C})$-conjugaison. Une manière de le voir, par exemple pour v premier, est d'observer que si $\gamma \in \mathrm{Spin}(V_n)$ a la propriété que son image γ' dans $\mathrm{SO}(V_n)$ admet la valeur propre 1, alors il existe $e \in V_n$ tel que $\mathrm{q}(e) = 1$ tel que $e\gamma = \gamma e$ (voir le §VI.4.7 pour ces notations). En effet, il suffit de choisir un quelconque e dans l'espace $V_n^{\gamma'=1}$ (qui est non-dégénéré et non nul) tel que $\mathrm{q}(e) = 1$. On observe que l'on a $\alpha(\gamma)e\gamma^{-1} = \gamma'(e) = e$ et $\alpha(\gamma) = \gamma$, puis $\gamma e = e\gamma$.

2. $\Pi_{\mathrm{disc}}(\mathrm{O}_8)$ et trialité

La première partie du résultat suivant est due à Waldspurger [Wal79] ; la proposition V.4.3 en est une vérification élémentaire dans le cas particulier $k = 12$. Sa seconde partie est une forme à la fois plus précise et plus conceptuelle de l'idée principale du §V.4. On rappelle que nous avons introduit la représentation irréductible $\mathrm{H}_{d,g}(\mathbb{R}^n)$ de $\mathrm{O}_n(\mathbb{R})$ au §V.4.1.

Théorème 2.1. *Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre de $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, k étant un entier pair ≥ 12.*

(i) Il existe $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{O}_8)$ telle que $\pi'_\infty \simeq \mathrm{H}_{k-4,1}(\mathbb{R}^8)$ et

$$\psi(\pi', \mathrm{St}) = \mathrm{Sym}^2\pi \oplus [5].$$

(ii) Il existe $\pi'' \in \Pi_{\mathrm{disc}}(\mathrm{O}_8)$ telle que $\pi''_\infty \simeq \mathrm{H}_{k/2-2,4}(\mathbb{R}^8)$ et

$$\psi(\pi'', \mathrm{St}) = \pi[4].$$

Démonstration. Soit $U = \mathrm{H}_{k-4,1}(\mathbb{R}^8)$. D'après [Wal79, Thm. 1], on a

$$\vartheta_{k-4,1}(\mathrm{M}_U(\mathrm{O}_8)) = \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z})).$$

D'après les relations de commutation d'Eichler on peut donc trouver une forme propre $F \in \mathrm{M}_U(\mathrm{O}_8)$ dont l'image $G = \vartheta_{k-4,1}(F)$ engendre π. Soit $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{SL}_2)$ la représentation engendrée par G. Considérons l'isogénie $i : \mathrm{SL}_2(\mathbb{C}) = \widehat{\mathrm{PGL}_2}(\mathbb{C}) \to \widehat{\mathrm{SL}_2}(\mathbb{C}) = \mathrm{SO}_3(\mathbb{C})$. La proposition 5.7 et la compatibilité de l'isomorphisme de Satake aux isogénies assurent que $\mathrm{c}(\pi') = i(\mathrm{c}(\pi))$. Mais $\mathrm{St} \circ i$ n'est autre que la représentation $\mathrm{Sym}^2\mathrm{St}_2$ de $\mathrm{SL}_2(\mathbb{C})$, de sorte que $\mathrm{St}(\mathrm{c}(\pi')) = \mathrm{Sym}^2\mathrm{c}(\pi)$. Le (i) se déduit alors du corollaire 1.3.

Vérifions le (ii). Quitte à modifier F, on peut supposer que $F_0 = F$ est propre pour $\mathrm{H}(\mathrm{PGO}_8)$, comme au §1.4. Soit $\pi_0 \in \Pi_{\mathrm{disc}}(\mathrm{PGO}_8)$ la représentation qu'elle engendre et soit $U' = U \otimes \nu^{k/2-2}$. Soit F_1 l'image de F_0 par l'application naturelle $\mathrm{res} : \mathrm{M}_{U'}(\mathrm{PGO}_8) \to \mathrm{M}_{U'}(\mathrm{PGSO}_8)$ (§IV.4.11). Cette application étant injective $\mathrm{H}(\mathrm{PGSO}_8)$-équivariante d'après *loc. cit.*, la forme F_1 est non nulle et si $\pi_1 \in \Pi_{\mathrm{disc}}(\mathrm{PGSO}_8)$ désigne la représentation engendrée, alors $\mathrm{c}(\pi_0) \in \mathcal{X}(\mathrm{Pin}_8)$ est l'image de $\mathrm{c}(\pi_1) \in \mathcal{X}(\mathrm{Spin}_8)$ par l'homomorphisme naturel. Cette dernière propriété détermine d'ailleurs uniquement $\mathrm{c}(\pi_1)$ par la remarque 1.6, de sorte que la proposition 1.5 s'écrit

$$\mathrm{c}(\pi_1) = \widetilde{\rho}_{3,8}(\mathrm{c}(\pi), e) \tag{2.1}$$

Considérons maintenant, suivant le §V.4.14, un automorphisme de trialité τ de PGSO_8 défini au moyen d'une structure d'octonions de Coxeter sur E_8. En particulier, $(U')^\tau$ est isomorphe à la représentation $V = \mathrm{H}^{\pm}_{k/2-2,4} \otimes \nu^{k-4}$ d'après le lemme V.4.18. Soit $\mathrm{tri} : \mathrm{M}_{U'}(\mathrm{PGSO}_8) \xrightarrow{\sim} \mathrm{M}_V(\mathrm{PGSO}_8)$ l'isomorphisme noté $(\tau^*)^{-1}$ *loc. cit.*. On pose enfin

$$F_2 = \mathrm{tri}(F_1), \;\; F_3 = \mathrm{ind}\,(F_2) \in \mathrm{M}_{\mathrm{Ind}(V)}(\mathrm{PGO}_8) \;\text{ et }\; F_4 = \mu^*(F_3) \in \mathrm{M}_{\mathrm{IndV}}(\mathrm{O}_8)$$

(§IV.4.4, §V.4.11). Ces fonctions sont non nulles et propres, et engendrent donc des représentations automorphes π_2, π_3 et π_4 des $\mathbb{Z}$-groupes respectifs PGSO_8, PGO_8 et O_8.

La compatibilité de l'isomorphisme de Satake aux isogénies assure que $\mathrm{c}(\pi_2)$ est l'image par $\tau^{\pm 1}$ de $\mathrm{c}(\pi_1)$, puis que $\mathrm{c}(\pi_4)$ est l'image de $\mathrm{c}(\pi_2)$ par l'homomorphisme naturel $\eta : \mathrm{Spin}_8(\mathbb{C}) \to \mathrm{SO}_8(\mathbb{C})$. Mais il est bien connu que la représentation $\mathrm{St} \circ \eta \circ \tau^{\pm 1}$ n'est autre que la représentation $V_{\mathrm{Spin}^\pm}$ de Spin_8. On a déjà dit que la restiction de $V_{\mathrm{Spin}^\pm}$ à $\mathrm{Spin}_3 \times \mathrm{Spin}_5$ est le produit tensoriel des représentations Spin de $\mathrm{Spin}_3 \simeq \mathrm{SL}_2$ (de dimension

2) et $\mathrm{Spin}_5 \simeq \mathrm{Sp}_4$ (de dimension 4) ; en particulier elle ne dépend pas du signe $\pm$. Or la représentation $\mathrm{Sym}^4 \mathrm{St}_2$ de SL_2, vue dans SO_5, puis relevée dans $\mathrm{Spin}_5 \simeq \mathrm{Sp}_4$ et composée avec la représentation standard de Sp_4, est la représentation $\mathrm{Sym}^3 \mathrm{St}_2$. Nous avons donc démontré la suite d'égalités

$$\pi[4] = \psi(\pi_1, V^{\pm}_{\mathrm{Spin}}) = \psi(\pi_2, \mathrm{St} \circ \eta) = \psi(\pi_4, \mathrm{St}),$$

et la représentation $\pi'' = \pi_4$ convient, ce qui conclut. □

Observons que le théorème de Gelbart-Jacquet (§VI.4.7) entraîne que le couple (π', St) satisfait la conjecture d'Arthur-Langlands. Il est de plus manifeste que le couple (π'', St) satisfait la conjecture d'Arthur-Langlands.

Donnons une seconde formulation du résultat précédent. On rappelle que l'homomorphisme $\mathrm{SO}_8 \to \mathrm{PGSO}_8$ détermine par dualité de Langlands un $\mathbb{C}$-morphisme $\eta : \widehat{\mathrm{PGSO}_8} \to \widehat{\mathrm{SO}_8}$; les 3 représentations irréductibles de dimension 8 de $\widehat{\mathrm{PGSO}_8}(\mathbb{C}) \simeq \mathrm{Spin}_8(\mathbb{C})$ sont donc $\mathrm{St} \circ \eta$, V^+_{Spin} et V^-_{Spin}.

Théorème 2.2. *Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre de $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, k étant un entier pair ≥ 12. Il existe $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{PGSO}_8)$ telle que*

$$\psi(\pi', \mathrm{St} \circ \eta) = \pi[4], \;\; \psi(\pi', V^+_{\mathrm{Spin}}) = \pi[4] \;\text{ et }\; \psi(\pi', V^-_{\mathrm{Spin}}) = \mathrm{Sym}^2\pi \oplus [5].$$

Démonstration. La représentation π_2 de la démonstration du théorème 2.1 satisfait $\psi(\pi_2, \mathrm{St} \circ \eta) = \pi[4]$ et

$$\{\psi(\pi_2, V^+_{\mathrm{Spin}}), \psi(\pi_2, V^-_{\mathrm{Spin}})\} = \{\pi[4], \mathrm{Sym}^2\pi \oplus [5]\}.$$

Soit π'_2 la représentation de PGSO_8 engendrée par l'image par la symétrie s d'une forme pour PGSO_8 engendrant π_2 (§V.4.11). Alors l'une des deux représentations π_2 et π'_2 convient pour π'. □

Le principe de la démonstration du théorème 2.1 est de portée plus large, et s'applique notamment aux séries thêta de genre supérieur. Il permet de produire des représentations de O_8 de paramètres de Langlands standards intéressants, fonctions de ceux des éléments de $\Pi_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$ pour $1 \leq g \leq 3$.

Théorème 2.3. *Supposons que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$ admette un θ-correspondant dans $\Pi_{\mathrm{disc}}(\mathrm{PGO}_8)$.*

(i) Supposons $g = 2$. Soient V_4 et V_5 les représentations irréductibles de $\mathrm{Sp}_4(\mathbb{C}) = \widehat{\mathrm{PGSp}_4}(\mathbb{C})$ de dimensions respectives 4 et 5, i.e. V_4 est la représentation standard et $\Lambda^2 V_4 \simeq V_5 \oplus 1$. Alors il existe :

– $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ *telle que* $\psi(\pi', \mathrm{St}) = \psi(\pi, V_5) \oplus [3]$,

– $\pi'' \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ *telle que* $\psi(\pi'', \mathrm{St}) = \psi(\pi, V_4)[2]$.

(ii) Supposons $g = 3$. Soient V_{Spin} la représentation Spin de $\mathrm{Spin}_7(\mathbb{C}) = \widehat{\mathrm{PGSp}_6}(\mathbb{C})$ et V_7 sa représentation naturelle de dimension 7. Alors il existe :

– $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ *telle que* $\psi(\pi', \mathrm{St}) = \psi(\pi, V_7) \oplus [1]$,

– $\pi'' \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ *telle que* $\psi(\pi'', \mathrm{St}) = \psi(\pi, V_{\mathrm{Spin}})$.

Démonstration. L'existence de π' dans les deux cas est classique et découle du corollaire 1.3. En ce qui concerne celle de π'', sa démonstration est très similaire à celle de la représentation du même nom dans le théorème 2.1, elle est donc laissée en exercice pour le lecteur. Par exemple dans le cas (i), on montre d'abord l'existence de $\pi_0 \in \Pi_{\mathrm{disc}}(\mathrm{PGSO}_8)$ telle que $\psi(\pi_0, V_{\mathrm{Spin}}^{\pm}) = \psi(\pi, V_4)[2]$ et $\psi(\pi_0, \mathrm{St} \circ \eta) = \psi(\pi, V_5) \oplus [3]$; l'application de la trialité à π_0 conduit alors à la représentation π''. □

Remarque 2.4. (Travaux de Böcherer) Disons un mot sur l'hypothèse du théorème et la question reliée de la surjectivité de l'application ϑ en général, qui est un problème classique remontant à Eichler (*problème de la base d'Eichler*). On dispose du résultat marquant suivant dû à Böcherer [Boc85][Boc89], généralisant le travail de Waldspurger sus-cité pour $g = 1$: pour $d > 0$ l'application

$$\vartheta_{d,g} : \mathrm{M}_{\mathrm{H}_{d,g}(\mathbb{R}^n)}(\mathrm{O}_n) \to \mathrm{S}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$$

est surjective dès que $n > 4g$ (voir également [Boc83] pour le cas $d = 0$ ainsi que la remarque VIII.6.3). De manière plus précise, Böcherer donne une condition nécessaire et suffisante pour qu'un forme propre $F \in \mathrm{S}_{\frac{n}{2}+d}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ soit dans l'image de $\vartheta_{d,g}$, quand $n \geq 2g$. Elle porte sur la fonction $\mathrm{L}(s, \pi, \mathrm{St})$, où $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ est engendrée par F, dont on sait qu'elle admet un prolongement méromorphe à $\mathbb{C}$ tout entier (voir §VIII.7). Si $n > 2g$ (resp. $n = 2g$), il montre que F est dans l'image de $\vartheta_{d,g}$ si et seulement si $\mathrm{L}(s, \pi, \mathrm{St})$ ne s'annule pas en $s = \frac{n}{2} - g$ (resp. si et seulement si $\mathrm{L}(s, \pi, \mathrm{St})$ admet un pôle simple en $s = 1$) : voir [Boc89, Thm. 4_1, Thm. 5]. Cette condition est automatiquement satisfaite si $n > 4g$. Böcherer a également étudié la question de l'injectivité de $\vartheta_g = \vartheta_{0,g}$, pour laquelle il obtient des critères du même type [Boc90].

Revenons à l'énoncé du théorème 2.2.

Corollaire 2.5. *Supposons que* $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ *et* $\pi' \in \Pi_{\mathrm{disc}}(\mathrm{PGSO}_8)$ *satisfont les hypothèses et conclusions du théorème 2.2. Supposons de plus que* π' *possède un* ϑ*-correspondant* $\pi'' \in \Pi_{\mathrm{cusp}}(\mathrm{PGSp}_8)$*, c'est-à-dire qu'il existe* $F \in \mathrm{M}_{\mathrm{H}^{\pm}_{k/2-2,4}(\mathbb{R}^8)}(\mathrm{PGSO}_8) \simeq \mathrm{M}_{\mathrm{H}_{k/2-2,4}(\mathbb{R}^8)}(\mathrm{PGO}_8)$ *engendrant* π' *et telle que* $\vartheta(F)$ *est un élément non nul de* $\mathrm{S}_{k/2+2}(\mathrm{Sp}_8(\mathbb{Z}))$*,* π'' *désignant alors la représentation engendrée par* $\vartheta(F)$*. Alors*

$$\psi(\pi'', V_{\mathrm{St}}) = \pi[4] \oplus [1] \quad \text{et} \quad \psi(\pi'', \mathrm{V}_{\mathrm{Spin}}) = \pi[4] \oplus \mathrm{Sym}^2\pi \oplus [5].$$

Démonstration. Cela découle immédiatement du théorème 2.2 et des relations d'Eichler-Rallis raffinées (Proposition 1.5 dans le cas $g = 4 = n/2$), car la restriction à $\mathrm{Spin}_8 \to \mathrm{Spin}_9$ de la représentation Spin de $\mathrm{Spin}_9(\mathbb{C})$ est la représentation $V^+_{\mathrm{Spin}} \oplus V^-_{\mathrm{Spin}}$ de $\mathrm{Spin}_8(\mathbb{C})$. □

Lorsque π est engendrée par $\Delta \in \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, nous avons vérifié dans la proposition V.4.22 que l'hypothèse sur π' est satisfaite (cela devrait pouvoir également se déduire d'une variante harmonique de [Boc90], voir [Boc89, §XI]). On rappelle que $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ est de dimension 1 engendré par la forme de Schottky J (§V.2). Nous noterons $\Delta_{11} \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par la forme modulaire Δ.

Corollaire 2.6. *(i) Si* $\pi_J \in \Pi_{\mathrm{cusp}}(\mathrm{PGSp}_8)$ *désigne la représentation engendrée par la forme de Schottky, alors* $\psi(\pi_J, V_{\mathrm{St}}) = \Delta_{11}[4] \oplus [1]$ *et*

$$\psi(\pi_J, V_{\mathrm{Spin}}) = \Delta_{11}[4] \oplus \mathrm{Sym}^2\Delta_{11} \oplus [5].$$

(ii) Soit $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGSO}_{16})$ *l'unique représentation non-triviale telle que* $\pi_\infty = \mathbb{C}$*. Alors* $\psi(\pi, V_{\mathrm{St}}) = \Delta_{11}[4] \oplus [7] \oplus [1]$ *et*

$$\psi(\pi, V^{\pm}_{\mathrm{Spin}}) = \psi(\pi_J, V_{\mathrm{Spin}}) \oplus \psi(\pi_J, V_{\mathrm{Spin}})[7]$$

Démonstration. L'assertion (i) résulte du corollaire 2.5 et de la discussion précédant l'énoncé. L'assertion (ii) s'en déduit, étant donné la relation $J = \vartheta_4(\mathrm{E}_8 \oplus \mathrm{E}_8) - \vartheta_4(\mathrm{E}_{16})$ (§ IV.V.2) et la proposition 1.5 (ii). On remarquera que si le $\mathbb{C}$-morphisme $g : \mathrm{SL}_2 \to \mathrm{SO}_7$ est tel que $\mathrm{St} \circ g \simeq \mathrm{Sym}^6\mathrm{St}_2$, et si $f : \mathrm{SL}_2 \to \mathrm{Spin}_7$ relève g, alors la restriction à f de la représentation Spin de Spin_7 est isomorphe à $\mathrm{Sym}^6\mathrm{St}_2 \oplus 1$ (voir par exemple [Gro00, §7]). □

Corollaire 2.7. *Pour tout nombre premier* p*, le nombre des perestroïkas de* $\mathrm{E}_8 \oplus \mathrm{E}_8$ *relativement à* p *qui sont isomorphes à* E_{16} *est*

$$\frac{405}{691}\left(\prod_{i=0}^{3}(p^i+1)\right)(p^{11}+p^7+p^6+p^5+p^4+1+\tau(p))(p^{11}+1-\tau(p)).$$

3. Quelques conséquences des travaux d'Ikeda et Böcherer

Comme nous l'avions déjà expliqué au §V.2, le premier point du corollaire 2.6 est également conséquence du théorème suivant dû à Ikeda [IKE01] (démonstration de la *conjecture de Duke-Imamoğlu*). Il étend un résultat de Andrianov, Maass et Zagier dans le cas du genre $g = 2$ (démonstration de la *conjecture de Saito-Kurokawa*, voir [KUR78][ZA80][EZ85]).

Théorème 3.1. [IKE01] *Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre de poids k pour $\mathrm{SL}_2(\mathbb{Z})$, et soit $g \geq 1$ un entier tel que $k \equiv g \bmod 4$, alors il existe une représentation $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$, engendrée par une forme modulaire de Siegel scalaire de poids $\frac{k+g}{2}$ pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, telle que $\psi(\pi', \mathrm{St}) = \pi[g] \oplus [1]$.*

Supposons π et π' comme dans l'énoncé ci-dessus. Étant donné que l'on connaît la fonction $\mathrm{L}(s, \pi', \mathrm{St})$, les résultats sus-cités de Böcherer (Remarque 2.4, [BOC89]) donnent une condition nécessaire et suffisante pour que π' admette un ϑ-correspondant.

Théorème 3.2. *Soient k, g et n des entiers pairs non nuls tels que $k \equiv g \bmod 4$, $n \equiv 0 \bmod 8$, et $2g \leq n \leq k + g$. Soient $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ et $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ satisfaisant les conclusions du théorème d'Ikeda relativement à π.*

(i) La représentation π' admet un ϑ-correspondant $\pi'' \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$ tel que $\pi''_\infty \simeq \mathrm{H}_{\frac{k+g-n}{2},g}(\mathbb{R}^n)$ si, et seulement si, $n > 3g$ ou $\mathrm{L}(\frac{1}{2}, \pi) \neq 0$.

(ii) Supposons $n > 3g$ ou $\mathrm{L}(\frac{1}{2}, \pi) \neq 0$ (auquel cas $k \equiv g \equiv 0 \bmod 4$). Si $n > 2g$ (resp. $n = 2g$), il existe $\pi'' \in \Pi_{\mathrm{cusp}}(\mathrm{O}_n)$ telle que $\psi(\pi'', \mathrm{St}) = \pi[g] \oplus [n - 2g - 1] \oplus [1]$ (resp. $\psi(\pi'', \mathrm{St}) = \pi[g]$) et $\pi''_\infty \simeq \mathrm{H}_{\frac{k+g-n}{2},g}(\mathbb{R}^n)$.

Démonstration. Soit $\mathcal{D} = \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ (les demi-entiers non entiers). Comme on a $\psi(\pi', \mathrm{St}) = \pi[g] \oplus [1]$, la fonction $\mathrm{L}(s, \pi', \mathrm{St})$ est le produit de la fonction $\zeta(s)$ de Riemann par les fonctions $\mathrm{L}(s + j, \pi)$ où j parcourt les éléments de $\mathcal{D}$ tels que $|j| \leq \frac{g-1}{2}$ (noter que $g \equiv 0 \bmod 2$). On considère le couple compatible $(\mathrm{H}_{\frac{k+g-n}{2},g}(\mathbb{R}^n), \mathrm{dét}^{\frac{k+g}{2}})$, qui est bien défini car $2g \leq n \leq k + g$. Si $n > 2g$ (resp. $n = 2g$), Böcherer montre que π' admet un ϑ-correspondant comme dans l'énoncé si, et seulement si, $\mathrm{L}(\frac{n}{2} - g, \pi', \mathrm{St}) \neq 0$ (resp. $\mathrm{L}(s, \pi', \mathrm{St})$ admet un pôle simple en $s = 1$). Comme $\zeta(s)$ admet un pôle simple en $s = 1$ et ne s'annule pas si $\mathrm{Re}(s) > 1$, il est équivalent de demander que $\mathrm{L}(s, \pi) \neq 0$ pour tout $s \in \mathcal{D}$ tel que $|s - \delta - \frac{n}{2} + g| \leq \frac{g-1}{2}$, où $\delta = 1$ si $n = 2g$ et 0 sinon.

Si $s \in \mathcal{D}$ et $s \neq \frac{1}{2}$ alors $\mathrm{L}(s,\pi) \neq 0$. En effet, pour $\mathrm{Re}(s) > 1$ c'est une conséquence de la convergence absolue du produit eulérien définissant $\mathrm{L}(s,\pi)$ (par exemple, d'après Deligne, ou Rankin-Selberg). En général, on rappelle que d'après Hecke la fonction $\xi(s,\pi) = (2\pi)^{-s-\frac{k-1}{2}}\Gamma(s+\frac{k-1}{2})\mathrm{L}(s,\pi)$ est une fonction entière de s satisfaisant (voir §4.9)

$$\xi(1-s,\pi) = i^k \xi(s,\pi). \tag{3.1}$$

On conclut car la fonction $\Gamma(s)$ n'admet pas de pôle en les éléments de $\mathcal{D}$. Pour conclure le (i), on observe que $|\frac{1}{2} - \delta - \frac{n}{2} + g| \leq \frac{g-1}{2}$ si, et seulement si, $n \leq 3g$.

Vérifions enfin l'assertion (ii). Sous les hypothèses de l'énoncé, on dispose d'un ϑ-correspondant $\pi'' \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$ de la représentation π', d'après le point (i). Appliquons le corollaire 1.3. Sous l'hypothèse $n > 2g$, il entraîne $\psi(\pi'',\mathrm{St}) = \psi(\pi',\mathrm{St}) \oplus [n-2g-1]$, ce que l'on voulait. Dans le cas d'égalité $n = 2g$, il s'écrit

$$\psi(\pi'',\mathrm{St}) \oplus [1] = \psi(\pi',\mathrm{St}) = \pi[g] \oplus [1],$$

ce qui équivaut manifestement à $\psi(\pi'',\mathrm{St}) = \pi[g]$. On observe enfin que l'hypothèse $\mathrm{L}(\frac{1}{2},\pi) \neq 0$ entraine $k \equiv 0 \bmod 4$ d'après l'équation fonctionnelle (3.1). $\square$

Remarque 3.3. Supposons que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ est engendrée par une forme propre F de poids $k \equiv 0 \bmod 4$ pour $\mathrm{SL}_2(\mathbb{Z})$. Si $12 \leq k \leq 20$ alors $F = \Delta\, \vartheta_1(\mathrm{E}_8)^{\frac{k-12}{4}}$; comme cette dernière ne prend que des valeurs strictement positives sur l'axe imaginaire, il vient que $\Gamma(s+\frac{k-1}{2})\mathrm{L}(s,\pi) > 0$ pour tout $s \in \mathbb{R}$ (formule VI.(4.1)). En particulier $\mathrm{L}(\frac{1}{2},\pi) \neq 0$. Il semblerait que l'on ne connaisse aucun exemple pour lequel $\mathrm{L}(\frac{1}{2},\pi) = 0$: voir à ce sujet [CoFa99], qui le vérifient pour tout $k \leq 500$ (d'ailleurs en lien avec le théorème 3.2, qu'ils n'explicitent pas toutefois).

Il est intéressant de confronter le théorème 3.2 aux résultats précédents. Tout d'abord, si on l'applique à $n = 16$, $g = 4 < n/3$ et $k = 12$ (de sorte que $d = 0$), on déduit aisément du (i) que $\vartheta_4(\mathrm{E}_8 \oplus \mathrm{E}_8) - \vartheta_4(\mathrm{E}_{16}) \in \mathrm{M}_8(\mathrm{Sp}_8(\mathbb{Z}))$ est une forme parabolique non nulle de paramètre standard $\Delta_{11}[4] \oplus [1]$. Cet argument "massue" redémontre donc à la fois la conjecture de Witt (Chap. IV (2.1)) et l'assertion concernant $\psi(\pi, V_{\mathrm{St}})$ dans le (ii) du corollaire 2.6 (et donc le théorème IV.2.2 !). De même, le théorème 3.2 s'applique pour $n = 24 = k + g$, ce qui se produit pour les 5 couples

$$(k,g) \in \{(12,12),(16,8),(18,6),(20,4),(22,2)\},$$

en prenant pour π la représentation engendrée par l'unique forme normalisée de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ quand $k \leq 22$. Nous noterons $\Delta_{k-1} \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ cette représentation. L'hypothèse du théorème est satisfaite dans les trois derniers cas car $g < 24/3 = 8$, ainsi que pour les deux premiers car $\mathrm{L}(\frac{1}{2}, \Delta_{k-1}) \neq 0$ si $k = 12$ ou 16.

Corollaire 3.4. *Pour tout $k \in \{12, 16, 18, 20, 22\}$, il existe $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\pi_\infty = \mathbb{C}$ et $\psi(\pi, \mathrm{St}) = \Delta_{k-1}[24-k] \oplus [2k-25] \oplus [1]$ si $k > 12$, $\psi(\pi, \mathrm{St}) = \Delta_{11}[12]$ si $k = 12$.*

En revanche, on observe que le cas $n = 2g = 8$ conduit à une version affablie, et paradoxalement plus chère, du théorème 2.1 (ii), puisqu'il ne le démontre que sous l'hypothèse supplémentaire $\mathrm{L}(\frac{1}{2}, \pi) \neq 0$ (et en particulier $k \equiv 0 \bmod 4$). Le cas $k \equiv 2 \bmod 4$ du théorème 2.1 (ii) apparaît donc particulièrement intéressant de ce point de vue. Ce phénomène un peu troublant, ainsi que la numérologie d'apparence un peu particulière de l'énoncé du théorème 3.2, sera très nettement éclairé lorsque nous expliquerons les résultats d'Arthur au chapitre suivant (voir notamment les §VIII.5.7 et §VIII.6).

Terminons ce paragraphe par un dernier exemple montrant qu'en général, l'inclusion $\vartheta_g(\mathbb{C}[\mathrm{X}_n]) \subset \mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est stricte.

Corollaire 3.5. *L'application $\vartheta_{14} : \mathbb{C}[\mathrm{X}_{32}] \to \mathrm{M}_{16}(\mathrm{Sp}_{28}(\mathbb{Z}))$ n'est pas surjective.*

Démonstration. En effet, considérons le cas $n = 32$, $k = 18$ et $g = 14$ (et donc encore $d = 0$). Le théorème d'Ikeda assure l'existence d'une forme propre F dans $\mathrm{S}_{16}(\mathrm{Sp}_{28}(\mathbb{Z}))$ engendrant une représentation de paramètre standard $\Delta_{17}[14] \oplus [1]$. On a $n < 3g$ et $\mathrm{L}(\frac{1}{2}, \Delta_{17}) = 0$ car $18 \equiv 2 \bmod 4$, de sorte que le théorème 3.2 (i) affirme que $F \notin \mathrm{Im}(\vartheta_{14})$. □

Cet exemple semble avoir échappé à Nebe et Venkov [NV01, §2.2], qui présentent la question de l'égalité entre $\vartheta_g(\mathbb{C}[\mathrm{X}_n])$ et $\mathrm{M}_{\frac{n}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$, pour tout $n \equiv 0 \bmod 8$ et tout $g \geq 1$, comme un problème ouvert. Comme nous le verrons au §VIII.5.7, la théorie d'Arthur suggère en fait qu'il n'existe pas de $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{32})$ tel que $\psi(\pi, \mathrm{St}) = \Delta_{17}[14] \oplus [3] \oplus [1]$.

4. Une table des premiers éléments de $\Pi_{\mathrm{disc}}(\mathrm{SO}_8)$

D'après [CR12, Ch. 2], on dispose d'une formule pour la dimension de $\mathrm{M}_{U_\lambda}(\mathrm{SO}_8)$ en fonction du plus haut poids $\lambda = \sum_{i=1}^4 m_i \varepsilon_i$ de la représentation U_λ (§VI.4.3). Pour des petites valeurs de λ, par exemple dès que $m_1(\lambda) := m_1$ est ≤ 9, on constate par inspection que ces dimensions sont ≤ 1, et même

presque toujours nulles [CR12, App. C. Table 2]. Quand cette dimension vaut 1, il existe donc une unique représentation $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ telle que $\pi_\infty \simeq U_\lambda$, notons-la $\pi(\lambda)$.

Les considérations de ce chapitre permettent de démontrer l'existence d'un certain nombre d'éléments de $\Pi_{\mathrm{disc}}(\mathrm{O}_8)$ ou $\Pi_{\mathrm{disc}}(\mathrm{SO}_8)$. On peut se demander si ces éléments suffisent à expliquer tous les $\pi(\lambda)$ ci-dessus. La réponse à cette question est donnée par la table VII.1, qui indique la liste de tous les $\psi(\pi(\lambda), \mathrm{St})$ quand $m_1(\lambda) \leq 8$. Pour des raisons de numérologie, il est plus significatif de faire apparaître dans cette table l'élément $\lambda + \rho$, caractère infinitésimal de U_λ (§VI.4.3), que nous coderons par le quadruple $z(\lambda) = (2m_1 + 6, 2m_2 + 4, 2m_3 + 2, 2|m_4|)$, si $\lambda = \sum_{i=1}^4 m_i \varepsilon_i$.

Table VII.1 – Paramètres standards des $\pi(\lambda)$ quand $m_1(\lambda) \leq 8$.

$z(\lambda)$	$\psi(\pi(\lambda), \mathrm{St})$	$z(\lambda)$	$\psi(\pi(\lambda), \mathrm{St})$
$(6, 4, 2, 0)$	$[7] \oplus [1]$	$(22, 16, 14, 0)$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{15}[2] \oplus [1]$
$(14, 12, 10, 8)$	$\Delta_{11}[4]$	$(22, 18, 16, 0)$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[2] \oplus [1]$
$(18, 16, 2, 0)$	$\Delta_{17}[2] \oplus [3] \oplus [1]$	$(22, 20, 2, 0)$	$\Delta_{21}[2] \oplus [3] \oplus [1]$
$(18, 16, 14, 12)$	$\Delta_{15}[4]$	$(22, 20, 6, 4)$	$\psi_{4,10}[2]$
$(20, 18, 8, 6)$	$\psi_{6,8}[2]$	$(22, 20, 10, 8)$	$\psi_{8,8}[2]$
$(20, 18, 16, 14)$	$\Delta_{17}[4]$	$(22, 20, 14, 12)$	$\psi_{12,6}[2]$
$(22, 4, 2, 0)$	$\mathrm{Sym}^2\Delta_{11} \oplus [5]$	$(22, 20, 18, 0)$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus [1]$
$(22, 12, 10, 0)$	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[2] \oplus [1]$	$(22, 20, 18, 16)$	$\Delta_{19}[4]$

Discutons un peu cette table. La représentation de paramètre $[7] \oplus [1]$ est bien entendu la représentation triviale. Rappelons que la notation $\Delta_w \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ a été introduite au §VII.3. Les quatres éléments $\psi_{j,k} \in \mathcal{X}(\mathrm{SL}_4)$ seront expliqués au §IX.1.17.

(i) L'existence des représentations de paramètre $\Delta_w[4]$ découle du théorème 2.1. Dans le cas du quadruple $(14, 12, 10, 8)$, c'est la représentation utilisée dans la démonstration du théorème V.2.

(ii) L'existence d'une représentation de $\Pi_{\mathrm{disc}}(\mathrm{O}_8)$ de paramètre $\Delta_w[2] \oplus [3] \oplus [1]$ pour $w \equiv 1 \bmod 4$ se déduit du théorème 3.2 : c'est le cas $n = 8$, $k = w + 1$ et $g = 2$, qui s'applique car $\mathrm{L}(\frac{1}{2}, \Delta_w) \neq 0$ pour $w = 17, 21$ (Exemple 3.3). Dans ces cas particuliers, un rôle important

est joué par les formes propres dans $\mathrm{S}_{\frac{w+3}{2}}(\mathrm{Sp}_4(\mathbb{Z}))$ de paramètre standard $\Delta_w[2] \oplus [1]$ (les deux "premières" formes de Saito-Kurokawa, cas $g = 2$ du théorème 3.1). Lorsque $w = 17, 21$, la surjectivité de $\vartheta_{\frac{w-5}{2},2}$: $\mathrm{M}_{\mathrm{H}_{\frac{w-5}{2},2}(\mathbb{R}^8)}(\mathrm{O}_8) \to \mathrm{S}_{\frac{w+3}{2}}(\mathrm{Sp}_4(\mathbb{Z}))$ se vérifie par un simple calcul de coefficient de séries thêta étant donné que l'on sait depuis Igusa [IGU62] que $\mathrm{S}_{\frac{w+3}{2}}(\mathrm{Sp}_4(\mathbb{Z}))$ est de dimension 1. Ce calcul sera justifié dans la proposition IX.1.2.

(iii) Le cas $z(\lambda) = (22, 20, 18, 0)$ admet également une histoire intéressante, puisqu'il a été étudié par Miyawaki dans [MIY92]. Il a montré que $\pi(\lambda)$ admet un θ-correspondant dans $\mathrm{S}_{12}(\mathrm{Sp}_6(\mathbb{Z}))$ qu'il a conjecturé de paramètre standard $\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2]$, ce qu'a par la suite démontré Ikeda [IKE06]. Le cas des autres paramètres, d'apparence pourtant similaire, de la forme $\mathrm{Sym}^2\Delta_{11} \oplus \Delta_w[2] \oplus [1]$ avec $w \in \{11, 15, 17\}$ est plus subtil. Quand $w = 11, 15$ nous pourrions les justifier comme pour $w = 19$ si nous disposions d'un analogue de la construction d'Ikeda pour des formes non scalaires, car pour les deux valeurs de λ pertinentes on pourrait sans doute vérifier que $\pi(\lambda)$ admet un ϑ-correspondant pour Sp_8 (voir le §VIII.6). Ces paramètres (indiqués en bleu dans la table) sont prédits par la théorie d'Arthur, comme nous le verrons au chapitre VIII.

Nous renvoyons au chapitre VIII.5.7 pour une confirmation directe mais conditionnelle de l'intégralité de cette table utilisant la théorie d'Arthur, ainsi qu'à [CR12, Ch. 2 & 7] pour des tables nettement plus fournies. Bien qu'il serait sans doute possible de le faire par des construction de séries thêta et les méthodes du §IX.5, nous ne justifierons pas inconditionnellement les trois paramètres en bleu de la table VII.1.

5. $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$

Dans ce paragraphe nous démontrons la proposition V.3.1.

Proposition 5.1. *Le paramètre standard de l'unique représentation π dans $\Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\pi_\infty \simeq$ dét est $\Delta_{11}[12]$.*

Démonstration. D'après le corollaire 3.4, il existe $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\pi_\infty = \mathbb{C}$ et $\psi(\pi, \mathrm{St}) = \Delta_{11}[12]$. On a

$$\tau(2)(2^{12} - 1) = 2^{11}\,\mathrm{trace}(\mathrm{c}_2(\pi), V_{\mathrm{St}})$$

qui n'est autre que la valeur propre λ_{24} dans les notations du §V.3. Soit $f_{24} \in \mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24})$ la fonction image de l'élément v_{24} par l'isomorphisme de $\mathrm{H}(\mathrm{O}_{24})$-modules $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24}) \simeq \mathbb{C}[\mathrm{X}_{24}]$ défini au corollaire IV.4.9.

On rappelle que $\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$ est muni d'une action de $\mathrm{H}(\mathrm{SO}_{24})$, ainsi que d'une involution s (le "changement d'orientation", voir la fin du §IV.4.4) dont la décomposition en espaces propres s'écrit

$$\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24}) = \mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24}) \oplus \mathrm{M}_{\text{dét}}(\mathrm{O}_{24}).$$

Cette décomposition n'est pas respectée à priori par $\mathrm{H}(\mathrm{SO}_{24})$, mais seulement par $\mathrm{H}(\mathrm{O}_{24})$, la relation dont on dispose étant : $T \circ s = s \circ \mathrm{H}(s)(T)$ pour tout $T \in \mathrm{H}(\mathrm{SO}_{24})$.

Soit $V \subset \mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$ le $\mathrm{H}(\mathrm{SO}_{24})[s]$-module engendré par f_{24} et soit $f'_{24} \in V$ une forme propre pour $\mathrm{H}(\mathrm{SO}_{24})$. Elle engendre naturellement une représentation $\pi' \in \Pi_{\text{disc}}(\mathrm{SO}_{24})$ de paramètre standard Δ_{11}[12]. En particulier, la classe de conjugaison $\mathrm{c}_2(\pi') \subset \mathrm{SO}_{24}(\mathbb{C})$ n'admet pas la valeur propre ± 1, car les valeurs propres de $\mathrm{c}_2(\Delta_{11})$ sont non réelles (ce sont les racines de $x^2 + \frac{24}{2^{11/2}}x + 1$). Cette classe de conjugaison sous $\mathrm{SO}_{24}(\mathbb{C})$ n'est donc pas stable par l'action de conjugaison de $\mathrm{O}_{24}(\mathbb{C})$. La compatibilité de l'isomorphisme de Satake aux isomorphismes montre donc que si $f''_{24} = s(f'_{24}) \in V$, et si $\pi'' \in \Pi_{\text{disc}}(\mathrm{SO}_{24})$ est engendrée par f''_{24}, alors on a

$$\mathrm{c}_2(\pi') \neq \mathrm{c}_2(\pi'').$$

En particulier, f'_{24} et f''_{24} ne sont pas proportionnelles et ont même valeurs propres que f_{24} sous l'action de $\mathrm{H}(\mathrm{O}_{24})$. On conclut car l'élément non nul $f'_{24} - f''_{24} = (1-s)f'_{24}$ engendre la droite $\mathrm{M}_{\text{dét}}(\mathrm{O}_{24})$. $\square$

VIII. La classification d'Arthur pour les $\mathbb{Z}$-groupes classiques

1. Paramètres standards pour les groupes classiques

Le but de ce chapitre est d'expliquer la description de $\Pi_{\mathrm{disc}}(G)$ issue des travaux d'Arthur [Art13] lorsque G est un $\mathbb{Z}$-groupe semi-simple *classique. Nous entendrons dorénavant par là que G est de la forme* Sp_{2g} *pour* $g \geq 1$*, ou* SO_L*, où L est soit un* q*-module sur $\mathbb{Z}$ de dimension $\neq 2$, soit un* q-i*-module sur $\mathbb{Z}$ au sens de l'appendice* B *(§V.4.7).* Si r est un entier ≥ 1, on pose

$$\mathrm{SO}_{r,r} = \mathrm{SO}_{\mathrm{H}(\mathbb{Z}^r)} \text{ et } \mathrm{SO}_{r+1,r} = \mathrm{SO}_{\mathrm{H}(\mathbb{Z}^r)\oplus \mathrm{A}_1}.$$

Les $\mathbb{Z}$-groupes classiques semi-simples qui sont des groupes de Chevalley [1] sont donc Sp_{2g} pour $g \geq 1$, $\mathrm{SO}_{r,r}$ pour $r \geq 2$ et $\mathrm{SO}_{r+1,r}$ pour $r \geq 1$. Il sera commode de considérer le $\mathbb{Z}$-groupe trivial comme un groupe classique de Chevalley, que l'on notera également $\mathrm{SO}_{1,0}$. De plus, un rôle important sera joué par les $\mathbb{Z}$-groupes SO_n, définis pour tout entier $n \geq 1$ tel que $n \equiv -1, 0, 1 \bmod 8$ par

$$\mathrm{SO}_n = \mathrm{SO}_{\mathrm{L}_n}$$

où : $\mathrm{L}_n = \mathrm{E}_n$ si $n \equiv 0 \bmod 8$, $\mathrm{L}_n = \mathrm{E}_{n-1} \oplus \mathrm{A}_1$ si $n \equiv 1 \bmod 8$, et où L_n désigne l'orthogonal d'une racine [2] de E_{n+1} si $n \equiv -1 \bmod 8$ (§IV.1.2 & §IV.1.10).

Rappelons que si G est un $\mathbb{Z}$-groupe classique semi-simple, le $\mathbb{C}$-groupe $\widehat{G}$ est un groupe classique complexe, et possède une représentation irréductible distinguée qui est sa représentation standard (§V.4.1, §V.4.7)

$$\mathrm{St} : \widehat{G} \to \mathrm{SL}_n(\mathbb{C}).$$

Théorème* **1.1.** [Art13, Thm. 1.5.2] *Si G est un $\mathbb{Z}$-groupe classique de Chevalley et si $\pi \in \Pi_{\mathrm{disc}}(G)$ alors $\psi(\pi, \mathrm{St}) \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$.*

1. Nous utiliserons dans ce chapitre le terme de *groupe de Chevalley* comme synonyme de *$\mathbb{Z}$-groupe semi-simple déployé.*

2. Le choix de cette racine est fixé une fois pour toutes, et ne jouera aucun rôle dans la suite. Comme toutes ces racines sont permutées transitivement par $\mathrm{W}(\mathbf{D}_{n+1}) \subset \mathrm{O}(\mathrm{E}_{n+1})$, la classe d'isomorphisme du $\mathbb{Z}$-groupe SO_n ne dépend par exemple que de n.

Ce résultat, qui est un cas particulier de la conjecture générale V.4.6, est aussi un cas très particulier du théorème sus-cité (cas des représentations "non ramifiées en tous les nombres premiers"). Il repose sur un édifice assez formidable de résultats difficiles, notamment de multiples variantes de la formule des traces d'Arthur-Selberg (Arthur), la décomposition spectrale des espaces des formes automorphes (Langlands), la théorie de l'endoscopie (Langlands, Shelstad, Kottwitz), et la démonstration du fameux *lemme fondamental* (Waldspurger [WAL06], Ngô [NGÔ10], Laumon, Chaudouard [CHAL10, CHAL12]). Ainsi que l'explique Arthur dans son livre, les résultats de [ART13] dépendent d'une variante "avec torsion" de ses travaux sur la "stabilisation" de la formule des traces. La formule requise a récemment été établie par Moeglin et Waldspurger, dans une longue série d'articles [WAL14, MW14] (voir aussi [LW13]). Arthur mentionne également une autre hypothèse concernant une extension des travaux de Shelstad concernant l'endoscopie tordue pour les groupes de Lie réels, et qui a fait l'objet depuis de travaux de Shelstad [SHE12a, SHE12b, SHE14] et Mezo [MEZ11, MEZ13]. Les énoncés de ce mémoire dépendant de ces travaux tous récents, par l'intermédiaire des énoncés de [ART13], seront affublés d'une étoile verte $\star$ en exposant.

Le travail d'Arthur [ART13] porte comme nous l'avons dit sur les $\mathbb{Z}$-groupes classiques de Chevalley. Cependant, ses travaux antérieurs permettent d'en déduire également une classification de $\Pi_{\mathrm{disc}}(G)$ lorsque G est un $\mathbb{Z}$-groupe classique quelconque. Cette classification est annoncée dans le chapitre 9 de [ART13], mais la rédaction complète n'est pas encore disponible, c'est pourquoi nous l'énoncerons sous forme de conjecture.[3] Comme nous le verrons, ces résultats ne seront pas nécessaires à l'établissement de nos résultats principaux. En revanche, ils éclairent substantiellement les questions qui nous préoccupent, de sorte qu'il serait dommage de les laisser sous silence. Par exemple, ils conduisent comme nous le verrons à une description directe et très précise de $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$, le thème principal de ce mémoire.

Conjecture 1.2. [ART13, Ch. 9] *L'énoncé du théorème 1.1 vaut encore si G est un $\mathbb{Z}$-groupe classique quelconque.*

NOTATIONS : Tout comme au §V.4.7, nous notons $\mathrm{Class}_{\mathbb{C}}$ l'ensemble constitué des $\mathbb{C}$-groupes Sp_{2g} ($g \geq 1$) et SO_m ($m \geq 0$, $m \neq 2$). Un groupe $H \in \mathrm{Class}_{\mathbb{C}}$ est uniquement déterminé par le couple associé $(\mathrm{n}_H, \mathrm{w}_H) \in \mathbb{N} \times \{0, 1\}$ défini de la manière suivante :

3. Mentionnons sur ce point qu'aucune des difficultés évoquées par Arthur dans son chapitre 9 ne semble s'appliquer à la situation qui nous intéresse, qui ne concerne que des "formes intérieures pures" des groupes de Chevalley [KAL13].

– n_H est la dimension de la représentation standard de H,

– $\mathrm{w}_H = 0$ si, et seulement si, $H \simeq \mathrm{SO}_m$ pour un entier $m \geq 0$.

2. Représentations autoduales de PGL_n

La description d'Arthur, et plus généralement la conjecture d'Arthur-Langlands, fait intervenir des représentations dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$ pour tout $m \geq 1$, que nous n'avons rencontrées jusqu'à présent essentiellement que dans le cas $m = 2$ et plutôt du point de vue de l'identité $\mathrm{GSp}_2 = \mathrm{GL}_2$. Nous revenons maintenant sur celles-là.

2.1. Dualité dans $\Pi_{\mathrm{disc}}(\mathrm{PGL}_n)$

Soient $n \geq 1$ un entier et $\mathcal{R}_n$ l'ensemble des sous-groupes discrets de rang n de $\mathbb{R}^n$. Il est muni d'une action naturelle transitive de $\mathrm{GL}_n(\mathbb{R})$ et l'orbite du réseau $\mathbb{Z}^n$ s'identifie à $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \xrightarrow{\sim} \mathcal{R}_n$. Le sous-groupe $\mathrm{GL}_n(\mathbb{Q})$ préserve le sous-espace $\mathcal{R}_{\mathbb{Z}}(\mathbb{Q}^n) \subset \mathcal{R}_n$ des réseaux de $\mathbb{Q}^n$; cette action est transitive et s'étend naturellement en une action de $\mathrm{GL}_n(\mathbb{A}_f)$ (§IV.1.1). L'application $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{A}_f) \to \mathcal{R}_n$, $(g_\infty, g_f) \mapsto g_\infty^{-1}(g_f(\mathbb{Z}^n))$ a donc un sens ; elle induit une bijection $\mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A})/\mathrm{GL}_n(\widehat{\mathbb{Z}}) \xrightarrow{\sim} \mathcal{R}_n$, puis un isomorphisme naturel

$$\mathcal{A}^2(\mathrm{PGL}_n) \xrightarrow{\sim} \mathrm{L}^2(\underline{\mathcal{R}}_n),$$

où $\underline{\mathcal{R}}_n$ désigne le quotient de $\mathcal{R}_n$ par le groupe $\mathbb{R}^\times$ des homothéties, muni d'une mesure $\mathrm{GL}_n(\mathbb{R})$ invariante non nulle (§IV.3.1). Les actions naturelles de $\mathrm{PGL}_n(\mathbb{R})$ et de $\mathrm{H}(\mathrm{PGL}_n)$ sur $\mathrm{L}^2(\underline{\mathcal{R}}_n)$ déduites par transport de structure sont alors les actions évidentes. En particulier, si $f \in \mathrm{L}^2(\underline{\mathcal{R}}_n)$ est continue, si $\mathrm{T}_A \in \mathrm{H}(\mathrm{PGL}_n)$ est l'opérateur défini au §IV.2.6, et si $L \in \mathcal{R}_n$, alors $\mathrm{T}_A(f)(\underline{L}) = \sum_M f(\underline{M})$ où M parcourt les sous-groupes de L tels que $L/M \simeq A$, la notation $\underline{N}$ désignant la classe d'homothétie de $N \in \mathcal{R}_n$.

Le $\mathbb{Z}$-groupe GL_n admet pour automorphisme $g \mapsto {}^t g^{-1}$, qui agit donc également sur $\mathcal{A}^2(\mathrm{PGL}_n)$ par une involution notée θ, qui préserve les sous-espaces $\mathcal{A}_{\mathrm{disc}}(\mathrm{PGL}_n)$ et $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGL}_n)$. Concrètement, munissons le $\mathbb{Z}$-module $\mathbb{Z}^n$ de la forme bilinéaire symétrique non dégénérée standard, et notons $L^\sharp$ le réseau dual de $L \in \mathcal{R}_n$ pour cette forme. L'involution en question de $\mathrm{L}^2(\underline{\mathcal{R}}_n)$, encore notée θ, est simplement définie par $\theta(f)(\underline{L}) = f(\underline{L^\sharp})$. Elle satisfait donc $\theta(T(f)) = \iota(T)(\theta(f))$ pour tout $T \in \mathrm{H}(\mathrm{PGL}_n)$ et tout $f \in \mathrm{L}^2(\underline{\mathcal{R}}_n)$, où ι est l'automorphisme involutif de $\mathrm{H}(\mathrm{PGL}_n)$ défini au §IV.2.6.

Si $\pi = \pi_\infty \otimes \pi_f \in \Pi(\mathrm{PGL}_n)$, on note $\pi^\vee \in \Pi(\mathrm{PGL}_n)$ l'élément défini de la manière suivante. D'une part, $(\pi^\vee)_\infty$ est la représentation ayant même espace

que π_∞ mais composée par l'automorphisme $g \mapsto {}^{\mathrm{t}}g^{-1}$ de $\mathrm{PGL}_n(\mathbb{R})$. D'autre part, si l'on voit $(\pi^\vee)_f$ et π_f comme des homomorphismes $\mathrm{H}(\mathrm{PGL}_n) \to \mathbb{C}$, alors $(\pi^\vee)_f = \pi_f \circ \iota$.

Si c est la classe de conjugaison d'un élément semisimple g de $\mathrm{SL}_n(\mathbb{C})$, nous noterons c^{-1} (resp. $\overline{c}$) la classe de conjugaison de g^{-1} (resp. du conjugué complexe de g). De plus, si c est la classe de conjugaison d'un élément semisimple X de $\mathfrak{sl}_n(\mathbb{C})$, nous noterons $-c$ la classe de conjugaison de $-X$. La proposition suivante est bien connue.

Proposition 2.2. *Soit $\pi \in \Pi(\mathrm{PGL}_n)$.*

(i) Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ (resp. $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGL}_n)$), il en va de même de $\pi^\vee$.

(ii) Pour tout premier p, on a l'égalité $\mathrm{c}_p(\pi^\vee) = \mathrm{c}_p(\pi)^{-1}$. Si l'on a de plus $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGL}_n)$, on a également $\mathrm{c}_p(\pi^\vee) = \overline{\mathrm{c}_p(\pi)}$.

(iii) La représentation $(\pi^\vee)_\infty$ est le dual de la représentation unitaire π_∞, et l'on a l'égalité $\mathrm{c}_\infty(\pi^\vee) = -\mathrm{c}_\infty(\pi)$.

Démonstration. Les paragraphes qui précédent l'énoncé justifient l'assertion (i). Soit p un nombre premier. Pour tout élément $T \in \mathrm{H}(\mathrm{PGL}_n)$, on a la relation $\iota(T) = T^{\mathrm{t}}$ d'après le §IV.2.6. La discussion suivant le scholie V.2.2 montre donc l'égalité $\mathrm{c}_p(\pi^\vee) = \mathrm{c}_p(\pi)^{-1}$. D'autre part, l'action de $\mathrm{H}(\mathrm{PGL}_n)$ sur $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGL}_n)$ étant une $\star$-action pour le produit de Petersson sur ce dernier d'après le §IV.3.1, on en déduit également que les éléments π_p et $\pi_p^\vee$, vus comme morphismes d'anneaux $\mathrm{H}_p(\mathrm{PGL}_n) \to \mathbb{C}$, sont conjugués complexes l'un de l'autre. Du point de vue de l'isomorphisme de Satake cela s'écrit $\mathrm{c}_p(\pi^\vee) = \overline{\mathrm{c}_p(\pi)}$. Le (iii) est conséquence de la théorie des caractères d'Harish-Chandra et du fait que tout élément de $\mathrm{GL}_n(\mathbb{R})$ est conjugué à sa transposée. Il n'est pas difficile de vérifier sur la définition de l'isomorphisme d'Harish-Chandra que l'on a $\mathrm{c}_\infty(\pi^\vee) = -\mathrm{c}_\infty(\pi)$. $\square$

Définition 2.3. *Soit $\pi \in \Pi(\mathrm{PGL}_n)$. La représentation $\pi^\vee$ est appelée représentation duale de π. On dit que π est autoduale si $\pi^\vee \simeq \pi$. On note $\Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_n) \subset \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ le sous-ensemble des représentations autoduales.*

Notons que d'après le théorème de multiplicité 1 de Jacquet-Shalika, pour que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ soit autoduale il suffit que $\mathrm{c}_p(\pi) = \mathrm{c}_p(\pi)^{-1}$ pour tout premier p (voire même, pour tout premier p sauf un nombre fini).

La représentation triviale de PGL_1 est bien sûr autoduale. De plus, l'automorphisme $g \mapsto {}^{t}g^{-1}$ étant intérieur quand $n = 2$, l'inclusion $\Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_2) \subset$

$\Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ est une égalité. Cela ne vaut pas dès que $n > 2$. L'intérêt principal des représentations autoduales pour nos préoccupations vient du théorème suivant, précisant l'énoncé du théorème 1.1.

Théorème* **2.4.** [Art13, Thm. 1.5.2] *Soient G un $\mathbb{Z}$-groupe classique de Chevalley et $\pi \in \Pi_{\mathrm{disc}}(G)$. Alors $\psi(\pi, \mathrm{St})$ est de la forme $\oplus_{i=1}^k \pi_i[d_i]$ avec $\pi_i \in \Pi_{\mathrm{cusp}}^{\perp}(\mathrm{PGL}_{n_i})$ pour tout $i = 1, \ldots, k$ et $\sum_{i=1}^k n_i d_i = \mathrm{n}_{\widehat{G}}$. De plus, cette écriture est unique et les couples (π_i, d_i), $i = 1, \ldots, k$, sont deux à deux distincts.*

Un raffinement similaire de la conjecture 1.2 est également attendu. Remarquons que tous les paramètres de Langlands mis en évidence aux chapitres V et VII ont bien la propriété ci-dessus. En particulier, on constate que la représentation de Gelbart-Jacquet $\mathrm{Sym}^2\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_3)$, où $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$, est autoduale. Une justification partielle de ces propriétés d'autodualité est donnée par la proposition élémentaire suivante.

Proposition 2.5. *Soient G un $\mathbb{Z}$-groupe classique et $\pi \in \Pi(G)$. Supposons que $\psi(\pi, \mathrm{St}) = \oplus_{i=1}^k \pi_i[d_i]$ où $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour tout $i = 1, \ldots, k$. Alors pour tout i il existe j tel que $\pi_j = \pi_i^\vee$ et $d_j = d_i$.*

Démonstration. En effet, la représentation St de $\widehat{G}$ étant autoduale, on a $\mathrm{St}(\mathrm{c}_p(\pi)) = \mathrm{St}(\mathrm{c}_p(\pi))^{-1}$ pour tout premier p (resp. $\mathrm{St}(\mathrm{c}_\infty(\pi)) = -\mathrm{St}(\mathrm{c}_\infty(\pi))$) et donc également $\psi(\pi, \mathrm{St}) = \oplus_{i=1}^k \pi_i^\vee[d_i]$. On conclut d'après la proposition V.4.5 (Théorème de Jacquet-Shalika). □

2.6. Représentations algébriques régulières

Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$. Les *poids* de π sont les valeurs propres de la classe de conjugaison semi-simple $\mathrm{c}_\infty(\pi) \subset \mathrm{M}_n(\mathbb{C})$. Leur ensemble sera noté $\mathrm{Poids}(\pi) \subset \mathbb{C}$.

Définition 2.7. *Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$. On dit que π est algébrique*[4] *si* $\mathrm{Poids}(\pi) \subset \frac{1}{2}\mathbb{Z}$ *et si* $\forall w, w' \in \mathrm{Poids}(\pi),\ w - w' \in \mathbb{Z}$.

Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est algébrique, son poids motivique *est le plus grand $w \in \mathbb{Z}$ tel que $-\frac{w}{2} \in \mathrm{Poids}(\pi)$, on le note $\mathrm{w}(\pi)$. En particulier,* $\mathrm{Poids}(\pi) \subset \frac{\mathrm{w}(\pi)}{2} + \mathbb{Z}$.

4. Le lecteur prendra garde qu'il existe plusieurs notions de représentations automorphes algébriques dans la littérature. La définition ci-dessus, qui est essentiellement celle considérée par exemple dans [Bor77, §18.2], mais qui n'est pas celle utilisée par Clozel dans [Clo90], est réminescente de la notion de caractère de Hecke de type A_0 au sens de Weil (voir [BG10] pour des clarifications entre les diverses notions).

Bien que les représentations algébriques forment une partie infime de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$, ce seront les seules à jouer un rôle dans ce travail. Un indicateur à cela est donné par la proposition suivante.

Proposition 2.8. *Soient G un $\mathbb{Z}$-groupe semi-simple, $\pi \in \Pi(G)$ et $r : \widehat{G} \to \mathrm{SL}_n$ une $\mathbb{C}$-représentation. On suppose que :*

(i) π_∞ a même caractère infinitésimal qu'une $\mathbb{C}$-représentation irréductible de dimension finie de $G_{\mathbb{C}}$.

(ii) $\psi(\pi, r) = \oplus_{i=1}^{k} \pi_i[d_i]$ avec $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour $i = 1, \ldots, k$ (§V.4.4).

Alors π_i est algébrique pour tout i. De plus, la classe de $\mathrm{w}(\pi_i) + d_i - 1$ dans $\mathbb{Z}/2\mathbb{Z}$ ne dépend que de r (et non de l'entier i, ou même de π).

Démonstration. Soit μ le plus haut poids de r (un co-poids de $G_{\mathbb{C}}$). Le caractère infinitésimal de π_∞ est de la forme $\lambda+\rho$ où λ est un poids dominant de $G_{\mathbb{C}}$ et ρ la demi-somme des racines positives (§V.3.4). Les valeurs propres de $r(\mathrm{c}_\infty(\pi))$ sont par définition de la forme $\langle \lambda + \rho, \mu' \rangle$, où μ' est un poids de r. Mais 2ρ est un poids de $G_{\mathbb{C}}$ et $\langle \mu - \mu', \rho \rangle \in \mathbb{Z}$ si $\mu' \leq \mu$, ces valeurs propres sont donc toutes dans $\frac{1}{2}\mathbb{Z}$ et diffèrent deux à deux d'un élément de $\mathbb{Z}$. Cette propriété est héritée par les poids des π_i. $\square$

Cette proposition s'applique notamment pour tout $\pi \in \Pi(G)$ si $G(\mathbb{R})$ est compact (§V.3.4). Elle s'applique également si $G = \mathrm{Sp}_{2g}$ et si π est engendrée par une forme propre dans $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ avec W positif, d'après le corollaire §V.3.6 (ainsi que la discussion qui suit) et le §V.1.3.

Soient G un $\mathbb{Z}$-groupe classique et $\mathrm{St} : \widehat{G} \to \mathrm{SL}_n$ la représentation standard de $\widehat{G}$. Nous aurons besoin de préciser l'analyse précédente dans ce contexte. Soit $\mathrm{Irr}(G_{\mathbb{C}})$ l'ensemble des classes d'isomorphisme de $\mathbb{C}$-représentations irréductibles de dimension finie de $G_{\mathbb{C}}$. Pour chaque $V \in \mathrm{Irr}(G_{\mathbb{C}})$ observons la classe de conjugaison semi-simple $\mathrm{St}(\mathrm{Inf}_V) \subset \mathrm{M}_n(\mathbb{C})$ (on rappelle que $\mathrm{Inf}_V \in \widehat{\mathfrak{g}}_{\mathrm{ss}}$ désigne le caractère infinitésimal de V). On constate par inspection des données radicielles (§VI.1.3) qu'il y a trois cas bien distincts :

I. Si $\widehat{G} = \mathrm{SO}_n(\mathbb{C})$ avec $n = 2g + 1$ impair, alors $V \mapsto \mathrm{St}(\mathrm{inf}_V)$ induit une bijection entre $\mathrm{Irr}(\widehat{G})$ et l'ensemble des classes de conjugaison semi-simples $X \subset \mathrm{M}_n(\mathbb{C})$ telles que $-X = X$ et dont toutes les valeurs propres sont distinctes et dans $\mathbb{Z}$.

II. Si $\widehat{G} = \mathrm{Sp}_n(\mathbb{C})$ (et donc n est pair), alors $V \mapsto \mathrm{St}(\mathrm{Inf}_V)$ induit une bijection entre $\mathrm{Irr}(\widehat{G})$ et l'ensemble des classes de conjugaison semi-simples $X \subset \mathrm{M}_n(\mathbb{C})$ telles que $-X = X$ et dont toutes les valeurs propres sont distinctes et dans $\frac{1}{2}\mathbb{Z} - \mathbb{Z}$.

III. Si $\widehat{G} = \mathrm{SO}_n(\mathbb{C})$ avec n pair, alors $V \mapsto \mathrm{St}(\mathrm{Inf}_V)$ induit une surjection entre $\mathrm{Irr}(\widehat{G})$ et l'ensemble des classes de conjugaison semi-simples $X \subset \mathrm{M}_n(\mathbb{C})$ telles que $-X = X$, dont toutes les valeurs propres sont dans $\mathbb{Z}$ et distinctes, sauf peut-être la valeur propre 0, dont la multiplicité est ≤ 2. De plus, $\mathrm{St}(\mathrm{Inf}_V) = \mathrm{St}(\mathrm{Inf}_{V'})$ si et seulement si V et V' sont conjuguées l'une de l'autre sous l'action extérieure de $\mathrm{O}_n(\mathbb{C})$ (ce qui entraîne $V = V'$ si, et seulement si, 0 est valeur propre de $\mathrm{Inf}_V = \mathrm{Inf}_{V'}$).

Dans tous les cas, les valeurs propres de $\mathrm{St}(\mathrm{Inf}_V)$ sont donc dans $\frac{\mathrm{w}_{\widehat{G}}}{2} + \mathbb{Z}$.

Définition 2.9. *On dit que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est* régulière *si $|\mathrm{Poids}(\pi)| = n$.*

Proposition 2.10. *Soient G un $\mathbb{Z}$-groupe classique et $\mathrm{St} : \widehat{G} \to \mathrm{SL}_n$ la représentation standard de $\widehat{G}$. On suppose que $\psi = \oplus_{i=1}^r \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$, où $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour tout $i = 1, \ldots, k$, et que $\psi_\infty = \mathrm{St}(\mathrm{Inf}_V)$ où $V \in \mathrm{Irr}(G_{\mathbb{C}})$.*

Soit $i \in \{1, \ldots, k\}$. Alors π_i est algébrique, de poids motivique $\mathrm{w}(\pi_i) \equiv d_i - 1 + \mathrm{w}_{\widehat{G}} \bmod 2$, et autoduale. De plus, π_i est régulière, à moins que l'on ne soit dans le cas exceptionnel suivant :

(a) $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_{2r}(\mathbb{C})$ et ψ_∞ admet 0 pour valeur propre double,

(b) $d_i = 1$, $n_i \equiv 0 \bmod 2$ et $|\mathrm{Poids}(\pi_i)| = n_i - 1$,

(c) et pour tout $j \neq i$, π_j est régulière et $n_j \equiv 0 \bmod 2$.

Démonstration. Hormis l'assertion concernant autodualité de π_i, la proposition découle immédiatement de l'analyse des cas I, II et III ci-dessus et de la proposition 2.8.

Vérifions l'autodualité de π_i. D'après la proposition 2.5, il existe j tel que $\pi_j = \pi_i^\vee$ et $d_j = d_i$. D'après la proposition 2.11 ci-dessous, $\pi_j = \pi_i^\vee$ entraîne $\mathrm{c}_\infty(\pi_j) = \mathrm{c}_\infty(\pi_i)$. Compte tenu de l'hypothèse sur ψ_∞, et de l'analyse des cas I, II et III, cela entraîne $j = i$ ou $n_i = n_j = 1$. Dans ce dernier cas, on a nécessairement $\pi_j = \pi_i = 1$, et donc dans tous les cas nous avons bien $\pi_i^\vee = \pi_i$. □

Dans la démonstration ci-dessus nous avons fait appel à la proposition suivante (évidente si π est supposée autoduale).

Proposition 2.11. *Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est algébrique alors π_∞ est isomorphe à son dual. En particulier, on a $\mathrm{c}_\infty(\pi) = \mathrm{c}_\infty(\pi^\vee)$ et :*

(i) $w \mapsto -w$ est une bijection de $\mathrm{Poids}(\pi)$ (préservant les multiplicités comme valeurs propres de $\mathrm{c}_\infty(\pi)$).

(ii) si $n \equiv 1 \bmod 2$*, alors* $0 \in \mathrm{Poids}(\pi)$ *et* $\mathrm{w}(\pi) \equiv 0 \bmod 2$.

Pour l'expliquer, il sera nécessaire d'étudier plus en détail les composantes archimédiennes des éléments de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$. Une autre motivation à cela est que les représentations algébriques régulières autoduales, ainsi que celles intervenant dans le cas exceptionnel de l'énoncé de la proposition 2.10, satisfont quelques propriétés supplémentaires cachées, qu'il nous faudra préciser. Cette analyse sera également nécessaire pour appliquer les énoncés d'Arthur. En effet, ils feront intervenir des *facteurs* ε *de paires de représentations* algébriques, qui se lisent aussi (comme les facteurs Γ) sur leurs composantes archimédiennes. Ce travail a déjà été mené dans [CR12, §3.11], dont nous allons rappeler quelques résultats dans les paragraphes suivants.

2.12. Représentations de $\mathrm{GL}_n(\mathbb{R})$

Soit $\mathrm{W}_{\mathbb{R}}$ le groupe de Weil du corps $\mathbb{R}$ [Tat79, §1]. C'est un groupe topologique, extension non-triviale de $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{C}^\times$, pour l'action naturelle de conjugaison. Il est engendré par son sous-groupe ouvert $\mathbb{C}^\times$ ainsi qu'un élément j, avec pour relations $j^2 = -1$ et $jzj^{-1} = \overline{z}$ pour tout $z \in \mathbb{C}^\times$.

Suivant Langlands [Lan73b], les représentations continues et semi-simples $\mathrm{W}_{\mathbb{R}} \to \mathrm{GL}_n(\mathbb{C})$ joueront un rôle important. Rappelons la forme des irréductibles, qui sont de dimension 1 ou 2. Soit

$$\eta : \mathrm{W}_{\mathbb{R}} \to \mathbb{R}^\times$$

l'unique morphisme de groupes tel que $\eta(j) = -1$ et $\eta(z) = z\overline{z}$ pour tout $z \in \mathbb{C}$; il induit un isomorphisme $\mathrm{W}_{\mathbb{R}}^{\mathrm{ab}} \xrightarrow{\sim} \mathbb{R}^\times$. Les morphismes continus $\mathrm{W}_{\mathbb{R}} \to \mathbb{C}^\times$ sont donc les $|\eta|^s$ et $\epsilon_{\mathbb{C}/\mathbb{R}}|\eta|^s$, où $s \in \mathbb{C}$ et $\epsilon_{\mathbb{C}/\mathbb{R}} = \eta/|\eta|$. Si w est un entier ≥ 0, considérons la représentation induite

$$\mathrm{I}_w = \mathrm{Ind}_{\mathbb{C}^\times}^{\mathrm{W}_{\mathbb{R}}} \left(z \mapsto (\frac{z}{|z|})^w \right).$$

Elle est irréductible si et seulement si $w \neq 0$, et de plus $\mathrm{I}_0 \simeq 1 \oplus \epsilon_{\mathbb{C}/\mathbb{R}}$. Les irréductibles de dimension 2 de $\mathrm{W}_{\mathbb{R}}$ sont les $\mathrm{I}_w \otimes |\eta|^s$ où $w \neq 0$ et $s \in \mathbb{C}$.

Notons $\Phi(\mathrm{GL}_n(\mathbb{R}))$ l'ensemble des classes d'isomorphisme de représentations continues semi-simples $\mathrm{W}_{\mathbb{R}} \to \mathrm{GL}_n(\mathbb{C})$. La *paramétrisation de Langlands* associe à chaque représentation irréductible unitaire U de $\mathrm{GL}_n(\mathbb{R})$ (et plus généralement à tout $(\mathfrak{g}, K)$-module irréductible de ce dernier) un élément $\mathrm{L}(U) \in \Phi(\mathrm{GL}_n(\mathbb{R}))$ qui détermine U à isomorphisme près [Lan73b] [Kna94]. Bien que l'application $U \mapsto \mathrm{L}(U)$ puisse être entièrement explicitée [Kna94], cela ne nous sera pas réellement utile : nous nous contenterons

des assertions de compatibilités suivantes, valables pour toute représentation unitaire irréductible U de $\mathrm{GL}_n(\mathbb{R})$.

(i) (dualité) $\mathrm{L}(U^*) \simeq \mathrm{L}(U)^*$.

(ii) (caractère central) $\det \mathrm{L}(U) = \chi_U \circ \eta$ où $\chi_U : \mathbb{R}^\times \to \mathbb{C}^\times$ désigne le caractère central de U.

(iii) (caractère infinitésimal) Écrivons $\mathrm{L}(U)_{|\mathbb{C}^\times} \simeq \oplus_{i=1}^n \chi_i$, où les χ_i pour $1 \leq i \leq n$ sont des caractères $\mathbb{C}^\times \to \mathbb{C}^\times$. Pour tout i, il existe donc un unique couple $(\lambda_i, \mu_i) \in \mathbb{C}^2$, avec $\lambda_i - \mu_i \in \mathbb{Z}$, tel que[5] $\chi_i(z) = (\frac{z}{|z|})^{\lambda_i - \mu_i} |z|^{\lambda_i + \mu_i}$. Alors Inf_U est la classe de conjugaison semi-simple de $\mathrm{M}_n(\mathbb{C})$ ayant pour valeurs propres les λ_i, $i = 1, \ldots, n$.

La paramétrisation ci-dessus s'applique notamment aux représentations irréductibles unitaires de $\mathrm{PGL}_n(\mathbb{R})$, vues comme représentations de $\mathrm{GL}_n(\mathbb{R})$ de caractère central trivial.

L'assertion (i) de la proposition suivante est le *lemme de pureté* de Clozel [Clo90, Lemma 4.9], elle entraîne la proposition 2.11.

Proposition 2.13. *Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ algébrique de poids les $\frac{\omega_i}{2}$ (comptés avec multiplicités), où $\omega_1 \geq \cdots \geq \omega_n$. Soient E et F les sous-ensembles de $\{1, \ldots, n\}$ définis par $E = \{i, \omega_i > 0\}$ et $F = \{i, \omega_i = 0\}$.*

(i) Il existe un unique $(m_j) \in \{0,1\}^F$ tel que

$$\mathrm{L}(\pi_\infty) \simeq \bigoplus_{i \in E} \mathrm{I}_{\omega_i} \oplus \bigoplus_{j \in F} \epsilon_{\mathbb{C}/\mathbb{R}}^{m_j},$$

en particulier $|F| \equiv n \bmod 2$ et π_∞ est isomorphe à son dual.

(ii) Si $\mathrm{w}(\pi) \equiv 0 \bmod 2$ alors $\sum_{j \in F} m_j \equiv |E| \bmod 2$.

(iii) Si π est régulière et $\mathrm{w}(\pi) \equiv n \equiv 0 \bmod 2$, alors $n \equiv 0 \bmod 4$.

(iv) Si $|\mathrm{Poids}(\pi)| = n - 1$ alors $n \equiv 0 \bmod 2$ et $F = \{\frac{n}{2}, \frac{n}{2} + 1\}$. De plus, $n \equiv 0 \bmod 4$ si et seulement si $\mathrm{L}(\pi_\infty) \simeq \oplus_{i=1}^{n/2} \mathrm{I}_{w_i}$.

Démonstration. (voir [CR12, §3.11]) Rappelons l'argument du lemme de pureté de Clozel. Supposons que $\mathrm{I}_w \otimes |\eta|^{s/2}$ (resp. $|\eta|^{s/2}$ ou $\varepsilon_{\mathbb{C}/\mathbb{R}} |\eta|^{s/2}$) est une sous-représentation de $\mathrm{L}(\pi_\infty)$, avec $w \in \mathbb{Z}$ et $s \in \mathbb{C}$. En particulier, $\frac{s \pm w}{2}$ (resp. $\frac{s}{2}$) est un poids de π, par compatibilité de la paramétrisation de

5. Suivant Langlands, il est suggestif de noter $z^\lambda \overline{z}^\mu$ l'élément $(\frac{z}{|z|})^{\lambda - \mu} |z|^{\lambda + \mu}$ quand $z \in \mathbb{C}^\times$, et $\lambda, \mu \in \mathbb{C}$ sont tels que $\lambda - \mu \in \mathbb{Z}$.

Langlands au caractère infinitésimal. L'hypothèse $\mathrm{Poids}(\pi) \subset \frac{1}{2}\mathbb{Z}$ entraîne donc $s \in \mathbb{Z}$. Mais d'après Jacquet et Shalika, l'hypothèse $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ entraîne $|\mathrm{Re}\, s| < \frac{1}{2}$, ce qui montre $s = 0$. Ainsi, $\mathrm{L}(\pi_\infty)$ est somme directe de représentations de la forme I_w, 1 et $\epsilon_{\mathbb{C}/\mathbb{R}}$. La première assertion du (i) est alors conséquence de la compatibilité de la paramétrisation de Langlands au caractère infinitésimal. La congruence $|F| \equiv n \bmod 2$ s'en déduit. L'autodualité de π_∞ est conséquence de celle de $\mathrm{L}(\pi_\infty)$ (comme représentation de $\mathrm{W}_\mathbb{R}$) et de la compatibilité de la paramétrisation de Langlands au dual.

Pour le (ii), on remarque que $\mathrm{dét}(\mathrm{L}(\pi_\infty)) = 1$ (compatibilité au caractère central), et on conclut car $\mathrm{dét}(\mathrm{I}_w) = \epsilon_{\mathbb{C}/\mathbb{R}}^{w+1}$ et $\omega_i \equiv \mathrm{w}(\pi) \bmod 2$ pour tout i. Le (iii) découle du (ii) car si π est régulière et $n \equiv 0 \bmod 2$, le (i) montre que $F = \emptyset$ et $|E| = n/2$. Si $|\mathrm{Poids}(\pi)| = n - 1$, le (i) montre que 0 est l'unique poids double et $n \equiv 0 \bmod 2$, donc $\mathrm{w}(\pi) \equiv 0 \bmod 2$, $|F| = 2$ et $|E| = n/2-1$, puis (ii) entraîne (iv). $\square$

Remarque 2.14. Soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ telle que l'on a $\lambda - \mu \in \mathbb{Z}$ pour tous $\lambda, \mu \in \mathrm{Poids}(\pi)$. Alors une modification de l'argument donné au (i) montre que π est algébrique, *i.e.* $\mathrm{Poids}(\pi) \subset \frac{1}{2}\mathbb{Z}$. En effet, $\mathrm{L}(\pi_\infty)$ est somme directe de représentations de la forme $r_i \otimes |\eta|^{s_i/2}$, avec $|\mathrm{Re}\, s_i| < \frac{1}{2}$ et r_i isomorphe à I_w, 1 ou $\varepsilon_{\mathbb{C}/\mathbb{R}}$. Les poids de π correspondants au facteur $r_i \otimes |\eta|^{s_i/2}$ sont de la forme $\frac{s_i+m_i}{2}$, avec $m_i = \pm w$ ou 0 selon que l'on a $r_i \simeq \mathrm{I}_w$ ou non. Il suffit donc de voir que l'on a $s_i = s_j$ pour tout i, j, car ceci entraîne $s_i = 0$ pour tout i à cause de la relation $\mathrm{dét}(\mathrm{L}(\pi_\infty)) = 1$. Mais pour tout i, j on a $\frac{s_i+m_i}{2} - \frac{s_j+m_j}{2} \in \mathbb{Z}$ par hypothèse. Comme on a $m_i \in \mathbb{Z}$ et $|\mathrm{Re}\, s_i| < \frac{1}{2}$ pour tout i, on en tire $s_i - s_j \in \mathbb{Z}$ et $|\mathrm{Re}\,(s_i - s_j)| < 1$, puis $s_i = s_j$.

Cet énoncé et la proposition 2.10 montrent que si G un $\mathbb{Z}$-groupe classique, et si $\pi \in \Pi_{\mathrm{disc}}(G)$ est telle que $\mathrm{Inf}_{\pi_\infty} = \mathrm{Inf}_V$ pour un certain $V \in \mathrm{Irr}(\widehat{G})$, alors $\psi(\pi, \mathrm{St})$ satisfait certaines contraintes de nature combinatoire, que l'on résume dans l'énoncé suivant [CR12, Lemma 3.23].

Corollaire 2.15. *Soient G un $\mathbb{Z}$-groupe classique et $\mathrm{St} : \widehat{G} \to \mathrm{SL}_n$ la représentation standard de $\widehat{G}$. On suppose que $\psi = \oplus_{i=1}^r \pi_i[d_i] \in \mathfrak{X}_{\mathrm{AL}}(\mathrm{SL}_n)$, où $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour tout $i = 1, \ldots, k$, et que $\psi_\infty = \mathrm{St}(\mathrm{Inf}_V)$ où $V \in \mathrm{Irr}(G_\mathbb{C})$.*

(i) Si $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_{2g+1}(\mathbb{C})$, alors il existe un unique $1 \leq i_0 \leq k$ tel que $n_{i_0} d_{i_0} \equiv 1 \bmod 2$. De plus, $n_i d_i \equiv 0 \bmod 4$ pour tout $i \neq i_0$.

(ii) Si $\widehat{G}(\mathbb{C}) \simeq \mathrm{Sp}_{2g}(\mathbb{C})$, alors $n_i d_i \equiv 0 \bmod 2$ pour tout i.

(iii) Si $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_n(\mathbb{C})$ avec $n \equiv 0 \bmod 4$, alors $n_i d_i \equiv 0 \bmod 4$ pour tout i, excepté dans le cas exceptionnel suivant : 0 est une valeur propre double de $\mathrm{St}(\mathrm{c}_\infty(\pi))$ et il existe exactement 2 entiers i, disons i_1 et i_2, tels que $n_i d_i \not\equiv 0 \bmod 4$. Ils satisfont $n_{i_1} d_{i_1} n_{i_2} d_{i_2} \equiv 3 \bmod 4$.

Démonstration. Supposons $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_{2g+1}(\mathbb{C})$. Comme on a $\sum_{i=1}^k n_i d_i = 2g+1$, il existe au moins un entier i_0 tel que $n_{i_0} d_{i_0} \equiv 1 \bmod 2$. Pour un tel entier, $\mathrm{c}_\infty(\pi_{i_0})$ admet la valeur propre 0 car $\pi_{i_0} = \pi_{i_0}^\vee$ et n_{i_0} est impair. Comme d_{i_0} est également impair, $[d_{i_0}]_\infty$ admet également la valeur propre 0, ainsi donc que $(\pi_{i_0}[d_{i_0}])_\infty$. La première partie du (i) s'en déduit car 0 est une valeur propre simple de ψ_∞ d'après le cas I de l'analyse du §2.6. Pour la seconde, on observe que pour tout $i = 1, \ldots, k$ on a $\mathrm{w}(\pi_i) \equiv d_i - 1 \bmod 2$, ce qui conclut quand $\mathrm{w}(\pi_i)$ est impair, le cas échéant résultant du (iii) de la proposition 2.13.

Si $\widehat{G}(\mathbb{C}) \simeq \mathrm{Sp}_{2g}(\mathbb{C})$, la relation $\mathrm{w}(\pi_i) + d_i - 1 \equiv 1 \bmod 2$ pour tout $i = 1, \ldots, k$ montre que si d_i est impair alors $\mathrm{w}(\pi_i)$ l'est aussi, et donc n_i est pair (Proposition 2.11). Cela démontre le (ii).

Supposons enfin $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_n(\mathbb{C})$ avec $n \equiv 0 \bmod 4$. En particulier, $\mathrm{w}(\pi_i) \equiv d_i - 1 \bmod 2$ pour tout $i = 1, \cdots, k$. Si $\mathrm{w}(\pi_i) \equiv 1 \bmod 2$ (et donc $n_i \equiv 0 \bmod 2$), alors d_i est pair et donc $n_i d_i \equiv 0 \bmod 4$. Si $\mathrm{w}(\pi_i) \equiv 0 \bmod 2$ et $n_i \equiv 0 \bmod 2$, la proposition 2.13 (iii) assure que $n_i \equiv 0 \bmod 4$, sauf peut-être si π_i n'est pas régulière. Cette éventualité, si elle se produit, se produit pour un unique i_0 d'après la proposition 2.10, et dans ce cas $n_i \equiv 0 \bmod 2$ pour tout $i \neq i_0$, de sorte qu'au final $n_i d_i \equiv 0 \bmod 4$ pour tout $i \neq i_0$. Le résultat est conséquence dans ce cas de l'identité $n = \sum_{i=1}^k n_i d_i \equiv n_{i_0} d_{i_0} \bmod 4$ et de l'hypothèse $n \equiv 0 \bmod 4$. On peut donc écarter l'éventualité ci-dessus et supposer que π_i est régulière pour tout i, en particulier $n_i d_i \equiv 0 \bmod 4$ pour tout i tel que n_i est pair. Soit $J \subset \{1, \ldots, k\}$ l'ensemble des i tels que n_i est impair (auquel cas d_i est impair et $\mathrm{w}(\pi_i)$ est pair), on peut supposer J non vide. D'après l'argument donné au (i), cela entraîne que 0 est valeur propre double de ψ_∞ et que $|J| \leq 2$. On conclut car $n \equiv \sum_{j \in J} n_j d_j \bmod 4$. $\square$

2.16. Conjecture de Ramanujan et représentations galoisiennes

Un cas particulier des conjectures de Langlands, dans l'esprit de la fameuse conjecture de Shimura-Taniyama-Weil, est que l'ensemble des fonctions L de la forme $\mathrm{L}(s + \frac{\mathrm{w}(\pi)}{2} + m, \pi)$, où $m \in \mathbb{Z}$ et π parcourt les représentations algébriques des $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ pour $n \geq 1$, devrait coïncider exactement avec celui des fonctions L des motifs sur $\mathbb{Q}$ ayant bonne réduction partout (et

disons “à coefficients dans $\overline{\mathbb{Q}}$” et “simples”) [Lan79] [Mot91]. La conjecture de Ramanujan pour un π algébrique (§V.4.10) serait alors conséquence de l'existence du motif $\mathrm{M}(\pi)$ associé et des conjectures de Weil, démontrées par Deligne. Grâce aux travaux de nombreux mathématiciens (dont Eichler-Shimura, Deligne, Langlands, Kottwitz, Clozel, Harris-Taylor, Waldspurger, Ngô, Laumon, Clozel-Harris-Labesse, Shin, Chenevier-Harris) on dispose désormais d'une construction affaiblie de $\mathrm{M}(\pi)$ pour les π algébriques régulières et polarisées qui est toutefois suffisante pour démontrer le théorème suivant. Si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est une telle représentation, il est connu que le polynôme caractéristique [6]

$$\mathrm{P}_p(\pi) = \text{dét}(t - \mathrm{c}_p(\pi)\, p^{w(\pi)/2}) \ \in \ \mathbb{C}[t]$$

est à coefficients dans le sous-corps $\overline{\mathbb{Q}} \subset \mathbb{C}$ des nombres algébriques. Le théorème suivant est démontré dans [CHL11],[Shin11],[CH13] et [Clo13] (voir aussi [Ca12]).

Théorème 2.17. *Soit $\pi \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_n)$ algébrique et régulière.*

(i) π satisfait la conjecture de Ramanujan.

(ii) Soient $\ell \in \mathrm{P}$, $\overline{\mathbb{Q}}_\ell$ une clôture algébrique de $\mathbb{Q}_\ell$, et $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$ un plongement. Il existe une représentation continue $\rho_{\pi,\iota} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, unique à isomorphisme près, qui est semi-simple, non ramifiée hors de ℓ, et telle que

$$\text{dét}(t - \rho_{\pi,\iota}(\mathrm{Frob}_p)) = \iota(\mathrm{P}_p(\pi))$$

pour tout nombre premier $p \neq \ell$.

Dans cet énoncé, Frob_p désigne une classe de conjugaison d'éléments de Frobenius arithmétiques en p. On sait de plus d'après *loc. cit.* que la restriction de la représentation $\rho_{\pi,\iota}$ à $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ est cristalline au sens de Fontaine, de poids de Hodge-Tate les $\lambda + \frac{\mathrm{w}(\pi)}{2}$ où $\lambda \in \mathrm{Poids}(\pi)$. On conjecture que $\rho_{\pi,\lambda}$ est irréductible mais ce n'est connu que si $n \leq 5$ [CG13]. Observons que l'autodualité de π et le théorème de Cebotarev entraînent l'isomorphisme

$$\rho^*_{\pi,\iota} \simeq \rho_{\pi,\iota} \otimes \omega_\ell^{-\mathrm{w}(\pi)}, \tag{2.1}$$

où $\omega_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ désigne le caractère cyclomotique ℓ-adique. On sait démontrer que si $\mathrm{w}(\pi) \equiv 1 \bmod 2$ (resp. $\mathrm{w}(\pi) \equiv 0 \bmod 2$) alors il existe un accouplement $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-équivariant non-dégénéré $\rho_{\pi,\iota} \otimes \rho_{\pi,\iota} \to \omega_\ell^{\mathrm{w}(\pi)}$ qui est alterné (resp. symétrique) [BC11].

6. Dans la définition de $\mathrm{P}_p(\pi)$, il est sous-entendu que $\mathrm{c}_p(\pi)\, p^{w(\pi)/2}$ désigne la classe de conjugaison semisimple de $\mathrm{GL}_n(\mathbb{C})$ obtenue en faisant le produit de la classe $\mathrm{c}_p(\pi)$, vue dans $\mathrm{GL}_n(\mathbb{C}) \supset \mathrm{SL}_n(\mathbb{C})$, par le scalaire $p^{w(\pi)/2} \in \mathbb{C}^* \subset \mathrm{GL}_n(\mathbb{C})$.

Remarque 2.18. On s'attend à ce que le *(ii)* du théorème soit valable sans supposer π régulière ou autoduale. Des travaux récents de Harris-Lan-Taylor-Thorne et Sholze montrent que l'on peut s'affranchir de l'hypothèse d'autodualité (mais ne démontrent pas *(i)* pour ces π). Mentionnons enfin que si $\pi \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est algébrique et satisfait $|\mathrm{Poids}(\pi)| = n-1$ et $n \equiv 0 \bmod 4$, on sait également démontrer *(ii)* [Gol14], mais pas *(i)*.

Corollaire 2.19. *Soient G un $\mathbb{Z}$-groupe classique et $\pi \in \Pi_{\mathrm{disc}}(G)$ telle que π_∞ a même caractère infinitésimal qu'une représentation irréductible de dimension finie de $G(\mathbb{C})$. On suppose la conjecture d'Arthur-Langlands satisfaite pour (π, St). Si $\widehat{G}(\mathbb{C}) \simeq \mathrm{SO}_m(\mathbb{C})$, on suppose de plus $m \not\equiv 2 \bmod 4$.*

Soient $\ell \in \mathrm{P}$, $\overline{\mathbb{Q}}_\ell$ une clôture algébrique de $\mathbb{Q}_\ell$, et $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$ un plongement. Il existe une unique représentation continue, semi-simple, non ramifiée hors de ℓ

$$\rho_{\pi,\iota} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_{\mathrm{n}_{\widehat{G}}}(\overline{\mathbb{Q}}_\ell)$$

telle que $\forall p \in \mathrm{P} - \{\ell\}$, $\mathrm{dét}(t - \rho_{\pi,\iota}(\mathrm{Frob}_p)) = \iota(\mathrm{dét}(t - \ \mathrm{St}(\mathrm{c}_p(\pi))\, p^{\frac{\mathrm{w}_{\widehat{G}}}{2}}))$.

Le fait que $\det(t - \ \mathrm{St}(\mathrm{c}_p(\pi))\, p^{\frac{\mathrm{w}_{\widehat{G}}}{2}}) \in \overline{\mathbb{Q}}[t]$ fait partie de l'assertion (et peut se vérifier directement simplement dans les cas qui nous intéressent).

Démonstration. Écrivons $\psi(\pi, \mathrm{St}) = \oplus_{i=1}^{k} \pi_i[d_i]$. Le théorème 2.17 et la remarque ci-dessus s'appliquent aux représentations automorphes π_i, d'après la proposition 2.10 et le corollaire 2.15 (iii). Il suffit alors de poser

$$\rho_{\pi,\iota} = \bigoplus_{i=1}^{k} \rho_{\pi_i,\iota} \otimes (\oplus_{j=0}^{d_i-1} \omega_\ell^j) \otimes \omega_\ell^{\frac{\mathrm{w}_{\widehat{G}} - \mathrm{w}(\pi_i) + 1 - d_i}{2}}.$$

L'assertion d'unicité découle du théorème de Cebotarev. □

Spécifions ce résultat dans le cas de O_n, en utilisant la formule VI.(2.5).

Corollaire 2.20. *Soient $n \equiv 0 \bmod 8$ et $F \in \mathrm{M}_U(\mathrm{O}_n)$ une forme propre pour $\mathrm{H}(\mathrm{O}_n)$, disons telle que $\mathrm{T}_p(F) = \lambda_p F$ pour tout premier p. On suppose vérifée la conjecture d'Arthur-Langlands pour le couple (π, St) où $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_n)$ est la représentation engendrée par F (§VI.4.7).*

Soient $\ell \in \mathrm{P}$, $\overline{\mathbb{Q}}_\ell$ une clôture algébrique de $\mathbb{Q}_\ell$, et $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$ un plongement. Il existe une unique représentation continue, semi-simple, non ramifiée hors de ℓ, $\rho_{F,\iota} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, telle que $\forall p \in \mathrm{P}\backslash\{\ell\}$, $\mathrm{trace}\, \rho_{F,\iota}(\mathrm{Frob}_p) = \iota(\lambda_p)$.

2.21. Fonctions L de paires de représentations algébriques

Soient $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ et $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n'})$, la fonction L du couple $\{\pi, \pi'\}$ est définie par le produit eulérien

$$\mathrm{L}(s, \pi \times \pi') = \prod_{p \in \mathrm{P}} \mathrm{dét}(\mathrm{I}_{nn'} - p^{-s}\ \mathrm{c}_p(\pi) \otimes \mathrm{c}_p(\pi'))^{-1}.$$

C'est un cas particulier de la construction de Langlands rappelée au §V.4.9 où $\mathrm{G} = \mathrm{PGL}_n \times \mathrm{PGL}_{n'}$ et où r est le produit tensoriel des représentations standards de SL_n et $\mathrm{SL}_{n'}$. On retrouve $\mathrm{L}(s, \pi)$ lorsque $\pi' = 1$ est la représentation triviale de PGL_1. Cette fonction L a été étudiée par Rankin et Selberg quand $n = n' = 2$ et pour tout n, n' par Jacquet, Piatetski-Shapiro et Shalika. Ces auteurs démontrent que le produit eulérien ci-dessus est absolument convergent quand $\mathrm{Re}\, s > 1$ et qu'il admet un prolongement méromorphe à $\mathbb{C}$ tout entier. De plus, ce prolongement analytique est une fonction entière de s, sauf si $\pi' \simeq \pi^\vee$ auquel cas $s = 1$ en est l'unique pôle (et il est simple). Enfin, si $\mathrm{L}_\infty(s, \pi \times \pi')$ est un produit convenable de *facteurs* Γ, et si $\xi(s, \pi \times \pi') = \mathrm{L}_\infty(s, \pi \times \pi')\, \mathrm{L}(s, \pi \times \pi')$, on dispose d'une équation fonctionnelle de la forme

$$\xi(s, \pi \times \pi') \ = \ \varepsilon(\pi \times \pi')\, \xi(1 - s, \pi^\vee \times (\pi')^\vee),$$

où $\varepsilon(\pi \times \pi') \in \mathbb{C}^\times$. Nous renvoyons au cours de Cogdell [Cog04, §9] pour un exposé synthétique de ces résultats. Ajoutons que si π et π' sont autoduales, la relation $\xi(s, \pi \times \pi') = \varepsilon(\pi \times \pi')\, \xi(1 - s, \pi \times \pi')$ entraîne que $\varepsilon(\pi \times \pi') = \pm 1$ est un simple signe. Il nous sera utile de rappeler la recette précise pour $\varepsilon(\pi \times \pi')$ et $\mathrm{L}_\infty(s, \pi \times \pi')$. Ils ne dépendent tous deux que des composantes archimédiennes de π et π'. Pour simplifier, nous restreindrons cette discussion au cas où π et π' sont des représentations algébriques, le seul cas dont nous aurons besoin.

Soit $\mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_\mathbb{R})$ l'ensemble des classes d'isomorphisme de représentations continues et semi-simples de $\mathrm{W}_\mathbb{R}$, sur des $\mathbb{C}$-espaces vectoriels de dimension finie, qui sont triviales sur le sous-groupe $\mathbb{R}_{>0} \subset \mathbb{C}^\times$ de $\mathrm{W}_\mathbb{R}$. Les éléments de $\mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_\mathbb{R})$ sont exactement les sommes directes de représentations de la forme $1, \epsilon_{\mathbb{C}/\mathbb{R}}$ où I_w pour $w > 0$ (§2.12). Suivant Weil, il existe une unique manière d'associer à tout $\rho \in \mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_\mathbb{R})$ une racine 4ème de l'unité $\varepsilon(\rho) \in \{1, i, -1, -i\}$ et une fonction méromorphe $\Gamma(s, \rho)$ de la variable complexe s, de sorte que pour tout $\rho, \rho' \in \mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_\mathbb{R})$ on ait

$$\varepsilon(\rho \oplus \rho') = \varepsilon(\rho)\varepsilon(\rho'),\ \Gamma(s, \rho \oplus \rho') = \Gamma(s, \rho)\Gamma(s, \rho'),$$

ainsi que :

(i) $\varepsilon(\mathrm{I}_w) = i^{w+1}$ et $\Gamma(s, \mathrm{I}_w) = \Gamma_{\mathbb{C}}(s + \frac{w}{2})$ pour tout $w \geq 0$,

(ii) $\varepsilon(1) = 1$ et $\Gamma(s, 1) = \Gamma_{\mathbb{R}}(s)$.

On rappelle que $\Gamma(s) = \int_0^\infty e^{-t}\, t^s\, \frac{dt}{t}$ si $\operatorname{Re} s > 0$, et qu'il est coutume de poser

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}) \text{ et } \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s),$$

de sorte que $\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$ (formule de duplication). Noter que du cas $w = 0$ nous déduisons $\varepsilon(\epsilon_{\mathbb{C}/\mathbb{R}}) = i$ et $\Gamma(s, \epsilon_{\mathbb{C}/\mathbb{R}}) = \Gamma_{\mathbb{R}}(s+1)$.

Proposition 2.22. *Soient $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ et $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n'})$ algébriques. Posons $\rho = \mathrm{L}(\pi_\infty) \otimes \mathrm{L}(\pi'_\infty)$. On a*

$$\varepsilon(\pi \times \pi') = \varepsilon(\rho) \text{ et } \mathrm{L}_\infty(s, \pi \times \pi') = \Gamma(s, \rho).$$

Démonstration. L'énoncé portant sur sur $\mathrm{L}_\infty(s, \pi \times \pi')$ a bien un sens car $\mathrm{L}(\pi_\infty)$ et $\mathrm{L}(\pi'_\infty)$ sont dans $\mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_{\mathbb{R}})$ d'après la proposition 2.13 (i). L'assertion sur $\mathrm{L}_\infty(s, \pi \times \pi') = \Gamma(s, \rho)$ vaut par définition [Cog04, Ch. 9]. Une inspection des formules dans [Tat79, §3] montre que pour tout $\rho \in \mathrm{Rep}_{\mathrm{alg}}(\mathrm{W}_{\mathbb{R}})$ le nombre $\varepsilon(\rho)$ défini ci-dessus est exactement celui noté $\varepsilon(\rho, \psi, dx)$ *loc. cit.* où dx est la mesure de Lebesgue sur $\mathbb{R}$ et $\psi : \mathbb{R} \to \mathbb{C}^\times$ le caractère $x \mapsto e^{2i\pi x}$. Comme π et π' sont "non ramifiées à toutes les places finies" dans la terminologie usuelle, ce facteur $\varepsilon(\rho)$ coïncide donc avec $\varepsilon(\pi \times \pi')$ [Cog04, Ch. 9]. □

Il découle de ces formules que $\varepsilon(\pi \times \pi')$ est une fonction explicite des poids de π et π'. Il est utile à ce stade d'observer que $\mathrm{I}_w \otimes \epsilon_{\mathbb{C}/\mathbb{R}} \simeq \mathrm{I}_w$ et

$$\mathrm{I}_w \otimes \mathrm{I}_{w'} \simeq \mathrm{I}_{w+w'} \oplus \mathrm{I}_{|w-w'|}$$

pour tous entiers $w, w' \geq 0$. En particulier, $\varepsilon(\mathrm{I}_w \otimes \mathrm{I}_{w'}) = (-1)^{1+\mathrm{Max}(w,w')}$.

3. La formule de multiplicité d'Arthur

3.1. L'alternative symplectique-orthogonal d'Arthur

Rappelons que si H est un $\mathbb{C}$-groupe classique, nous notons n_H la dimension de sa représentation standard.

Théorème* 3.2. (Arthur) *Soit $\pi \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_n)$. Il existe un $\mathbb{Z}$-groupe classique de Chevalley G^π, unique à isomorphisme près, ayant les propriétés suivantes :*

(i) $\mathrm{n}_{\widehat{G^\pi}} = n$,

(ii) il existe $\pi' \in \Pi_{\mathrm{disc}}(G^\pi)$ *telle que* $\mathrm{c}(\pi) = \psi(\pi', \mathrm{St})$.

C'est un cas particulier de [Art13, Thm.1.4.1 & Thm. 1.5.2] (voir aussi la *méthode de descente* de Ginzburg, Rallis et Soudry [GRS11] pour un énoncé affaibli). Par définition, le groupe G^π satisfait $\mathrm{n}_{\widehat{G^\pi}} = n$. Lorsque n est impair, la seule possibilité est donc $G^\pi \simeq \mathrm{Sp}_{n-1}$, mais lorsque n est pair G^π est isomorphe à $\mathrm{SO}_{\frac{n}{2},\frac{n}{2}}$ ou $\mathrm{SO}_{\frac{n}{2}+1,\frac{n}{2}}$ (exclusivement). Si $n = 2$ alors $G^\pi \simeq \mathrm{SO}_{2,1} \simeq \mathrm{PGL}_2$, étant donné que $\mathrm{SO}_{1,1} \simeq \mathbb{G}_m$ n'est pas semi-simple. Lorsque $n = 1$, de sorte que π est la représentation triviale de PGL_1, on a enfin $G^\pi = \mathrm{SO}_{1,0}$ (le $\mathbb{Z}$-groupe trivial).

La représentation $\pi \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_n)$ est dite orthogonale si $\widehat{G^\pi}(\mathbb{C}) \simeq \mathrm{SO}_m(\mathbb{C})$ pour un certain entier $m \geq 1$ (ou encore si $\mathrm{w}_{\widehat{G^\pi}} = 0$ dans les notations du §VIII), et symplectique sinon.

Proposition* **3.3.** *Soit* $\pi \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_n)$ *algébrique. On suppose que* π *possède au moins un poids qui soit valeur propre simple de* $\mathrm{c}_\infty(\pi)$*. Alors* π *est symplectique si, et seulement si,* $\mathrm{w}(\pi) \equiv 1 \bmod 2$.

Démonstration. C'est une variante de [CR12, Cor. 3.8]. D'après Arthur [Art13, Thm. 11.4.2], la représentation $\mathrm{L}(\pi_\infty)$ de $\mathrm{W}_\mathbb{R}$ sur $\mathbb{C}^n$ préserve une forme bilinéaire non-dégénérée b, qui est alternée si π est symplectique et symétrique sinon. L'hypothèse faite sur π entraîne qu'au moins une des représentations $1, \varepsilon_{\mathbb{C}/\mathbb{R}}$, où I_w avec $w > 0$, intervient dans $\mathrm{L}(\pi_\infty)$ avec multiplicité 1 (Proposition 2.13 (i)) ; notons $E \subset \mathbb{C}^n$ le sous-espace correspondant. Chacune de ces représentations étant irréductible et autoduale, la restriction de b à E est non-dégénérée. Étant donné la relation $\det \mathrm{I}_w = \varepsilon_{\mathbb{C}/\mathbb{R}}^{w+1}$, on constate que b est alternée si, et seulement si, on a $E \simeq \mathrm{I}_w$ avec $w \equiv 1 \bmod 2$. □

Les résultats d'Arthur admettent également des conséquences concernant les fonctions L de paires de représentations autoduales : voir [Art13, Thm. 1.5.3]. En particulier, si $\pi \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_n)$ et $\pi' \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{GL}_m)$ sont soit toutes deux symplectiques, soit toutes deux orthogonales, alors $\varepsilon(\pi \times \pi') = 1$ (c'est un Théorème*). Dans le cas où $\pi' = 1$, on en déduit que

$$\varepsilon(\pi) := \varepsilon(\pi \times 1)$$

vaut 1 si π est orthogonale. Quand π est algébrique autoduale et orthogonale, cela donne une relation non-triviale sur ses poids : voir [CR12, Prop. 1.8].

3.4. La formule de multiplicité : hypothèses générales

Soient G un $\mathbb{Z}$-groupe classique et $n = \mathrm{n}_{\widehat{G}}$ la dimension de la représentation standard St de $\widehat{G}$. Fixons un entier $k \geq 1$, ainsi que pour tout $i = 1, \ldots, k$ un couple (π_i, d_i) où $d_i \geq 1$ est un entier et $\pi_i \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$. On suppose que $n = \sum_{i=1}^{k} n_i d_i$ et on considère l'élément

$$\psi = \oplus_{i=1}^{k} \pi_i[d_i]$$

de $\mathcal{X}(\mathrm{SL}_n)$.

Soit U une représentation irréductible unitaire de $G(\mathbb{R})$. La formule de multiplicité d'Arthur, conjecturée en toute généralité dans [Art89], et démontrée dans [Art13] lorsque G est un groupe classique de Chevalley, donne une condition nécessaire est suffisante pour qu'il existe un $\pi \in \Pi_{\mathrm{disc}}(G)$ telle que $\pi_\infty \simeq U$ et $\psi(\pi, \mathrm{St}) = \psi$. Elle s'exprime sous la forme d'une formule d'orthogonalité entre deux caractères sur un 2-groupe abélien fini élémentaire C_ψ, que nous allons expliciter dans les paragraphes qui suivent. Le premier de ces caractères, noté ε_ψ et décrit au §3.5, est indépendant de U. Il est introduit en grande généralité par Arthur dans [Art89] et tient compte des signes $\varepsilon(\pi_i \times \pi_j)$ (§2.21) selon une combinatoire bien précise. Le second de ces caractères, qui est le plus fin des deux, a son origine qui remonte aux travaux de Shelstad [She82] (voir aussi [KZ77, LL79, LS87, AJ87, Art89, Art13, ABV92, She08a, She14]). Il ne dépend essentiellement que de U et d'un certain morphisme $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \to \widehat{G}$ associé à ψ ; il sera décrit aux §3.8 et §4.14.

Les travaux d'Arthur [Art13] sont très généraux, et nous ne les appliquerons que dans des cas très particuliers, pour lesquels les énoncés sont sensiblement simplifiés. Nous ferons les deux hypothèses suivantes :

(H1) $n \not\equiv 2 \bmod 4$,

(H2) $\psi_\infty = \mathrm{St}(\mathrm{Inf}_V)$ où $V \in \mathrm{Irr}(G_{\mathbb{C}})$ (§2.6).

La première hypothèse n'est une contrainte que si G est un groupe spécial orthogonal pair. Dans ce cas, $G(\mathbb{R})$ a pour signature (p, q) avec $p \equiv q \bmod 8$ d'après le Scholie II.2.2 (b), de sorte que l'hypothèse s'écrit également $p \equiv q \equiv 0 \bmod 2$ (elle est bien sûr satisfaite si $G = \mathrm{SO}_n$ avec $n \equiv 0 \bmod 8$).

La seconde hypothèse, portant sur ψ_∞, a été explicitée au §2.6 (cas I, II ou III), où nous en avons donné quelques conséquences de nature combinatoire portant sur les π_i. En particulier :

(a) pour tout $i = 1, \ldots, k$, π_i est autoduale algébrique (et même régulière, hormis dans un cas exceptionnel),

(b) pour tout $i = 1, \ldots, k$, $\mathrm{w}(\pi_i) + d_i - 1 \equiv \mathrm{w}_{\widehat{G}} \bmod 2$,

(c) pour tous $i \neq j$, si $(n_i, d_i) = (n_j, d_j)$ alors $\pi_j \not\simeq \pi_i$.

En effet, (a) et (b) découlent de la proposition 2.10. Le point (c), qui n'est non-trivial sous (H2) que si $n_i = n_j = 1$ et $d_i = d_j = 1$, découle de (H1) et du corollaire 2.15 (iii).

3.5. Le groupe C_ψ et le caractère ε_ψ

On conserve les hypothèses et notations du paragraphe précédent. D'après le (b) ci-dessus et la proposition 3.3, observons qu'il existe un $\mathbb{C}$-morphisme

$$\nu : \mathrm{SL}_2 \times \prod_{i=1}^{k} \widehat{G^{\pi_i}} \longrightarrow \widehat{G}$$

tel que la $\mathbb{C}$-représentation $\mathrm{St} \circ \nu$, d'espace sous-jacent $V \simeq \mathbb{C}^n$, se décompose comme somme directe

$$V = \oplus_{i=1}^{k} V_i,$$

où V_i est isomorphe au produit tensoriel de la représentation $\mathrm{Sym}^{d_i - 1}\mathrm{St}_2$ de SL_2 par la représentation standard de $\widehat{G^{\pi_i}}$ (les autres facteurs $\widehat{G^{\pi_j}}$ pour $j \neq i$ agissant trivialement). Un tel morphisme ν n'est pas unique : il l'est seulement modulo composition à l'arrivée par un automorphisme du $\mathbb{C}$-groupe $\widehat{G}$. Il sera fixé une fois pour toutes dans ce qui suit ; nous discuterons en temps voulu de la dépendance en ce choix dans la formule finale.

Soit C_ν le centralisateur dans $\widehat{G}(\mathbb{C})$ de l'image de ν. La représentation St l'identifie au sous-groupe de $\mathrm{SL}(V)$ constitué des éléments g préservant chaque V_i et tels que $g_{|V_i} = \epsilon_i \, \mathrm{Id}_{V_i}$, où $(\epsilon_i) \in \{\pm 1\}^k$. Comme on a $\dim(V_i) = n_i d_i$, le groupe C_ν est donc dans une suite exacte naturelle

$$1 \longrightarrow \mathrm{C}_\nu \xrightarrow{\mathrm{St}} \{\pm 1\}^k \xrightarrow{\delta} \{\pm 1\},$$

où $\delta(\epsilon_i) = \prod_{i=1}^{k} \epsilon_i^{n_i d_i}$. Cette description abstraite de C_ν est manifestement indépendante du choix de ν, c'est pourquoi nous le noterons simplement C_ψ.

Le centre $\mathrm{Z}_{\widehat{G}}$ de $\widehat{G}(\mathbb{C})$ est un sous-groupe de C_ψ. Notons $I \subset \{1, \ldots, k\}$ le sous-ensemble constitué des entiers i tels que $n_i d_i \equiv 0 \bmod 2$, et pour tout $i \in I$ notons

$$s_i \in \mathrm{C}_\psi$$

l'élément agissant par -1 sur V_i et 1 sur V_j pour $j \neq i$. D'après (H1) et (H2), le corollaire 2.15 s'applique. Il entraîne $|I| \geq k - 1$ ainsi que le lemme suivant.

Lemme 3.6. C_ψ *est engendré par* $\mathrm{Z}_{\widehat{G}}$ *et les* s_i *pour* $i \in I$.

Arthur définit ensuite [Art13, p. 47] un homomorphisme $\varepsilon_\psi : \mathrm{C}_\psi \longrightarrow \{\pm 1\}$ trivial sur $\mathrm{Z}_{\widehat{G}}$. Pour le décrire, il suffit de donner sa valeur sur l'élément s_i pour $i \in I$. Arthur considère pour cela la restriction à ν de la représentation adjointe de $\widehat{G}$ sur $\mathrm{Lie}\,\widehat{G}$, c'est donc une représentation du produit $\mathrm{C}_\nu \times \mathrm{SL}_2 \times (\prod_{i=1}^k \widehat{G^{\pi_i}})$. L'entier $i \in I$ étant fixé, c'est un exercice de vérifier que le sous-espace de $\mathrm{Lie}\,\widehat{G}$ sur lequel s_i agit par -1 est isomorphe à $\bigoplus_{j \neq i} V_j \otimes V_i$ comme représentation de $\mathrm{SL}_2 \times (\prod_{i=1}^k \widehat{G^{\pi_i}})$. Mais si pour $d \geq 1$ on note r_d la représentation $\mathrm{Sym}^{d-1}\mathrm{St}_2$ de SL_2 (où St_2 désigne la représentation standard, §VI.4.4), et si $a \geq b$ sont des entiers ≥ 1, il est bien connu que

$$r_a \otimes r_b \simeq \oplus_{i=1}^b r_{a-b+2i-1};$$

en particulier, $r_a \otimes r_b$ admet $\mathrm{Min}(a,b)$ facteurs irréductibles pour tout $a, b \geq 1$. La recette pour ε_ψ décrite par Arthur *loc. cit.* prend donc la forme explicite suivante, où l'on a incorporé le résultat* d'Arthur affirmant que $\varepsilon(\pi \times \pi') = 1$ si π et π' sont simultanément symplectiques ou orthogonales.

Proposition-Définition 3.7. *Il existe un unique homomorphisme* $\varepsilon_\psi : \mathrm{C}_\psi \to \{\pm 1\}$ *trivial sur* $\mathrm{Z}_{\widehat{G}}$ *et tel que* $\forall i \in I$, $\varepsilon_\psi(s_i) = \prod_{j \neq i} \varepsilon(\pi_i \times \pi_j)^{\mathrm{Min}(d_i, d_j)}$.

Précisons que le produit ci-dessus est pris sur tous les $j = 1, \ldots, k$ distincts de i. D'après le résultat* d'Arthur sus-cité, on peut même se restreindre aux entiers $j = 1, \ldots, k$ tels que $\mathrm{w}(\pi_j) \not\equiv \mathrm{w}(\pi_i) \bmod 2$. Pour justifier directement l'existence de ε_ψ, le lecteur observera que les $s_i, i \in I$, sont linéairement indépendants sur $\mathbb{F}_2$ dans C_ψ, et que s'ils engendrent un sous-groupe rencontrant non trivialement $\mathrm{Z}_{\widehat{G}}$, alors $|I| = k$ et $\mathrm{Z}_{\widehat{G}}$ est engendré par $\prod_{i=1}^k s_i$.

3.8. Le cas des groupes de Chevalley

On maintient les notations et hypothèses des §3.4 et §3.5. Arthur considère un morphisme de groupes

$$\nu_\infty : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_\mathbb{R} \to \widehat{G}(\mathbb{C})$$

défini de la manière suivante.

Pour tout $i = 1, \ldots, k$, un argument similaire à celui donné dans la démonstration de la proposition 3.3, basé sur la proposition 2.13, assure qu'il existe un morphisme de groupes $\mu_i : \mathrm{W}_\mathbb{R} \to \widehat{G^{\pi_i}}(\mathbb{C})$ dont la composée avec la représentation standard de $\widehat{G^{\pi_i}}$ est isomorphe à $\mathrm{L}((\pi_i)_\infty)$.

Cette propriété détermine uniquement μ_i modulo composition à l'arrivée par $\mathrm{Aut}(\widehat{G^{\pi_i}})$, mais il sera commode de fixer arbitrairement un tel μ_i. Le morphisme ν_∞ est par définition la composée du morphisme diagonal $(g, w) \mapsto (g, \prod_{i=1}^k \mu_i(w))$ par le morphisme ν. La $\mathrm{Aut}(\widehat{G})$-orbite de ν_∞ dans l'ensemble $\mathrm{Hom}(\mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_\mathbb{R}, \widehat{G}(\mathbb{C}))$ sera notée $\psi_\mathbb{R}$; il ne faudra pas la confondre avec la classe de conjugaison semi-simple ψ_∞, qui renferme une information nettement moins fine. L'orbite $\psi_\mathbb{R}$ ne dépend que de ψ (et non du choix de ν ou des μ_i), et même mieux, que de l'ensemble des k couples $((\pi_i)_\infty, d_i)$ pour $i = 1, \dots k$.

Soit C_{ν_∞} le centralisateur de l'image de ν_∞ dans $\widehat{G}$. Il est évident que

$$\mathrm{C}_\nu \subset \mathrm{C}_{\nu_\infty}.$$

Il est aisé de décrire C_{ν_∞} à la manière de la description précédente de C_ν.

Lemme 3.9. *La représentation* $\mathrm{St} \circ \nu_\infty$ *de* $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_\mathbb{R}$ *est semi-simple, sans multiplicités, et tous ses constituants irréductibles sont autoduaux. En particulier,* C_{ν_∞} *est un* 2*-groupe abélien fini élémentaire.*

Démonstration. C'est [CR12, Lemma 3.15]. La seconde assertion découle de la première. Le seul point de cette dernière qui ne découle pas immédiatement des définitions et de (H2) est l'assertion de multiplicité 1, qui est non triviale quand ψ_∞ admet 0 pour valeur propre double (et donc $\mathrm{w}_{\widehat{G}} = 0$). Dans ce cas, $\mathrm{St} \circ \nu_\infty$ pourrait alors contenir soit 1, soit $\epsilon_{\mathbb{C}/\mathbb{R}}$ avec multiplicité 2 (avec action triviale du facteur $\mathrm{SL}_2(\mathbb{C})$ dans les deux cas). D'après (H1), le corollaire 2.15 (iii) et la proposition 2.13 (iii), ces caractères ne peuvent toutefois intervenir avec multiplicité 2 dans un même $\mathrm{L}((\pi_i)_\infty)$. Ils apparaissent donc (nécessairement avec multiplicité 1) dans $\mathrm{L}((\pi_i)_\infty)$ et $\mathrm{L}((\pi_j)_\infty)$ avec $i \neq j$, avec de plus $d_i = d_j = 1$ et n_i et n_j sont impairs et non congrus modulo 4 d'après *loc. cit.* Mais comme $\mathrm{w}(\pi_i) = \mathrm{w}(\pi_j) = 0$, cela contredit la proposition 2.13 (ii). □

Afin de poursuivre l'analyse de la formule d'Arthur, nous supposerons dans un premier temps que $G = \mathrm{Sp}_{2g}$ ou $\mathrm{SO}_{r+1,r}$. Notons $\Pi_{\mathrm{unit}}(H)$ l'ensemble des classes d'isomorphisme de représentations unitaires irréductibles du groupe de Lie réel H. Arthur [Art13, Thm. 1.5.1] associe à ν_∞ un ensemble fini [7] $\Pi(\nu_\infty)$ muni de deux applications

$$\Pi_{\mathrm{unit}}(G(\mathbb{R})) \xleftarrow{\iota} \Pi(\nu_\infty) \xrightarrow{u \mapsto \chi_u} \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_{\nu_\infty}, \mathbb{C}^\times).$$

7. Précisons que ce que nous notons ici $\psi_\mathbb{R}$, C_{ν_∞} et $\Pi(\psi_\mathbb{R})$ est noté respectivement ψ, $\mathcal{S}_\psi$ et $\widetilde{\Pi}_\psi$ dans l'énoncé d'Arthur ; de plus il ne donne pas de nom à ι et si $u \in \Pi(\nu_\infty)$ il note $x \mapsto \langle x, u \rangle$ le caractère χ_u. L'image de ι, un sous-ensemble fini de $\Pi_{\mathrm{unit}}(G(\mathbb{R}))$, est communément appelé *paquet d'Arthur associé à* $\psi_\mathbb{R}$.

L'ensemble $\Pi(\nu_\infty)$ et ι, ainsi en fait que χ une fois clarifiée la dépendence de C_{ν_∞} en le choix de ν_∞, ne dépendent que de la classe de $\mathrm{Aut}(\widehat{G})$-conjugaison $\psi_\mathbb{R}$ de ν_∞, c'est pourquoi nous noterons aussi $\Pi(\psi_\mathbb{R})$ pour $\Pi(\nu_\infty)$. Arthur démontre une propriété qui caractérise entièrement le triplet $(\Pi(\psi_\mathbb{R}), \iota, \chi)$ [Art13, Thm. 2.2.1], sans toutefois expliciter concrètement ce triplet. Nous reviendrons sur ce point au paragraphe suivant. Comme l'explique Arthur [Art13, p. 42], on s'attend à ce que ι soit injective, de sorte que $\Pi(\psi_\mathbb{R})$ serait défini comme une partie de $\Pi_{\mathrm{unit}}(G(\mathbb{R}))$ et ι serait simplement ignorée.

Théorème* 3.10. (Formule de multiplicité d'Arthur [Art13, Thm. 1.5.2]) *Supposons que $G = \mathrm{Sp}_{2g}$ ou $\mathrm{SO}_{r+1,r}$. Fixons $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{\mathrm{n}_{\widehat{G}}})$ satisfaisant (H2) ainsi que $U \in \Pi_{\mathrm{unit}}(G(\mathbb{R}))$.*

Soit $\pi \in \Pi(G)$ l'unique représentation telle que $\pi_\infty \simeq U$ et $\mathrm{St}(\mathrm{c}_p(\pi)) = \psi_p$ pour tout premier p. Alors $\pi \in \Pi_{\mathrm{disc}}(G)$ si, et seulement si, il existe $u \in \Pi(\psi_\mathbb{R})$ tel que

$$U = \iota(u) \text{ et } \chi_{u|\mathrm{C}_\nu} = \varepsilon_\psi.$$

Plus précisément, la multiplicité $\mathrm{m}(\pi)$ de π dans $\mathcal{A}_{\mathrm{disc}}(G)$ (§IV.3.2) est exactement le nombre des éléments $u \in \Pi(\psi_\mathbb{R})$ ayant la propriété ci-dessus.

Décryptons cet énoncé. Observons d'abord que l'existence et l'unicité de π viennent de ce que si $G = \mathrm{Sp}_{2g}$ ou $\mathrm{SO}_{r+1,r}$, l'application $\mathrm{St} : \widehat{G}(\mathbb{C})_{\mathrm{ss}} \to \mathrm{SL}_{\mathrm{n}_{\widehat{G}}}(\mathbb{C})_{\mathrm{ss}}$ est injective et d'image l'ensemble des classes égales à leur inverse. En particulier, la représentation π de l'énoncé est l'unique candidate possible telle que $\pi_\infty \simeq U$ et $\psi(\pi, \mathrm{St}) = \psi$. Le théorème affirme d'abord que si U n'est pas dans $\iota(\Pi(\psi_\mathbb{R}))$ alors $\mathrm{m}(\pi) = 0$. Supposons donc que $U \in \iota(\Pi(\psi_\mathbb{R}))$, et supposons également pour simplifier que l'on sache que $\iota^{-1}(U)$ est un singleton $\{u\}$. Le théorème affirme alors que $\mathrm{m}(\pi) \neq 0$ si et seulement si $\chi_{u|\mathrm{C}_\psi} = \varepsilon_\psi$, auquel cas $m(\pi) = 1$.

Pour des raisons d'exhaustivité, décrivons maintenant le cas restant du groupe $G = \mathrm{SO}_{r,r}$, où $r \equiv 0 \mod 2$ par l'hypothèse (H1). Dans ce cas, $\widehat{G}(\mathbb{C}) = \mathrm{SO}_{2r}(\mathbb{C})$. L'image de l'application $\mathrm{St} : \widehat{G}(\mathbb{C})_{\mathrm{ss}} \to \mathrm{SL}_{2r}(\mathbb{C})_{\mathrm{ss}}$ est encore l'ensemble des classes égales à leur inverse, mais elle n'est plus injective : deux éléments semi-simples de $\mathrm{SO}_{2r}(\mathbb{C})$ conjugués dans $\mathrm{SL}_{2r}(\mathbb{C})$ ne sont pas toujours conjugués dans $\mathrm{SO}_{2r}(\mathbb{C})$, mais seulement dans $\mathrm{O}_{2r}(\mathbb{C})$. Les fibres non vides de l'application ci-dessus sont donc exactement les orbites de l'action naturelle de

$$\mathrm{O}_{2r}(\mathbb{C})/\mathrm{SO}_{2r}(\mathbb{C}) = \mathrm{Out}(\widehat{G}) = \mathbb{Z}/2\mathbb{Z}$$

sur $\widehat{G}(\mathbb{C})_{\mathrm{ss}}$. Un phénomène analogue se produit pour $\mathrm{St} : \widehat{\mathfrak{g}}_{\mathrm{ss}} \to (\mathfrak{sl}_{2r})_{\mathrm{ss}}$. L'action de $\mathrm{O}_{r,r}(\mathbb{R})$ par conjugaison sur $G(\mathbb{R})$ définit également une action de

$\mathbb{Z}/2\mathbb{Z} = \mathrm{O}_{r,r}(\mathbb{R})/\mathrm{SO}_{r,r}(\mathbb{R})$ sur $\Pi_{\mathrm{unit}}(G(\mathbb{R}))$, dont l'ensemble des orbites est noté par Arthur $\widetilde{\Pi}_{\mathrm{unit}}(G(\mathbb{R}))$. Le théorème [Art13, Thm. 1.5.1] d'Arthur associe alors à ν_∞ un triplet $(\Pi(\psi_{\mathbb{R}}), \iota, \chi)$ comme plus haut, à la seule différence près que ι est cette-fois ci une application $\Pi(\psi_{\mathbb{R}}) \to \widetilde{\Pi}_{\mathrm{unit}}(G(\mathbb{R}))$.

Théorème* **3.11.** (Formule de multiplicité d'Arthur pour $\mathrm{SO}_{r,r}$ [Art13, Thm. 1.5.2]) *Supposons que $G = \mathrm{SO}_{r,r}$ avec $r \equiv 0 \bmod 2$. Fixons $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2r})$ satisfaisant (H2) ainsi que $U \in \widetilde{\Pi}_{\mathrm{unit}}(G(\mathbb{R}))$. Soit $E \subset \Pi(G)$ l'ensemble des $\pi \in \Pi(G)$ telles que $\psi(\pi, \mathrm{St}) = \psi$ et $\pi_\infty \in U$. Soit $F \subset \Pi(\psi_{\mathbb{R}})$ l'ensemble des éléments u tels que $U \in \iota(u)$ et $\chi_{u|\mathrm{C}_\nu} = \varepsilon_\psi$. Alors*

$$\sum_{\pi \in E} \mathrm{m}(\pi) = m_\psi |F|,$$

où $m_\psi = 1$ à moins que $\psi = \oplus_{i=1}^k \pi_i[d_i]$ avec $d_i \equiv 0 \bmod 2$ pour tout i, auquel cas $m_\psi = 2$.

(Arthur s'attend encore à l'injectivité de ι, et donc à ce que $|F| \in \{0, 1\}$). En vue d'appliquer les théorèmes 3.10 ou 3.11, il est évidemment crucial d'en savoir plus sur le triplet $(\Pi(\psi_{\mathbb{R}}), \iota, \chi)$. L'objectif des paragraphes qui suivent est de rappeler des choses connues à ce sujet.

4. Séries discrètes

4.1. Séries discrètes, d'après Harish-Chandra.

Les résultats de ce paragraphe sont dûs à Harish-Chandra. Il sera commode de renvoyer à l'ouvrage de Knapp [Kna86] pour les démonstrations.

Soit H un $\mathbb{R}$-groupe semi-simple. On rappelle que $\pi \in \Pi_{\mathrm{unit}}(H(\mathbb{R}))$ est une *série discrète* si elle intervient comme sous-représentation de la représentation régulière $\mathrm{L}^2(H(\mathbb{R}))$ [Kna86, Ch. IX §3]. Harish-Chandra a démontré que $H(\mathbb{R})$ admet des séries discrètes si, et seulement si, H possède un *tore maximal anisotrope*, c'est-à-dire un $\mathbb{R}$-sous-groupe $T \subset H$ tel que $T_{\mathbb{C}} \subset H_{\mathbb{C}}$ est un tore maximal et $T(\mathbb{R})$ est compact [Kna86, Thm. 12.20]. C'est le cas de Sp_{2g}, ainsi que du groupe spécial orthogonal réel de signature (p, q) si et seulement si $pq \equiv 0 \bmod 2$ ou $p + q \equiv 1 \bmod 2$, de sorte que la condition (H1) du §3.4 est en fait équivalente à demander que $G(\mathbb{R})$ admet des séries discrètes.

On suppose désormais que $H(\mathbb{R})$ admet des séries discrètes. Les tores maximaux anisotropes de H forment une seule orbite sous l'action de conjugaison de $H(\mathbb{R})$; fixons l'un d'entre eux que nous notons T. Introduisons quelques

objets associés au couple (H, T). Les caractères et cocaractères de $T_{\mathbb{C}}$ étant tous définis sur $\mathbb{R}$, on notera simplement $\mathrm{X}_*(T)$ (resp. $\mathrm{X}^*(T)$) pour $\mathrm{X}_*(T_{\mathbb{C}})$ (resp. $\mathrm{X}^*(T_{\mathbb{C}})$). Soient

$$\Phi = \Phi(H_{\mathbb{C}}, T_{\mathbb{C}}) \subset \mathrm{X}^*(T) \text{ et } W = \mathrm{W}(H_{\mathbb{C}}, T_{\mathbb{C}})$$

le groupe de Weyl de Φ. Posons également

$$W_{\mathrm{r}} = \mathrm{W}(H, T) \overset{\text{déf.}}{=} \mathrm{N}_{H(\mathbb{R})}(T(\mathbb{R}))/T(\mathbb{R}),$$

où $\mathrm{N}_{H(\mathbb{R})}(T(\mathbb{R}))$ est le normalisateur de $T(\mathbb{R})$ dans $H(\mathbb{R})$ (*groupe de Weyl réel* de (H, T)). On dispose enfin d'un unique sous-groupe compact maximal K de $H(\mathbb{R})$ contenant $T(\mathbb{R})$ (et donc $\mathrm{N}_{H(\mathbb{R})}(T(\mathbb{R}))$) et l'on note $\Phi_{\mathrm{c}} \subset \Phi$ le système de racines (dites *compactes*) de K relativement à $T(\mathbb{R})$. On dispose d'inclusions naturelles $\mathrm{W}(\Phi_{\mathrm{c}}) \subset W_{\mathrm{r}} \subset W$, qui sont strictes en général.

Si $V \in \mathrm{Irr}(H_{\mathbb{C}})$, notons $\Pi_V \subset \Pi_{\mathrm{unit}}(H(\mathbb{R}))$ l'ensemble des séries discrètes ayant même caractère infinitésimal que V. Harish-Chandra a démontré que toute série discrète de $H(\mathbb{R})$ appartient à Π_V, pour un unique V. Si Δ est une base du système de racines Φ, il a défini une représentation $\pi_{\Delta,V} \in \Pi_V$, uniquement déterminée par les valeurs prises par son caractère $\Theta_{\Delta,V}$ sur l'ensemble $T(\mathbb{R})_{\mathrm{reg}} \subset T(\mathbb{R})$ des éléments $t \in T(\mathbb{R})$ tels que $\alpha(t) \neq 1$ pour tout $\alpha \in \Phi$. Précisément, en notant t^{μ} pour $\mu(t)$ si $t \in T(\mathbb{R})$ et $\mu \in \mathrm{X}^*(T)$,

$$\Theta_{\Delta,V}(t) = (-1)^{\frac{1}{2}\dim H(\mathbb{R})/K} \frac{\sum_{w \in W_{\mathrm{r}}} \varepsilon(w) t^{w(\lambda+\rho)-\rho}}{\prod_{\alpha \in \Phi^+}(1 - t^{-\alpha})}, \quad \forall t \in T(\mathbb{R})_{\mathrm{reg}},$$

où $\lambda \in \mathrm{X}^*(T)$ désigne le plus haut poids de V relativement au sous-groupe de Borel $T_{\mathbb{C}} \subset B \subset H_{\mathbb{C}}$ défini par Δ, $\Phi^+ \subset \Phi$ est le système positif défini par Δ, et 2ρ la somme des éléments de Φ^+ [Kna86, Thm. 9.20 & 12.7]. Il démontre que tout élément de Π_V est de la forme $\pi_{\Delta,V}$, et que $\pi_{\Delta,V} \simeq \pi_{\Delta',V}$ si, et seulement si, $\Delta' = w(\Delta)$ avec $w \in W_{\mathrm{r}}$ [Kna86, Thm. 12.21]. En particulier, $|\Pi_V| = |W_{\mathrm{r}} \backslash W|$ est indépendant de V.

Supposons qu'il existe un sous-groupe $S \subset K$ isomorphe à $\mathbb{S}^1$ et dont l'action adjointe sur $\mathrm{Lie}\, H(\mathbb{R})$ admet exactement $\mathrm{Lie}(K)$ pour points fixes (en particulier, S est dans le centre de la composante neutre de K). Cela se produit par exemple quand H est Sp_{2g} ou le groupe spécial orthogonal de signature $(p, 2)$ avec $p \geq 1$. Dans ce cas, $H(\mathbb{R})$ possède des séries discrètes *holomorphes* [Kna86, Chap. VI], et nous en avons déjà rencontré des exemples au §VI.3.4. Dans la classification d'Harish-Chandra ce sont exactement les représentations $\pi_{\Delta,V}$ obtenues lorsque Δ est la base d'un système positif de

la forme $\{\alpha \in \Phi, \varphi(\alpha) > 0\}$ où $\varphi : \mathrm{X}^*(T) \to \mathbb{R}$ est une forme linéaire telle que

$$\forall\, \alpha \in \Phi_c,\ \forall\, \beta \in \Phi - \Phi_c, \quad 0 < |\varphi(\alpha)| < |\varphi(\beta)|$$

(les racines compactes "sont plus petites" que les racines non compactes), d'après la remarque suivant [Kna86, Thm. 9.20].

4.2. Paramétrisation canonique de Shelstad, cas des groupes déployés

Il sera nécessaire de rappeler une seconde paramétrisation des éléments de Π_V, $V \in \mathrm{Irr}(H_{\mathbb{C}})$ étant fixé, qui comme nous l'avons déjà dit au §3.4 est due à Shelstad, intervenant dans l'énoncé de la formule de multiplicité d'Arthur. Elle doit son origine aux identités existantes entre les caractères des séries discrètes de H et ceux des séries discrètes d'une collection de $\mathbb{R}$-groupes associés, appelés *endoscopiques* par Langlands [She82]. Une exposition détaillée de ces identités dépasserait très nettement le cadre de ce mémoire (et la compétence des auteurs), et nous ne nous y aventurerons pas. Nous suivrons l'exposé synthétique de Shelstad [She11], qui décrit notamment les normalisations précises utilisées par Arthur, tout en empruntant parfois le point de vue éclairant d'Adams [Ada11].

Faisons désormais l'hypothèse supplémentaire que H est déployé sur $\mathbb{R}$ (semi-simple, et tel que $H(\mathbb{R})$ possède des séries discrètes). Soit T un tore maximal anisotrope de H ; on reprend les notations du §4.1 pour les objets associés. La paramétrisation de Shelstad n'est complètement canonique que si H est adjoint. En général, elle dépendra du choix d'une W_{r}-orbite de l'ensemble $\mathcal{B}(T)$ des bases Δ du système de racines Φ telles que $\Delta \cap \Phi_{\mathrm{c}} = \emptyset$. Cet ensemble est non vide et muni d'une action naturelle, simplement transitive, du groupe de Weyl réel $W_{\mathrm{r}}^{\mathrm{ad}}$ de $(H/\mathrm{Z}(H))(\mathbb{R})$ relativement à l'image de $T(\mathbb{R})$, qui vérifie $W_{\mathrm{r}} \subset W_{\mathrm{r}}^{\mathrm{ad}} \subset W$. Le $\mathrm{W}(H,T)$-ensemble $\mathcal{B}(T)$ dépend évidemment du choix de T, mais le fait que l'ensemble de ces T ne forme qu'une classe de $H(\mathbb{R})$-conjugaison assure que l'ensemble quotient $\mathrm{W}(H,T)\backslash\mathcal{B}(T)$ ne dépend que de H, il sera noté $\mathcal{B}(H)$. Des résultats de Kostant et Vogan montrent que le choix d'une W_{r}-orbite $O \subset \mathcal{B}(T)$, ce que l'on notera aussi $O \in \mathcal{B}(H)$, est équivalent à celui d'une *classe d'équivalence de données de Whittaker* D pour $H(\mathbb{R})$, une notion que nous n'introduirons pas ici, mais qui est précisément la donnée de référence chez Arthur : l'unique série discrète dans Π_V qui est générique pour D est $\pi_{\Delta,V}$ pour $\Delta \in O$.

Définition 4.3. *Soient T un tore maximal anisotrope de H, $\Delta \in \mathcal{B}(T)$ et $\rho^\vee$ la demi-somme des co-racines de T positives relativement à Δ. La*

paramétrisation de Shelstad de Π_V *relative à* (T, Δ) *est l'application*

$$\kappa_\Delta : \Pi_V \longrightarrow \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}, \pi \mapsto \kappa_\Delta(\pi),$$

définie par $\kappa_\Delta(\pi_{w^{-1}\Delta,V}) \equiv w\rho^\vee - \rho^\vee \bmod 2\mathrm{X}_*(T)$ *pour tout* $w \in W$.

Soulignons que $\rho^\vee \in \frac{1}{2}\mathrm{X}_*(T)$ n'est pas dans $\mathrm{X}_*(T)$ en général. En revanche, le terme $w\rho^\vee - \rho^\vee$ est bien dans $\mathrm{X}_*(T)$: il appartient même au sous-groupe engendré par les co-racines. Nous verrons plus loin que $\pi \mapsto \kappa_\Delta(\pi)$ est injective.

Expliquons pourquoi cette définition coïncide avec celle donnée par Shelstad [SHE11, §8]. Suivant Langlands et Shelstad, considérons le premier groupe de cohomologie $H^1(\mathbb{R}, T)$ de $T(\mathbb{C})$ vu comme $\mathbb{Z}[\mathrm{Gal}(\mathbb{C}/\mathbb{R})]$-module. Comme on a $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} = \langle 1, \sigma \rangle$, c'est simplement le quotient du groupe abélien

$$Z^1(\mathbb{R}, T) = \{t \in T(\mathbb{C}), t\sigma(t) = 1\}$$

par le sous-groupe des éléments de la forme $t\sigma(t)^{-1}$ avec $t \in T(\mathbb{C})$. Rappelons d'abord que $H^1(\mathbb{R}, T)$ s'identifie canoniquement avec le but de l'application κ_Δ (dualité de Tate-Nakayama). En effet, soit $T_2 = \{t \in T(\mathbb{R}), t^2 = 1\} = T(\mathbb{R}) \cap Z^1(\mathbb{R}, T)$. La composée des applications naturelles

$$T_2 \hookrightarrow Z^1(\mathbb{R}, T) \to H^1(\mathbb{R}, T) \tag{4.1}$$

est manifestement un isomorphisme, le tore T étant $\mathbb{R}$-isomorphe à un produit fini de copies de $\mathbb{S}^1$. Si $\mu \in \mathrm{X}_*(T) \otimes \mathbb{C}$, notons e^μ l'unique élément $z \in T(\mathbb{C})$ tel que $\lambda(z) = e^{\langle \lambda, \mu \rangle}$ pour tout $\lambda \in \mathrm{X}^*(T)$. L'application $\mu \mapsto e^{i\pi\mu}$ induit donc un isomorphisme naturel $\mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} T_2$. En mettant bout-à-bout les isomorphismes ci-dessus, on obtient l'isomorphisme naturel annoncé $H^1(\mathbb{R}, T) \xrightarrow{\sim} \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}$.

On dispose également d'une action naturelle de W sur $H^1(\mathbb{R}, T)$ induite par l'inclusion $T \subset H$, définie de la manière suivante [BOR14]. Si N est le normalisateur de $T(\mathbb{C})$ dans $H(\mathbb{C})$, alors $n\sigma(n)^{-1} \in T(\mathbb{C})$ pour tout $n \in N$, et donc $(n, t) \mapsto n \star t := nt\sigma(n)^{-1}$ définit une action de N sur $Z^1(\mathbb{R}, T)$. Elle induit par passage au quotient une action de $W = N/T(\mathbb{C})$ sur $H^1(\mathbb{R}, T)$, que nous noterons encore $(w, x) \mapsto w \star x$. Ceci étant dit, si $w \in W$ alors l'élément $\kappa_\Delta(\pi_{w^{-1}\Delta,V}) \in \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}$ considéré par Shelstad [SHE11, p. 15] est par définition l'image de $w \star 1 \in H^1(\mathbb{R}, T)$, $1 \in H^1(\mathbb{R}, T)$ désignant l'élément neutre, par l'isomorphisme $H^1(\mathbb{R}, T) \xrightarrow{\sim} \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}$ rappelé au paragraphe précédent.

Prenons garde que l'isomorphisme $\gamma : T_2 \to H^1(\mathbb{R}, T)$, défini par la formule (4.1), n'entrelace pas l'action évidente par conjugaison de W sur T_2

et celle sur $H^1(\mathbb{R}, T)$ définie ci-dessus. L'identité $gt\sigma(g)^{-1} = gtg^{-1}g\sigma(g)^{-1}$ montre toutefois que c'est vrai pour l'action du sous-groupe W_{r}. Pour s'éviter des confusions, nous noterons $(w, t) \mapsto w(t)$ l'action usuelle de W sur $T(\mathbb{C})$ et $(w, t) \mapsto w \cdot t = \gamma^{-1}(w \star \gamma(t))$ l'action "tordue" sur T_2. La relation précise entre les deux est donnée par le lemme suivant (ii), essentiellement dû à Langlands [She79, §3][Kot90, Lemma 5.1][Ada11, Lemma 7.8]. Fixons $\Delta \in \mathcal{B}(T)$ et notons $\rho^\vee \in \frac{1}{2}\mathrm{X}_*(T)$ la demi-somme des coracines de $(H_{\mathbb{C}}, T_{\mathbb{C}})$ positives relativement à Δ. Suivant [Ada11], posons

$$t_{\mathrm{b}} = e^{i\pi\rho^\vee} \in T(\mathbb{C}).$$

On a $t_{\mathrm{b}}^4 = 1$ donc $t_{\mathrm{b}} \in T(\mathbb{R})$.

Lemme 4.4. *(i) Le centralisateur de t_{b} dans $H(\mathbb{R})$ est K et $t_{\mathrm{b}}^2 \in \mathrm{Z}(H)$.*

(ii) Pour tout $t \in T_2$ et $w \in W$ on a $w \cdot t = w(tt_{\mathrm{b}})t_{\mathrm{b}}^{-1}$.

La relation $w \cdot 1 = e^{i\pi(w\rho^\vee - \rho^\vee)}$ s'en déduit et conclut. Observons que le (i) entraîne que l'élément t_b ne dépend que de la W_{r}-orbite de Δ dans $\mathcal{B}(T)$.

Démonstration. Si $\alpha \in \Phi$ alors $\alpha(t_{\mathrm{b}}) = (-1)^{\langle \rho^\vee, \alpha \rangle}$. Soit $s : \Phi \to \mathbb{Z}/2\mathbb{Z}$ l'application telle que $s^{-1}(0) = \Phi_c$. La décomposition de Cartan de $\mathrm{Lie}\, H(\mathbb{R})$ relativement à K montre que $s(\alpha + \beta) = s(\alpha) + s(\beta)$ chaque fois que α, β et $\alpha + \beta$ sont dans Φ. Par récurrence sur la "hauteur" $|\langle \rho^\vee, \alpha \rangle|$, on a $s(\alpha) \equiv \langle \rho^\vee, \alpha \rangle \bmod 2$ pour tout $\alpha \in \Phi$. Cela montre que l'automorphisme intérieur de H défini par t_{b} est l'involution de Cartan de $H(\mathbb{R})$ relativement à K, puis le (i).

Comme on a $t_{\mathrm{b}}^2 \in \mathrm{Z}(H)$, la fonction $f(w) = w(t_{\mathrm{b}})t_{\mathrm{b}}^{-1}$ définit un 1-cocyle de W à valeurs dans T_2. De même, $g(w) = w \cdot 1$ est aussi un 1-cocyle à valeurs dans T_2. Comme $w \cdot t = w(t)\, w \cdot 1$, il suffit de voir que f et g coïncident sur les s_α avec $\alpha \in \Delta$, soit encore que $\mathrm{s}_\alpha \cdot 1 = f(s_\alpha) = e^{i\pi\alpha^\vee}$. C'est exactement le calcul de Langlands [She79, Prop. 2.1]. Cela démontre le (ii). □

Observons enfin que si $\Delta \in \mathcal{B}(T)$, $w \in W_{\mathrm{r}}$ et $\pi \in \Pi_V$, on a

$$\kappa_{w\Delta}(\pi) = w\kappa_\Delta(\pi), \tag{4.2}$$

à cause de l'identité immédiate $(ww') \cdot 1 = w \cdot (w' \cdot 1)$ pour tout $w' \in W$. En particulier, la W_{r}-orbite de $\kappa_\Delta(\pi)$ ne dépend que de celle de Δ dans $\mathcal{B}(T)$.

4.5. Interpretation duale et lien avec les paquets d'Arthur

On conserve les notations et hypothèses des §4.1 et §4.2. Avant de donner un exemple, donnons l'interprétation duale utile de la paramétrisation de Shelstad. Soit $\widehat{H}$ le $\mathbb{C}$-groupe dual de $H_{\mathbb{C}}$ (rappelons que H est déployé sur $\mathbb{R}$). Suivant Langlands [Lan73b], il existe une bijection naturelle entre $\mathrm{Irr}(H_{\mathbb{C}})$ et l'ensemble des $\widehat{H}$-classes de conjugaison de *paramètres discrets* $\varphi : \mathrm{W}_{\mathbb{R}} \to \widehat{H}$. Rappelons qu'un tel objet est par définition un morphisme de groupes continu tel que le sous-groupe $\varphi(\mathrm{W}_{\mathbb{R}}) \subset \widehat{H}$ est constitué d'éléments semi-simples et possède un centralisateur fini dans $\widehat{H}$, noté C_{φ}. Cette bijection est caractérisée par le fait que le caractère infinitésimal d'un tel φ coïncide avec celui de la représentation dans $\mathrm{Irr}(H_{\mathbb{C}})$ qui lui correspond.

Expliquons cette assertion. Le sous-groupe $\varphi(\mathbb{C}^{\times}) \subset \widehat{H}$ est commutatif, connexe, et constitué d'éléments semi-simples. Son adhérence Zariski dans $\widehat{H}$ est donc un tore, et son centralisateur dans $\widehat{H}$, noté S, un sous-groupe de Levi (d'un sous-groupe parabolique) de $\widehat{H}$. Par définition, $\mathrm{C}_{\varphi} \subset S$ est le sous-groupe fixé par la conjugaison par $\varphi(j)$. Comme il est fini, cela force S à être un tore maximal et $\varphi(j)$ à agir par l'inversion $s \mapsto s^{-1}$ (en particulier, -1 est un élément du groupe de Weyl de $\widehat{H}$, ce qui est bien le cas sous notre hypothèse sur H). Soient $\lambda_{\phi}, \mu_{\phi} \in \mathrm{X}_*(S) \otimes \mathbb{C}$ les uniques éléments tels que $\lambda_{\phi} - \mu_{\phi} \in \mathrm{X}_*(S)$ et $\xi(\varphi(z)) = z^{\langle \xi, \lambda_{\phi} \rangle} \overline{z}^{\langle \xi, \mu_{\phi} \rangle}$ pour tout $z \in \mathbb{C}^{\times}$ et $\xi \in \mathrm{X}^*(S)$ (voir la note de bas de page §2.12) Le caractère infinitésimal de φ est par définition la classe de $\widehat{H}$-conjugaison de λ_{ϕ}, vue dans $\mathrm{Lie}\,\widehat{H}$ (formule VI.(3.1)). De plus, $\mu_{\phi} = -\lambda_{\phi}$.

Fixons maintenant un paramètre discret $\varphi : \mathrm{W}_{\mathbb{R}} \to \widehat{H}$. Observons que si φ' est dans la classe de $\widehat{H}$-conjugaison de φ, et si $h \in \widehat{H}$ est tel que $\varphi' = h\varphi h^{-1}$, l'isomorphisme $\mathrm{C}_{\varphi} \to \mathrm{C}_{\varphi'}$ induit par conjugaison par h est indépendant du choix de h, de sorte que C_{φ} est un groupe abélien canonique. Soit S le tore maximal de $\widehat{H}$ contenant $\varphi(\mathbb{C}^{\times})$ et $B \subset \widehat{H}$ l'unique sous-groupe de Borel contenant S tel que l'élément $\lambda_{\phi} \in \frac{1}{2}\mathrm{X}_*(S)$ défini ci-dessus soit dominant par rapport à B. La donnée de $\Delta \in \mathcal{B}(T)$, qui définit un unique sous-groupe de Borel $T_{\mathbb{C}} \subset Q \subset H_{\mathbb{C}}$, et celle de $\widehat{H}$, définissent un isomorphisme unique $\Psi(H_{\mathbb{C}}, T, Q)^{\vee} \simeq \Psi(\widehat{H}, S, B)$, et en particulier un isomorphisme privilégié $\widehat{T} \to S$, soit encore un isomorphisme

$$i_{\Delta} : \mathrm{X}_*(T) \xrightarrow{\sim} \mathrm{X}^*(S).$$

Ceci étant dit, $\mathrm{C}_{\varphi} = S_2 = \{s \in S, s^2 = 1\}$ et l'application naturelle $\beta : \mathrm{X}_*(S) \otimes \mathbb{Z}/2\mathbb{Z} \to \mathrm{Hom}(S_2, \mathbb{C}^{\times})$ est un isomorphisme de groupes. Au final, l'application κ_{Δ} de Shelstad (définition 4.3) induit une application naturelle

$$\chi_O : \Pi_V \longrightarrow \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_{\varphi}, \mathbb{C}^{\times}), \tag{4.3}$$

définie par $\chi_O := \beta \circ (i_\Delta \otimes \mathbb{Z}/2\mathbb{Z}) \circ \kappa_\Delta$, où $O \in \mathcal{B}(T)$ désigne la W_{r}-orbite de Δ. On observe en effet que si $w \in W$ alors $i_{w\Delta} = i_\Delta \circ w^{-1}$, de sorte que l'application χ_O ne dépend bien que O, d'après la relation (4.2). Son image est constituée d'homomorphismes triviaux sur $\mathrm{Z}(\widehat{H})$ car $w\rho^\vee - \rho^\vee$ est une somme de racines de $(\widehat{H}, S)$ pour tout $w \in W$. Elle est injective mais non surjective en général.

Le lien avec le §3.8 est que lorsque l'homomorphisme ν_∞ défini *loc. cit.* est trivial sur le facteur $\mathrm{SL}_2(\mathbb{C})$, ce qui équivaut à demander $d_i = 1$ pour tout $i = 1, \ldots, k$, alors c'est un paramètre discret $\mathrm{W}_\mathbb{R} \to \widehat{G}$ (Lemme 3.9) ayant même caractère infinitésimal que la représentation $V \in \mathrm{Irr}(G_\mathbb{C})$ fixée par l'hypothèse (H2) §3.4. Il sera commonde de traiter à part le cas de $\mathrm{SO}_{r,r}$.

(a) Supposons que $G = \mathrm{Sp}_{2g}$ ou $\mathrm{SO}_{r+1,r}$. Alors d'après [She11, She12a] et [Mez13], l'ensemble $\Pi(\psi_\mathbb{R})$ considéré par Arthur est Π_V, l'application ι est l'inclusion évidente $\Pi_V \subset \Pi_{\mathrm{unit}}(G(\mathbb{R}))$, et l'application χ *loc. cit.* est l'application χ_O définie ci-dessus. Quand $G = \mathrm{SO}_{r+1,r}$ (adjoint) il n'y a qu'un choix possible de $O \in \mathcal{B}(G_\mathbb{R})$, de sorte que tout est canoniquement défini. Lorsque $G = \mathrm{Sp}_{2g}$, il y en a exactement deux (voir ci-dessous), et il faut bien sûr s'en tenir au choix fait par Arthur [Art13, p. 55]. Étant donné que l'application naturelle $\mathrm{PGSp}_{2g}(\mathbb{Z}) \to \pi_0(\mathrm{PGSp}_{2g}(\mathbb{R})) = \mathbb{Z}/2\mathbb{Z}$ est surjective, ce choix ne jouera en fait aucun rôle dans nos applications.

(b) Supposons enfin $G = \mathrm{SO}_{r,r}$ avec $r \equiv 0 \bmod 2$. Le groupe à deux éléments $\mathrm{O}_{r,r}(\mathbb{R})/\mathrm{SO}_{r,r}(\mathbb{R}) = \{1, \theta\}$ agit naturellement sur $\Pi_{\mathrm{unit}}(G(\mathbb{R}))$ et $\mathrm{Irr}(G_\mathbb{C})$. On observe que θ induit une bijection $\Pi_V \xrightarrow{\sim} \Pi_{\theta(V)}$.

Lemme 4.6. *Soient $H = \mathrm{SO}_{r,r}$ avec $r \equiv 0 \bmod 2$, T un tore maximal anisotrope de H, $\Phi = \Phi(H_\mathbb{C}, T_\mathbb{C})$, Δ une base de Φ, et $V \in \mathrm{Irr}(H_\mathbb{C})$. Alors $\theta(\pi_{\Delta,V}) \simeq \pi_{\Delta,\theta(V)}$.*

Démonstration. Il est équivalent de se donner T ou une décomposition de $\mathrm{H}(\mathbb{R}^r)$ comme somme orthogonale $\oplus_{i\in I} P_i$ de plans P_i supposés définis (postifs ou négatifs). Ceci étant fait, il est équivalent de se donner Δ, un sous-groupe de Borel de $H_\mathbb{C}$ contenant $T_\mathbb{C}$, ou encore un ordre total sur l'ensemble I avec pour chaque $i \in I$ un choix de l'une des deux droites isotropes de $P_i \otimes \mathbb{C}$ (§VI.1.3). Soit i_0 le plus grand élément de I. Soit $s \in \mathrm{O}(\mathrm{H}(\mathbb{R}^r))$ l'unique élement qui agit par l'identité sur P_i pour $i < i_0$, et qui échange les deux droites isotropes de P_{i_0}. C'est un représentant de θ préservant T ainsi que la base $\Delta \subset \Phi$. On conclut car la propriété caractéristique de $\pi_{\Delta,V}$ montre que $\theta(\pi_{\Delta,V}) = \pi_{s(\Delta),\theta(V)}$ et on a vu que $s(\Delta) = \Delta$. $\square$

En particulier, si $\theta(V) \simeq V$ on constate que θ agit par l'identité sur Π_V : tout $\pi \in \Pi_V$ se prolonge à $\mathrm{O}(\mathrm{H}(\mathbb{R}^r))$. Retournons au $\mathbb{Z}$-groupe $G = \mathrm{SO}_{r,r}$. D'après les résultats sus-cités de Shelstad et Mezo, l'ensemble $\Pi(\psi_{\mathbb{R}})$ considéré par Arthur est l'image $\widetilde{\Pi}_V$ de Π_V dans $\widetilde{\Pi}_{\mathrm{unit}}(G(\mathbb{R}))$, et l'application ι est l'inclusion évidente. Si $\pi \in \Pi_V$, le lemme 4.6 assure que π et $\theta(\pi)$ ont même caractère de Shelstad, ce qui fournit par passage au quotient une application bien définie $\widetilde{\Pi}_V \longrightarrow \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_{\nu_\infty}, \mathbb{C}^\times)$: c'est l'application considérée par définition chez Arthur. Pour être tout-à-fait exact, comme dans le cas $G = \mathrm{PGSp}_{2g}$ l'ensemble $\mathcal{B}(G_{\mathbb{R}})$ contient deux éléments, et il faut choisir celui correspondant à la donnée de Whittaker fixée par Arthur, mais là encore ce choix ne jouera pas de rôle dans nos applications.

4.7. Exemple : la série discrète holomorphe de $\mathrm{Sp}_{2g}(\mathbb{R})$

Considérons l'exemple du groupe $H = \mathrm{Sp}_{2g}$, de $\mathbb{C}$-groupe dual $\widehat{H} = \mathrm{SO}_{2g+1}$. Posons $E = \mathrm{H}(\mathbb{R}^g)$, muni de sa forme alternée hyperbolique a, de sorte que $H = \mathrm{Sp}_E$. Rappelons que si $I \in \mathrm{Sp}(E)$ est tel que $I^2 = -\mathrm{id}_E$, il munit E d'une structure complexe ainsi que d'une forme hermitienne non dégénérée h pour cette structure, de forme bilinéaire associée

$$(e, f) \mapsto \mathrm{a}(Ie, f) + i\mathrm{a}(e, f).$$

Le centralisateur de I dans Sp_E est alors le $\mathbb{R}$-groupe unitaire $\mathrm{U_h}$. Choisissons l'élément I de sorte que h soit définie positive, auquel cas $\mathrm{U_h}(\mathbb{R})$ est un sous-groupe compact maximal de Sp_E. Il existe une unique classe de conjugaison de tels éléments sous $\mathrm{Sp}(E)$. Par exemple, on peut prendre $I = \mathrm{J}_{2g}$ dans les notations du §IV.5.1, $\mathrm{U_h}(\mathbb{R})$ étant alors le groupe K du §IV.5.3 (de complexifié $\mathrm{j}(-, i1_g) : K \to \mathrm{GL}_g(\mathbb{C})$ *loc. cit.*). Le choix d'une décomposition de l'espace hermitien (E, h) en somme orthogonale de droites détermine un tore maximal anisotrope T tel que $T(\mathbb{R}) \subset K$. Dans les notations du §4.1 (et conformément au §VI.3.4), on a $\mathrm{X}^*(T) = \oplus_{i=1}^g \mathbb{Z}\varepsilon_i$,

$$\Phi = \{\pm 2\varepsilon_i, i = 1, \ldots, g\} \cup \{\pm\varepsilon_i \pm \varepsilon_j, 1 \leq i < j \leq g\}$$

et $\Phi_{\mathrm{c}} = \{\pm(\varepsilon_i - \varepsilon_j), 1 \leq i < j \leq g\}$. En particulier, $W_{\mathrm{r}} = \mathrm{W}(\Phi_c)$ n'est autre que le groupe symétrique $\mathfrak{S}_g$ agissant sur $\mathrm{X}^*(T) \simeq \mathbb{Z}^g$ de manière habituelle et $W_{\mathrm{r}}^{\mathrm{ad}} = W_{\mathrm{r}} \times \{\pm\mathrm{id}\}$. L'ensemble de bases $\mathcal{B}(T)$ est constitué de deux W_{r}-orbites, échangées entre elles par $x \mapsto -x$, l'une d'entre étant par exemple

$$\Delta = \{2\varepsilon_g, -\varepsilon_g - \varepsilon_{g-1}, \varepsilon_{g-1} + \varepsilon_{g-2}, -\varepsilon_{g-2} - \varepsilon_{g-3}, \ldots, (-1)^{g-1}(\varepsilon_2 + \varepsilon_1)\}.$$

Si $\varepsilon_i^* \in \mathrm{X}_*(T)$ est la base duale de (ε_i), observons que Δ est la base du système positif $\{\alpha \in \Phi, f(\alpha) > 0\}$ où $f = \varepsilon_g^* - 2\,\varepsilon_{g-1}^* + 3\,\varepsilon_{g-2}^* + \cdots + (-1)^{g-1}\,(g-1)\,\varepsilon_1^*$. Un petit calcul montre alors que $\rho^\vee = \sum_{i=1}^g (-1)^{i-g}\,\frac{2g-2i+1}{2}\,\varepsilon_i^*$, de sorte que

$$\rho^\vee \equiv \frac{1}{2}\sum_{i=1}^g \varepsilon_i^* \bmod 2\mathrm{X}_*(T).$$

Observons que cet élément est bien invariant par W_{r}. Soit $A \subset W$ le sous-groupe constitué des éléments $a \in W$ tels que $a(\varepsilon_i) = \pm\varepsilon_i$; il est manifestement isomorphe à $\{\pm 1\}^g$. On constate que tout élément de $\mathrm{X}_*(T)$ est congru modulo 2 à un élément de la forme $a\rho^\vee - \rho^\vee$ pour un unique $a \in A$: l'action de A sur $H^1(\mathbb{R}, T)$ est donc simplement transitive, et κ_Δ (resp. χ_O) est bijective. Observons enfin que si l'on remplace O par la W_{r}-orbite $-O$, ce qui revient à changer w en $-w$, on a

$$\kappa_\Delta \equiv \kappa_{-\Delta} + 2\rho^\vee \bmod 2\mathrm{X}_*(T).$$

Considérons maintenant la série discrète holomorphe dans Π_V (§VI.3.4,§4.1). On vérifie aisément qu'il existe exactement deux W_r-orbites de bases de Φ dont le système positif associé est tel que les racines compactes sont plus petites que les racines non-compactes, à savoir celles des bases $\pm\Delta'$ où

$$\Delta' = \{2\varepsilon_g\} \cup \{\varepsilon_{i+1} - \varepsilon_i, i = 1, \ldots, g-1\},$$

(considérer par exemple la forme linéaire $\sum_{i=1}^g (g+i)\,\varepsilon_i^*$). Suivant les conventions choisies, qu'il ne sera pas nécéssaire de préciser, l'une de ces bases donne lieu aux représentations notées π'_W au §VI.3.4, et son opposée à sa conjuguée extérieure sous $\mathrm{PGSp}_{2g}(\mathbb{R})$ (dans la littérature on trouve parfois le nom de séries discrètes *holomorphes* et *anti-holomorphes* pour distinguer ces deux types). On constate alors que $\Delta' = w^{-1}\Delta$ où $w \in W$ est l'élément envoyant ε_i sur $(-1)^{g-i}\varepsilon_i$. Ainsi,

$$\kappa_\Delta(\pi_{\Delta',V}) \equiv w\rho^\vee - \rho^\vee \equiv \sum_{i \not\equiv g \bmod 2} \varepsilon_i^* \bmod 2, \tag{4.4}$$

conformément au calcul fait dans [CR12, Lemma 9.1]. On obtient de même $\kappa_\Delta(\pi_{-\Delta',V}) \equiv \kappa_\Delta(\pi_{\Delta',V}) + 2\rho^\vee \bmod 2\mathrm{X}_*(T)$.

4.8. Formes pures des groupes déployés

Dans ce paragraphe, nous rappelons comment la paramétrisation du §4.2 s'étend à toutes les formes pures du $\mathbb{R}$-groupe déployé H, suivant Vogan,

Kottwitz, Arthur, Shelstad et Adams [ABV92][Art99, §1]. Notre exposé est largement inspiré de la présentation agréable d'Adams [Ada11] ainsi que des notes de Shelstad [She08b, She11]. Nous renvoyons à [Ser64, Ch. III §1], [ABV92, §2] et [Bor14] pour des généralités sur les formes des groupes réels.

Considérons d'abord un $\mathbb{R}$-groupe G quelconque. L'ensemble $G(\mathbb{C})$ est muni d'une action de $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. On considère

$$Z^1(\mathbb{R}, G) = \{x \in G(\mathbb{C}), x\sigma(x) = 1\}.$$

Le groupe $G(\mathbb{C})$ opère sur $Z^1(\mathbb{R}, G)$ par $(g, x) \mapsto gx\sigma(g)^{-1}$, l'ensemble quotient étant l'ensemble de cohomologie usuel $H^1(\mathbb{R}, G)$. À tout élément $x \in Z^1(\mathbb{R}, G)$ est associé une involution

$$\sigma_x = \mathrm{int}_x \circ \sigma$$

de $G(\mathbb{C})$. C'est l'involution galoisienne d'une unique structure réelle du $\mathbb{C}$-groupe $G_{\mathbb{C}}$, dont nous noterons G_x le $\mathbb{R}$-groupe associé. En particulier,

$$G_x(\mathbb{R}) = \{g \in G(\mathbb{C}), \sigma(g) = x^{-1}gx\}.$$

Une telle forme réelle de G est dite *pure*. Le lemme suivant est évident.

Lemme 4.9. *Le stabilisateur dans $G(\mathbb{C})$ de $x \in Z^1(\mathbb{R}, G)$ est $G_x(\mathbb{R})$.*

Si x et $x' \in Z^1(\mathbb{R}, G)$ ont même classe dans $H^1(\mathbb{R}, G)$, et si $h \in G(\mathbb{C})$ est tel que $hx\sigma(h)^{-1} = x'$, alors $\sigma_{x'} \circ \mathrm{int}_h = \mathrm{int}_h \circ \sigma_x$, de sorte que

$$\mathrm{int}_h : G_x \to G_{x'}$$

est un isomorphisme défini sur $\mathbb{R}$. Un point important est qu'il ne dépend pas du h choisi ci-dessus, du moins *modulo les* int_g *avec* $g \in G_x(\mathbb{R})$, d'après le lemme ci-dessus. Autrement dit, les $\mathbb{R}$-groupes G_x et $G_{x'}$ sont naturellement isomorphes, et même canoniquement modulo "automorphismes intérieurs", si x et x' sont équivalents. Tout en s'imposant une certaine prudence, il y a donc un sens à parler du $\mathbb{R}$-groupe G_c défini "à automorphismes intérieurs prés" comme étant le $\mathbb{R}$-groupe G_x pour n'importe quel $x \in Z^1(\mathbb{R}, G)$ dans la classe $c \in H^1(\mathbb{R}, G)$. En particulier, il y a un sens évident à parler de $\Pi_{\mathrm{unit}}(G_c(\mathbb{R}))$ pour $c \in H^1(\mathbb{R}, G)$.

Exemple 4.10. Donnons quelques exemples classiques [Ser64, Ch. III §1.2]. Si E est un $\mathbb{R}$-espace vectoriel de dimension finie alors $\mathrm{Z}^1(\mathbb{R}, \mathrm{GL}_E)$ est l'ensemble des involutions semi-linéaires de $E \otimes_{\mathbb{R}} \mathbb{C}$. D'après le théorème de Hilbert 90, $x \mapsto E_x = (E \otimes_{\mathbb{R}} \mathbb{C})^{x=\mathrm{Id}}$ identifie $\mathrm{Z}^1(\mathbb{R}, \mathrm{GL}_E)$ à l'ensemble des

structures réelles du $\mathbb{C}$-espace vectoriel $E \otimes_{\mathbb{R}} \mathbb{C}$, et $(\mathrm{GL}_E)_x = \mathrm{GL}_{E_x}$ pour tout $x \in \mathrm{Z}^1(\mathbb{R}, \mathrm{GL}_E)$. On vérifie immédiatement que si E est un q-module sur $\mathbb{R}$, alors $\mathrm{Z}^1(\mathbb{R}, \mathrm{O}_E) \subset \mathrm{Z}^1(\mathbb{R}, \mathrm{GL}_E)$ s'identifie aux structures réelles $E_x \subset E \otimes_{\mathbb{R}} \mathbb{C}$ telles que $\mathrm{q}(E_x) \subset \mathbb{R}$. Si $x \in \mathrm{Z}^1(\mathbb{R}, \mathrm{O}_E)$ on dispose donc d'un q-module E_x pour la forme $\mathrm{q}_{|E_x}$ et l'on a $(\mathrm{O}_E)_x = \mathrm{O}_{E_x}$. L'application $x \mapsto E_x$ induit alors une bijection entre $H^1(\mathbb{R}, \mathrm{O}_E)$ et l'ensemble à $\dim(E)+1$ éléments des classes d'isomorphisme de q-modules sur $\mathbb{R}$ de rang $\dim E$ (la signature). On vérifie enfin que $x \in \mathrm{Z}^1(\mathbb{R}, \mathrm{SO}_E)$ si, et seulement si, E et E_x ont même discriminant, auquel cas $(\mathrm{SO}_E)_x = \mathrm{SO}_{E_x}$, puis que $x \mapsto E_x$ induit une bijection entre $H^1(\mathbb{R}, \mathrm{SO}_E)$ et l'ensemble des classes d'isomorphisme de q-modules sur $\mathbb{R}$ de même rang et discriminant que E. On dispose d'un discours analogue dans le cas alterné, qui est seulement plus simple car il n'y a qu'une forme alternée non dégénérée de chaque dimension paire ($H^1(\mathbb{R}, \mathrm{Sp}_{2g}) = 1$).

Revenons maintenant à notre $\mathbb{R}$-groupe déployé H, muni d'un tore maximal anisotrope T. Si $c \in H^1(\mathbb{R}, H)$ nous allons rappeler la paramétrisation de Shelstad de l'ensemble Π_V^c des séries discrètes de $H_c(\mathbb{R})$ ayant même caractère infinitésimal que $V \in \mathrm{Irr}(H_{\mathbb{C}}) = \mathrm{Irr}((H_c)_{\mathbb{C}})$. L'inclusion $T \subset H$ induit une injection naturelle $Z^1(\mathbb{R}, T) \to Z^1(\mathbb{R}, H)$ ainsi qu'une application

$$W \backslash H^1(\mathbb{R}, T) \longrightarrow H^1(\mathbb{R}, H), \tag{4.5}$$

l'action de W sur $H^1(\mathbb{R}, T)$ étant celle rappelée au §4.2. Cette application est bijective d'après Shelstad (voir aussi [Bor14]). En particulier toute forme pure de H est isomorphe comme $\mathbb{R}$-groupe à H_t pour $t \in T_2$.

Les formes H_t avec $t \in T_2$, et plus généralement $t \in Z^1(\mathbb{R}, T)$, ont de sympatique qu'elles partagent toutes T pour tore maximal anisotrope, car σ_t coïncide avec σ sur T. Comme de plus $H_{\mathbb{C}} = (H_t)_{\mathbb{C}}$, le système de racines Φ de $(H_{\mathbb{C}}, T_{\mathbb{C}})$ est canoniquement celui de $((H_t)_{\mathbb{C}}, T_{\mathbb{C}})$, et il en va de même de son groupe de Weyl W (le sous-groupe de Weyl réel $\mathrm{W}(H_t, T) \subset W$ dépend en revanche de t bien entendu). Si Δ est une base de Φ et $t \in T_2$, il y a donc un sens à considérer la série discrète $\pi_{\Delta,V,t}$ de $H_t(\mathbb{R})$ associée par Harish-Chandra à la base Δ de Φ, dans les notations du §4.1. On rappelle que l'ensemble $\mathcal{B}(T)$ défini au §4.2 est relatif au couple (H, T).

Définition 4.11. *Soient $c \in H^1(\mathbb{R}, H)$ et $V \in \mathrm{Irr}(H_{\mathbb{C}})$. Soient T un tore maximal anisotrope de H, $\Delta \in \mathcal{B}(T)$ et $\rho^\vee$ la demi-somme des co-racines de T positives relativement à Δ. L'application de paramétrisation de Shelstad relativement à Δ est l'unique application*

$$\kappa_\Delta^c : \Pi_V^c \longrightarrow \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}, \pi \mapsto \kappa_\Delta^c(\pi),$$

telle que pour tout $t \in T_2$ dans la classe c, et tout $w \in W$, on ait $\kappa_\Delta^c(\pi_{w^{-1}\Delta,V,t}) \equiv w(\mu + \rho^\vee) - \rho^\vee \bmod 2\mathrm{X}_*(T)$, où $\mu \in \mathrm{X}_*(T)$ est tel que $t = e^{i\pi\mu}$.

Caché derrière cette définition se trouve le fait suivant : soient $w \in W$ et $t \in T_2$, soit $n \in H(\mathbb{C})$ un représentant de w tel que $n \star t = w \cdot t$, de sorte que $\mathrm{int}_n : H_t \to H_{w\cdot t}$ définisse un $\mathbb{R}$-isomorphisme, alors la restriction de la représentation $\pi_{w\Delta,V,w\cdot t}$ de $H_{w\cdot t}(\mathbb{R})$ à int_n est isomorphe à la représentation $\pi_{\Delta,V,t}$ de $H_t(\mathbb{R})$. Lorsque $c = 1$ alors $\kappa^1_\Delta = \kappa_\Delta$, et l'on retrouve bien entendu la définition 4.3. On vérifierait comme au §4.2 que $\kappa^c_{w\Delta} = w \circ \kappa^c_\Delta$ pour tout $w \in \mathrm{W}(H,T)$. Le lemme ci-dessous (i) assure de plus qu'elle est injective, de sorte que l'application

$$\coprod_{c\in H^1(\mathbb{R},G)} \kappa^c_\Delta : \coprod_{c\in H^1(\mathbb{R},H)} \Pi^c_V \longrightarrow \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}$$

est bijective.

La concordance de cette présentation avec la définition donnée par Shelstad *loc. cit.*, qui associe à $\pi_{w^{-1}\Delta,V,t}$ la classe de $w \cdot t$ dans $H^1(\mathbb{R},T)$, découle encore immédiatement du lemme 4.4. C'est essentiellement le point de vue donné par Adams dans [Ada11], à ceci près que son point de départ est un $\mathbb{R}$-groupe à points réels compact, plutôt que déployé (et qu'il considère les formes intérieures générales). La définition ci-dessus admet une interprétation duale identique à celle mentionnée au §4.5 en terme des paramètres discrets de H, et conduit à une application canonique

$$\chi^c_O = \beta \circ (i_\Delta \otimes \mathbb{Z}/2\mathbb{Z}) \circ \kappa^c_\Delta, \quad \Pi^c_V \to \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_\varphi, \mathbb{C}^\times),$$

qui ne dépend que de la W_{r}-orbite O de Δ dans $\mathcal{B}(T)$ (soulignons encore que ce choix est relatif à H, et non à H_c). Mentionnons que dans son exposé, et suivant Arthur et Kottwitz, Shelstad se limite aux $c \in H^1(\mathbb{R},H)$ qui sont dans l'image de l'application naturelle $H^1(\mathbb{R},H_{\mathrm{sc}}) \to H^1(\mathbb{R},H)$, $H_{\mathrm{sc}} \to H$ désignant le revêtement simplement connexe de H. La réunion disjointe des H_c indexée par les telles classes c forme alors un *K-groupe* au sens d'Arthur. Cela revient à se restreindre aux éléments $t \in T_2$ de la forme $e^{i\pi\mu}$ où $\mu \in \mathrm{X}_*(T)$ est une somme de coracines de $(H_{\mathbb{C}}, T_{\mathbb{C}})$, soit encore aux éléments de $\mathrm{X}^*(\widehat{T}) \otimes \mathbb{Z}/2\mathbb{Z}$ triviaux sur le centre de $\widehat{H}$.

Lemme 4.12. *Soient T un tore maximal anisotrope de H et $t \in T_2$.*

(i) $\mathrm{W}(H_t,T) = \{w \in W, w \cdot t = t\}$.

(ii) $\mathrm{Int}\, tt_{\mathrm{b}}$ *est une involution de Cartan de H_t, où $t_{\mathrm{b}} \in T_2$ est l'élément défini au §4.2 et associé à une W_{r}-orbite dans $\mathcal{B}(T)$.*

Démonstration. On constate que $w \cdot t = t$ si, et seulement si, il existe un représentant $n \in H(\mathbb{C})$ de w qui fixe $t \in Z^1(\mathbb{R},H)$, i.e. dans $H_t(\mathbb{R})$ d'après le lemme 4.9. Le (ii) résulte du cas particulier $t = 1$, qui est le lemme 4.4 (i). □

Si $c \in H^1(\mathbb{R}, H)$ et si $V \in \mathrm{Irr}(H_{\mathbb{C}})$ alors V peut être vue par restriction comme une représentation irréductible de dimension finie de $H_c(\mathbb{R})$ bien définie à isomorphisme près. Lorsque $H_c(\mathbb{R})$ est compact, c'est l'unique élément du singleton Π_V^c (§4.1). Le point (ii) du lemme ci-dessus montre que cela se produit si, et seulement si, $t_{\mathrm{b}} \in T_2$ et c est la classe d'un $t \in t_b \mathrm{Z}(H)$. On rappelle que $\mathrm{Z}(H) \subset T_2$ car $-1 \in W$ (cela vient de ce que H est à la fois déployé sur $\mathbb{R}$ et possède un tore maximal compact).

Corollaire 4.13. *Soient $c \in H^1(\mathbb{R}, H)$ telle que $H_c(\mathbb{R})$ est compact, $V \in \mathrm{Irr}(H_{\mathbb{C}})$, $\Delta \in \mathcal{B}(T)$ et $\rho^\vee \in \frac{1}{2}\mathrm{X}_*(T)$ associé à Δ. Alors $\rho^\vee \in \mathrm{X}_*(T)$ et $\kappa_\Delta^c(V) \equiv \rho^\vee + \nu \bmod 2\mathrm{X}_*(T)$, où $e^{i\pi\nu} \in \mathrm{Z}(H)$.*

Considérons l'exemple plus intéressant de la série discrète holomorphe du groupe spécial orthogonal de signature $(m, 2)$ pour $m \geq 1$ impair (qui n'est déployé que si $m \leq 3$). Partons du $\mathbb{R}$-groupe déployé $H = \mathrm{SO}_{r+1,r}$. Écrivons $\mathrm{H}(\mathbb{R}^r) \oplus \mathbb{R}$ comme somme orthogonale d'une droite D et de plans P_i, $i = 1, \ldots r$, chacun supposé défini et de signe que nous préciserons plus tard. Cette décomposition définit un unique tore anisotrope T de H préservant D et chacun des P_i. Choisissons de manière arbitraire, pour $i = 1, \ldots, r$, l'une des deux droites isotropes ℓ_i de $\mathrm{P}_i \otimes \mathbb{C}$, et notons $\varepsilon_i \in \mathrm{X}^*(T_{\mathbb{C}})$ le caractère de T sur ℓ_i. La suite $\ell_1, \ldots, \ell_r$ définit comme au §VI.1.3 un unique sous-groupe de Borel de $H_{\mathbb{C}}$ contenant $T_{\mathbb{C}}$, correspondant à la base standard

$$\Delta = \{\varepsilon_i, i = 1, \ldots, r\} \cup \{\varepsilon_i \pm \varepsilon_j, 1 \leq i < j \leq r\}$$

de $\Phi = \Phi(H_{\mathbb{C}}, T_{\mathbb{C}})$. Supposons maintenant que l'on a choisi les P_i de signe $(-1)^{i-1}$, et D de signe $(-1)^r$, ce qui est loisible. On constate qu'aucun élément de Δ n'est compact, de sorte que $\Delta \in \mathcal{B}(T)$ (il n'est pas difficile de voir que $\mathcal{B}(T)$ ne forme qu'une W_r-orbite). De plus, le §VI.1.3 montre que la demi-somme $\rho^\vee$ des coracines de $(H_{\mathbb{C}}, T_{\mathbb{C}})$ positives relativement à Δ est

$$\rho^\vee = \sum_{i=1}^{r} (r - i + 1)\varepsilon_i^* \in \mathrm{X}_*(T_{\mathbb{C}}),$$

où $\varepsilon_i^* \in \mathrm{X}_*(T_{\mathbb{C}})$ désigne la base duale de (ε_i), de sorte que $\varepsilon_i(t_{\mathrm{b}}) = (-1)^{r-i+1}$.

Ceci étant dit intéressons-nous aux formes réelles de H. D'après l'exemple 4.10, il existe une unique classe $c \in H^1(\mathbb{R}, H)$ telle que H_c soit isomorphe au groupe spécial orthogonal de signature $(2, 2r - 1)$. Concrètement, si $t \in T_2$ agit par multiplication par $s_j = \pm 1$ sur le plan P_j, et par 1 sur D, la forme réelle du q-module $\mathrm{H}(\mathbb{R}^r) \oplus \mathbb{R}$ associée à t est la somme directe de D, des P_j tels que $s_j = 1$, et des iP_j tels que $s_j = -1$. En particulier, H_t est le groupe spécial orthogonal de signature $(2a, b)$ où a est le nombre des $1 \leq j \leq r$ tels

que $s_j(-1)^{j-1} \neq (-1)^r$ et $2a+b = 2r+1$. Autrement dit, $H_t \simeq H'$ si, et seulement si, il existe un entier $1 \leq s \leq r$ tel que $t = t_{\mathrm{b}} e^{i\pi\varepsilon_s^*}$. Ces éléments de T_2 ne formant qu'une W-orbite pour l'action tordue, ils appartiennent bien à une même classe $c \in \mathrm{H}^1(\mathbb{R}, H)$. Identifions par exemple H' à $H_{t'}$ où

$$t' = t_{\mathrm{b}} e^{i\pi\varepsilon_1^*}$$

(tout $\mathbb{R}$-isomorphisme de H' étant de la forme $\operatorname{Int} h$ avec $h \in H'(\mathbb{R})$, le choix de l'identification n'importe pas). L'ensemble $\Phi'_{\mathrm{c}} \subset \Phi$ des racines compactes de $(H_{t'}, T)$ est manifestement

$$\Phi'_{\mathrm{c}} = \{\pm\varepsilon_i, i = 2, \ldots, r\} \cup \{\pm\varepsilon_i \pm \varepsilon_j, 2 \leq i < j \leq r\},$$

d'après le lemme 4.12. En considérant la forme linéaire $(2r-2)\,\varepsilon_1^* + \sum_{i=2}^r (r-i+1)\,\varepsilon_i^*$ on constate que le système positif de la base Δ plus haut est tel que tout élément de Φ'_{c} est plus petit que tout élément de $\Phi - \Phi'_c$ (§4.1). C'est même l'unique telle base modulo action du groupe de Weyl réel de $(H_{t'}, T)$. Il existe donc une unique série discrète holomorphe $\pi_{\mathrm{hol},V}$ de H' ayant même caractère infinitésimal que $V \in \operatorname{Irr}(H_{\mathbb{C}})$, et l'on a

$$\kappa_\Delta^c(\pi_{\mathrm{hol,V}}) \equiv (r-1)(\varepsilon_1^* + \varepsilon_2^*) + \sum_{i=3}^{r} (r-i+1)\varepsilon_i^* \bmod 2\mathrm{X}_*(T_{\mathbb{C}}). \tag{4.6}$$

En effet, c'est la définition 4.11 appliquée à $w = 1$ et $t = t' = e^{i\pi(\rho^\vee + \varepsilon_1^*)}$.

4.14. Paquets d'Adams-Johnson

Soient H un $\mathbb{R}$-groupe semi-simple déployé possédant des séries discrètes et T un tore maximal anisotrope de H. On note encore $\Phi = \Phi(H_{\mathbb{C}}, T_{\mathbb{C}}) \subset \mathrm{X}^*(T)$ son système de racines et W le groupe de Weyl de Φ.

Dans les paragraphes qui suivent nous allons rappeler brièvement certains ensembles, ou *paquets*, de représentations irréductibles unitaires de $H(\mathbb{R})$ qui ont été définis par Adams et Johnson dans [AJ87] et qui jouent un rôle important dans la théorie d'Arthur [Art89, §5] (voir aussi [ABV92] pour un contexte très général). Le point de départ est la donnée d'un *paramètre d'Adams-Johnson*

$$\varphi : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \to \widehat{H}(\mathbb{C})$$

qui est un morphisme de groupes satisfaisant certaines propriétés, qui seront d'abord discutées informellement et précisées plus bas. Adams et Johnson lui associent un sous-ensemble fini

$$\Pi_{\mathrm{AJ}}(\varphi) \subset \Pi_{\mathrm{unit}}(H(\mathbb{R})),$$

ne dépendant que de la classe de $\widehat{H}(\mathbb{C})$-conjugaison de φ.

Le paramètre φ détermine d'abord une représentation $V_\varphi \in \mathrm{Irr}(H_\mathbb{C})$. Par exemple, les paramètres d'Adams-Johnson triviaux sur le facteur $\mathrm{SL}_2(\mathbb{C})$ s'identifient exactement avec les paramètres discrets de Langlands rappelés au §4.5, et pour un tel φ alors par définition $\Pi_{\mathrm{AJ}}(\varphi) = \Pi_{V_\varphi}$. En général, $\Pi_{\mathrm{AJ}}(\varphi)$ est constitué de représentations ayant même caractère infinitésimal que V_φ ; mieux, elles possèdent de la $(\mathfrak{h}, K)$-cohomologie à coefficients dans V_φ^* [VZ84]. Concrètement, à chaque base $\Delta \subset \Phi$ le paramètre φ fait correspondre un sous-groupe parabolique $P_{\Delta,\varphi} \subset H_\mathbb{C}$ contenant $T_\mathbb{C}$. Soit $L_{\Delta,\varphi} \subset H$ le sous-groupe de Levi de $P_{\Delta,\varphi}$ contenant T, il est nécessairement défini sur $\mathbb{R}$ car $T(\mathbb{R})$ est compact (bien sûr, aucun des paraboliques propres de $H_\mathbb{C}$ contenant T n'est défini sur $\mathbb{R}$). Enfin, φ détermine une représentation ρ de $L_{\Delta,\varphi}(\mathbb{R})$ dimension 1. Sa description exacte par Adams et Johnson est assez délicate, du moins quand $L_{\Delta,\varphi}(\mathbb{R})$ n'est pas connexe[8], mais dans une large mesure sa compréhension ne sera heureusement pas nécessaire à notre discussion. La donnée de $P_{\Delta,\varphi}$ et de ρ permet alors de définir une représentation

$$\pi_{\Delta,\varphi} \in \Pi_{\mathrm{unit}}(H(\mathbb{R}))$$

par induction cohomologique en un degré approprié [Vog81, Vog84]. L'ensemble de ces représentations, lorsque Δ parcourt les bases de Φ, est par définition le paquet $\Pi_{\mathrm{AJ}}(\varphi)$. Soit $W_\mathrm{r} = \mathrm{W}(H,T) \subset W$ (§4.1). Une base $\Delta \subset \Phi$ étant fixée, et si $L = L_{\Delta,\varphi}$, l'application $W \to \Pi_{\mathrm{AJ}}(\varphi)$, $w \mapsto \pi_{w\Delta,\varphi}$, induit alors une bijection (dépendante de Δ)

$$W_\mathrm{r}\backslash W/\mathrm{W}(L_\mathbb{C}, T_\mathbb{C}) \xrightarrow{\sim} \Pi_{\mathrm{AJ}}(\varphi).$$

Précisons maintenant les axiomes (AJ1) & (AJ2) définissant les paramètres d'Adams-Johnson, suivant [AJ87][Kot90, p. 195][CR12, App. A]. Soit $\varphi : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_\mathbb{R} \to \widehat{H}(\mathbb{C})$ un morphisme de groupes supposé continu, algébrique sur le facteur $\mathrm{SL}_2(\mathbb{C})$, et tel que $\varphi(1 \times \mathrm{W}_\mathbb{R})$ est constitué d'éléments semi-simples. Considérons l'homomorphisme $\widetilde{\varphi} : \mathrm{W}_\mathbb{R} \to \widehat{H}(\mathbb{C})$ obtenu en composant φ par le morphisme d'Arthur

$$\mathrm{W}_\mathbb{R} \to \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_\mathbb{R},\ g \mapsto \begin{bmatrix} |\eta(g)|^{1/2} & 0 \\ 0 & |\eta(g)|^{-1/2} \end{bmatrix} \times g,$$

où $\eta : \mathrm{W}_\mathbb{R} \to \mathbb{R}^\times$ est le caractère rappelé au §2.12. Le sous-groupe $\widetilde{\varphi}(\mathbb{C}^*) \subset \widehat{H}(\mathbb{C})$ est connexe et constitué d'éléments semi-simples, on peut donc l'inclure

8. Lorsque $L_{\Delta,\varphi}(\mathbb{R})$ est connexe, le caractère ρ est déterminé par sa différentielle en l'identité, elle-même caractérisée par la propriété que la représentation $\pi_{\Delta,\varphi}$ définie ci-après doit avoir le même caractère infinitésimal que V.

dans un tore maximal

$$S \subset \widehat{H}.$$

Il existe alors un unique couple $\lambda, \mu \in \mathrm{X}_*(S) \otimes \mathbb{C}$ tels que $\lambda - \mu \in \mathrm{X}_*(S)$ et $\xi(\widetilde{\varphi}(z)) = z^{\langle \xi, \lambda \rangle} \overline{z}^{\langle \xi, \mu \rangle}$ pour tout $\xi \in \mathrm{X}^*(S)$ et tout $z \in \mathbb{C}^*$ (voir la note de bas de page §2.12).

(AJ1) – *La classe de $\widehat{H}(\mathbb{C})$-conjugaison de λ, vue dans* $\mathrm{Lie}\,\widehat{H}$*, est le caractère infinitésimal d'une représentation de dimension finie $V_\varphi \in \mathrm{Irr}(H_\mathbb{C})$.*

Cela entraîne en particulier que S est l'unique tore maximal de $\widehat{H}$ contenant $\widetilde{\varphi}(\mathbb{C}^*)$. Cela munit également $\widehat{H}$ d'un unique sous-groupe de Borel B contenant S tel que λ soit dominant relativement à B. On considère ensuite le centralisateur $M \subset \widehat{H}(\mathbb{C})$ du sous-groupe connexe commutatif constitué d'éléments semi-simples $\varphi(1 \times \mathbb{C}^\times)$; c'est donc un sous-groupe de Levi (d'un parabolique) de $\widehat{H}$. Il contient S.

La donnée d'une base Δ de Φ permet d'identifier la donnée radicielle basée $(\mathrm{X}^*(T), \Phi, \Delta, \cdots)^\vee$ à $\Psi(\widehat{H}, S, B)$, et fournit en particulier un isomorphisme privilégié

$$i_\Delta : \mathrm{X}_*(T) \xrightarrow{\sim} \mathrm{X}^*(S)$$

envoyant $\Delta^\vee$ sur la base de $\Phi(\widehat{H}, S)$ associée à B. Soit $L_{\Delta,\varphi} \subset H_\mathbb{C}$ l'unique sous-groupe de Levi (de sous-groupes paraboliques) contenant T tel que $i_\Delta(\Phi^\vee(L_{\Delta,\varphi}, T_\mathbb{C})) = \Phi(M, S)$ (en particulier, $M \simeq \widehat{L_{\Delta,\varphi}}$). Soit $P_{\Delta,\Phi} \subset H_\mathbb{C}$ l'unique sous-groupe parabolique de sous-groupe de Levi $L_{\Delta,\varphi}$ contenant le sous-groupe de Borel de $H_\mathbb{C}$ contenant T et associé à Δ, c'est le sous-groupe mentionné dans la description informelle plus haut. L'axiome restant sert à la définition du caractère χ (voir [AJ87] et la rédaction de Taïbi [Tai14, §4.2.2] pour plus de précisions à ce sujet).

(AJ2) – *L'homomorphisme* $\mathrm{SL}_2(\mathbb{C}) \to M$ *induit par φ est principal, c'est-à-dire qu'il induit un $\mathfrak{sl}_2$-triplet de* $\mathrm{Lie}\,M$ principal *au sens de Kostant* [Kos59]. *De plus, le centralisateur* C_φ *de* $\mathrm{Im}\,\varphi$ *dans $\widehat{H}(\mathbb{C})$ est fini.*

La première hypothèse entraîne que le centralisateur de $\varphi(\mathrm{SL}_2(\mathbb{C}) \times \mathbb{C}^\times)$ dans $\widehat{H}(\mathbb{C})$ est le centre $\mathrm{Z}(M)$ de M. Le groupe C_φ est donc le sous-groupe de $\mathrm{Z}(M)$ fixé par la conjugaison par $\varphi(1 \times j)$. La seconde hypothèse assure que

$$\mathrm{C}_\varphi = \mathrm{Z}(M)_2 \overset{\text{déf.}}{=} \{z \in \mathrm{Z}(M), z^2 = 1\}.$$

(voir par exemple [CR12, Lemma A.1]) Comme l'a remarqué Taïbi [Tai14, §4.2.2], sous la première hypothèse de (AJ2), alors la seconde est aussi équivalente à demander que φ est trivial sur $1 \times \mathbb{R}_{>0}$ (c'est évidemment nécessaire, car $\mathbb{R}^\times$ est le centre de $\mathrm{W}_\mathbb{R}$, mais également suffisant). Quand H est un groupe

classique, il est facile déterminer tous ses paramètres d'Adams-Johnson : voir l'exemple 4.15 et le lemme 4.16.

Cas des formes réelles pures

Considérons pour clore ce paragraphe le cas général des formes réelles pures de H. Soit $c \in H^1(\mathbb{R}, H)$. La construction *loc. cit.* d'Adams et Johnson, qui n'est pas spécifique aux groupes déployés, associe également à tout paramètre d'Adams-Johnson φ de H, un ensemble de représentations

$$\Pi^c_{\mathrm{AJ}}(\varphi) \subset \Pi_{\mathrm{unit}}(H_c(\mathbb{R})).$$

Si $t \in T_2$ est dans la classe c, et si Δ est une base de Φ, on dispose encore du sous-groupe parabolique $T_{\mathbb{C}} \subset P_{\Delta,\varphi} \subset (H_t)_{\mathbb{C}} = H_{\mathbb{C}}$. Son sous-groupe de Levi $T \subset L_{\Delta,\varphi,t} \subset H_t$, défini sur $\mathbb{R}$, est la forme réelle pure de $L_{\Delta,\varphi}$ associée à σ_t (§4.8). Adams et Johnson lui associent encore un caractère $\rho : L_{\Delta,\varphi,t}(\mathbb{R}) \to \mathbb{C}^*$, et définissent une représentation

$$\pi_{\Delta,\varphi,t} \in \Pi_{\mathrm{unit}}(H_t(\mathbb{R})) \xrightarrow{\sim} \Pi_{\mathrm{unit}}(H_c(\mathbb{R}))$$

par induction chomologique de ρ à $H_t(\mathbb{R})$, relativement à $P_{\Delta,\varphi}$, en un degré adéquat. Ils posent $\Pi^c_{\mathrm{AJ}}(\varphi) = \{\pi_{\Delta,\varphi,t}\}$, où Δ parcourt les bases de Φ et $t \in T_2$ les représentants de c. Comme au §4.8, les variables Δ et t sont redontantes et reliées par la relation $\pi_{w\Delta,\varphi,w\cdot t} \simeq \pi_{\Delta,\varphi,t}$ valable pour toute base $\Delta \subset \Phi$, tout $t \in T_2$ et tout $w \in W$. Si $t \in T_2$ et une base $\Delta \subset \Phi$ sont fixés, et si $L = L_{\Delta,\varphi,t} \subset H_t$ est le sous-groupe de Levi associé, l'application $W \to \Pi_{\mathrm{unit}}(H(\mathbb{R}))$, $w \mapsto \pi_{w\Delta,\varphi,t}$, induit cette fois-ci une bijection

$$\mathrm{W}(H_t, T)\backslash W/\mathrm{W}(L_{\mathbb{C}}, T_{\mathbb{C}}) \xrightarrow{\sim} \Pi^c_{\mathrm{AJ}}(\varphi).$$

Le cas particulier $c = 1$ donne un autre point de vue sur $\Pi^1_{\mathrm{AJ}}(\varphi) = \Pi_{\mathrm{AJ}}(\varphi)$.

4.15. Exemple : paramètres d'Adams-Johnson de Sp_{2g}

Considérons le $\mathbb{R}$-groupe $H = \mathrm{Sp}_{2g}$. Notons $V = \mathbb{C}^{2g+1}$ l'espace sous-jacent à la représentation standard de $\widehat{H} = \mathrm{SO}_{2g+1}$, muni de la forme quadratique q standard. Soit $\varphi : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \to \mathrm{SO}(V)$ un homomorphisme continu, algébrique sur le facteur $\mathrm{SL}_2(\mathbb{C})$, et trivial sur $1 \times \mathbb{R}_{>0}$. Comme $\mathrm{W}_{\mathbb{R}}/\mathbb{R}_{>0}$ est compact, le groupe $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}}$ agit de manière semi-simple sur V, qui se décompose donc en somme orthogonale

$$V = \bigoplus_{j \in J} V_j$$

de sous-espaces irréductibles V_j. En tant que représentation de $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}}$ triviale sur $1 \times \mathbb{R}_{>0}$, V_j est nécessairement autoduale. Observons aussi que si $\mathrm{q}_{|V_j}$ est dégénérée, alors $\mathrm{q}(V_j) = 0$ et il existe $j' \neq j$ tel que $V_{j'} \simeq V_j^* \simeq V_j$.

Supposons que φ satisfait (AJ1), nous allons analyser φ et constater notamment que (AJ2) est automatiquement satisfaite. D'après le cas I du §2.6, les V_j sont deux-à-deux non isomorphes (donc non-dégénérés), et un seul d'entre eux est de dimension impaire, disons V_0. Il est alors évident que C_φ est le sous-groupe fini de $\mathrm{SL}(V)$ constitué des éléments g tels que $g(V_j) \subset V_j$ pour tout j et $g_{|V_j} = \pm \mathrm{id}_{V_j}$. De plus, V_0 est une représentation irréductible de $\mathrm{SL}_2(\mathbb{C})$, avec $\mathrm{W}_{\mathbb{R}}$ agissant par multiplication par un caractère χ_0, et pour $j \neq 0$ on peut écrire

$$V_j \simeq Q_j \otimes R_j, \;\; Q_j \simeq \mathrm{Sym}^{d_j - 1}\mathrm{St}_2, \;\; R_j \simeq \mathrm{I}_{r_j},$$

avec $r_j > 0$ et $d_j + r_j \equiv 1 \bmod 2$. On peut munir Q_j et R_j de formes bilinéaires non-dégénérées, préservées respectivement par $\mathrm{SL}_2(\mathbb{C})$ et $\mathrm{W}_{\mathbb{R}}$, et dont le produit tensoriel est la forme bilinéaire sur V_j associée à q. La restriction de R_j à $\mathbb{C}^* \subset \mathrm{W}_{\mathbb{R}}$ est somme directe des deux droites stables et isotropes, disons ℓ_j et ℓ'_j, l'élément $z \in \mathbb{C}^*$ agissant par multiplication par $(\frac{z}{|z|})^{r_j}$ sur ℓ_j. Ainsi, $M \subset \mathrm{SO}_V$ est le sous-groupe

$$\mathrm{SO}_{V_0} \times \prod_{j \neq 0} M_j$$

où $M_j \subset \mathrm{SO}_{V_j}$ est le stabilisateur des lagrangiens transverses $Q_j \otimes \ell_j$ et $Q_j \otimes \ell'_j$. En particulier, $M_j \simeq \mathrm{GL}_{d_j}$, M est bien le sous-groupe de Levi d'un parabolique de SO_V, et $\mathrm{C}_\varphi = \mathrm{Z}(M)_2$. Rappelons qu'un $\mathbb{C}$-morphisme $\mathrm{SL}_2 \to L$ avec L classique (resp. GL_d) est principal si, et seulement si, la représentation de SL_2 composée de f et de la représentation standard (resp. tautologique) de L est irréductible, ou somme de la représentation triviale et d'une irréductible non triviale si $L(\mathbb{C}) \simeq \mathrm{SO}_{2r}(\mathbb{C})$. Cela montre que (AJ2) est satisfaite. Une analyse similaire à celle faite jusqu'à présent montre plus généralement le lemme suivant.

Lemme 4.16. *Supposons que* $H_{\mathbb{C}} \in \mathrm{Class}_{\mathbb{C}}$ *et soit* $\mathrm{St} : \widehat{H}(\mathbb{C}) \to \mathrm{SL}_n(\mathbb{C})$ *la représentation standard. Soit* $\varphi : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \to \widehat{H}(\mathbb{C})$ *un morphisme continu, algébrique sur le facteur* $\mathrm{SL}_2(\mathbb{C})$*, et trivial sur* $1 \times \mathbb{R}_{>0}$*. Alors* φ *est un paramètre d'Adams-Johnson si, et seulement si, il satisfait* (AJ1) *et si la représentation* $\mathrm{St} \circ \varphi : \mathrm{W}_{\mathbb{R}} \to \mathrm{SL}_n(\mathbb{C})$ *est sans multiplicités.*

Poursuivons l'étude de l'exemple précédent : décrivons le tore S et le sous-groupe de Borel B de SO_V associés à φ. Convenons que $Q_0 := V_0$.

Observons que la restriction de Q_j au tore diagonal de $\mathrm{SL}_2(\mathbb{C})$ est somme directe de d_j droites stables canoniques $\ell_{j,n}$, où $n = \frac{d_j-1}{2}, \cdots, \frac{1-d_j}{2}$, l'élément $\begin{bmatrix} |z|^{1/2} & 0 \\ 0 & |z|^{-1/2} \end{bmatrix}$ agissant sur $\ell_{j,n}$ par multiplication par $|z|^n$. On a d'une part une décomposition orthogonale

$$V = V^+ \oplus V^- \oplus \ell_{0,0},$$

où V^+ (resp. V^-) est le lagrangien somme directe des $Q_j \otimes \ell_j$ (resp. $Q_j \otimes \ell'_j$) et des $\ell_{0,n}$ avec $n > 0$ (resp. $n < 0$). D'autre part, l'espace V^+ est lui-même somme directe des g droites $\ell_{0,n}$ (avec $n > 0$) et $\ell_{j,m} \otimes \ell_j$ ($j \neq 0$, m arbitraire). La condition (AJ1) determine une unique manière d'ordonner ces g droites isotropes, disons $\mathbb{C}e_1, \ldots, \mathbb{C}e_g \subset V^+$, sorte que pour tout $z \in \mathbb{C}^\times$ l'élément $\widetilde{\varphi}(z)$ agisse par multiplication par $z^{w_i}\overline{z}^{w'_i}$ sur e_i, où (w_i, w'_i) est un couple d'entiers tel que

$$w_1 > w_2 > \cdots > w_g > 0$$

(ils s'expriment bien sûr simplement en terme des r_j et d_j, mais il ne sera pas nécessaire d'expliciter comment). Le tore S est le stabilisateur dans SO_V des droites $\mathbb{C}e_i$, $i = 1, \ldots, g$, et de V^-. Le sous-groupe de Borel $S \subset B \subset \mathrm{SO}_{2g+1}$ est le stabilisateur du drapeau associé aux e_i comme au §VI.1.3, il rend l'élément λ_φ dominant par décroissance et positivité des w_i.

Décrivons enfin les $L_{\Delta,\varphi}$. Considérons le a-module hyperbolique $E = \mathrm{H}(\mathbb{R}^g)$, $I \in \mathrm{Sp}(E)$ de carré $-\mathrm{id}_E$ et h la forme hermitienne définie positive sur E associée comme dans le §4.7. Choisissons une décomposition de l'espace hermitien (E, h) en somme orthogonale de $\mathbb{R}$-plans I-stables, et notons $T \subset \mathrm{U_h}$ le tore associé, constitué des éléments de Sp_E stabilisant chacun de ces plans ; c'est un tore maximal anisotrope de H. Si $P \subset E$ est un $\mathbb{R}$-plan I-stable, on dispose d'une décomposition canonique

$$P \otimes_{\mathbb{R}} \mathbb{C} = P^+ \oplus P^-$$

en somme de droites propres de I pour les valeurs propres respectives de $+i$ et $-i$. Le choix d'une base Δ de $\Phi(H_\mathbb{C}, T_\mathbb{C})$ équivaut à celui d'une numérotation $P_1, \ldots, P_g$ des $\mathbb{R}$-plans définissant T, ainsi que pour tout $i = 1, \ldots, g$ d'un signe $s_i \in \{+, -\}$: le sous-groupe de Borel contenant T associé à une telle donnée est le stabilisateur du drapeau formé sur

$$P_1^{s_1}, P_2^{s_2}, \ldots, P_g^{s_g}$$

(voir le §VI.1.3). Un tel choix étant fait, décrivons le $\mathbb{R}$-groupe $L_{\Delta,\varphi}$ associé. Notons $\eta_i \in \mathrm{X}^*(T_\mathbb{C})$ le caractère de $T_\mathbb{C}$ sur $P_i^{s_i}$, ainsi que (η_i^*) la base

duale des (η_i) dans $\mathrm{X}_*(T_{\mathbb{C}})$. D'après le §VI.1.3, l'isomorphisme $i_\Delta : \mathrm{X}_*(T_{\mathbb{C}}) \simeq \mathrm{X}^*(S)$ envoie η_i^* sur le caractère de S sur la droite $\mathbb{C}e_i$, et par définition $i_\Delta(\Phi^\vee(L_{\Delta,\varphi}, T_{\mathbb{C}})) = \Phi(M, S)$. On en déduit immédiatement le $\mathbb{C}$-groupe $L_{\Delta,\varphi}$. Concrètement, il existe une unique décomposition $E = \oplus_{j\in J} E_j$, où E_j est la somme directe des $\mathbb{R}$-plans P_i pour les indices i tels que $\mathbb{C}e_i \subset V_j$. En particulier, $\dim_{\mathbb{R}} E_j = \dim_{\mathbb{C}} V_j$ si $j \neq 0$ et $\dim_{\mathbb{R}} E_0 = \dim_{\mathbb{C}} V_0 - 1$. De plus, si $j \neq 0$ il existe une décomposition en somme de lagrangiens transverses

$$E_j \otimes \mathbb{C} = E_j^+ \oplus E_j^-$$

où E_j^+ (resp. E_j^-) est la somme directe des $P_i^{s_i}$ (resp. $P_i^{-s_i}$) appartenant à $E_j \otimes \mathbb{C}$. Par définitions, le $\mathbb{C}$-groupe $L_{\Delta,\varphi}$ est le sous-groupe de $\mathrm{Sp}_{E\otimes\mathbb{C}}$

$$\mathrm{Sp}_{E_0\otimes\mathbb{C}} \times \prod_{j\neq 0} L_j,$$

où $L_j \simeq \mathrm{GL}_{E_i^+}$ est le stabilisateur dans $\mathrm{Sp}_{E_i\otimes\mathbb{C}}$ des sous-espaces E_j^+ et E_j^-. Il ne reste qu'à expliciter sa structure réelle. Soit $I' \in T(\mathbb{R}) \subset \mathrm{Sp}(E)$ l'élément de carré $-\mathrm{id}_E$ coïncidant avec $s_i I$ sur P_i. Soient h' la forme hermitienne sur E associée à I', définie par $\mathrm{h}'(u) = \mathrm{a}(I'u, u)$, et $\mathrm{h}'_j : E_j \to \mathbb{R}$ la restriction de h' à E_j ; elle est de signature (p_j, q_j) où q_j est le nombre des indices i tels que $P_i^- \subset E_j^+$. L'élément I' induit un élément central de L_j pour tout $j \neq 0$ et donc $L_j = \mathrm{U}_{\mathrm{h}'_j}$. Au final, on a l'isomorphisme de $\mathbb{R}$-groupes

$$L_{\Delta,\varphi} \simeq \mathrm{Sp}_{E_0} \times \prod_{j\neq 0} \mathrm{U}_{\mathrm{h}'_j}.$$

En particulier, $L_{\Delta,\varphi}(\mathbb{R})$ est connexe.

4.17. Paramétrisation duale de $\Pi^c_{\mathrm{AJ}}(\varphi)$

Soient φ un paramètre d'Adams-Johnson du $\mathbb{R}$-groupe déployé H et $c \in H^1(\mathbb{R}, H)$ une forme réelle pure de H. Suivant [AJ87, §3] et [Art89, §5], le paquet $\Pi^c_{\mathrm{AJ}}(\varphi)$ est encore muni d'une application de paramétrisation naturelle

$$\Pi^c_{\mathrm{AJ}}(\varphi) \longrightarrow \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_\varphi, \mathbb{C}^\times), \pi \mapsto \chi^c_{O,\varphi}(\pi),$$

induite par celle de Shelstad, que nous allons maintenant rappeler (voir aussi [Kot90, §8] [CR12, App. A] [Tai14, §4.2.2]). Elle ne dépend, comme au §4.2, que du choix d'un $O \in \mathcal{B}(H)$, et que l'on fixe désormais.

Soient $M \supset S \subset B \subset \widehat{H}$ associés à φ comme au §4.14. En particulier, $\mathrm{C}_\varphi = \mathrm{Z}(M)_2$. Fixons $\Delta \in O$, ce qui définit $\rho^\vee \in \frac{1}{2}\mathrm{X}_*(T)$ (§4.2), un isomorphisme

privilégié $i_\Delta : \mathrm{X}_*(T) \xrightarrow{\sim} \mathrm{X}^*(S)$ (§4.5), ainsi qu'un sous-groupe de Levi $L = L_{\Delta,\varphi} \subset H$ (§4.14). L'inclusion $T \to L$ induit une bijection

$$\mathrm{W}(L_{\mathbb{C}}, T_{\mathbb{C}})\backslash H^1(\mathbb{R}, T) \xrightarrow{\sim} H^1(\mathbb{R}, L)$$

d'après Shelstad (voir aussi [Bor14]). Cette bijection et le lemme 4.12 (i) montrent que l'application

$$f_\Delta : \Pi^c_{\mathrm{AJ}}(\varphi) \to H^1(\mathbb{R}, L),$$

envoyant $\pi_{w^{-1}\Delta,\varphi,t}$, pour $w \in W$ et $t \in T_2$ dans la classe c, sur l'image de l'élément $w \star t \in H^1(\mathbb{R}, T)$ dans $H^1(\mathbb{R}, L)$, est bien définie. De plus, elle est injective, d'image égale à la fibre de l'application naturelle $H^1(\mathbb{R}, L) \to H^1(\mathbb{R}, H)$ au dessus de la classe c. On dispose également d'un diagramme commutatif

$$\begin{tikzcd}
H^1(\mathbb{R}, L) \arrow[r, "g_\Delta"] & \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{Z}(M)_2, \mathbb{C}^\times) \\
H^1(\mathbb{R}, T) \arrow[u, "\mathrm{can}"] \arrow[r, "h_\Delta"] & \mathrm{X}^*(S) \otimes \mathbb{Z}/2\mathbb{Z} \arrow[u, "\mathrm{can}"']
\end{tikzcd}$$

Les applications verticales sont les applications évidentes (celle de droite étant notamment induite par l'inclusion $\mathrm{Z}(M)_2 \subset S$), l'application h_Δ est la composée de $i_\Delta \otimes \mathbb{Z}/2\mathbb{Z}$ par l'isomorphisme canonique $H^1(\mathbb{R}, T) \xrightarrow{\sim} \mathrm{X}_*(T) \otimes \mathbb{Z}/2\mathbb{Z}$ rappelé au §4.5, et l'application g (un cas particulier des constructions générales de Kottwitz [Kot84]) est l'unique application faisant commuter ce diagramme. Concrètement, si $x \in H^1(\mathbb{R}, L)$, et si $t \in T_2$ est dans la classe x, que l'on écrit $t = e^{i\pi\mu}$ avec $\mu \in \mathrm{X}_*(T)$, alors $g(x)$ est la restriction à $\mathrm{Z}(M)_2$ du caractère $i_\Delta(\mu) \in \mathrm{X}^*(S)$ (elle ne dépend ni du choix de t dans la classe x, ni bien sûr de celui de μ). Au final, on pose

$$\chi^c_{O,\varphi}(\pi) \overset{\text{déf.}}{=} g_\Delta \circ f_\Delta(\pi)$$

(il ne dépend que O et non de $\Delta \in O$). Concrètement, pour tout $w \in W$ et $t = e^{i\pi\mu} \in T_2$ dans la classe c, le caractère $\chi^c_{O,\varphi}(\pi_{w^{-1}\Delta,\varphi,t})$ est la restriction à $\mathrm{Z}(M)_2$ de $i_\Delta(w(\mu + \rho^\vee) - \rho^\vee)$, où $\rho^\vee$ est relatif à Δ.

On prendra garde que comme l'ont remarqué Adams et Johnson, $\pi \mapsto \chi^c_{O,\varphi}(\pi)$ n'est pas injective en générale. Terminons par quelques observations simples mais importantes concernant le comportement des séries discrètes, suivant [Kot90, §8] et [CR12, App. A]. Tout d'abord, nous avons déjà dit que lorsque φ est trivial sur le facteur SL_2, alors la construction d'Adams et Johnson redonne $\Pi^c_{\mathrm{AJ}}(\varphi) = \Pi_{V_\varphi}$. Plus précisément, dans ce cas on a $M = S$,

$L_{\Delta,\varphi} = T$ pour toute base Δ de Φ, et la représentation $\pi_{\Delta,\varphi,t}$ coïncide avec π_{Δ,V_φ}. Il est alors évident que les deux paramétrisations $\chi^c_{O,\varphi}$ et χ^c_O coïncident. Correctement formulée, cette propriété s'étend aux séries discrètes de $H_c(\mathbb{R})$ intervenant dans $\Pi^c_{\mathrm{AJ}}(\varphi)$ pour tout φ, comme l'a observé Kottwitz [Kot90, p. 196], rappelons comment. Pour cela, fixons un paramètre d'Adams-Johnson φ de H. Il lui est associé une suite d'inclusions

$$\mathrm{C}_\varphi = \mathrm{Z}(M)_2 \subset S \subset B \subset \widehat{H} \tag{4.7}$$

définie au §4.14. Suivant Kottwitz, observons qu'il existe un paramètre discret $\varphi_{\mathrm{disc}} : \mathrm{W}_{\mathbb{R}} \to \widehat{H}(\mathbb{C})$, unique à conjugaison près par $S(\mathbb{C})$, ayant disons même caractère infinitésimal que V_φ, tel que $\varphi_{\mathrm{disc}}(\mathbb{C}^\times) \subset S(\mathbb{C})$, et de caractère infinitésimal dominant relativement à B (§4.5). En particulier, on dispose d'une inclusion canonique

$$\mathrm{C}_\varphi = \mathrm{Z}(M)_2 \to \mathrm{C}_{\varphi_{\mathrm{disc}}} = S_2. \tag{4.8}$$

Proposition 4.18. *Soient φ un paramètre d'Adams-Johnson de H et $c \in H^1(\mathbb{R}, H)$. Soient $T \subset H$ un tore maximal anisotrope, O une W_{r}-orbite dans $\mathcal{B}(T)$, $t_{\mathrm{b}} \in T_2$ l'élément associé à O, $t \in T_2$ dans la classe c, et Δ une base de $\Phi(H_{\mathbb{C}}, T_{\mathbb{C}})$.*

(i) La série discrète $\pi_{\Delta,V_\varphi,t}$ appartient à $\Pi^c_{\mathrm{AJ}}(\varphi)$ si, et seulement si, $tt_{\mathrm{b}} \in \mathrm{Z}(L_{\Delta,\varphi})$, auquel cas $\pi_{\Delta,V_\varphi,t} \simeq \pi_{\Delta,\varphi,t}$.

(ii) Si $\pi \in \Pi^c_{\mathrm{AJ}}(\varphi)$ est une série discrète, alors $\chi^c_{O,\varphi}(\pi)$ est la restriction de $\chi^c_O(\pi)$ à C_φ via l'homomorphisme canonique (4.8).

Démonstration. [CR12, Lemma A.3 & A.5] et [Kot90, p. 196]. □

Exemple 4.19. Soit $c \in H^1(\mathbb{R}, H)$ telle que $H_c(\mathbb{R})$ est compact. Alors $\Pi^c_{\mathrm{AJ}}(\varphi) = \{V_\varphi\}$ pour tout paramètre d'Adams-Johnson φ. De plus, d'après le lemme 4.13 et la proposition 4.18, $\delta^c_{V_\varphi}$ est la restriction à $\mathrm{C}_\varphi = S_2 \to S$ de $\rho^\vee + \mu \in \mathrm{X}^*(S)$. Ici, S désigne le tore maximal de $\widehat{H}$ associé à φ, $\rho^\vee$ désigne la demi-somme des racines positives de $(\widehat{H}, S)$ relativement à l'unique sous-groupe de Borel rendant le caractère infinitésimal de φ dominant (§4.14), et l'image de μ dans $\mathrm{X}^*(S) \otimes \mathbb{Z}/2\mathbb{Z}$ est définie *loc. cit.* De manière alternative, elle appartient au noyau de l'application naturelle $\mathrm{X}^*(S) \otimes \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{X}^*(S_{\mathrm{sc}}) \otimes \mathbb{Z}/2\mathbb{Z}$, où le tore S_{sc} désigne l'image inverse de S dans le revêtement universel de $\widehat{H}$ [CR12, Lemma A.6].

Exemple 4.20. Soient $H = \mathrm{Sp}_{2g}(\mathbb{R})$, $V \in \mathrm{Irr}(H_{\mathbb{C}})$ et π la série discrète holomorphe ou anti-holomorphe de $H(\mathbb{R})$ ayant même caractère infinitésimal que V (§4.7). Soient $T \subset H$ un tore maximal anisotrope et $K \subset H(\mathbb{R})$ le sous-groupe compact maximal contenant $T(\mathbb{R})$, choisis par exemple comme au §4.7. Nous avons vu dans ce paragraphe que $\pi \simeq \pi_{\pm\Delta',V_\varphi,1}$ où Δ' est la base donnée *loc. cit.*. Soit $\varphi : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \to \widehat{H}(\mathbb{C})$ un paramètre d'Adams-Johnson tel que $V_\varphi \simeq V$. La proposition 4.18 montre donc que $\pi \in \Pi_{\mathrm{AJ}}(\varphi)$ si, et seulement si, $t_{\mathrm{b}} \in \mathrm{Z}(L_{\pm\Delta',\varphi})$. D'après le lemme 4.4 (i), il est encore équivalent à demander que $L_{\pm\Delta',\varphi}(\mathbb{R}) \subset K$. Mais $L_{\pm\Delta',\varphi}$ est décrit par la recette du §4.15 ; sachant que la base Δ' a par construction la propriété que tous les s_i sont de même signe, on constate que $L_{\pm\Delta',\varphi}(\mathbb{R}) \subset K$ si, et seulement si, $\dim E_0 = d_0 - 1 = 0$ dans les notations *loc. cit.* Au final, $\pi \in \Pi_{\mathrm{AJ}}(\varphi)$ si, et seulement si, le seul constituant de dimension impaire de la représentation semi-simple $\mathrm{St} \circ \varphi$ est de dimension 1 (on a redémontré le [CR12, Lemma 9.4]).

4.21. Lien avec les paquets d'Arthur

La conjecture suivante fait partie du folklore [Art89, §5] [Art13, p. 43].

Conjecture 4.22. *Soient H le $\mathbb{R}$-groupe déployé Sp_{2g} ou $\mathrm{SO}_{r+1,r}$, ainsi que φ une classe de $\widehat{H}(\mathbb{C})$-conjugaison de paramètres d'Adams-Johnson de H. Si $(\Pi(\varphi), \iota, \chi)$ désigne le triplet qui lui est associé par Arthur* [Art13, Thm. 1.5.1]*, suivant les notations du §3.8, alors :*

(a) $\iota : \Pi(\varphi) \to \Pi_{\mathrm{unit}}(H(\mathbb{R}))$ est une injection d'image $\Pi_{\mathrm{AJ}}(\varphi)$.

(b) le caractère $\chi \circ \iota^{-1} : \Pi_{\mathrm{AJ}}(\varphi) \to \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_\varphi, \mathbb{C}^\times)$, bien défini d'après le (a), coïncide avec le caractère $\pi \mapsto \chi^1_{O,\varphi}(\pi)$ défini au §4.17.

Dans le (b) ci-dessus, $O \in \mathcal{B}(H)$ correspond à la donnée de Whittaker choisie par Arthur [Art13, p. 55].

Remarque 4.23. Comme nous l'avons déjà dit au §4.5, cette conjecture est connue si φ est trivial sur le facteur $\mathrm{SL}_2(\mathbb{C})$ par les travaux de Shelstad et Mezo. En général, des progrès concernant cette conjecture ont récemment été obtenus par Colette Moeglin et Nicolas Arancibia (thèse en préparation). Plus précisément, Arancibia annonce la démonstration de la conjecture 4.22 dans le cas particulier où chaque constituant irréductible de la représentation $\mathrm{St}\circ\varphi$, que l'on peut écrire sous la forme $U \otimes V$ avec U (resp. V) représentation irréductible de $\mathrm{SL}_2(\mathbb{C})$ (resp. $\mathrm{W}_{\mathbb{R}}$), satisfait $\dim V = 1$ ou $\dim U \leq 4$.

Remarque 4.24. La conjecture 4.22 (et le théorème ci-dessus) admettent une variante pour le $\mathbb{R}$-groupe $H = \mathrm{SO}_{r,r}$ avec $r \equiv 0 \bmod 2$ dans laquelle

$\Pi_{\mathrm{unit}}(H(\mathbb{R}))$ est remplacé par $\widetilde{\Pi}_{\mathrm{unit}}(H(\mathbb{R}))$ (§3.8), et $\Pi_{\mathrm{AJ}}(\varphi)$ par son image dans $\widetilde{\Pi}_{\mathrm{unit}}(H(\mathbb{R}))$ (on dispose d'un analogue pour $\Pi_{\mathrm{AJ}}(\varphi)$ du lemme 4.6).

Ainsi que l'annonce Arthur [Art13, Chap. 9], sa description de $\Pi_{\mathrm{disc}}(G)$ et la formule de multiplicité énoncée au §3.8 pour les $\mathbb{Z}$-groupes G de Chevalley admet un analogue aux autres $\mathbb{Z}$-groupes classiques, à savoir les $\mathbb{Z}$-groupes spéciaux orthogonaux SO_L introduits au §VIII.1. Fixons donc un tel L et posons $G = \mathrm{SO}_L$; on suppose de plus que $G(\mathbb{R})$ a des séries discrètes, *i.e.* que $L \otimes \mathbb{R}$ est de signature paire s'il est de rang pair (le cas important pour la suite est $G = \mathrm{SO}_n$). Notons également $G^\star$ le groupe (special orthogonal) de Chevalley tel que $G_{\mathbb{C}} \simeq G^\star_{\mathbb{C}}$.

Dans la généralité considérée par Arthur, l'énoncé même de sa formule dépend d'une donnée auxiliaire, à savoir d'une "réalisation" de G comme forme intérieure de $G^\star$. Le cas particulier du $\mathbb{Z}$-groupe $G = \mathrm{SO}_L$ est particulièrement agréable car G peut être construit comme forme intérieure pure "sur $\mathbb{Z}$" de $G^\star$; disons simplement que cela vient de ce que $\langle \pm 1 \rangle \otimes L$ est localement isomorphe pour la topologie étale sur $\mathrm{Spec}(\mathbb{Z})$ à $\mathrm{H}(\mathbb{Z}^r)$ si le rang de L est pair, et à $\mathrm{H}(\mathbb{Z}^r) \oplus \mathrm{A}_1$ sinon (§II.2, Appendice B). Cette propriété semble sensiblement simplificatrice pour les questions de normalisation des facteurs de transferts évoquées par Arthur *loc. cit.* et étudiées par Kaletha [Kal13].

Plus concrètement, appelons *réalisation réelle* de G la donnée d'un couple $\xi = (c, f)$ où $c \in \mathrm{H}^1(\mathbb{R}, G^\star_{\mathbb{R}})$ et $f : G_{\mathbb{R}} \xrightarrow{\sim} (G^\star_{\mathbb{R}})_c$ est un isomorphisme. Il existe toujours des réalisations réelles de G : on l'a vu au cours de l'exemple traité à la fin du §4.8 quand L est de rang impair, le cas du rang pair étant analogue (il utilise que la signature de $L \otimes \mathbb{R}$ est paire). Une telle réalisation étant donnée, il y a un sens à définir pour tout paramètre d'Adams-Johnson φ de $G_{\mathbb{R}}$, ainsi que $O \in \mathcal{B}(G^\star_{\mathbb{R}})$, un couple

$$(\Pi^{\xi}_{\mathrm{AJ}}(\varphi), \chi^{\xi}_{O,\varphi}),$$

avec $\Pi^{\xi}_{\mathrm{AJ}}(\varphi) \subset \Pi_{\mathrm{unit}}(G(\mathbb{R}))$ et $\chi^{\xi}_{O,\varphi} : \Pi_{\mathrm{AJ}}(\varphi) \to \mathrm{Hom}_{\mathrm{groupes}}(\mathrm{C}_\varphi, \mathbb{C}^\times)$, en transportant simplement le couple $(\Pi^{c}_{\mathrm{AJ}}(\varphi), \chi^{c}_{O,\varphi})$ par la bijection $\Pi_{\mathrm{unit}}(G(\mathbb{R})) \xrightarrow{\sim} \Pi_{\mathrm{unit}}((G^\star_{\mathbb{R}})_c(\mathbb{R}))$ induite par f.

Un second phénomène intéressant est que le groupe de similitudes projectives $\mathrm{P}\widetilde{G}(\mathbb{Z})$ rencontre toutes les composantes connexes de $\mathrm{P}\widetilde{G}(\mathbb{R})$ (pour le voir, utiliser par exemple le théorème II.2.7). Comme cela a déjà été observé dans [CR12], cela suggère que la formule finale d'Arthur doit est complètement canonique. Tout comme au §3.8, elle fait intervenir certains ensembles de représentations unitaires de $G(\mathbb{R})$ (dépendant d'un choix de réalisation réelle de G) dont l'existence, ainsi qu'une caractérisation, est annoncée par

Arthur. On s'attend encore à ce que ceux qui contiennent des séries discrètes de $G(\mathbb{R})$ soient exactement les paquets d'Adams-Johnson. Afin, de ne pas multiplier les énoncés, et comme nous avons déjà traité en détail le cas des groupes de Chevalley, nous ne formulerons précisément que la conjecture finale attendue, étant entendu qu'il s'agit de la concaténation de deux énoncés. Si $U, U' \in \Pi_{\mathrm{unit}}(G(\mathbb{R}))$, nous noterons $U \sim U'$ si $U \simeq U'$, ou si $G(\mathbb{R})$ est un groupe spécial orthogonal pair et U et U' sont conjugués extérieurs l'un de l'autre par le groupe orthogonal pair réel correspondant ; si $X \subset \Pi_{\mathrm{unit}}(G(\mathbb{R}))$ on note enfin $\widetilde{X} = \{U \in \Pi_{\mathrm{unit}}(G(\mathbb{R})) \mid \exists U' \in X, U \sim U'\}$.

Conjecture 4.25. *Soient G un $\mathbb{Z}$-groupe classique,* $\mathrm{St} : \widehat{G} \to \mathrm{SL}_n$ *la représentation standard, $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$ et $U \in \Pi_{\mathrm{unit}}(G(\mathbb{R}))$ une série discrète telle que* $\mathrm{St}(\mathrm{Inf}_U) = \psi_\infty$.

Soient ξ une réalisation réelle de G, $E \subset \Pi(G)$ l'ensemble des représentations π telles que $\pi_\infty \sim U$ et $\psi(\pi, \mathrm{St}) = \psi$ (c'est un singleton si G n'est pas un groupe spécial orthogonal pair), ainsi que $\nu_\infty : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \longrightarrow \widehat{G}$ un paramètre d'Adams-Johnson associé à ψ par la recette décrite au §3.8. Alors $E \cap \Pi_{\mathrm{disc}}(G) = \emptyset$, sauf si $U \in \Pi^{\xi}_{\mathrm{AJ}}(\nu_\infty)$ et

$$(\chi^{\xi}_{O,\nu_\infty}(U))_{|\mathrm{C}_\psi} = \varepsilon_\psi, \tag{4.9}$$

auquel cas $\sum_{\pi \in E} \mathrm{m}(\pi) = m_\psi$ où l'entier m_ψ vaut 1, sauf si G est spécial orthogonal pair et $\psi = \oplus_i \pi_i[d_i]$ avec $d_i \equiv 0 \bmod 2$ pour tout i, auquel cas $m_\psi = 2$.

L'assertion de canonicité mentionnée plus haut signifie précisément que bien que le caractère $\chi^{\xi}_{O,\nu_\infty}$ dépende des choix de O et de ξ, sa restriction à $\mathrm{C}_\psi \subset \mathrm{C}_{\nu_\infty}$ n'en dépend pas. En effet, c'est évident si G est spécial orthogonal impair, car tout $\mathbb{R}$-automorphisme de $G_{\mathbb{R}}$ est intérieur et $|\mathcal{B}(G_{\mathbb{R}})| = 1$. Si $G \simeq G^* \simeq \mathrm{Sp}_{2g}$, le groupe $\mathrm{Aut}_{\mathbb{R}}(G_{\mathbb{R}})/\mathrm{Int}(G(\mathbb{R})) = \mathbb{Z}/2\mathbb{Z}$ agit simplement transitivement sur $|\mathcal{B}(G_{\mathbb{R}})| = 2$, de sorte qu'il y a exactement deux choix à considérer ; comme cela avait déjà été observé dans [CR12, Lemma 9.5 & 9.6], le critère (4.9) est en fait le même dans les deux cas (cela sera manifeste dans la démonstration du théorème 5.2). La situation est similaire si G est spécial orthogonal pair, pour lequel il faut de plus tenir compte de l'automorphisme extérieur provenant du groupe orthogonal correspondant (il est d'ailleurs défini sur $\mathbb{Z}$ dès que L possède une racine, i.e. un élément α tel que $\mathrm{q}(\alpha) = 1$).

5. Formules de multiplicité explicites : un formulaire

Si l'on confronte le théorème général d'Arthur Thm. 3.10 (ou la conjecture 4.25) aux considérations et exemples du paragraphe VIII.4, on obtient

des formes explicites de la formule de multiplicité d'Arthur. Dans cette partie, nous nous proposons de les décrire, à la manière de [CR12, §3.29], dans les cas particuliers d'importance pour ce mémoire, à savoir quand $G = \mathrm{Sp}_{2g}$ et pour une composante archimédienne π_∞ dans la série discrète holomorphe, ou quand $G = \mathrm{SO}_n$ pour $n \equiv -1, 0, 1 \bmod 8$.

5.1. Formule explicite pour Sp_{2g}

Dans tout ce paragraphe, g désigne un entier ≥ 1. Soit

$$\psi = \oplus_{i=1}^{k} \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1}),$$

où $k \geq 1$ est un entier et $\pi_i \in \Pi_{\mathrm{cusp}}^{\perp}(\mathrm{PGL}_{n_i})$ et $d_i \geq 1$ pour tout $i = 1, \ldots, k$. On suppose que ψ_∞ satisfait la condition (H2) relativement à Sp_{2g} (§3.4), ce qui signifie que ψ_∞ admet pour valeurs propres $2g+1$ entiers distincts

$$w_1 > \cdots > w_g > 0 > -w_g > \cdots > -w_1.$$

(§2.6 cas I.). D'après le lemme 2.15 (i), il existe un unique entier $i_0 \in \{1, \ldots, k\}$ tel que $n_{i_0} d_{i_0}$ est impair. Quitte à réindexer les π_i, on peut supposer que $i_0 = k$ sans perte de généralité. Observons que d'après ce même lemme, on a également $n_i \equiv 0 \bmod 2$ et $n_i d_i \equiv 0 \bmod 4$ pour tout $i \neq k$, et $n_k d_k \equiv 2g+1 \bmod 4$.

Considérons l'homomorphisme de groupes multiplicatifs $\chi : \{\pm 1\}^{k-1} \to \{\pm 1\}$ défini de la manière suivante. Fixons $1 \leq i \leq k-1$ et notons $s_i \in \{\pm 1\}^{k-1}$ l'élément défini par $(s_i)_j = -1 \Leftrightarrow j = i$. Il y a deux cas :

(i) Si $d_i \equiv 0 \bmod 2$, on pose $\chi(s_i) = (-1)^{\frac{n_i d_i}{4}}$.

(ii) Si $d_i \equiv 1 \bmod 2$, on pose $\chi(s_i) = (-1)^{|K_i|}$ où K_i est l'ensemble des indices $1 \leq j \leq g$ qui sont impairs et tels que $w_j \in \mathrm{Poids}(\pi_i)$.

Théorème* **5.2.** *Soit $\psi = \oplus_{i=1}^{k} \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1})$ tel que ψ_∞ admet $2g+1$ valeurs propres entieres et distinctes, et pour lequel $\pi_k \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_k})$ est telle que $d_k n_k \equiv 1 \bmod 2$. Soit $\pi \in \Pi(\mathrm{Sp}_{2g})$ l'unique représentation telle que $\psi(\pi, \mathrm{St}) = \psi$ et π_∞ est série discrète holomorphe. Supposons la conjecture 4.22 satisfaite pour Sp_{2g} et le morphisme ν_∞ associé à ψ défini au §3.8 (par exemple, $d_i = 1$ pour tout $i = 1, \ldots, k$).*

Alors $\pi \in \Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ si, et seulement si, les deux conditions suivantes sont satisfaites :

(a) $d_k = 1$,

(b) pour tout $i = 1, \ldots, k-1$, on a $\chi(s_i) = \prod_{1 \leq j \leq k, j \neq i} \varepsilon(\pi_i \times \pi_j)^{\mathrm{Min}(d_i, d_j)}$,

où χ désigne le caractère de $\{\pm 1\}^{k-1}$ associé à ψ qui est défini ci-dessus. Enfin, si ces conditions sont satisfaites alors $\mathrm{m}(\pi) = 1$.

Démonstration. Reprenons quelques constructions du §3.8. On choisit notamment $\nu : \mathrm{SL}_2(\mathbb{C}) \times \prod_{i=1}^{k} \widehat{G^{\pi_i}}(\mathbb{C}) \to \mathrm{SO}_{2g+1}(\mathbb{C})$ associé à ψ comme dans ce paragraphe, ainsi que pour chaque $i = 1, \ldots, k$, un homomorphisme $\mu_i : \mathrm{W}_{\mathbb{R}} \to \widehat{G^{\pi_i}}(\mathbb{C})$ tel que $\mathrm{St} \circ \mu_i \simeq \mathrm{L}((\pi_i)_\infty)$. Le groupe C_ν défini *loc. cit.* s'identifie naturellement avec $\{\pm 1\}^{k-1}$, avec leurs éléments distingués $s_1, \ldots, s_{k-1}$. On dispose de plus d'un homomorphisme

$$\nu_\infty : \mathrm{SL}_2(\mathbb{C}) \times \mathrm{W}_{\mathbb{R}} \longrightarrow \mathrm{SO}_{2g+1}(\mathbb{C})$$

déduit de ν et des μ_i. La condition (H2) et les lemmes 4.16 et 3.9 assurent que c'est un paramètre d'Adams-Johnson de Sp_{2g} (et même un paramètre de Langlands discret si $d_i = 1$ pour tout i). Cela donne un sens à l'hypothèse, affirmant que la conjecture 4.22 est satisfaite pour $\mathrm{Sp}_{2g}(\mathbb{R})$ et ν_∞.

D'après l'exemple 4.20, la série discrète holomorphe π_{hol} de $\mathrm{Sp}_{2g}(\mathbb{R})$ de caractère infinitésimal z tel que $\mathrm{St}(z) = \psi_\infty$ est dans $\Pi(\nu_\infty)$ si, et seulement si, $\mathrm{St} \circ \nu_\infty$ ne contient pas de représentation de la forme $\mathrm{Sym}^{d-1}\mathrm{St}_2 \otimes \chi$ avec $d > 1$ et $\chi \in \{1, \epsilon_{\mathbb{C}/\mathbb{R}}\}$. Il est équivalent de demander que $d_k = 1$. En effet, si $i = 1, \ldots, k$ on constate que $\mathrm{c}_\infty(\pi_i)$ admet la valeur propre 0 si, et seulement si, n_i est impair, i.e. $i = k$ (§2.6). D'après le théorème 3.10 et la conjecture 4.22 pour le couple $(\mathrm{Sp}_{2g}, \nu_\infty)$, il ne reste donc qu'à démontrer que

$$\chi^1_{O,\nu_\infty}(\pi_{\mathrm{hol}})_{|\mathrm{C}_\nu} = \chi.$$

Nous allons pour cela spécifier les constructions du §4.14 relatives à ν_∞, à la manière de l'étude faite dans l'exemple 4.15. On considère l'homomorphisme $\widetilde{\nu_\infty} : \mathrm{W}_{\mathbb{R}} \to \mathrm{SO}_{2g+1}(\mathbb{C})$ déduit en composant ν_∞ et le morphisme d'Arthur comme au §4.14. L'analyse du §4.15 montre qu'il existe un unique couple (V^+, V^-) de lagrangiens transverses du q-module $V = \mathbb{C}^{2g+1}$ tels que :

- V^+ et V^- sont stables par $\widetilde{\nu_\infty}(\mathbb{C}^\times)$,
- V^+ possède une $\mathbb{C}$-base $e_1, \ldots, e_g$ vérifiant pour tout $j = 1, \ldots, g$ et tout $z \in \mathbb{C}^\times$, la relation $\widetilde{\nu_\infty}(z)(e_j) = z^{w_j} \overline{z}^{w'_j} e_j$.

Dans cette relation $w_1, \ldots, w_g$ sont les entiers déduits de ψ_∞ définis avant l'énoncé du théorème, et les w'_i sont également des entiers uniquement déterminés (qu'il ne sera pas nécessaire de préciser). La donnée de cette $\mathbb{C}$-base lagrangienne $(e_j)_{1 \leq j \leq g}$ détermine comme au §4.15 un unique tore maximal

$S \subset \mathrm{SO}_{2g+1}$ ainsi qu'unique sous-groupe de Borel de B contenant S. Écrivons comme au §VI.1.3

$$\mathrm{X}^*(S) = \oplus_{j=1}^g \mathbb{Z}\varepsilon_j,$$

ε_j désignant le caractère de S sur $\mathbb{C}e_j$. Soit $\varepsilon_j^* \in \mathrm{X}_*(S)$ la base duale de (ε_j). Soit $\lambda \in \frac{1}{2}\mathrm{X}_*(S)$ est l'élément associé à $\widetilde{\nu_\infty}$ intervenant dans la définition (AJ1) du §4.14. On a manifestement

$$\lambda = \sum_{j=1}^g w_j \varepsilon_j^*,$$

de sorte que λ est dominant relativement à B d'après les inégalités $w_1 > w_2 > \cdots > w_g > 0$. Nous avons explicité jusqu'ici la suite d'inclusions

$$\mathrm{C}_\nu \subset \mathrm{C}_{\nu_\infty} \subset S \subset B \subset \mathrm{SO}_{2g+1}$$

associée à ν et ν_∞. La proposition 4.18 (ii) ainsi que l'exemple §4.7 entraînent que le caractère $\chi^1_{O,\nu_\infty}(\pi_{\mathrm{hol}}) : \mathrm{C}_{\nu_\infty} \to \mathbb{C}^\times$ est la restriction à C_{ν_∞} de l'un des deux éléments suivants de $\mathrm{X}^*(S)$:

$$\chi_0 = \sum_{j \equiv 0 \bmod 2} \varepsilon_j \quad \text{ou} \quad \chi_1 = \sum_{j \equiv 1 \bmod 2} \varepsilon_j,$$

les deux sommes portant sur tous les $j \in \{1, \ldots, g\}$ de parité indiquée.

Vérifions enfin que la restriction à C_ν de n'importe lequel de ces deux caractères χ_u, $u \in \{0, 1\}$, coïncide avec le caractère χ. Fixons $1 \leq i \leq k-1$. Soit J_i le sous-ensemble de $\{1, \ldots, g\}$ constitué des entiers j tels que w_j est valeur propre de $(\pi_i[d_i])_\infty$. Observons tout d'abord que par construction, l'image de l'élément $s_i \in \mathrm{C}_\nu = \{\pm 1\}^{k-1}$ par l'inclusion naturelle $\mathrm{C}_\nu \subset S$ est déterminée par la relation suivante, satisfaite pour tout $j \in \{1, \ldots, g\}$:

$$\varepsilon_j(s_i) = -1 \;\Leftrightarrow\; j \in J_i.$$

Écrivons $J_i = J_i^0 \coprod J_i^1$ où $J_i^u = \{j \in J_i, j \equiv u \bmod 2\}$. Par définition,

$$\chi_u(s_i) = (-1)^{|J_i^u|}.$$

Observons que si d_i est pair, auquel cas π_i est symplectique et n_i est également pair, alors J_i est réunion disjointe de $\frac{|J_i|}{2} = \frac{n_i d_i}{2}$ paires d'entiers consécutifs, de sorte que

$$\chi_0(s_i) = \chi_1(s_i) = (-1)^{\frac{n_i d_i}{4}} = \chi(s_i).$$

Supposons enfin d_i impair, de sorte que π_i est orthogonale et $n_i \equiv 0 \bmod 4$ d'après le corollaire 2.15. Soit $P_i \subset J_i$ le sous-ensemble des $j \in J_i$ tels que $w_j \in \mathrm{Poids}(\pi_i)$. Alors J_i est la réunion disjointe de P_i et de ses translatés par

$$\pm 1, \pm 2, \ldots, \pm \frac{d_i - 1}{2}.$$

Mais si $1 \leq d \leq \frac{d_i - 1}{2}$, on a nécessairement $w_i + d = w_{i-d}$ et $w_i - d = w_{i+d}$. Les indices $i - d$ et $i + d$ étant congrus modulo 2, on en déduit

$$\chi_u(s_i) = (-1)^{|P_i^u|}$$

où $P_i^u = \{j \in P_i, j \equiv u \bmod 2\}$. On a donc $\chi_1(s_i) = \chi(s_i)$, et aussi $\chi_0(s_i) = \chi_1(s_i)$ car $|P_i| = \frac{n_i}{2} \equiv 0 \bmod 2$. □

Exemple 5.3. En guise d'exemple, comparons l'énoncé du théorème 5.2 au théorème VII.3.1 d'Ikeda. Soit $k > 0$ un entier pair et soit $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre dans $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$. Considérons le paramètre $\psi = \pi[g] \oplus [1]$. Comme $\mathrm{Poids}(\pi) = \{\pm \frac{k-1}{2}\}$, on constate que ψ satisfait la condition (H2) si, et seulement si, $g \equiv 0 \bmod 2$ et $k > g$, auquel cas les valeurs propres de ψ_∞ sont

$$\frac{k-1}{2}, \frac{k-3}{2}, \cdots, \frac{k-g}{2}, 0, -\frac{k-g}{2}, \cdots, -\frac{k-3}{2}, -\frac{k-1}{2}.$$

On a bien sûr $k = 2$, $d_2 = 1$, et $\mathrm{C}_\psi = \{\pm 1\}$ est engendré par l'élément s_1. On a également

$$\varepsilon_\psi(s_1) = \varepsilon(\pi \times 1) = \varepsilon(\pi) = i^k = (-1)^{k/2}.$$

De plus, on constate que g étant pair, $\chi(s_1) = (-1)^{g/2}$. Sous la conjecture 4.22, la condition nécessaire et suffisante d'existence de $\pi' \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ telle que π'_∞ est série discrète holomorphe et $\psi(\pi', \mathrm{St}) = \psi$ s'écrit donc

$$(-1)^{k/2} = (-1)^{g/2}$$

soit $k \equiv g \bmod 4$. C'est bien la condition intervenant dans l'énoncé d'Ikeda. Le résultat d'Ikeda est en fait plus fort, d'abord car il est inconditionnel, mais aussi car il n'a pas besoin de supposer $k > g$ (et il serait intéressant d'étudier également les paquets d'Arthur correspondant à ce cas plus général). Mentionnons également que dans son supplément [Ike13] à [Ike06], Ikeda démontre que si $k \equiv g \bmod 4$ (resp. $k \not\equiv g \bmod 4$) alors $\mathrm{m}(\pi') = 1$ (resp. $\mathrm{m}(\pi') = 0$) : voir [Ike13, Thm. 7.1, §15].

Terminons ce paragraphe par une traduction dans le langage classique de l'assertion de multiplicité 1 dans le théorème 5.2.

Corollaire* **5.4.** *Soit W la $\mathbb{C}$-représentation de GL_g de plus haut poids $\sum_{i=1}^g m_i\varepsilon_i$ avec $m_1 > m_2 > \cdots > m_g > g+1$ (§3.4). Si $F, G \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ sont deux formes propres pour $\mathrm{H}(\mathrm{Sp}_{2g})$, et si tout élément de $\mathrm{H}(\mathrm{Sp}_{2g})$ admet même valeur propre sur F et G, alors F et G sont proportionnelles. Lorsque $g = 2$, la même assertion vaut en supposant seulement $m_1 > m_2 > 2$.*

Démonstration. Rappelons que l'on dispose d'un isomorphisme de $\mathrm{H}^{\mathrm{opp}}(\mathrm{Sp}_{2g})$-modules $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \xrightarrow{\sim} \mathcal{A}_{\pi'_W}(\mathrm{Sp}_{2g})$ (§VI.3.7 et la remarque qui suit). Il suffit donc de voir que si π désigne la représentation engendrée par une forme propre de $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ sous l'action de $\mathrm{H}(\mathrm{Sp}_{2g})$, alors $\mathrm{m}(\pi) = 1$. On rappelle que $\pi_\infty \simeq \pi'_W$ et $\mathrm{St}(\mathrm{Inf}_{\pi'_W})$ admet pour valeurs propres 0 et les $\pm(m_r - r)$ pour $r = 1, \ldots, g$ (Proposition §VI.3.6,) : elles sont donc deux-à-deux distinctes et non consécutives par hypothèse. Si l'on écrit $\psi(\pi, \mathrm{St}) = \oplus_i \pi_i[d_i]$, ce qui est loisible d'après le théorème 1.1, on a donc $d_i = 1$ pour tout i, et on conclut par le théorème 5.2. Lorsque $g = 2$ et $m_1 > m_2 = 2$, on conclut encore car l'unique autre possibilité $\psi(\pi, \mathrm{St}) = \pi_1 \oplus [3]$ avec $\pi_1 \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ est impossible, puisqu'un tel π_1 est nécessairement symplectique (§3.1 ou proposition 2.13 (i)). □

On s'attend à ce que le corollaire soit valable pour tout W : cela découle de la conjecture 4.22 dès que $m_g > g$!

5.5. Formule explicite pour SO_n avec $n \equiv \pm 1 \bmod 8$.

Supposons maintenant que n est un entier $\equiv \pm 1 \bmod 8$ et considérons le $\mathbb{Z}$-groupe SO_n. Soit

$$\psi = \oplus_{i=1}^k \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{n-1}),$$

où $k \geq 1$ est un entier et $\pi_i \in \Pi^\perp_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ et $d_i \geq 1$ pour tout $i = 1, \ldots, k$. On suppose que ψ_∞ satisfait la condition (H2) relativement à SO_n (§3.4), ce qui signifie que ψ_∞ admet pour valeurs propres $n-1$ demi-entiers (non entiers) distincts

$$w_1 > \cdots > w_{\frac{n-1}{2}} > -w_{\frac{n-1}{2}} > \cdots > -w_1.$$

(§2.6 cas II.). D'après le lemme 2.15 (ii), pour tout $i = 1, \ldots, k$ on a $n_i d_i \equiv 0 \bmod 2$.

Considérons l'homomorphisme de groupes multiplicatifs $\chi : \{\pm 1\}^k \to \{\pm 1\}$ défini de la manière suivante. Fixons $1 \leq i \leq k$ et notons $s_i \in \{\pm 1\}^k$ l'élément défini par $(s_i)_j = -1 \Leftrightarrow j = i$. Il y a deux cas :

(i) L'entier d_i est pair. Si n_i est pair, on pose $\chi(s_i) = (-1)^{\frac{n_i d_i}{4}}$. Si n_i est impair, on pose $\chi(s_i) = \epsilon_i \cdot (-1)^{\frac{(n_i-1)d_i}{4}}$, où $\epsilon_i = (-1)^{[\frac{3d_i}{4}]}$ vaut -1 si $\frac{d_i}{2} \equiv 1, 2 \bmod 4$ et 1 sinon. (Dans tous les cas, $\chi(s_i) = (-1)^{[\frac{3n_i d_i}{4}]}$.)

(ii) L'entier d_i est impair. On pose $\chi(s_i) = (-1)^{|K_i|}$ où K_i est l'ensemble des indices $1 \leq j \leq \frac{n-1}{2}$ qui sont $\equiv \frac{n-1}{2} \bmod 2$ et tels que $w_j \in \mathrm{Poids}(\pi_i)$.

Théorème 5.6. (Cas $n \equiv \pm 1 \bmod 8$) *Soit $\psi = \oplus_{i=1}^k \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{n-1})$ tel que ψ_∞ admet $n-1$ valeurs propres distinctes et dans $\frac{1}{2}\mathbb{Z}-\mathbb{Z}$. Soit $\pi \in \Pi(\mathrm{SO}_n)$ l'unique représentation telle que $\psi(\pi, \mathrm{St}) = \psi$. Supposons la conjecture 4.25 satisfaite pour SO_n et le morphisme ν_∞ associé à ψ défini au §3.8. Alors $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ si, et seulement si, pour tout $i = 1, \ldots, k$, on a*

$$\chi(s_i) = \prod_{1 \leq j \leq k, j \neq i} \varepsilon(\pi_i \times \pi_j)^{\mathrm{Min}(d_i, d_j)},$$

où χ désigne le caractère de $\{\pm 1\}^k$ associé à ψ qui est défini ci-dessus. Enfin, si ces conditions sont satisfaites alors $\mathrm{m}(\pi) = 1$.

Démonstration. (voir [CR12, §3.30.1]) La démonstration est similaire à celle du théorème 5.2, c'est pourquoi nous n'insisterons que sur les différences avec celle-là. Une analyse de ν_∞ similaire à celle du §4.15, tenant compte de ce que le groupe dual est celle fois-ci Sp_{n-1}, conduit à une explicitation de la suite d'inclusions canoniques

$$\mathrm{C}_\nu = \{\pm 1\}^k \subset \mathrm{C}_{\nu_\infty} \subset S \subset B \subset \mathrm{Sp}_{n-1}.$$

On invoque alors le corollaire 4.13 à la place de l'exemple 4.7 (et la conjecture 4.25 à la place de la conjecture 4.22 et du théorème 3.10). Comme le centre de SO_n est trivial, ce corollaire affirme que le caractère $\chi^{\xi}_{O,\nu_\infty}(\pi_\infty)$ est la restriction à C_{ν_∞} de la demi-somme $\rho^\vee$ des racines positives de T relativement à B, qu'il suffit donc d'expliciter. Posons $n = 2r+1$ et considérons pour cela la donnée radicielle basée standard de Sp_{2r} rappelée au §VI.1.3. Dans les notations *loc. cit.*, on constate que

$$\rho^\vee = \sum_{i=1}^{r} (r-i+1)\varepsilon_i \equiv \varepsilon_r + \varepsilon_{r-2} + \cdots \bmod 2.$$

On conclut comme dans la démonstration du théorème 5.2 que la restriction de ce caractère à C_ψ est le caractère χ de l'énoncé. On prendra garde au cas où l'entier $i \in \{1, \ldots, k\}$ vérifie $d_i \equiv 0 \bmod 2$ et $n_i \equiv 1 \bmod 2$, car alors 0 est un poids de π_i. Dans ce cas, l'ensemble J_i défini dans cette démonstration est réunion disjointe de $\frac{(n_i-1)d_i}{2}$ paires d'entiers consécutifs, ainsi que de l'ensemble $\{r, r-1, \ldots, r+1-\frac{d_i}{2}\}$, d'où la modification à apporter à la définition de χ dans le cas (i). $\square$

5.7. Formule explicite pour SO_n avec $n \equiv 0 \bmod 8$.

Considérons enfin le $\mathbb{Z}$-groupe SO_n pour $n \equiv 0 \bmod 8$. Soit

$$\psi = \oplus_{i=1}^{k} \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n),$$

où $k \geq 1$ est un entier et $\pi_i \in \Pi_{\mathrm{cusp}}^{\perp}(\mathrm{PGL}_{n_i})$ et $d_i \geq 1$ pour tout $i = 1, \ldots, k$. On suppose que ψ_∞ satisfait la condition (H2) relativement à SO_n (§3.4), ce qui signifie que ψ_∞ admet pour valeurs propres n entiers

$$w_1 > \cdots > w_{n/2} \geq -w_{n/2} > \cdots > -w_1$$

(§2.6 cas III.) Notons $I_1 \subset \{1, \cdots, k\}$ le sous-ensemble des indices i tels que $n_i d_i \equiv 1 \bmod 2$ et posons $I_0 = \{1, \ldots, k\} - I_1$. D'après le lemme 2.15 (ii), on a soit $I_1 = \emptyset$, soit $|I_1| = 2$ (ce qui ne peut se produire que si $w_{n/2} = 0$). De plus, $n_i d_i \equiv 0 \bmod 4$ si $i \in I_0$.

Considérons l'homomorphisme de groupes multiplicatifs $\chi : \{\pm 1\}^{I_0} \to \{\pm 1\}$ défini de la manière suivante. Fixons $i \in I_0$ et notons $s_i \in \{\pm 1\}^{I_0}$ l'élément défini par $(s_i)_j = -1 \Leftrightarrow j = i$.

(i) Si $d_i \equiv 0 \bmod 2$, on pose $\chi(s_i) = (-1)^{\frac{n_i d_i}{4}}$.

(ii) Si $d_i \equiv 1 \bmod 2$, on pose $\chi(s_i) = (-1)^{|K_i|}$ où K_i est l'ensemble des indices $1 \leq j \leq \frac{n}{2}$ qui sont impairs et tels que $w_j \in \mathrm{Poids}(\pi_i)$.

Théorème 5.8. (Cas $n \equiv 0 \bmod 8$) *Soient $\psi = \oplus_{i=1}^{k} \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$ tel que ψ_∞ admet n valeurs propres entières, au moins $n-1$ d'entre elles étant distinctes, ainsi que $\{1, \ldots, k\} = I_0 \coprod I_1$ la partition associée ci-dessus. Soit $\Pi \subset \Pi(\mathrm{SO}_n)$ le sous-ensemble des représentations π telles que $\psi(\pi, \mathrm{St}) = \psi$; c'est un singleton si $I_1 \neq \emptyset$. Supposons la conjecture 4.25 satisfaite pour SO_n et le morphisme ν_∞ associé à ψ défini au §3.8. Alors $\Pi \cap \Pi_{\mathrm{disc}}(\mathrm{SO}_n) \neq \emptyset$ si, et seulement si, on a*

$$\chi(s_i) = \prod_{1 \leq j \leq k, j \neq i} \varepsilon(\pi_i \times \pi_j)^{\mathrm{Min}(d_i, d_j)}, \quad \forall i \in I_0, \tag{5.1}$$

où χ désigne le caractère de $\{\pm 1\}^{I_0}$ associé à ψ qui est défini ci-dessus. Enfin, si cette condition est satisfaite alors $\sum_{\pi \in \Pi} \mathrm{m}(\pi) = 1$ si $I_1 \neq \emptyset$, et $\sum_{\pi \in \Pi} \mathrm{m}(\pi) = 2$ sinon.

Démonstration. (voir [CR12, §3.30.2]) La démonstration est similaire à celle du théorème 5.6. On explicite à la manière du §4.15 la suite d'inclusions canoniques

$$\mathrm{C}_\nu \subset \mathrm{C}_{\nu_\infty} \subset S \subset B \subset \mathrm{SO}_n.$$

L'homomorphisme $\{\pm 1\}^{I_0} \to \mathrm{C}_\nu$ envoyant l'élément s_i pour $i \in I_0$ défini ci-dessus sur l'élément du même nom défini au §3.5 induit une surjection $\{\pm 1\}^{I_0} \to \mathrm{C}_\nu/\mathrm{Z}(\mathrm{SO}_n)$. Dans la donnée radicielle basée standard de (SO_n, S, B) rappelée au §VI.1.3, on constate cette fois-ci que la demi-somme des racines positives vaut

$$\rho^\vee = \sum_{i=1}^{r} (r-i)\varepsilon_i \equiv \varepsilon_{r-1} + \varepsilon_{r-3} + \cdots \bmod 2,$$

où $r = \frac{n}{2}$. Comme le centre de SO_n est non trivial, le corollaire 4.13 affirme seulement que $\chi^{\xi}_{O,\nu_\infty}(\pi_\infty)$ est la restriction à $\mathrm{C}_{\nu_\infty} \subset S$ de $\rho^\vee$ ou $\rho^\vee + \nu$, où

$$\nu \equiv \sum_{i=1}^{r} \varepsilon_i \bmod 2.$$

Mais $\nu_{|\mathrm{C}_\nu} = 1$ car $n_i d_i \equiv 0 \bmod 4$ pour tout $i \in I_0$, et le reste s'en déduit. $\square$

Remarque 5.9. (Sur la multiplicité 2) Soit $\alpha \in \mathrm{E}_n$ tel que $\alpha \cdot \alpha = 2$ ainsi que $\mathrm{s}_\alpha \in \mathrm{O}(\mathrm{E}_n)$ la symétrie orthogonale associée à cette racine. La conjugaison extérieure par s_α induit une involution, disons notée S, de $\Pi(\mathrm{SO}_n)$, dont nous avons déjà étudié certains aspects au §IV.4.4, ainsi que dans les exemples du §VI.2.1 et du §VI.4.7. Ces paragraphes montrent que si $\pi \in \Pi(\mathrm{SO}_n)$ alors $\mathrm{m}(\pi) = \mathrm{m}(S(\pi))$, et pour tout $v \in \mathrm{P} \cup \{\infty\}$ les classes de conjugaison $\mathrm{c}_v(\pi)$ et $\mathrm{c}_v(S(\pi))$ sont images l'une de l'autre par l'action de l'élément non-trivial de $\mathrm{O}_n(\mathbb{C})/\mathrm{SO}_n(\mathbb{C})$. En particulier, S préserve $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ et $\psi(S(\pi), \mathrm{St}) = \psi(\pi, \mathrm{St})$. De plus, cela entraîne que $S(\pi)$ est isomorphe à π si, et seulement si, ± 1 (resp. 0) est valeur propre de $\mathrm{c}_p(\pi)$ (resp. de $\mathrm{c}_\infty(\pi)$) pour tout premier p. Plaçons-nous maintenant dans les hypothèses du théorème ci-dessus, et supposons $I_1 = \emptyset$ ainsi que (5.1) satisfaite. Les observations précédentes montrent que l'ensemble Π de l'énoncé est stable par S. En particulier, si S n'admet aucun point fixe dans Π le théorème assure que $\Pi \cap \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ est constitué deux représentations échangées par S, chacune étant de multiplicité 1. Voici deux cas particuliers où ceci s'applique.

I. 0 n'est pas valeur propre de ψ_∞ : $S(\pi)_\infty \neq \pi_\infty$ pour tout $\pi \in \Pi$.

II. π_i est symplectique pour $i = 1, \ldots k$: $S(\pi)_p \neq \pi_p$ pour tout $\pi \in \Pi$ et p premier. En effet, les valeurs propres λ de $\mathrm{c}_p(\pi_i)$ satisfont $p^{-\frac{1}{2}} < |\lambda| < p^{\frac{1}{2}}$ d'après Jacquet-Shalika (et même $|\lambda| = 1$ par la conjecture de Ramanujan §VI.4.10), alors que les valeurs propres μ de $[d_i]_p$ satisfont $|\mu| \geq p^{\frac{1}{2}}$ ou $|\mu| \leq p^{-\frac{1}{2}}$ (car $d_i \equiv 0 \bmod 2$), de sorte que $|\lambda\mu| \neq 1$ et ± 1 n'est pas valeur propre de ψ_p.

Dans le cas général, une combinaison de ces idées montre que pour qu'il existe une représentation de multiplicité > 1 dans un $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ il faut et suffit qu'il existe $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{4m})$ autoduale, algébrique, orthogonale, telle que $|\mathrm{Poids}(\pi)| = 4m-1$ et $\mathrm{c}_p(\pi)$ admet la valeur propre ± 1 pour tout p. On pourrait montrer qu'il n'en existe pas quand $m = 1$.

Deux critères

Donnons deux critères pour que la relation (5.1) soit satisfaite.

Critère 5.10. *On suppose ψ de la forme $\left(\bigoplus_{i=1}^{k-2} \pi_i[d_i]\right) \oplus [d_{k-1}] \oplus [1]$ avec $d_i \equiv 0 \bmod 2$ pour tout $i = 1, \ldots, k-2$ et $d_{k-1} > 1$ impair. Alors la relation* (5.1) *est satisfaite si, et seulement si, pour tout $i = 1, \ldots, k-2$ on a*

$$(-1)^{\frac{n_i d_i}{4}} = \varepsilon(\pi_i)^{1+\mathrm{Min}(d_i, d_{k-1})}.$$

Démonstration. C'est une application immédiate des formules et du fait que $\varepsilon(\pi_i \times \pi_j) = 1$ si $i, j \in I_0 = \{1, \ldots, k-2\}$. Ce dernier point peut soit être vu comme cas particulier du résultat général d'Arthur car les représentations π_i et π_j sont symplectiques (§3.1), soit se démontrer directement car $\varepsilon(\mathrm{I}_a \otimes \mathrm{I}_b) = (-1)^{1+\mathrm{Max}(a,b)} = 1$ si a et b sont impairs (§2.21). □

Critère 5.11. *On suppose ψ de la forme $\left(\bigoplus_{i=1}^{k-2} \pi_i[d_i]\right) \oplus \pi_{k-1} \oplus [d_k]$ avec :*

(i) $d_i \equiv 0 \bmod 2$ *pour tout* $i = 1, \ldots, k-2$,

(ii) et $\pi_{k-1} \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_3)$ *telle que* $\mathrm{w}(\pi_{k-1}) > \underset{1 \leq i \leq k-2}{\mathrm{Max}} \mathrm{w}(\pi_i)$.

La relation 5.1 est satisfaite si, et seulement si, pour tout $i = 1, \ldots, k-2$

$$(-1)^{\frac{n_i}{2}(\frac{d_i}{2}-1)} = \varepsilon(\pi_i)^{1+\mathrm{Min}(d_i, d_k)}.$$

Démonstration. Rappelons que $\varepsilon(\mathrm{I}_w \otimes \mathrm{I}_{w'}) = (-1)^{1+\mathrm{Max}(w,w')}$ et $\mathrm{I}_w \otimes \epsilon_{\mathbb{C}/\mathbb{R}} \simeq \mathrm{I}_w$. Comme $\mathrm{w}(\pi_i)$ est impair si $i < k-1$ et pair si $i = k-1$, l'hypothèse sur $\mathrm{w}(\pi_{k-1})$ assure que pour tout $i \leq k-2$,

$$\varepsilon(\pi_i \times \pi_{k-1}) = \varepsilon(\mathrm{L}(\pi_i)_\infty \otimes \mathrm{I}_{\mathrm{w}(\pi_{k-1})})\varepsilon(\mathrm{L}(\pi_i)_\infty \otimes \epsilon_{\mathbb{C}/\mathbb{R}}) = (-1)^{\frac{n_i}{2}}\varepsilon(\pi_i).$$

On conclut car $\varepsilon(\pi_i \times \pi_j) = 1$ si $i, j \leq k-2$. □

Exemples

Admettant la conjecture 4.25, le théorème 5.8 devient un outil formidable pour vérifier (et peut-être, dans un futur proche, redémontrer !) les résultats précédemment obtenus dans ce mémoire. Son application la plus immédiate concerne le cas où ψ est tel que soit $I_0 = \emptyset$, soit $k = 1$, puisqu'alors la condition (5.1) est trivialement satisfaite. On retrouve par exemple la conclusion du théorème VII.2.1 (ii), ainsi que celle du (i) si l'on demande simplement que la représentation π' soit dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_8)$ plutôt que dans $\Pi_{\mathrm{disc}}(\mathrm{O}_8)$. On retrouve aussi l'assertion concernant $\Delta_{11}[12]$ du corollaire VII.3.4 (voir le §IX.2.10).

En guise d'autre exemple, considérons le cas où

$$\psi = \pi_1[d_1] \oplus [d_2] \oplus [1]$$

avec $\pi_1 \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ de poids $\{\pm\frac{k-1}{2}\}$, k étant un entier pair > 0. On a $\varepsilon(\pi_1) = (-1)^{k/2}$. D'après le critère 5.10, la relation (5.1) est satisfaite si, et seulement si :

(I) soit $d_1 < d_2$ et $d_1 \equiv k \bmod 4$,

(II) soit $d_1 > d_2$ et $d_1 \equiv 0 \bmod 4$.

Par exemple, si $\psi = \Delta_{11}[4] \oplus [7] \oplus [1]$, auquel cas $n = 16$ et $\psi_\infty = \mathrm{St}(\mathrm{Inf}_1)$, on est dans le cas (I) ci-dessus. Cela redémontre immédiatement l'assertion concernant $\psi(\pi, V_{\mathrm{St}})$ du corollaire VII.2.6, ainsi donc que le (i) du théorème V.2.2. On retrouve aussi les assertions du corollaire 3.4 pour $k > 12$ (voir IX.§2.10) : on est dans le cas (II) pour $k = 16$ car $(d_1, d_2) = (8, 7)$, et dans le cas (I) pour $k > 16$ car $24 - k \equiv k \bmod 4$ et $2k - 25 > 24 - k$. En ce qui concerne $\psi = \Delta_{17}[14] \oplus [3] \oplus [1]$, on n'est ni dans le cas (I), ni dans le cas (II), ce qui corrobore comme promis le corollaire VII.3.5.

Expliquons enfin la table du §VII.4. Compte tenu de l'analyse ci-dessus, il ne reste qu'à comprendre les cases bleues de cette table. Mais si $\psi = \Delta_w[2] \oplus \mathrm{Sym}^2\Delta_{11} \oplus [1]$ avec $w < 22 = \mathrm{w}(\mathrm{Sym}^2\Delta_{11})$, le critère 5.11 montre que la relation (5.1) est satisfaite, ce qui conclut.

6. Compatibilité à la correspondance thêta

Soient $n \equiv 0 \bmod 8$ et $g \geq 1$ des entiers tels que $n > 2g$. Soit

$$\psi_S = \oplus_{i=1}^k \pi_i[d_i] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1}),$$

où $k \geq 1$ et, pour tout $i = 1, \ldots, k$, $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$. On suppose que

$$\psi_O := \psi_S \oplus [n - 2g - 1] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$$

satisfait la condition (H2) relativement à SO_n. Il est équivalent de demander que les valeurs propres de $(\psi_S)_\infty$ soient $2g + 1$ entiers

$$w_1 > \cdots > w_g > 0 > -w_g > \cdots > -w_1$$

avec de plus $w_g \geq \frac{n}{2} - g$. Il sera commode de choisir l'indexation des π_i de sorte que $n_k d_k \equiv 1 \bmod 2$ (§5.1). On suppose enfin $d_k = 1$, c'est d'ailleurs automatique si $n \neq 2g + 2$.

Soit $\pi_O \in \Pi(\mathrm{SO}_n)$ (resp. $\pi_S \in \Pi(\mathrm{Sp}_{2g})$) l'unique représentation telle que $\psi(\pi_O, \mathrm{St}) = \psi_O$ (resp. $\psi(\pi_S, \mathrm{St}) = \psi_S$). Notons $\mathrm{m}(\pi_O)$ et $\mathrm{m}(\pi_S)$ les multiplicités respectives de π_O et π_S dans $\Pi_{\mathrm{disc}}(\mathrm{SO_n})$ et $\pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$). Elles valent chacune 0 ou 1 d'après la formule de multiplicité Arthur, sous la conjecture 4.25.

Proposition 6.1. *Admettons la conjecture 4.25. On a* $\mathrm{m}(\pi_O) = \mathrm{m}(\pi_S)$ *si, et seulement si, pour tout* $i = 1, \ldots, k-1$ *tel que* $d_i \equiv 0 \bmod 2$ *et* $d_i \geq n - 2g$,

$$\varepsilon(\pi_i) = 1.$$

Démonstration. C'est immédiat sur les formules explicites données dans les §5.1 et §5.7. On observe en effet que l'injection naturelle

$$\mathrm{C}_{\psi_S} \to \mathrm{C}_{\psi_O}$$

induit un isomorphisme $\mathrm{C}_{\psi_S} \xrightarrow{\sim} \mathrm{C}_{\psi_O}/\mathrm{Z}(\mathrm{SO}_n)$. Le groupe C_{ψ_S} s'identifie naturellement à $\{\pm 1\}^{k-1}$ (voir la démonstration du théorème 5.2), et l'injection ci-dessus l'identifie (avec ses éléments privilégiés s_i) au sous-groupe $\{\pm 1\}^{I_0}$ défini au §5.7 (en particulier, $\mathrm{I}_0 = \{1, \ldots, k-1\}$). Via cet identification, on constate que le caractère χ de $\{\pm 1\}^{k-1}$ défini au §5.1 coïncide avec le caractère χ de $\{\pm 1\}^{I_0}$ défini au §5.7. D'après les théorèmes 5.2 et 5.8, la condition pour que $\mathrm{m}(\pi_O) = \mathrm{m}(\pi_S)$ équivaut donc à

$$\varepsilon(\pi_i)^{\mathrm{Min}(d_i, n-2g-1)} = 1$$

tout $i = 1, \ldots, k-1$. C'est automatique quand d_i est impair car alors π_i est orthogonale. $\square$

Lorsque $\mathrm{m}(\pi_S) = 1$, le critère de Böcherer (remarque VII.2.4) donne une condition nécessaire est suffisante, du moins si les entiers w_i sont consécutifs, pour que la forme propre de $\mathrm{S}_{w_1+1}(\mathrm{Sp}_{2g})$ (bien définie à un scalair près) engendrant π_S admette un ϑ-correspondant π' dans $\Pi_{\mathrm{disc}}(\mathrm{O}_n)$: il faut et suffit que $\mathrm{L}(s, \pi_S, \mathrm{St})$ ne s'annule pas en $s = \frac{n}{2} - g$. Par restriction à SO_n (§IV.4.4), l'existence de π' entraîne que $\mathrm{m}(\pi_O)$ est non nul (corollaire VII.1.3). Il est donc important de vérifier que le critère de Böcherer est compatible à la proposition ci-dessus, et c'est bien le cas :

Proposition 6.2. $\mathrm{L}(s, \pi_{\mathrm{S}}, \mathrm{St})$ *ne s'annule pas en* $s = \frac{n}{2} - g$ *si, et seulement si, pour tout* $i = 1, \ldots, k-1$ *tel que* $d_i \geq n - 2g$ *et* $d_i \equiv 0 \bmod 2$*, on a* $\mathrm{L}(\frac{1}{2}, \pi_i) \neq 0$ *(et donc* $\varepsilon(\pi_i) = 1$*). En particulier,* $\mathrm{L}(\frac{n}{2} - g, \pi_{\mathrm{S}}, \mathrm{St}) \neq 0$ *dès que* $n > 3g$*.*

Démonstration. La fonction $\mathrm{L}(s, \pi_{\mathrm{S}}, \mathrm{St})$ est produit des $\mathrm{L}(s + j, \pi_i)$ pour $i = 1, \ldots, k$ et $j \in \frac{d_i - 1}{2} + \mathbb{Z}$ tel que $|j| \leq \frac{d_i - 1}{2}$. On rappelle que si $\pi_i \neq 1$, le produit eulérien de $\mathrm{L}(s, \pi_i)$ est absolument convergent pour $\operatorname{Re} s > 1$, et que $\xi(s, \pi_i) = \Gamma(s, \mathrm{L}((\pi_i)_\infty))\mathrm{L}(s, \pi_i)$ admet un prolongement holomorphe sur $\mathbb{C}$ tel que $\xi(1 - s, \pi_i) = \varepsilon(\pi_i)\xi(s, \pi)$ (§VI.4.9). De plus, on a $\mathrm{L}(1, \pi_i) \neq 0$ [JS76]. Par hypothèse, si $\pi_i = 1$ alors $i = k$, $d_k = 1$, et $\mathrm{L}(s, \pi_i)$ est la fonction ζ de Riemann. Observons que si ce cas se produit alors $n - 2g - 1 \equiv 3 \bmod 4$; en particulier s'il on pose

$$s_0 = \frac{n}{2} - g$$

alors $s_0 \geq 2$ n'est ni un zéro, ni un pôle, de ζ. Comme $d_k = 1$ et $s_0 \leq 1$, on a $\mathrm{L}(s_0, \pi_{\mathrm{S}}, \mathrm{St}) = 0$ si, et seulement si, il existe $1 \leq i \leq k - 1$ et $j \in \frac{d_i - 1}{2} + \mathbb{Z}$ avec $|j| \leq \frac{d_i - 1}{2}$ tels que $\mathrm{L}(s_0 + j, \pi_i) = 0$.

Fixons $i < k$. La représentation π_k étant la seule parmi les π_s à posséder le poids 0, $\mathrm{L}((\pi_i)_\infty)$ est somme directe des I_w où w parcourt les poids > 0 de π_i. La fonction $\Gamma(s)$ ne s'annule nulle part sur l'axe réel et admet pour seuls pôles les entiers ≤ 0. La recette pour $\Gamma(s, \mathrm{L}((\pi_i)_\infty))$ (§2.21) et les propriétés rappelées ci-dessus de $\xi(s, \pi_i)$ montrent donc que si $\mathrm{L}(s, \pi_i) = 0$, disons pour $s \in \mathbb{R}$, alors soit $0 < s < 1$, soit $s \leq -w$, où w est le plus petit poids > 0 de π_i. Mais $w - \frac{d_i - 1}{2} \geq w_g \geq \frac{n}{2} - g = s_0$, de sorte que pour $j \geq \frac{1 - d_i}{2}$ on a

$$s_0 + j > -s_0 + \frac{1 - d_i}{2} \geq -w.$$

Enfin, $0 < s_0 + j < 1$ équivaut à $s_0 + j = \frac{1}{2}$ si $j \in \frac{1}{2}\mathbb{Z}$. On conclut la première assertion car $\frac{1}{2}$ est de la forme $\frac{n}{2} - g + j$ avec $\frac{1 - d_i}{2} \leq j \leq \frac{1 - d_i}{2}$ et $j \in \frac{d_i - 1}{2} + \mathbb{Z}$ si, et seulement si, $d_i \equiv 0 \bmod 2$ et $n - 2g \leq d_i$. La seconde provient de la relation évidente $d_i \leq g$. $\square$

Remarque 6.3. Notons que la condition suffisante $n > 3g$ obtenue ci-dessus, légitime en pratique d'après le théorème* 1.1 d'Arthur, s'avère meilleure que la condition générale $n > 4g$ de Böcherer.

En théorie, il pourrait exister des paramètres ψ_{S} tels que $\mathrm{m}(\pi_O) = \mathrm{m}(\pi_S) = 1$ mais tels que π_O et π_S ne soient pas ϑ-correspondants. Pour fabriquer un tel exemple, il faudrait trouver une représentation algébrique régulière autoduale symplectique ϖ telle que $\mathrm{L}(\frac{1}{2}, \varpi) = 0$ mais $\varepsilon(\varpi) = 1$. Les auteurs ne connaissent aucun tel exemple (comparer avec la remarque VII.3.3). C'est un fait que nous exploitons d'ailleurs positivement à plusieurs reprises dans ce mémoire !

7. Compatibilité à la fonction L de Böcherer

Soient $g \geq 1$ un entier, $k \in \mathbb{Z}$, $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre, ainsi que $\pi_F \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ la représentation engendrée par F. Böcherer a démontré dans [Boc85] que le produit eulérien $\mathrm{L}(s, \pi_F, \mathrm{St})$ (défini au §VI.4.9) est absolument convergent si $\mathrm{Re}\, s > g + 1$, et que la fonction

$$\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) := \left(\Gamma(s, \epsilon^g_{\mathbb{C}/\mathbb{R}}) \prod_{i=1}^{g} \Gamma_{\mathbb{C}}(s + k - i) \right) \mathrm{L}(s, \pi_F, \mathrm{St}),$$

admet un prolongement méromorphe à $\mathbb{C}$ ainsi qu'une équation fonctionelle

$$\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) = \xi_{\mathrm{B}}(1 - s, \pi_F, \mathrm{St})$$

(voir aussi [Lan76, AK79, PSR87]). Rappelons que l'on a $\Gamma(s, 1) = \Gamma_{\mathbb{R}}(s)$ et $\Gamma(s, \epsilon_{\mathbb{C}/\mathbb{R}}) = \Gamma_{\mathbb{R}}(s + 1)$ dans les notations du §2.21. Les pôles de $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$ ont été étudiés par Mizumoto [Miz91, Theorem 1, §3 Corollary]. Il démontre les énoncés suivants, dans lesquels ν désigne l'élément de $\{0, 1\}$ défini par la congruence $\nu \equiv k \bmod 2$:

(a) si $k \geq g$ alors $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$ admet au plus des pôles simples en $s = 0$ et $s = 1$, et elle est holomorphe ailleurs.

(b) si $g > k$ alors $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$ admet au plus des pôles simples en $s = g - k + \nu + 1, g - k + \nu, k - g - \nu + 1, k - g - \nu$, au plus des pôles doubles aux entiers $s \in \mathbb{Z}$ tel que $g - k + \nu - 1 \geq s \geq 2 + k - g - \nu$, et elle est holomorphe ailleurs.

Supposons maintenant que l'on ait la relation

$$\psi(\pi_F, \mathrm{St}) = \oplus_{i=1}^{r} \pi_i[d_i],$$

avec $\pi_i \in \Pi_{\mathrm{cusp}}^{\perp}(\mathrm{PGL}_{n_i})$ et $d_i \geq 1$ pour tout $1 \leq i \leq r$, ce qui est loisible d'après Arthur (Théorème 2.4). La théorie des fonctions L standards des éléments de $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$, par Godement et Jacquet, montre que la fonction définie par $\xi(s, \pi_i) = \Gamma(s, \mathrm{L}((\pi_i)_\infty))\mathrm{L}(s, \pi_i)$ (§2.21) posséde un prolongement méromorphe à $\mathbb{C}$ et une équation fonctionnelle $s \mapsto 1 - s$. Cela fournit donc une seconde façon naturelle de compléter $\mathrm{L}(s, \pi_F, \mathrm{St})$ en posant simplement

$$\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) \ := \ \prod_{i=1}^{r} \prod_{j=0}^{d_i-1} \xi(s + j - \frac{d_i - 1}{2}, \pi_i).$$

Cette fonction est également méromorphe sur $\mathbb{C}$ et invariante par $s \mapsto 1-s$ (à un signe près à priori, mais qui est en fait égal à 1 car d'après Arthur [Art13, Thm. 1.5.3 (b)] on a $\varepsilon(\pi) = 1$ pour toute représentation $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$ autoduale et orthogonale).

Ainsi, $\frac{\xi_{\mathrm{B}}(s,\pi_F,\mathrm{St})}{\xi_{\mathrm{A}}(s,\pi_F,\mathrm{St})}$ est un quotient "explicite" de produits de facteurs Γ. Lorsque $k > g + 1$, il est facile de voir sur les recettes respectives pour ces facteurs que ce quotient vaut 1, i.e. $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) = \xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})$. La situation s'avère plus intéressante lorsque $k \leq g + 1$, auquel cas la comparaison de ces facteurs, combinée aux propriétés rappelées ci-dessus des pôles de $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$ et $\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})$, admet des conséquences non triviales sur $\psi(\pi_F, \mathrm{St})$. L'énoncé de la proposition 7.1 ci-dessous est suggéré par le point (a) du théorème 5.2 (et donc par la conjecture 4.22) lorsque $k = g + 1$. Il nécessite l'introduction de quelques quantités préliminaires.

Pour tout entier $a \geq 1$ on pose

$$\delta(\pi_F, a) \ = \ \mathrm{ord}_{s=a} \prod_{\{i, \pi_i \neq 1\}} \prod_{j=0}^{d_i-1} \xi(s + j - \frac{d_i - 1}{2}, \pi_i).$$

On rappelle que si $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_m)$ est telle que $\pi \neq 1$ alors $\xi(s, \pi)$ est une fonction entière de s. De plus, si $s \in \frac{1}{2}\mathbb{Z}$ satisfait $\xi(s, \pi) = 0$ alors d'après Jacquet-Shalika on a $s = \frac{1}{2}$ et $\mathrm{ord}_{s=\frac{1}{2}}\Gamma(s, \mathrm{L}(\pi_\infty)) = 0$. Pour tout entier $a \geq 1$ on a donc l'égalité

$$\delta(\pi_F, a) \ := \sum_{\{i \ \mid \ d_i \equiv 0 \bmod 2, d_i \geq 2a\}} \mathrm{ord}_{s=\frac{1}{2}} \mathrm{L}(s, \pi_i). \tag{7.1}$$

En particulier, on a les inégalités $0 \leq \delta(\pi_F, b) \leq \delta(\pi_F, a)$ pour $b \geq a \geq 1$. Il sera commode également de poser, pour tout entier $n \geq 0$:

$$p_n(s) \ = \ \frac{\Gamma_{\mathbb{C}}(s + n)}{\Gamma_{\mathbb{C}}(s - n)} \ \text{ et } \ \gamma_n(s) \ = \ \frac{\Gamma(s, \varepsilon_{\mathbb{C}/\mathbb{R}}^n)}{\Gamma_{\mathbb{R}}(s)} \prod_{i=1}^{n} \frac{\Gamma_{\mathbb{C}}(s + i)}{\Gamma_{\mathbb{R}}(s - i)\Gamma_{\mathbb{R}}(s + i)}.$$

À l'aide des formules $\Gamma_{\mathbb{C}}(s+1) = \frac{s}{2\pi}\Gamma_{\mathbb{C}}(s)$ et $\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$, on vérifie que les égalités suivantes sont valables pour tout entier $n \geq 0$:

$$p_n(s) \;=\; (2\pi)^{-2n} \prod_{1-n\leq m\leq n} (s-m) \;\text{ et }\; \gamma_n(s) = \prod_{0\leq 2m\leq n} p_{n-2m}(s).$$

En particulier, p_n et γ_n sont des polynômes en s invariants par $s \mapsto 1-s$.

Proposition[⋆] **7.1.** *Soit $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre avec $k = g$ ou $k = g+1$. Supposons $\psi(\pi_F, \mathrm{St}) = \oplus_{i=1}^r \pi_i[d_i]$ avec $\pi_r = 1$ et $d_r > 1$. Alors on a l'inégalité $\delta(\pi_F, \frac{d_r+1}{2}) > 0$.*

Démonstration. Traitons d'abord le cas $k = g+1$. Comme $\psi(\pi_F, \mathrm{St})_\infty$ admet 0 pour valeur propre simple (ce sont les $2g+1$ entiers n tels que $|n| \leq g$ d'après le §VI.3.6), on a $\pi_i \neq 1$ si $i < r$, ainsi donc que l'égalité

$$\mathrm{ord}_{s=\frac{d_r+1}{2}}\; \xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) \;=\; \delta(\pi, \frac{d_r+1}{2}) - 1 \tag{7.2}$$

d'après les rappels ci-dessus. On constate aussi que si $i < r$ alors π_i est régulière, chacun de ses poids étant $> \frac{d_i-1}{2} \geq 0$, on a donc par définitions les égalités

$$\frac{\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})}{\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})} = \frac{\Gamma(s, \epsilon^g_{\mathbb{C}/\mathbb{R}})}{\Gamma_{\mathbb{R}}(s)} \prod_{i=1}^{\frac{d_r-1}{2}} \frac{\Gamma_{\mathbb{C}}(s+i)}{\Gamma_{\mathbb{R}}(s+i)\Gamma_{\mathbb{R}}(s-i)} = \frac{\Gamma(s, \epsilon^g_{\mathbb{C}/\mathbb{R}})}{\Gamma(s, \epsilon_{\mathbb{C}/\mathbb{R}}^{\frac{d_r-1}{2}})} \gamma_{\frac{d_r-1}{2}}(s).$$

Ce terme ne s'annule pas, et il est fini, en $s = \frac{d_r+1}{2}$. En supposant $\delta(\pi, \frac{d_r+1}{2}) = 0$, on a donc $\mathrm{ord}_{s=\frac{d_r+1}{2}} \xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) = -1$. Mais d'après Mizumoto, les seuls pôles éventuels de $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$ sont en $s = 0$ ou $s = 1$, ce qui montre $d_r = 1$.

Le cas $k = g$ est similaire. Dans ce cas, $\psi(\pi_F, \mathrm{St})_\infty$ admet 0 pour valeur propre triple et les entiers $\pm 1, \ldots, \pm(g-1)$ pour valeurs propres simples. En particulier, il est possible que π_i admette le poids 0 pour $i < r$, mais dans ce cas on a $d_i = 1$. L'égalité (7.2) est donc encore satisfaite. De plus, ce même argument montre $\frac{\xi_{\mathrm{B}}(s,\pi_F,\mathrm{St})}{\xi_{\mathrm{A}}(s,\pi_F,\mathrm{St})} = \mu(s)\,\gamma_{\frac{d_r-1}{2}}(s)$ avec

$$\mu(s) = \frac{\Gamma_{\mathbb{C}}(s)\Gamma(s, \epsilon^g_{\mathbb{C}/\mathbb{R}})}{\Gamma(s, \epsilon_{\mathbb{C}/\mathbb{R}}^{\frac{d_r-1}{2}})\Gamma_{\mathbb{R}}(s+e_1)\Gamma_{\mathbb{R}}(s+e_2)},$$

pour certains éléments $e_1, e_2 \in \{0, 1\}$ qu'il sera inutile de préciser (voir la remarque 7.2). La fonction $\mu(s)$ est finie et non nulle en $s = \frac{d_r+1}{2}$, et on conclut comme dans le cas $k = g+1$ par le résultat de Mizumoto. □

Remarque 7.2. Soient $a, b \in \mathbb{Z}$. Observons que si la fonction méromorphe $\Gamma_{\mathbb{R}}(s)^a \Gamma_{\mathbb{R}}(s+1)^b$ est invariante par $s \mapsto 1-s$, alors on a $a = b = 0$. En effet, l'ordre d'annulation de cette fonction en $s = 2, 1, 0$ et -1 vaut respectivement 0, 0, $-a$ et $-b$. L'invariance par $s \mapsto 1-s$ des fonctions $\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})$, $\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$, ainsi que $\gamma_n(s)$ pour tout $n \geq 0$, permet donc de préciser la démonstration précédente. Tout d'abord, on en déduit la congruence $\frac{d_r-1}{2} \equiv g \bmod 2$ pour $k = g+1$, que nous avions déjà obtenue autrement au §5.1. Dans le cas $k = g$, on en déduit l'égalité des images dans $\mathbb{Z}/2\mathbb{Z}$ des ensembles $\{e_1, e_2\}$ et $\{\frac{d_r+1}{2}, g\}$.

La proposition suivante, qui sera utile au §IX.5, suggère des propriétés cachées du paramètre standard de π_F dans le cas $g \geq k$, soit encore des paquets d'Arthur de $\mathrm{Sp}_{2g}(\mathbb{R})$ contenant les représentations de la forme π'_W qui ne sont pas des séries discrètes (§VI.3.4). Il serait intéressant de les clarifier. La notation $[x]$ désigne la partie entière du réel x.

Proposition* **7.3.** *Soit $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre avec $g \geq k$. On suppose $\psi(\pi_F, \mathrm{St}) = \oplus_{i=1}^r \pi_i[d_i]$ et, pour tout $i = 1, \ldots, r$ tel que $\pi_i \neq 1$, la propriété suivante satisfaite :*

$$\forall \lambda \in \mathrm{Poids}(\pi_i), \quad |\lambda| \geq \frac{d_i - 1}{2}. \tag{7.3}$$

On a alors l'égalité

$$\frac{\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})}{\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})} = \left(\prod_{i=1}^{g-k} \frac{1}{p_i(s)} \right) \left(\prod_{i \in I} \gamma_{\frac{d_i-1}{2}} \right). \tag{7.4}$$

Si l'on pose $I = \{1 \leq i \leq r, \pi_i = 1\}$ et $I' = \{i \in I, d_i = 1\}$, on a alors

$$\delta(\pi_F, 1) + \sum_{i \in I} [\frac{d_i + 1}{4}] \geq g - k - 2 + |I'| + 2|I - I'|. \tag{7.5}$$

Si I est non vide, on pose enfin $d = \max\{d_i, i \in I\}$; on a l'inégalité $d \geq 2|I - I'| + 1$. Définissons $\nu \in \{0, 1\}$ par la congruence $\nu \equiv k \bmod 2$. Alors on est dans un des cas suivants :

(a) $|I| = 3$, $\frac{d+1}{2} \geq g - k + 4 - \delta(\pi_F, 1)$, et l'une des deux inégalités suivantes est vérifiée : $\delta(\pi_F, 1) > 2 - \nu$ ou $\delta(\pi_F, \frac{d+1}{2}) > 0$.

(b) $|I| = 2$, $|I'| = 0$, $\frac{d+1}{2} \geq g - k + 3 - \delta(\pi_F, 1)$, et l'une des deux inégalités suivantes est vérifiée : $\delta(\pi_F, 1) > 1 - \nu$ ou $\delta(\pi_F, \frac{d+1}{2}) > 0$.

(c) $|I| = 2$, $|I'| = 1$, $\frac{d+1}{4} \geq g - k + 1 - \delta(\pi_F, 1)$, *et l'une des deux inégalités suivantes est vérifiée :* $\delta(\pi_F, 1) > \frac{g-k-\nu}{2}$ *ou* $\delta(\pi_F, \frac{d+1}{2}) > 0$.

(d) $|I| = 1$, $|I'| = 0$, $\frac{d+1}{4} \geq g - k - \delta(\pi_F, 1)$, *et l'une des deux inégalités suivantes est vérifiée :* $\delta(\pi_F, 1) > \frac{g-k-\nu-2}{2}$ *ou* $\delta(\pi_F, \frac{d+1}{2}) > 0$.

(e) $I' = I$ *et* $\delta(\pi_F, 1) \geq g - k - 2 + |I'|$.

Démonstration. Par définition, on a la relation

$$\mathrm{ord}_{s=1}\ \xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) \ = \ -|I'| - 2|I - I'| + \delta(\pi_F, 1).$$

On rappelle que $\psi(\pi_F, \mathrm{St})_\infty$ admet pour valeurs propres les $2g+1$ entiers 0 et $\pm(k-j)$, $j = 1, \ldots, g$. En particulier, 0 en est valeur propre de multiplicité 3 et les π_i sont algébriques. De plus, si l'on a $\pi_i \neq 1$ et si 0 est un poids de π_i, alors on a nécessairement $d_i = 1$ d'après l'hypothèse (7.3). Ainsi, l'hypothèse (7.3) et la recette pour les $\mathrm{L}(s, (\pi_i)_\infty)$ (§2.13, §2.21) entraînent qu'il existe $e_1, e_2, e_3 \in \{0, 1\}$ tels que si l'on pose $\mu(s) = \frac{\Gamma_{\mathbb{C}}(s)\Gamma(s, \epsilon^g_{\mathbb{C}/\mathbb{R}})}{\Gamma_{\mathbb{R}}(s+e_1)\Gamma_{\mathbb{R}}(s+e_2)\Gamma_{\mathbb{R}}(s+e_3)}$, on a

$$\frac{\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})}{\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})} = \left(\prod_{i=1}^{g-k} \frac{1}{p_i(s)}\right) \left(\prod_{i \in I} \gamma_{\frac{d_i-1}{2}}\right) \mu(s).$$

La remarque 7.2, et l'invariance des $p_n(s)$ par $s \mapsto 1 - s$, montrent $\mu(s) = 1$, d'où la formule (7.4).

Comme on a $\mathrm{ord}_{s=1}\, p_n(s) = 1$ si $n \geq 1$, et $p_0 = 1$, on a aussi $\mathrm{ord}_{s=1}\gamma_n(s) = [\frac{n+1}{2}]$. On a donc

$$\mathrm{ord}_{s=1}\frac{\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})}{\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})} \ = \ -(g-k) \ + \ \sum_{i \in I} [\frac{d_i + 1}{4}]$$

d'après la relation (7.4). L'inégalité (7.5) de l'énoncé découle alors de l'inégalité $\mathrm{ord}_{s=1}\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) \geq -2$ de Mizumoto.

Supposons $|I| \neq 0$ et vérifions la dernière assertion. D'après le théorème 2.4 d'Arthur, les d_i avec $i \in I$ sont deux à deux distincts. En particulier, on a $|I'| \leq 1$. Comme $\mathrm{St}\, \mathrm{c}_\infty(\pi_F)$ admet ± 1 pour valeur propre de multiplicité ≤ 2, on a aussi $|I - I'| \leq 2$ (et donc $|I| \leq 3$). Les d_i étant évidemment impairs, on a enfin $d \geq 2|I - I'| + 1$.

Supposons d'abord $|I| = 3$, auquel cas on a $|I'| = 1$. L'inégalité (7.5), associée à l'inégalité évidente $\sum_{i \in I}[\frac{d_i+1}{4}] \leq \sum_{i \in I - I'} \frac{d_i+1}{4} < \frac{d+1}{2}$, entraînent

$$\frac{d+1}{2} \geq g - k + 4 - \delta(\pi_F, 1) \ = \ (g - k + 2 + \nu) + (2 - \nu - \delta(\pi_F, 1)).$$

Supposant l'inégalité $\delta(\pi_F, 1) \leq 2 - \nu$, on en déduit $\frac{d+1}{2} \geq g - k + 2 + \nu$. On a donc $\mathrm{ord}_{s=\frac{d+1}{2}} \xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) \geq 0$ d'après Mizumoto. D'autre part, on a aussi $\mathrm{ord}_{s=\frac{d+1}{2}} \xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) = -1 + \delta(\pi_F, \frac{d+1}{2})$, et

$$\mathrm{ord}_{s=\frac{d+1}{2}} \frac{\xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})}{\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St})} \leq 0$$

d'après la formule (7.4), on obtient l'inégalité attendue $\delta(\pi_F, \frac{d+1}{2}) \geq 1$. Cela démontre le cas (a). On procède de même dans les cas (b), (c), (d) et (e). $\square$

IX. Démonstration des théorèmes principaux

1. Les formes modulaires de genre 2 de Tsushima

Si $j \geq 0$ et $k \in \mathbb{Z}$ sont des entiers, notons $\mathrm{S}_{j,k}$ l'espace $\mathrm{S}_W(\mathrm{Sp}_4(\mathbb{Z}))$ où W est la représentation $\mathrm{Sym}^j \mathbb{C}^2 \otimes \text{dét}^k$ de $\mathrm{GL}_2(\mathbb{C})$ (§IV.5, §VI.3.4). Il est nul si $j \equiv 1 \bmod 2$, car alors -1_2 agit par $-\mathrm{id}$ sur W, ou si $k \leq 0$ (Freitag [VDG08, Prop. 4.6]), c'est pourquoi nous supposerons toujours $j \equiv 0 \bmod 2$ et $k > 0$.

1.1. La formule de dimension de Tsushima

Une formule explicite pour $\dim \mathrm{S}_{j,k}$ a été déterminée par R. Tsushima quand $k \geq 5$ [TSU83], étendant un résultat d'Igusa concernant les formes scalaires (cas $j = 0$, $k \in \mathbb{Z}$ quelconque [IGU62]). Lorsque $j + 2k - 3 \leq 21$, qui s'avèrera être le cas d'intérêt pour ce mémoire, la formule de Tsushima montre que $\mathrm{S}_{j,k} = 0$, sauf pour 6 valeurs (j, k) données dans la table suivante et pour lesquelles $\dim \mathrm{S}_{j,k} = 1$. Comme nous le verrons plus loin, $\dim \mathrm{S}_{j,k}$ est également nul quand $k \leq 4$ et $j + 2k - 3 \leq 21$: voir la remarque 3.41. La ligne (w, v) sera expliquée au §1.3.

(j,k)	$(0,10)$	$(6,8)$	$(0,12)$	$(4,10)$	$(8,8)$	$(12,6)$
(w,v)	$(17,1)$	$(19,7)$	$(21,1)$	$(21,5)$	$(21,9)$	$(21,13)$

TABLE IX.1 – Les couples (j, k) tels que $\dim \mathrm{S}_{j,k} \neq 0$, pour $j + 2k - 3 \leq 21$ et $k \geq 5$, d'après Tsushima.

Pour chacun des 6 couples (j, k) ci-dessus, notons $F_{j,k}$ un générateur de $\mathrm{S}_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$. Étant donné le grand rôle joué par ces formes de Siegel dans la suite, expliquons comment montrer directement leur existence, par une construction de série thêta bâtie sur le réseau E_8.

Fixons pour cela $j \geq 0$ pair et $k \geq 4$, des entiers pour l'instant quelconque. Il existe un unique isomorphisme de $\mathbb{C}$-algèbres $\mathbb{C}[X, Y] \xrightarrow{\sim} \mathrm{Sym}\, \mathbb{C}^2$ envoyant

respectivement X et Y sur les éléments $(1,0)$ et $(0,1)$ de $\mathbb{C}^2$. Par transport de structure, cette isomorphisme munit $\mathbb{C}[X,Y]$ d'une représentation de $\mathrm{GL}_2(\mathbb{C})$. Le sous-espace $\mathbb{C}[X,Y]_j \subset \mathbb{C}[X,Y]$ des polynômes homogènes de degré j est une sous-représentation isomorphe à $\mathrm{Sym}^j \mathbb{C}^2$.

Soit $I \subset \mathrm{E}_8 \otimes \mathbb{C}$ un sous-espace isotrope de dimension 2, ainsi que u, v et w trois éléments de I. Considérons l'application $\mathrm{E}_8^2 \to \mathbb{C}[X,Y]_j$ définie par

$$\mathrm{P}_{j,k,u,v,w}(x,y) = \mathrm{dét}^{k-4} \begin{bmatrix} x \cdot u & x \cdot v \\ y \cdot u & y \cdot v \end{bmatrix} ((x \cdot w)X + (y \cdot w)Y)^j.$$

L'équation fonctionnelle de la fonction ϑ de Jacobi (à deux variables) permet de démontrer que la fonction

$$\vartheta_2(\mathrm{E}_8, \mathrm{P}_{j,k,u,v,w}) = \sum_{(x,y) \in \mathrm{E}_8 \times \mathrm{E}_8} \mathrm{P}_{j,k,u,v,w}(x,y)\ q^{\frac{1}{2}\begin{bmatrix} x \cdot x & x \cdot y \\ y \cdot x & y \cdot y \end{bmatrix}}$$

est une forme modulaire de Siegel pour $\mathrm{Sp}_4(\mathbb{Z})$ à coefficients dans la représentation $\mathrm{Sym}^j \otimes \mathrm{dét}^k$ [Fre80, §2]. Elle est manifestement parabolique si $k > 4$, et si $k = 4$ le coefficient en X^j de son image par l'opérateur Φ_1 de Siegel est la série thêta du polynôme harmonique $x \mapsto (x \cdot w)^j$ sur E_8 (§V.4.1), un élément de $\mathrm{M}_{j+4}(\mathrm{SL}_2(\mathbb{Z}))$ qui est parabolique si $j > 0$.

Application numérique : Il n'est pas difficile, à l'aide de l'ordinateur, de déterminer les coefficients de Fourier de $f_{j,k,u,v,w} = \vartheta_2(\mathrm{E}_8, \mathrm{P}_{j,k,u,v,w})$ en des matrices de Gram de petit discriminant : nous renvoyons à la feuille de calculs [CL `PARI`] pour une justification des affirmations qui vont suivre. Décrivons le résultat du calcul en discriminant ≤ 12, obtenu en prenant $u = (2,i,i,i,i,0,0,0)$, $v = (0,0,0,i,-i,i,i,2)$, $w = u + v$, et en énumérant bêtement tous les couples $(x,y) \in \mathrm{E}_8^2$ de matrice de Gram l'une des 7 matrices apparaissant dans la table C.2. On constate que pour chacun des 6 couples (j,k) en question, tous les coefficients calculés sont non nuls, hormis l'un d'eux pour $(j,k) = (6,8)$. La table C.2 indique précisément les coefficients de Fourier de $\frac{1}{\lambda_{j,k}} f_{j,k,u,v,u+v}$, où $\lambda_{j,k} \in \mathbb{Z} - \{0\}$ est une constante qui n'a pas de signification particulière (tout comme notre choix de u, v, w), et que nous n'expliciterons pas ici. En guise de vérification, mentionnons que lorsque $(j,k) = (0,10)$ nos calculs sont compatibles avec la table IV de [RS74]. Comme on a $\mathrm{S}_{14}(\mathrm{SL}_2(\mathbb{Z})) = 0$, cela redémontre $\mathrm{S}_{j,k} \neq 0$ dans tous les cas. $\square$

Le couple (j,k) étant fixé, on peut également vérifier que si l'on fait varier les paramètres u, v et w dans le calcul ci-dessus (ou même par appel à un

calcul formel), alors le quadruplet de coefficients calculés (des polynômes !) n'est modifié que par un scalaire, comme il se doit car $\dim \mathrm{S}_{j,k} = 1$. Cela peut également se démontrer autrement, de la manière suivante.

Posons $W_{j,k} = \mathrm{Sym}^j \mathbb{C}^2 \otimes \det^k$ et notons $U_{j,k}$ la représentation naturelle de $\mathrm{O}_8(\mathbb{C})$ sur l'espace des polynômes $\mathrm{E}_8 \otimes \mathbb{C}^2 \to W_{j,k-4}$ qui sont $\mathrm{GL}_2(\mathbb{C})$-équivariant et *pluriharmoniques* [KV78] [FRE80] ; la fonction $\mathrm{P}_{j,k,u,v,w}$ est un élément typique de $U_{j,k}$. Ces références assurent que si $k \geq 4$, le couple $(U_{j,k}, W_{j,k})$ est compatible au sens du §VII.1.1. Précisément, on dispose d'une application linéaire

$$\vartheta : \mathrm{M}_{U_{j,k}}(\mathrm{O}_8) \longrightarrow \mathrm{M}_{W_{j,k}}(\mathrm{Sp}_4(\mathbb{Z})). \tag{1.1}$$

envoyant l'élément $[\mathrm{E}_8, \mathrm{P}_{j,k,u,v,w}]$, défini à la fin paragraphe IV.4.7, sur la série thêta $\vartheta_2(\mathrm{E}_8, \mathrm{P}_{j,k,u,v,w})$, pour tout triplet d'éléments u, v, w appartenant à un même sous-espace isotrope de rang 2 de $\mathrm{E}_8 \otimes \mathbb{C}$.

On vérifie aisément que la représentation $U_{j,k}$, qui est irréductible restreinte à $\mathrm{SO}_8(\mathbb{C})$ d'après [KV78], admet un plus haut poids de la forme $(j+k-4)\varepsilon_1+(k-4)\varepsilon_2$ dans les notations du §VI.4.3. Or les tables [1] de [CR12] montrent que pour les 6 couples (j,k) d'intérêt, on a $\dim \mathrm{M}_{U_{j,k}}(\mathrm{O}_8) = 1$. Nous en déduisons, comme promis, que l'espace $\vartheta(\mathrm{M}_{U_{j,k}}(\mathrm{O}_8))$ est de dimension 1 pour ces couples. Étant donné que l'on a aussi $\dim \mathrm{S}_{j,k} = 1$, on obtient la proposition suivante.

Proposition 1.2. *Si (j,k) est l'un des 6 couples de la table IX.1, alors l'application* (1.1) *induit un isomorphisme $\mathrm{M}_{U_{j,k}}(\mathrm{O}_8) \xrightarrow{\sim} \mathrm{S}_{j,k}$ entre espaces de dimension* 1.

1.3. Paramètres standards des 6 premières formes de genre 2

Soit $F \in \mathrm{S}_{j,k}$ une forme propre pour l'action de $\mathrm{H}(\mathrm{PGSp}_4)$. Notons $\pi_F \in \Pi_{\mathrm{cusp}}(\mathrm{PGSp}_4)$ la représentation engendrée par F (Corollaire VI.3.7). Observons que le groupe de Chevalley PGSp_4 est un $\mathbb{Z}$-groupe classique, étant isomorphe au $\mathbb{Z}$-groupe $\mathrm{SO}_{3,2}$; son dual de Langlands est le $\mathbb{C}$-groupe Sp_4, il est muni de sa représentation standard de dimension 4. D'après la fin du §VI.3.4, la classe de conjugaison semi-simple $\mathrm{St}(\mathrm{c}_\infty(\pi_F)) \subset \mathrm{M}_4(\mathbb{C})$ a pour valeurs propres $\pm\frac{w}{2}$ et $\pm\frac{v}{2}$, où

$$(w, v) = (j + 2k - 3, j + 1),$$

ce qui explique la seconde ligne de la table IX.1. Observons que l'application $(j,k) \mapsto (w,v)$ est une bijection entre l'ensemble des couples (j,k) avec $j \geq 0$

1. Voir http://gaetan.chenevier.perso.math.cnrs.fr/table/dim_SO8_dom.txt

pair et $k \geq 3$, et l'ensemble des couples (w, v) avec w, v impairs tels que $w > v > 0$.

Pour chacun des 6 couples (j, k) de la table IX.1, l'action de $\mathrm{H}(\mathrm{PGSp}_4)$ sur $\mathrm{S}_{j,k}$ est alors trivialement scalaire, *i.e.* $F_{j,k}$ est propre, et nous allons nous intéresser au paramètre

$$\psi_{j,k} = \psi(\pi_{F_{j,k}}, \mathrm{St}) \in \mathcal{X}(\mathrm{SL}_4).$$

Le cas de la forme scalaire $F_{0,10}$ a une histoire fameuse puisque c'est la première forme de Saito-Kurokawa, associée à la forme modulaire de poids 18 pour $\mathrm{SL}_2(\mathbb{Z})$ ([Kur78], §VII.3). Du fait que l'on considère $\pi_{F_{0,10}}$ comme représentation de PGSp_4, plutôt que Sp_4, on a la relation (voir [EZ85],[Za80])

$$\psi_{0,10} = \Delta_{17} \oplus [2],$$

ce qui est manifestement compatible avec l'égalité $(w, v) = (17, 1)$ (la notation Δ_w est introduite au §VII.3). Le cas de la forme $F_{0,12}$ est similaire, et l'on a $\psi_{0,12} = \Delta_{21} \oplus [2]$ d'après Andrianov, Maass et Zagier. Comme l'avait également deviné Kurokawa, et expliqué Arthur [Art04], la situation est très différente pour les 4 autres représentations.

Proposition* **1.4.** *On suppose $j > 0$ pair et $k \geq 3$.*

(i) (Multiplicité 1) *Si $F, G \in \mathrm{S}_{j,k}$ sont deux formes propres pour l'action de $\mathrm{H}(\mathrm{Sp}_4)$, et si tout élément de $\mathrm{H}(\mathrm{Sp}_4)$ a même valeur propre sur F et G, alors F et G sont proportionnelles.*

(ii) Si $F \in \mathrm{S}_{j,k}$ est propre pour l'action de $\mathrm{H}(\mathrm{PGSp}_4)$ alors $\psi(\pi_F, \mathrm{St}) = \pi$ avec $\pi \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_4)$.

(iii) L'application $F \mapsto \psi(\pi_F, \mathrm{St})$ induit une bijection entre l'ensemble des droites propres de $\mathrm{S}_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$ sous l'action de $\mathrm{H}(\mathrm{PGSp}_4)$ et l'ensemble des $\pi \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_4)$ telles que $\mathrm{Poids}(\pi) = \{\pm\frac{j+2k-3}{2}, \pm\frac{j+1}{2}\}$.

Démonstration. Le (i) est le cas particulier $g = 2$ du corollaire VIII.5.4 : dans les notations *loc. cit.* on a $(m_1, m_2) = (j + k, k)$ de sorte que $m_1 > m_2$.

Posons $(w, v) = (j + 2k - 3, j + 1)$. Soit $F \in \mathrm{S}_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$ une forme propre pour $\mathrm{H}(\mathrm{PGSp}_4)$. On applique le théorème 1.1 au $\mathbb{Z}$-groupe classique $\mathrm{PGSp}_4 \simeq \mathrm{SO}_{3,2}$ et à sa représentation $\pi_F \in \Pi_{\mathrm{disc}}(\mathrm{PGSp}_4)$. Étant donné qu'un $\pi \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_2)$ est symplectique (Proposition 1.5), et que $\pm\frac{1}{2}$ n'est pas valeur propre de $\mathrm{St}(\mathrm{c}_\infty(\pi_F))$ car $j > 0$, il n'y a que deux possibilités pour $\psi(\pi_F, \mathrm{St})$ (corollaire VIII.2.15 (ii)) :

(a) soit $\psi(\pi_F, \mathrm{St}) = \pi_1 \in \Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_4)$,

(b) soit $\psi(\pi_F, \mathrm{St}) = \pi_1 \oplus \pi_2$ avec $\pi_1, \pi_2 \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ tels que $\mathrm{w}(\pi_1) = w$ et $\mathrm{w}(\pi_2) = v$.

Pour démontrer le (ii), il faut donc montrer que le cas (b) ne se produit pas. Observons que pour les quatres couples (j, k) de la table IX.1 on a $v \in \{5, 7, 9, 13\}$, de sorte que cela découle directement de la proposition 1.5 et de ce que $\dim \mathrm{S}_{v+1}(\mathrm{SL}_2(\mathbb{Z})) = 0$ pour ces valeurs de v. Pour un couple (j, k) général, c'est plutôt une conséquence de la formule de multiplicité d'Arthur pour $\mathrm{SO}_{3,2}$ (Thm. VIII.3.10).

Supposons en effet que $\psi = \pi_1 \oplus \pi_2 \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_4)$ où π_1 et π_2 sont comme dans le (b) ci-dessus. Considérons des homomorphismes ν et ν_∞ associés à ψ comme au §VIII.3.8. Par définition, $\nu : \mathrm{SL}_2 \times (\mathrm{SL}_2 \times \mathrm{SL}_2) \to \mathrm{Sp}_4$ est trivial sur le premier facteur SL_2 et $\mathrm{St} \circ \nu$ est la somme directe des représentations tautologiques de chacun des deux autres facteurs SL_2, de sorte que l'inclusion $\{\pm 1\}^2 = \mathrm{C}_\nu \hookrightarrow \mathrm{C}_{\nu_\infty}$ est une égalité. On en déduit que $\varepsilon_\psi = 1$ (car "$d_i = 1$ pour tout i") et que $\Pi(\nu_\infty)$ est l'ensemble des deux séries discrètes de $\mathrm{SO}_{3,2}(\mathbb{R})$ de caractère infinitésimal ψ_∞ d'après le §VIII.4.5. L'une est holomorphe, disons π_{hol}, et l'autre générique (la notion est canonique ici car $\mathrm{SO}_{3,2}$ est adjoint), de sorte que le caractère de Shelstad $\chi_{\pi_{\mathrm{hol}}}$ est le caractère non trivial de C_{ν_∞} qui est trivial sur le centre de $\widehat{\mathrm{SO}_{3,2}} = \mathrm{Sp}_4$, à savoir le sous-groupe $\{\pm 1\}$ diagonal dans C_{ν_∞}. Une autre manière de le voir consiste à appliquer simplement la formule VIII.(4.6) dans le cas particulier $r = 2$. Ainsi, la restriction la restriction de $\chi_{\pi_{\mathrm{hol}}}$ à $\mathrm{C}_\nu = \mathrm{C}_{\nu_\infty}$ est non triviale, et la formule de multiplicité d'Arthur affirme que l'unique $\pi \in \Pi(\mathrm{PGSp}_4)$ telle que $\pi \simeq \pi_{\mathrm{hol}}$ et $\psi(\pi, \mathrm{St}) = \psi$ est de multiplicité nulle (Thm. VIII.3.10). Comme $\mathrm{m}(\pi_F) > 0$, on est dans le cas (a) ci-dessus, ce qui prouve le (ii). La même formule de multiplicité d'Arthur affirme alors que $\mathrm{m}(\pi_F) = 1$ et plus généralement que pout tout $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_4)$ de poids $\{\pm\frac{w}{2}, \pm\frac{v}{2}\}$ il existe un (unique) $\pi \in \Pi_{\mathrm{disc}}(\mathrm{PGSp}_4)$ tel que $\psi(\pi, \mathrm{St}) = \pi$ et $\pi_\infty \simeq \pi_{\mathrm{hol}}$, et qu'il vérifie $\mathrm{m}(\pi) = 1$ (c'est le cas où il n'y a rien à vérifier car $\mathrm{C}_\psi = \mathrm{Z}(\widehat{G})$). L'assertion (iii) suit alors du corollaire VI.3.7. $\square$

Nous avons fait appel à l'énoncé très classique suivant.

Proposition 1.5. *Soient $k \geq 2$ un entier pair et $\mathcal{F}_k \subset \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z})$ l'ensemble des formes modulaires propres pour $\mathrm{H}(\mathrm{PGL}_2)$ et normalisées (i.e. de coefficient de Fourier en q égal à 1). L'application associant à $F \in \mathcal{F}_k$ la représentation engendrée $\pi_F \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ induit une bijection entre $\mathcal{F}_k$ et l'ensemble des $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ telles que $\mathrm{Poids}(\pi) = \{\pm\frac{k-1}{2}\}$.*

Démonstration. On rappelle qu'une forme propre $F \in \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ a toujours son coefficient en q non nul, et que si elle est normalisée elle est uniquement déterminée par ses valeurs propres sous $\mathrm{H}(\mathrm{PGL}_2)$[Ser70, Chap. VII Thm. 7], en particulier $\mathcal{F}_k$ est une base de l'espace vectoriel $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$. Soit U_k la série discrète de $\mathrm{PGL}_2(\mathbb{R})$ telle que $\mathrm{Inf}_{U_k} \subset \mathrm{M}_2(\mathbb{C})$ a pour valeurs propres $\pm\frac{k-1}{2}$. Un cas particulier bien connu de la proposition IV.3.7 est que l'on dispose d'un isomorphisme $\mathrm{H}(\mathrm{PGL}_2)$-équivariant entre $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ et $\mathcal{A}_{U_k}(\mathrm{PGL}_2) = \mathrm{Hom}_{\mathrm{PGL}_2(\mathbb{R})}(U_k, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGL}_2))$ [GGPS66, Ch. I §4]. Cela montre que l'application de l'énoncé est bien définie et injective.

Une justification sophistiquée de la surjectivité consiste à invoquer la proposition 2.13 (i). On peut aussi utiliser la classification de Bargmann [Bar47] du dual unitaire de $\mathrm{SL}_2(\mathbb{R})$. Elle montre que si U est une représentation irréductible unitaire de $\mathrm{PGL}_2(\mathbb{R})$ telle que $\mathrm{Inf}_U \subset \mathrm{M}_2(\mathbb{C})$ a pour valeurs propres $\pm\frac{k-1}{2}$, alors soit $U \simeq U_k$, soit $\dim U = 1$ et $k = 2$. En effet, les représentations de la série principale ont un caractère infinitésimal dont les valeurs propres sont de la forme $\pm is$ avec $s \in \mathbb{R}$ (cas "tempéré") ou de la forme $\pm s$ avec $s \in]-\frac{1}{2}, \frac{1}{2}[$ ("série complémentaire") ; de plus, le caractère infinitésimal de la "limite de série discrète" est 0. Pour éliminer le cas $\dim U = 1$, on observe que la fomule IV.(5.1) entraîne que les seuls éléments de $\mathcal{A}^2(\mathrm{PGL}_2)$ invariants par $\mathrm{PGL}_2(\mathbb{R})^+$ sont les fonctions constantes, qui ne sont pas cuspidales, ce qui conclut. □

La proposition 1.4 et la table de Tsushima justifient la définition-proposition suivante.

Proposition-Définition⋆ 1.6. *Si $(w, v) \in \{(19, 7), (21, 5), (21, 9), (21, 13)\}$, il existe une unique représentation dans $\Pi^{\perp}_{\mathrm{cusp}}(\mathrm{PGL}_4)$ qui est algébrique de poids l'ensemble $\{\pm\frac{w}{2}, \pm\frac{v}{2}\}$. On la note $\Delta_{w,v}$.*

Ainsi, pour les 4 dernières colonnes de la table IX.1 on a la relation $\psi_{j,k} = \Delta_{w,v}$ et $\psi_{j,k}$ ne s'exprime pas à l'aide de formes de genre 1.

1.7. Quelques valeurs propres des opérateurs de Hecke

Soient $(j, k) \in \{(6, 8), (4, 10), (8, 8), (12, 6)\}$, $(w, v) = (j + 2k - 3, j + 1)$, p un nombre premier et $n \geq 1$ un entier. On pose

$$(1.2) \qquad \tau_{j,k}(p^n) \;=\; p^{\frac{nw}{2}} \operatorname{trace} \mathrm{St}(\mathrm{c}_p(\pi_{F_{j,k}})^n) \;=\; p^{\frac{nw}{2}} \operatorname{trace}\big(\,\mathrm{c}_p(\Delta_{w,v})^n\,\big).$$

La classe de conjugaison $\mathrm{St}(\mathrm{c}_p(\pi_{F_{j,k}})) \subset \mathrm{SL}_4(\mathbb{C})$ est égale à son inverse, elle

a donc pour polynôme caractéristique

$$t^4 - \tau_{j,k}(p)\, t^3 + \frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2}\, t^2 - \tau_{j,k}(p) p^{j+2k-3}\, t + p^{2j+4k-6}. \tag{1.3}$$

En particulier, le nombre complexe $\tau_{j,k}(p^n)$ est un polynôme à coefficients entiers en $\tau_{j,k}(p)$ et $\frac{\tau_{j,k}(p)^2-\tau_{j,k}(p^2)}{2}$.

La proposition suivante était connue de Shimura [Shi63]. Comme l'avait déjà expliqué Gross dans [Gro98, §6], c'est également une conséquence immédiate de la relation VI.(2.8) (voir aussi le §VI.4.3).

Proposition 1.8. *Soient j, k comme ci-dessus et p un nombre premier.*

(a) Le nombre complexe $\tau_{j,k}(p)$ est la valeur propre de l'opérateur de Hecke $p^{\frac{j+2k-6}{2}}\mathrm{K}_p$ agissant sur la droite $\mathrm{S}_{j,k}$.

(b) Le nombre complexe $\frac{\tau_{j,k}(p)^2-\tau_{j,k}(p^2)}{2}$ est la valeur propre de l'opérateur de Hecke $p^{j+2k-5}(\mathrm{T}_p+1)+p^{j+2k-3}$ agissant sur la droite $\mathrm{S}_{j,k}$.

D'après la relation IV.5.4, l'opérateur $p^{\frac{j+2k-6}{2}}\,\mathrm{K}_p$ coïncide avec celui noté $\mathrm{T}(p)$ chez van der Geer [vdG08, §16], du moins lorsque ce dernier est défini en incluant la normalisation entre parenthèses dans la définition 16.5 *loc. cit.* L'opérateur noté ici T_p est parfois noté $\mathrm{T}_1(p^2)$ dans la littérature, au facteur près d'une puissance de p dépendant des auteurs.

Le problème de déterminer les valeurs propres des opérateurs de Hecke agissant sur les espaces $\mathrm{S}_{j,k}$ est sensiblement plus difficile en pratique que son analogue en genre 1. Une raison est la difficulté à déterminer les coefficients de Fourier des formes de genre 2, notamment en des matrices de Gram de grand déterminant. De plus, la relation entre coefficients de Fourier et valeurs propres, étudiée dans ce contexte par Andrianov [And74] pour les formes scalaires et étendue aux formes vectorielles par Arakawa [Ara83], est plus subtile qu'en genre 1. Dans ce qui suit, nous rappelons cette relation dans le cas des opérateurs de Hecke K_p et T_p. Nous en déduirons à la fois la proposition suivante, ainsi que le calcul de quelques valeurs des entiers $\tau_{j,k}(p)$.

Proposition 1.9. *Soient $(j,k) \in \{(6,8),(4,10),(8,8),(12,6)\}$, p un nombre premier et $n \geq 1$ un entier. On a $\tau_{j,k}(p^n) \in \mathbb{Z}$ ainsi que la congruence*

$$\tau_{j,k}(p^2) \;\equiv\; \tau_{j,k}(p)^2 \mod 2\,p^{k-2}.$$

Posons $\Gamma = \mathrm{Sp}_4(\mathbb{Z})$ et considérons les éléments suivants de $\mathrm{GSp}_4(\mathbb{Z}[\frac{1}{p}])^+$

$$\gamma := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix}, \qquad \gamma' := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}.$$

Lemme 1.10. *(a) L'opérateur de Hecke* $\mathrm{K}_p \in \mathrm{H}_p(\mathrm{PGSp}_4)$ *est de degré* $(1+p)(1+p^2)$*. Sa matrice est la fonction caractéristique de l'image de* $\Gamma\gamma^{-1}\Gamma$ *dans* $\mathrm{PGSp}_4(\mathbb{Z}[\frac{1}{p}])^+$*, au sens des identifications* IV.(2.2) *et* IV.(5.3)*. La double-classe* $\Gamma\gamma\Gamma$ *est réunion disjointe des classes à droite* $\Gamma\gamma_i$*, où* γ_i *parcourt la liste des éléments de la forme suivante :*

$$\begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & a & b \\ 0 & 1 & b & c \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix}, \quad \begin{bmatrix} p & 0 & 0 & 0 \\ -d & 1 & 0 & e \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & p \end{bmatrix} \text{ ou } \begin{bmatrix} 1 & 0 & f & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

avec a, b, c, d, e, f *des entiers compris entre* 0 *et* $p-1$ *;*

(b) De même, $\mathrm{T}_p \in \mathrm{H}_p(\mathrm{PGSp}_4)$ *est de degré* $p\,\frac{p^4-1}{p-1}$ *et a pour matrice la fonction caractéristique de l'image de* $\Gamma\gamma'^{-1}\Gamma$ *dans* $\mathrm{PGSp}_4(\mathbb{Z}[\frac{1}{p}])^+$*. La double-classe* $\Gamma\gamma'\Gamma$ *est la réunion disjointe des classes à droite* $\Gamma\gamma'_i$*, où* γ'_i *parcourt la liste des éléments de la forme suivante :*

$$\begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p^2 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} p^2 & 0 & 0 & 0 \\ -ap & p & 0 & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & p \end{bmatrix}, \quad \begin{bmatrix} p & 0 & b & c \\ 0 & p & c & d \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix},$$

$$\begin{bmatrix} p & 0 & 0 & pe \\ -f & 1 & e & ef+g \\ 0 & 0 & p & pf \\ 0 & 0 & 0 & p^2 \end{bmatrix} \text{ ou } \begin{bmatrix} 1 & 0 & h & i \\ 0 & p & pi & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix},$$

avec a, b, c, d, e, f, i *des entiers compris entre* 0 *et* $p-1$*, tels que* $c^2 \equiv bd \bmod p$ *et* $(b, c, d) \neq (0, 0, 0)$*, et avec* g *et* h *des entiers compris entre* 0 *et* p^2-1*.*

Démonstration. Le fait que les matrices de K_p et T_p sont les fonctions caractéristiques respectives des images des doubles-classes $\Gamma\gamma^{-1}\Gamma$ et $\Gamma\gamma'^{-1}\Gamma$ est la formule VI.(2.7).

Le degré de $\mathrm{K}_p \in \mathrm{H}_p(\mathrm{PGSp}_{2g})$ est le nombre des lagrangiens du a-module hyperbolique $\mathrm{H}(\mathbb{F}_p^g)$, à savoir $\prod_{i=1}^g (1+p^i)$. De même, le degré de T_p est le nombre de droites (isotropes) de $\mathrm{H}(\mathbb{F}_p^g)$, multiplié par le nombre des droites (isotropes) de $\mathrm{H}(\mathbb{F}_p)$ transverses à une droite donnée, ce qui fait $p\frac{p^g-1}{p-1}$.

Les assertions relatives aux décompositions des doubles-classes sont dues à Andrianov [And74, And87]. Justifions-les brièvement, en suivant les notes de Buzzard [Buz]. Un élément de GL_4, disons donné par blocs de taille 2×2, et supposé de la forme

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix},$$

est dans GSp_4 pour le facteur de similitude ν si, et seulement si, $a\,{}^{\mathrm{t}}b = b\,{}^{\mathrm{t}}a$ et $a\,{}^{\mathrm{t}}d = \nu 1_g$ (§IV.5.1). Cela montre que chacun des éléments de l'énoncé est dans $\mathrm{GSp}_4(\mathbb{Z}[\frac{1}{p}])$, avec pour facteur de similitude p dans le cas (a) et p^2 dans le cas (b).

Soient $h \in \mathrm{GSp}_4(\mathbb{Z}[1/p]) \cap \mathrm{M}_4(\mathbb{Z})$ et $\overline{h} \in \mathrm{M}_4(\mathbb{Z}/p)$ la réduction modulo p de h. La théorie des "diviseurs élémentaires symplectiques" montre que h est dans $\Gamma\gamma'\Gamma$ (resp. $\Gamma\gamma\Gamma$) si, et seulement si, $\nu(h) = p^2$ et le rang de $\overline{h}$ est 1 (resp. $\nu(h) = p$). Cela montre $\gamma_i \in \Gamma\gamma\Gamma$ et $\gamma'_i \in \Gamma\gamma'\Gamma$ pour tout i.

Enfin, on vérifie que $\gamma_i\gamma_j^{-1} \in \Gamma$ (resp. $\gamma'_i\gamma'^{-1}_j \in \Gamma$) force $i = j$; il est commode pour cela d'observer que tous les éléments ci-dessus sont dans un même sous-groupe de Borel de GSp_4, la "projection sur la diagonale" étant un homomorphisme. On conclut car dans chacun des deux cas le cardinal de la liste est le degré de l'opérateur de Hecke. $\square$

Soit $j \geq 0$ un entier. Notons ρ_j la représentation naturelle de $\mathrm{GL}_2(\mathbb{C})$ sur l'espace $W_j := \mathrm{Sym}^j\mathbb{C}^2$. On rappelle que pour $w \in W_j$ et $n \in \mathrm{M}_2(\mathbb{C})$, la notation $w\,\mathrm{q}^n$ désigne la fonction $\mathbb{H}_2 \to W_j,\ \tau \mapsto e^{2i\pi\,\mathrm{tr}(n\tau)}\,w$ (§IV.5.2).

Soient $k \in \mathbb{Z}$ et F une forme modulaire de Siegel pour $\mathrm{Sp}_4(\mathbb{Z})$ à coefficients dans la représentation $W_{j,k} := W_j \otimes \mathrm{dét}^k$ de $\mathrm{GL}_2(\mathbb{C})$. Par définition, cette représentation a pour espace sous-jacent W_j, et $\mathrm{GL}_2(\mathbb{C})$ y agit par $g \mapsto \rho_j(g)\mathrm{dét}(g)^k$. On rappelle que la forme F admet un développement de Fourier, que nous écrirons ici

$$F = \sum_{n\in\mathcal{N}} \mathrm{a}(n;F)\ \mathrm{q}^n,$$

où $\mathcal{N} \subset \frac{1}{2}\mathrm{M}_2(\mathbb{Z})$ est le sous-ensemble des matrices symétriques, positives, et de coefficients diagonaux dans $\mathbb{Z}$, et où $\mathrm{a}(n;F) \in W_j$ pour tout $n \in \mathcal{N}$ (§IV.5.2). Il sera commode de poser $\mathrm{a}(n,F) = 0$ si $n \in \mathrm{M}_2(\mathbb{Q}) - \mathcal{N}$.

On rappelle que l'on a défini au §IV.5.1 une action à droite de $\mathrm{GSp}_4(\mathbb{R})^+$ sur l'espace des fonctions $\mathbb{H}_2 \to W_{j,k}$, notée $(f,\gamma) \mapsto f_{|W_{j,k}}\gamma$. Soient $w \in W_j$, $n \in \mathrm{M}_2(\mathbb{C})$, et $\gamma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ dans $\mathrm{GSp}_4(\mathbb{R})^+$ de facteur de similitude ν, on a

$$(1.4) \qquad w\ \mathrm{q}^n{}_{|W_{j,k}}\gamma \ = \ \nu^{-\frac{j+2k}{2}} \cdot \mathrm{dét}(a)^k \cdot e^{\frac{2i\pi}{\nu}\mathrm{tr}({}^{\mathrm{t}}anb)} \cdot \rho_j({}^{\mathrm{t}}a) w\ \mathrm{q}^{\frac{{}^{\mathrm{t}}ana}{\nu}}$$

(on rappelle la relation $d^{-1} = \nu^{-1}\,{}^{\mathrm{t}}a$). Il sera commode de faire agir le groupe $\mathrm{GL}_2(\mathbb{C})$ sur $\mathrm{M}_2(\mathbb{C})$ par $(g,s) \mapsto g \cdot s := g\, s\, {}^{\mathrm{t}}g$.

Corollaire 1.11. *Soient $j,k \in \mathbb{Z}$ tels que $j \geq 0$, $F \in S_{j,k}$, p un nombre premier et $n \in \mathcal{N}$. On a :*

$$\begin{aligned} p^{\frac{j+2k}{2}}\mathrm{a}(n;\mathrm{K}_p F) = \ & p^{j+2k}\ \mathrm{a}(n/p;F) \ + \ p^3\ \mathrm{a}(np;F) \\ & + \ p^{k+1} \sum_{d=0}^{p-1} \rho_j(\begin{bmatrix} p & -d \\ 0 & 1 \end{bmatrix})\ \mathrm{a}(\begin{bmatrix} 1 & d \\ 0 & p \end{bmatrix} \cdot \frac{n}{p};F) \\ & + \ p^{k+1}\ \rho_j(\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix})\ \mathrm{a}(\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \cdot \frac{n}{p};F), \end{aligned}$$

et

$$\begin{aligned} p^{j+2k}\mathrm{a}(n;\mathrm{T}_p F) = \ & p^{j+3k}\ \rho_j(\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix})\ \mathrm{a}(\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \cdot \frac{n}{p^2};F) \\ + \ p^{j+3k} \sum_{a=0}^{p-1} \rho_j(\begin{bmatrix} p & -a \\ 0 & 1 \end{bmatrix})\ & \mathrm{a}(\begin{bmatrix} 1 & a \\ 0 & p \end{bmatrix} \cdot \frac{n}{p^2};F) \ + \ \delta(n,p)\ p^{j+2k}\ \mathrm{a}(n;F) \\ & + \ p^{k+3} \sum_{f=0}^{p-1} \rho_j(\begin{bmatrix} p & -f \\ 0 & 1 \end{bmatrix})\ \mathrm{a}(\begin{bmatrix} 1 & f \\ 0 & p \end{bmatrix} \cdot n;F) \\ & + \ p^{k+3}\ \rho_j(\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix})\ \mathrm{a}(\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \cdot n;F), \end{aligned}$$

où $\delta(n,p) \in \mathbb{Z}$ est défini par la formule (1.5) *ci-dessous ; $\delta(n,p) \equiv -1 \bmod p$.*

Démonstration. D'après le lemme 1.10 et le diagramme IV.5.4, on a

$$\mathrm{K}_p F = \sum_i F_{|W_{j,k}}\gamma_i \ \text{ et } \ \mathrm{T}_p F = \sum_i F_{|W_{j,k}}\gamma'_i.$$

Compte tenu de la convergence uniforme du développement de Fourier de F sur tout compact de $\mathbb{H}_2$, le corollaire est une application directe de la formule

(1.4). On observera que si $a, d \in \mathrm{GL}_2(\mathbb{C})$, $b \in \mathrm{M}_2(\mathbb{C})$, $\nu \in \mathbb{C}^*$ et $m, n \in \mathrm{M}_2(\mathbb{C})$ sont tels que $n = \frac{{}^{\mathrm{t}}ama}{\nu}$ et $d^{-1} = \nu^{-1}\,{}^{\mathrm{t}}a$, alors $m = d \cdot \frac{n}{\nu}$ et $\mathrm{tr}({}^{\mathrm{t}}amb) = \mathrm{tr}(bn\,{}^{\mathrm{t}}d)$.

En guise d'exemple, déterminons la contribution des $p^2 - 1$ éléments γ_i' de la forme

$$\begin{bmatrix} p & 0 & b & c \\ 0 & p & c & d \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix},$$

avec b, c, d comme dans le lemme 1.10 (ii), à la somme définissant $p^{j+2k}\,\mathrm{a}(n, \mathrm{T}_p F)$. Elle s'écrit $p^{j+2k}\,\delta(n,p)\,\mathrm{a}(n;F)$ où

$$\delta(n,p) := \sum_{v \in V - \{0\},\ \text{dét}(v)=0} e^{\frac{2i\pi}{p}\mathrm{tr}(vn)} \tag{1.5}$$

et $V \subset \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ désigne le sous-espace des matrices symétriques. La forme quadratique dét : $V \to \mathbb{Z}/p\mathbb{Z}$ admet $p+1$ droites isotropes. Si a désigne le nombre de ces droites qui sont dans le noyau de la forme linéaire $v \mapsto \mathrm{tr}(vn)$, de sorte que $a \in \{0, 1, 2, p+1\}$, alors $\delta(n,p) = (p-1) \cdot a - (p+1-a) = p(a-1) - 1$. □

Le monoïde $\rho_j(\mathrm{M}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{C}))$ préservant le réseau $\mathrm{Sym}^j\mathbb{Z}^2 \subset W_j$, on en tire le corollaire suivant.

Corollaire 1.12. *Soient j, k des entiers avec $j \geq 0$ et $k \geq 2$. Pour tout nombre premier p, les opérateurs de Hecke $p^{\frac{j+2k-6}{2}}\,\mathrm{K}_p$ et $p^{j+k-3}\,(\mathrm{T}_p + 1)$ préservent le sous-groupe de $\mathrm{S}_{j,k}$ constitué des éléments dont tous les coefficients de Fourier sont à valeurs dans le sous-groupe $\mathrm{Sym}^j\mathbb{Z}^2 \subset W_j$.*

Démonstration de la proposition 1.9. Notons $\mathrm{S}_{j,k}^{\mathrm{ent}} \subset \mathrm{S}_{j,k}$ le sous-groupe défini dans l'énoncé. Le $\mathbb{C}$-espace vectoriel $\mathrm{S}_{j,k}$ étant de dimension finie, il existe une partie finie $N \subset \mathcal{N}$ telle que l'application linéaire

$$F \mapsto (\mathrm{a}(n;F))_{n \in N}, \quad \mathrm{S}_{j,k} \to W_j^N,$$

soit injective. Elle envoit le $\mathbb{Z}$-module $\mathrm{S}_{j,k}^{\mathrm{ent}}$ dans $(\mathrm{Sym}^j\mathbb{Z}^2)^N$. Cela montre d'une part que le $\mathbb{Z}$-module $\mathrm{S}_{j,k}^{\mathrm{ent}}$ est libre de rang fini, et d'autre part que l'application naturelle $\eta : \mathrm{S}_{j,k}^{\mathrm{ent}} \otimes_{\mathbb{Z}} \mathbb{C} \to \mathrm{S}_{j,k}$ est injective, puisque c'est le cas de l'application naturelle $\mathrm{Sym}^j\mathbb{Z}^2 \otimes \mathbb{C} \to W_j$.

Il est plausible qu'en toute généralité l'application η soit bijective, mais nous n'avons pas trouvé de référence sur ce point. Démontrons-le lorsque

(j,k) est dans la liste de l'énoncé de la proposition 1.9. Dans ce cas, $\mathrm{S}_{j,k}$ est de dimension 1, de sorte qu'il suffit de vérifier que $\mathrm{S}_{j,k}^{\mathrm{ent}}$ est non nul. Considérons pour cela la forme modulaire $f_{j,k,u,v,w} = \vartheta_2(\mathrm{E}_8, \mathrm{P}_{j,k,u,v,w})$ dans $\mathrm{S}_{j,k}$ que nous avons construite au §1.1. Elle a ses coefficients dans $\mathbb{Z}[i][X,Y]$, où $\mathbb{Z}[i]$ désigne l'anneau des entiers de Gauss, puisque le polynôme harmonique $\mathrm{P}_{j,k,u,v,w}$ envoie E_8^2 dans $\mathbb{Z}[i][X,Y]$; les quelques coefficients de Fourier non nuls de $f_{j,k,u,v,w}$ que nous avons déterminés sont même dans $\mathbb{Z}$ (Table C.2). On observe que pour tout $n \in \mathcal{N}$, on a $\overline{\mathrm{a}(n; f_{j,k,u,v,w})} = \mathrm{a}(n; f_{j,k,\overline{u},\overline{v},\overline{w}})$, $z \mapsto \overline{z}$ désignant respectivement la conjugaison complexe sur $\mathbb{C}[X,Y]$ et sur $\mathrm{E}_8 \otimes \mathbb{C}$. Ainsi, $f_{j,k,u,v,w} + f_{j,k,\overline{u},\overline{v},\overline{w}}$ est un élément non nul de $\mathrm{S}_{j,k}^{\mathrm{ent}}$.

Pour terminer la démonstration de la proposition 1.9 , il suffit d'appliquer la proposition 1.8 et le corollaire 1.12. □

Soient $n = \begin{bmatrix} n_{11} & \frac{n_{12}}{2} \\ \frac{n_{12}}{2} & n_{22} \end{bmatrix} \in \mathcal{N}$ et p premier. On constate les identités

$$\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \cdot \frac{n}{p} = \begin{bmatrix} pn_{11} & \frac{n_{12}}{2} \\ \frac{n_{12}}{2} & n_{22}/p \end{bmatrix},$$

$$\begin{bmatrix} 1 & d \\ 0 & p \end{bmatrix} \cdot \frac{n}{p} = \begin{bmatrix} \frac{n_{11}+dn_{12}+d^2n_{22}}{p} & \frac{n_{12}}{2} + dn_{22} \\ \frac{n_{12}}{2} + dn_{22} & pn_{22} \end{bmatrix}.$$

Ainsi, si la forme quadratique sur $\mathbb{Z}^2$ définie par n est anisotrope modulo le nombre premier p, alors ni n/p, ni l'une des deux matrices ci-dessus n'est dans $\mathcal{N}$. La proposition 1.11 admet donc la conséquence suivante.

Scholie 1.13. *Supposons que $F \in \mathrm{S}_{j,k}$ est vecteur propre de l'opérateur $\mathrm{p}^{\frac{j+2k}{2}-3}\mathrm{K}_p$ de valeur propre λ. Si $n \in \mathcal{N}$ et $2n$ est une matrice de Gram d'une forme quadratique sur $\mathbb{Z}^2$ qui est anisotrope modulo le nombre premier p, on a la relation $\lambda\ \mathrm{a}(n;F) = \mathrm{a}(pn;F)$. En particulier, cette relation détermine λ si $\mathrm{a}(n;F) \neq 0$.*

Ce scholie s'applique par exemple lorsque

$$2\,n = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix},$$

qui n'est autre que la matrice de Gram standard du réseau A_2, lorsque $\mathrm{A}_2 \otimes \mathbb{F}_p$ ne représente pas 0, *i.e.* $p \equiv -1 \bmod 3$. On déduit donc de la table C.2 le corollaire suivant.

Corollaire 1.14. *Les entiers $\tau_{6,8}(2)$, $\tau_{4,10}(2)$, $\tau_{8,8}(2)$ et $\tau_{12,6}(2)$ valent respectivement $0, -1680, 1344$ et -240.*

Remarque 1.15. Supposons que $F \in \mathrm{S}_{j,k}$ est vecteur propre de l'opérateur $2^{j+2k-5}(\mathrm{T}_2+1)+2^{j+2k-3}$ de valeur propre λ et posons

$$n = \frac{1}{2}\begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix} \quad \text{et} \quad m = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}.$$

Nous laissons au lecteur le soin de déduire du corollaire 1.11 la relation

$$(\lambda - 2^{j+2\,k-4})\ \mathrm{a}(n;F) = 2^{k-2}\left(\rho_j(\begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix}) + \rho_j(\begin{bmatrix} -1 & 1 \\ 2 & 0 \end{bmatrix}) + \rho_j(\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix})\right)\ \mathrm{a}(m;F).$$

(Vérifier en particulier $\delta(n,2) = -3$). En utilisant les valeurs de la table C.2, cette formule permet de démontrer que les entiers $\tau_{6,8}(4)$, $\tau_{4,10}(4)$, $\tau_{8,8}(4)$ et $\tau_{12,6}(4)$ valent respectivement 409600, -700160, 348160 et 4276480.

Il se trouve que les valeurs propres des $F_{j,k}$ ont été étudiées par Faber et van der Geer [FvDG04][vDG08, §24] de manière complètement différente, en comptant *à la Deligne* des courbes de genre 2 sur des corps fini. Si q désigne une puissance d'un nombre premier, ils ont pu ainsi déterminer $\tau_{j,k}(q)$ pour tout $q \leq 37$ (en admettant toutefois une propriété attendue de la cohomologie de certains faisceaux sur l'espace de Siegel de genre 2 [vDG08, §24]) ; ils donnent *loc. cit.* un certain nombre de valeurs, y compris la valeur $\tau_{j,k}(2)$ ci-dessus. Nous exposerons un peu plus loin une méthode très différente permettant de déterminer $\tau_{j,k}(q)$, qui nous permettra de démontrer le théorème suivant.

Théorème* **1.16.** *Soient p un nombre premier et (j,k) l'un des couples $(6,8)$, $(4,10)$, $(8,8)$ ou $(12,6)$.*

(i) Si $p \leq 113$, l'entier $\tau_{j,k}(p)$ est donné par la table C.3.

(ii) Si $p \leq 29$, l'entier $\tau_{j,k}(p^2)$ est donné par la table C.4.

Signalons enfin que dans un travail récent [CvDG14, §8], Cléry et van der Geer ont ré-obtenu les valeurs $\tau_{6,8}(q)$ pour $q \leq 49$ par une méthode encore différente.

1.17. Où l'on explique l'apparition des $\psi_{j,k}$ dans la table VII.1.

Fixons l'un des quatres couples (j,k) de la table IX.1 tel que $j > 0$. Soit $U'_{j,k}$ la représentation irréductible de $\mathrm{SO}_8(\mathbb{C})$ de plus haut poids $(\frac{j}{2}+k-4)(\varepsilon_1+\varepsilon_2)+\frac{j}{2}(\varepsilon_3+\varepsilon_4)$ (§VI.4.3), elle se factorise par $\mathrm{PGSO}_8(\mathbb{C})$. On dispose alors d'isomorphismes naturels

$$\mathrm{M}_{U'_{j,k}}(\mathrm{SO}_8) \xleftarrow{\sim} \mathrm{M}_{U'_{j,k}}(\mathrm{PGSO}_8) \xrightarrow{\sim} \mathrm{M}_{U_{j,k}}(\mathrm{PGSO}_8) \xrightarrow{\sim} \mathrm{M}_{U_{j,k}}(\mathrm{SO}_8) \xleftarrow{\sim} \mathrm{M}_{U_{j,k}}(\mathrm{O}_8) \xrightarrow{\sim} \mathrm{S}_{j,k}.$$

En effet, le premier et le troisième sont généraux (variante du lemme V.4.8 basée sur la proposition IV.1.4). Le dernier isomorphisme est celui de la proposition 1.2. L'avant dernier morphisme est injectif pour des raisons générales (§IV.4.4), bijectif car $\dim \mathrm{M}_{U_{j,k}}(\mathrm{SO}_8) = 1$ d'après [CR12, Table 2]. Celui du milieu est induit par la trialité. En effet, par un calcul laissé au lecteur, basé sur l'action bien connue de la trialité sur le diagramme de Dynkin de type $\mathbf{D}_4$, on observe que si une $\mathbb{C}$-représentation irréductible de $\mathrm{PGSO}_8(\mathbb{C})$ admet pour plus haut poids $\sum_{i=1}^4 n_i\varepsilon_i$, alors ses deux représentations triales ont pour plus haut poids $\sum_{i=1}^4 m_i\varepsilon_i$ où $(m_1, m_2, m_3, \pm m_4)$ vaut

$$(\frac{n_1+n_2+n_3+n_4}{2}, \frac{n_1+n_2-n_3-n_4}{2}, \frac{n_1-n_2+n_3-n_4}{2}, |\frac{n_1-n_2-n_3+n_4}{2}|).$$

L'apparition des $\psi_{j,k}$ dans la table VII.1 est donc conséquence de la suite d'isomorphismes ci-dessus et du théorème VII.2.3 (i).

Mentionnons enfin que ce paragraphe suggère une méthode alternative pour déterminer les $\tau_{j,k}(q)$, basée sur un calcul de valeurs propres d'opérateurs de Hecke pour O_8. Nous renvoyons au travail à venir de Mégarbané [Meg] à ce sujet.

2. $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ et la conjecture de Nebe-Venkov

2.1. Une caractérisation de la table I.2

Considérons le sous-ensemble suivant de $\coprod_{n\geq 1} \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$:

$$\Pi = \{1, \Delta_{11}, \Delta_{15}, \Delta_{17}, \Delta_{19}, \Delta_{21}, \mathrm{Sym}^2\Delta_{11}, \Delta_{19,7}, \Delta_{21,5}, \Delta_{21,9}, \Delta_{21,13}\}.$$

La proposition ci-dessus donne une "définition" directe de la table I.2.

Proposition* **2.2.** *L'ensemble des $\psi \in \mathcal{X}(\mathrm{SL}_{24})$ tels que :*

(i) ψ_∞ admet pour valeurs propres simples les entiers $\pm 11, \pm 10, \ldots, \pm 1$, ainsi que 0 pour valeur propre double,

(ii) ψ est de la forme $\oplus_{i=1}^k \pi_i[d_i]$ avec $\pi_i \in \Pi$ pour tout i,

est exactement celui donné par la table I.2. Il a 24 éléments.

Démonstration. C'est un simple exercice de combinatoire que l'on peut traiter de la manière suivante. Considérons plus généralement, pour tout entier $n \geq 1$, l'ensemble Ψ_n des éléments $\psi \in \mathcal{X}(\mathrm{SL}_n)$ verifiant l'assertion (ii) de l'énoncé et tels que :

– ψ_∞ admet pour valeurs propres simples les entiers $\pm\frac{n-1}{2}, \pm\frac{n-3}{2}, \ldots, \pm 1$ et 0 si n est impair,

– ψ_∞ admet pour valeurs propres simples les entiers $\pm\frac{n-2}{2}, \pm\frac{n-4}{2}, \ldots, \pm 1$, ainsi que 0 pour valeur propre double, si n est pair.

La question est de déterminer Ψ_{24}. Nous allons plus généralement expliciter Ψ_n pour tout $1 \leq n \leq 24$ par récurrence sur n. Pour $c \in \mathcal{X}(\mathrm{SL}_a)$ et $\Psi \subset \mathcal{X}(\mathrm{SL}_b)$ il sera commode de noter $c \oplus \Psi$ l'ensemble des éléments de $\mathcal{X}(\mathrm{SL}_{a+b})$ de la forme $c \oplus \psi$ avec $\psi \in \Psi$.

Soient $1 \leq n \leq 24$ un entier pair et $\psi \in \Psi_n$. Écrivons $\psi = \oplus_{i=1}^k \pi_i[d_i]$ comme dans l'assertion (ii). L'inégalité $n \leq 24$ entraîne que pour tout i, les valeurs propres de $(\pi_i[d_i])_\infty$ sont ≤ 11. Fixons un entier i tel que $(\pi_i[d_i])_\infty$ admette la valeur propre 0. Le lemme 2.3 montre que l'on est dans l'un des cas suivants :

– $\pi_i = 1$,

– $\pi_i = \Delta_{11}$, $d_i = 12$, $n = 24$ et donc $\psi = \Delta_{11}[12]$,

– Si $\pi_i = \mathrm{Sym}^2\Delta_{11}$, $d_i = 1$ et $n = 24$.

En particulier, on constate que sous l'hypothèse $n \leq 22$, il existe deux entiers i tels que $\pi_i = 1$, un et un seul d'entre eux vérifiant de plus $d_i = 1$. On a donc l'égalité $\Psi_n = [1] \oplus \Psi_{n-1}$ pour n pair ≤ 22. De plus, cette analyse montre

$$\Psi_{24} \;=\; \{\ \Delta_{11}[12]\ \} \;\cup\; [1] \oplus \Psi_{23} \;\cup\; \mathrm{Sym}^2\Delta_{11} \oplus \Psi_{21}.$$

Il ne reste qu'à décrire Ψ_n pour n impair ≤ 23. Les éléments non triviaux de Π étant de poids motivique ≥ 11, on a évidemment $\Psi_n = \{\ [n]\ \}$ pour tout entier $1 \leq n \leq 11$ impair. La seule représentation dans Π de poids motivique < 15 étant Δ_{11}, on a de plus

$$\Psi_{13} \;=\; \{\ [13],\ \Delta_{11}[2] \oplus [9]\ \} \quad \text{et} \quad \Psi_{15} \;=\; \{\ [15],\ \Delta_{11}[4] \oplus [7]\ \},$$

On constate de même les assertions suivantes :

– Ψ_{17} est réunion de $\{\ [17],\ \Delta_{11}[6] \oplus [5]\ \}$ et $\Delta_{15}[2] \oplus \Psi_{13}$,

– Ψ_{19} est réunion de $\{\ [19],\ \Delta_{11}[8] \oplus [3],\ \Delta_{15}[4] \oplus [11]\ \}$ et $\Delta_{17}[2] \oplus \Psi_{15}$,

– Ψ_{21} est réunion des ensembles $\Delta_{17}[4] \oplus \Psi_{13}$, $\Delta_{19}[2] \oplus \Psi_{17}$, et

$$\{\ [21],\ \Delta_{11}[10] \oplus [1],\ \Delta_{15}[6] \oplus [9],\ \Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [5]\ \},$$

– Ψ_{23} est réunion de $\{\ [23],\ \Delta_{15}[8] \oplus [7],\ \Delta_{17}[6] \oplus [11],\ \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10]\ \}$, $\Delta_{19}[4] \oplus \Psi_{15}$, $\Delta_{21}[2] \oplus \Psi_{19}$, et de l'ensemble :

$$\{\Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [3],\ \Delta_{21,9}[2] \oplus \Delta_{15}[4] \oplus [7],\ \Delta_{21,13} \oplus \Delta_{17}[2] \oplus [11]\ \}.$$

Cette analyse montre au final que l'ensemble Ψ_{24} est l'ensemble des 24 éléments de la table I.2. Une manière de justifier que ces 24 éléments sont distincts consiste à invoquer la proposition VI.4.5 (Théorème de Jacquet-Shalika). On observera que l'intersection de $[1] \oplus \Psi_{23}$ et $\mathrm{Sym}^2\Delta_{11} \oplus \Psi_{21}$ est le singleton $\{\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10] \oplus [1]\}$. Plus généralement, la table IX.2 indique le cardinal de Ψ_n en fonction de $n \leq 24$. (Une autre méthode pour justifier que les 24 éléments de la table I.2 sont distincts, sur laquelle nous reviendrons au §2.4, consisterait à observer que les composantes en le nombre premier 2 de ces éléments ont des traces distinctes.) □

n	≤ 12	13	14	15	16	17	18	19	20	21	22	23	24
$\lvert\Psi_n\rvert$	1	2	2	2	2	4	4	5	5	10	10	14	24

TABLE IX.2 – Cardinal du sous-ensemble $\Psi_n \subset \mathcal{X}(\mathrm{SL}_n)$ introduit dans la démonstration de la proposition 2.2.

Lemme 2.3. *Soient $\pi \in \Pi - \{1\}$, d un entier ≥ 1, $\psi = \pi[d]$ et $\Lambda \subset \mathbb{C}$ l'ensemble des valeurs propres de ψ_∞. On suppose $\Lambda \subset \mathbb{Z}$ et $|\lambda| \leq 11$ pour tout $\lambda \in \Lambda$. Alors on a*

$$|\lambda| \geq \frac{d-1}{2}$$

pour tout $\lambda \in \mathrm{Poids}(\pi)$. De plus, les assertions suivantes sont satisfaites :

(i) Si $0 \in \Lambda$, alors on a $\pi = \mathrm{Sym}^2\Delta_{11}$ et $d = 1$, ou $\pi = \Delta_{11}$ et $d = 12$.

(ii) Si $1 \in \Lambda$, alors on a $\pi = \Delta_{11}$ et $d \in \{10, 12\}$.

Démonstration. Il s'agit d'une inspection immédiate de la liste Π. □

2.4. Énoncés et survol des démonstrations

Soit ψ l'un des 24 éléments listés dans la table I.2. D'après la proposition 2.2 et les exemples du §VI.4.3, on a $\psi_\infty = \mathrm{St}(\mathrm{inf}_V)$, où V est la représentation triviale de $\mathrm{SO}_{24}(\mathbb{R})$. L'ensemble Π étant constitué de représentations autoduales, l'énoncé suivant (qui est aussi le théorème I.E) n'est pas absurde !

Théorème* **2.5.** *Les* 24 *représentations* $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ *telles que* $\pi_\infty = 1$ *ont pour paramètres standards* $\psi(\pi, \mathrm{St})$ *les* 24 *éléments de la table I.2.*

Soulignons que dans son travail [IKE06] (reposant notamment sur [BFW98], [IKE01] et [NV01]), Ikeda était parvenu à identifier 20 de ces 24 paramètres, à savoir tous ceux de cette liste ne "contenant pas" l'une des 4 représentations $\Delta_{w,v}$.

Afin d'en dire un peu plus, rappelons quelques notations introduites au §V.3. On note λ_i, $i = 1, \ldots, 24$, les 24 valeurs propres distinctes de l'opérateur T_2 agissant sur $\mathbb{C}[\mathrm{X}_{24}]$, rangées par ordre décroissant à la manière de Nebe et Venkov (Table (V.1)). Fixons $\mathrm{v}_i \in \mathbb{Z}[\mathrm{X}_{24}]$ un vecteur propre de T_2, et donc de $\mathrm{H}(\mathrm{O}_{24})$, associé à λ_i. On note $\pi_i \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ la représentation engendrée par v_i et

$$\psi_i = \psi(\pi_i, \mathrm{St})$$

son paramètre standard. Le théorème 2.5 affirme que ces 24 paramètres ψ_i sont ceux de la table I.2. Étant donné que les 24 valeurs propres de T_2 sont différentes, la relation

$$\lambda_i \;=\; 2^{11}\,\mathrm{trace}\;(\psi_i)_2 \;=\; 2^{11}\,\mathrm{trace}\,\mathrm{St}\,\mathrm{c}_2(\pi_i)$$

caractérise uniquement l'application $i \mapsto \psi_i$. Cela fournit par ailleurs une première vérification du théorème 2.5 car on peut montrer que les 4 valeurs $\tau_{j,k}(2)$ (Corollaire 1.14, [VDG08, §24, §27]), ainsi que les coefficients $\tau_k(2)$ en q^2 des formes modulaires normalisées pour $\mathrm{SL}_2(\mathbb{Z})$ de poids $k \leq 22$, sont compatibles avec le calcul des λ_i par Nebe et Venkov.

En guise d'exemple considérons le paramètre

$$\psi = \Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [3].$$

On a $\tau_{4,10}(2) = -1680$, $\tau_{12}(2) = -24$ et $\tau_{18}(2) = -528$, de sorte que

$$2^{11}\,\mathrm{trace}(\mathrm{St}(\psi_2)) = (1+2)\cdot(-1680) + 2^2\cdot(1+2)\cdot(-528)$$

$$+2^4\cdot(1+2+2^2+2^3)\cdot(-24) + 2^{11} + 2^{10}\cdot(1+2+2^2) = -7920.$$

On retrouve bien la valeur propre λ_{21} de Nebe-Venkov, *i.e.* $\psi = \psi_{21}$.

On note enfin g_i le degré de v_i, défini au §V.3 : la valeur propre λ_i ayant multiplicité 1, c'est le plus petit entier g tel que π_i admette un ϑ-correspondant dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ au sens du §VII.1.1. Par convention on a $g_1 = 0$. Comme nous l'avons déjà expliqué au §V.3, les g_i ont été déterminés par Nebe et Venkov pour $i \neq 19, 21$ dans [NV01] ; ils ont de plus conjecturé $g_{19} = 9$ et $g_{21} = 10$.

Théorème* **2.6.** *(i) Les g_i sont donnés par la table C.5. En particulier, la conjecture de Nebe-Venkov* [NV01, §3.3] *est vraie.*

(ii) Pour tout $i \leq 23$, g_i est le plus petit entier $m \geq 0$ tel que ψ_i soit de la forme $[23-2m] \oplus \psi_i'$ avec $\psi_i' \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2m+1})$. Enfin, on a $g_{24} = 12$.

On prendra garde que dans notre table C.5, les degrés g_i sont rangés par ordre croissant, mais pas tout à fait les indices i. Nous allons d'abord démontrer au §2.8 que le théorème 2.5 entraîne le théorème 2.6. Nous donnerons ensuite trois démonstrations du théorème 2.5, les deux premières étant conditionnelles :

– La première, sans doute la plus naturelle, est une application directe de la fomule de multiplicité d'Arthur pour SO_{24}. Son inconvénient évident est qu'elle dépend de l'établissement de la formule de multiplicité d'Arthur pour les $\mathbb{Z}$-groupes SO_n, non encore rédigé, ainsi que de l'analogue à ces groupes de la conjecture VIII.4.22, que nous avons englobés en une seule conjecture VIII.4.25 au chapitre précédent. Cette démonstration conditionnelle est expliquée au §2.10.

– Nous donnerons ensuite au §2.11 une seconde démonstration conditionnelle, n'utilisant cette fois-ci que la théorie d'Arthur pour les groupes de Chevalley, la conjecture VIII.4.22, et des arguments de "correspondance ϑ". Dans cette seconde approche, nous démontrerons en fait en même temps les deux théorèmes ci-dessus.

– Nous donnerons enfin une dernière démonstration du théorème 2.5, cette fois-ci inconditionnelle, au §4.3. Cette démonstration, assez différente dans l'esprit et déjà discutée dans l'introduction, ne reposera plus du tout sur la formule de multiplicité d'Arthur. Elle fournira une justification plus profonde de l'énoncé du théorème 2.5.

Remarque 2.7. (i) Curieusement, l'opérateur de Hecke T_3 sur $\mathbb{C}[\mathrm{X}_{24}]$ admet la valeur propre 1827360 avec multiplicité 2. Cela traduit l'égalité un peu miraculeuse des traces des composantes en $p = 3$ des paramètres $\psi_{19} = \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [5]$ et $\psi_{21} = \Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [3]$, comme on le vérifie à l'aide la table C.3.

(ii) L'opérateur de Hecke T_2 agissant sur $\mathbb{C}[\mathrm{X}_{32}]$ admet des valeurs propres non entières. En effet, soit Δ_{23} l'une des deux formes propres normalisées de poids 24 pour $\mathrm{SL}_2(\mathbb{Z})$. Il est bien connu que ses coefficients de Fourier sont dans $\mathbb{Q}(\sqrt{144169})$, par exemple le second vaut $540 \pm 12\sqrt{144169}$. On conclut car d'après Ikeda et Böcherer (§VII.3), il existe $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{32})$ telle que $\psi(\pi, \mathrm{St}) = \Delta_{23}[8] \oplus [15] \oplus [1]$.

2.8. Le théorème 2.5 entraîne le théorème 2.6.

Nous allons déduire de la liste des ψ_i dans la table C.5 la valeur des g_i.

Lemme 2.9. *On a les inégalités $g_{23} \leq 11$ et $g_i \leq 10$ pour $i \leq 22$, ainsi que l'égalité $g_{24} = 12$.*

Démonstration. En effet, ainsi qu'on l'a rappelé au §V.3, Erokhin a montré $g_i \leq 12$ pour tout i dans [Ero79]. Ce résultat a été ré-obtenu par Borcherds, Freitag et Weissauer dans [BFW98], qui ont vérifié de plus l'inégalité $g_i \leq 11$ pour tout i sauf pour exactement l'un d'entre eux (c'est l'assertion que $\operatorname{Ker} \vartheta_{11}$ est de dimension 1). Ils calculent pour cela explicitement les coefficients des séries thêta des réseaux de Niemeier en les matrices de Gram des réseaux de la forme $\mathrm{Q}(R)$ où R est un système de racines irréductible de type ADE et de rang ≤ 12 [BFW98, Table p. 146]. Comme l'ont observé Nebe et Venkov [NV01, §3.1, Lemma 3.3], ces calculs montrent plus exactement les inégalités $g_{23} \leq 11$, $g_i \leq 10$ pour tout $i \leq 22$, et $g_{24} = 12$ (au moins l'un des g_i doit être égal à 12 d'après le résultat de [BFW98] sus-mentionné). □

Démonstration. (Le théorème 2.5 entraîne le théorème 2.6) Soit $1 \leq i \leq 23$ et soit $\psi_i' \in \mathcal{X}(\mathrm{SL}_{2g_i+1})$ le paramètre standard du ϑ-correspondant dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g_i})$ de π_i. D'après le lemme 2.9 on a $g_i \leq 11$, de sorte que d'après Rallis (corollaire VII.1.3) on a l'identité

$$\psi_i = \psi_i' \oplus [23 - 2g_i].$$

D'après le théorème VIII.1.1 d'Arthur, on a $\psi_i' \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g_i+1})$. L'unicité des paramètres d'Arthur-Langlands (Jacquet-Shalika, Proposition V.4.5) montre donc que g_i a la propriété que $[23 - 2g_i]$ est un "constituant" de ψ_i dans la table C.5.

Si $i \leq 22$, le lemme 2.9 entraîne $g_i \leq 10$, soit encore $23 - 2g_i \geq 3$. Dans ce cas, $23 - 2g_i$ est l'unique entier $m_i > 1$ tel que $[m_i]$ est un constituant de ψ_i, l'autre constituant éventuel de ψ_i de la forme $[d]$ étant $[1]$. Cela détermine trivialement g_i pour $i \leq 22$ par inspection directe de la table C.5. L'inégalité $g_{23} \leq 11$ et l'identité $\psi_{23} = \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10] \oplus [1]$ montrent de même que l'on a nécessairement $g_{23} = 11$. Cela termine la démonstration. □

Observons que l'approche utilisée ici ne repose pas sur les calculs fins des §3.3 et §3.4 de [NV01], mais "seulement" de la table [BFW98, p. 146] de Borcherds-Freitag-Weissauer et du calcul de T_2 par Nebe et Venkov.

2.10. Première démonstration, conditionnelle, du théorème 2.5

Admettons la conjecture VIII.4.25 et appliquons le théorème VIII.5.8 à chaque paramètre ψ de la table I.2 (on est dans ses hypothèses avec $\psi_\infty = \mathrm{St}(\mathrm{Inf}_1)$). Nous affirmons que l'égalité VIII.(5.1) est toujours satisfaite, ce qui est un phénomène en soit assez miraculeux. C'est bien entendu quelque chose que l'on peut simplement vérifier bêtement dans chacun des 24 cas. On peut aussi faire les remarques suivantes :

(a) Si ψ ne contient pas $\mathrm{Sym}^2\Delta_{11}$, et $\psi \neq \Delta_{11}[12]$, alors ψ satisfait l'hypothèse du critère VIII.5.10, c'est-à-dire qu'il est de la forme

$$(\oplus_{i=1}^{k-2}\pi_i[d_i]) \oplus [d_{k-1}] \oplus [1]$$

avec π_i est symplectique pour tout $i \leq k-2$. Une rapide inspection montre que l'on a toujours soit $d_i < d_{k-1}$ et $\varepsilon(\pi_i) = (-1)^{\frac{n_i d_i}{4}}$, soit $d_i > d_{k-1}$ et $d_i \equiv 0 \bmod 4$ (ce qui ne se produit que pour ψ_{13}, ψ_{21} et ψ_{22}). Concrètement, on observe que le facteur epsilon $\varepsilon(\Delta_{j,k}) = (-1)^k$ vaut 1 pour les 4 couples (j,k) d'intérêt, et que chaque fois qu'un constituant de la forme $\Delta_w[d]$ apparaît dans ψ alors on a $d \equiv w+1 \bmod 4$. On conclut donc par le critère VIII.5.10.

(b) Si ψ contient $\mathrm{Sym}^2\Delta_{11}$, alors ψ est de la forme

$$(\oplus_{i=1}^{k-2}\pi_i[d_i]) \oplus \mathrm{Sym}^2\Delta_{11} \oplus [1]$$

avec π_i symplectique pour tout $i \leq k-2$; il satisfait donc l'hypothèse du critère VIII.5.11. On conclut encore par ce critère en observant que l'on a toujours soit $d_i < d_{k-1}$ et $\varepsilon(\pi_i)(-1)^{\frac{n_i}{2}} = (-1)^{\frac{n_i d_i}{4}}$, soit $d_i > d_{k-1}$ et $d_i \equiv 2 \bmod 4$ (ce qui ne se produit que pour ψ_{20} et ψ_{23}).

Ainsi, pour tout $i \leq 23$ l'unique représentation $\pi'_i \in \Pi(\mathrm{SO}_{24})$ telle que $\psi(\pi'_i, \mathrm{St}) = \psi_i$ satisfait $\mathrm{m}(\pi'_i) = 1$. Enfin, si l'on a $\psi = \psi_{20} = \Delta_{11}[12]$ l'égalité VIII.(5.1) est trivialement satisfaite, et la remarque VIII.5.9 assure qu'il existe exactement deux représentations $\pi'_{24}, \pi''_{24} = \mathrm{S}(\pi'_{24}) \in \Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ de paramètre standard ψ_{24}, et que de plus $\mathrm{m}(\pi'_{24}) = \mathrm{m}(\pi''_{24}) = 1$.

Cette discussion nous fournit 25 éléments distincts de $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$, chacun étant de multiplicité 1. Comme $\mathrm{h}(\mathrm{SO}_{24}) = |\widetilde{\mathrm{X}}_{24}| = 25$ (Corollaire IV.1.9), ce sont exactement les $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ telles que $\pi_\infty = 1$. La décomposition $\mathrm{H}(\mathrm{O}_{24})$-équivariante (§IV.4.4)

$$\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24}) = \mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24}) \oplus \mathrm{M}_{\text{dét}}(\mathrm{O}_{24}),$$

combinée au fait que T_2 a 24 valeurs propres distinctes sur $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24})$, montre que les 24 représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telles que $\pi_\infty = 1$ ont exactement pour paramètres standards les ψ_i de la table I.2, et aussi que l'unique représentation $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\pi_\infty = \text{dét}$ a pour paramètre $\Delta_{11}[12]$ (autrement dit, on retrouve également la proposition VII.5.1 !).

2.11. Deuxième démonstration du théorème 2.5, modulo la conjecture VIII.4.22

Donnons maintenant une démonstration "moins conditionnelle" du théroème 2.5, qui se passe de la conjecture VIII.4.25, et repose seulement sur la conjecture VIII.4.22. Commençons par deux observations.

Observation 1. Soit $1 \leq g < 12$ et considérons l'application du §V.1

$$\vartheta_g : \mathbb{C}[\mathrm{X}_{24}] \longrightarrow \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z})).$$

Supposons que $F \in \mathrm{S}_{12}(\mathrm{Sp}_{2g})$ est propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$ et notons $\pi_F \in \Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ la représentation engendrée. D'après le théorème VIII.1.1 d'Arthur, on peut écrire

$$\psi(\pi_F, \mathrm{St}) = \oplus_{j=1}^k \pi_j[d_j] \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1}).$$

D'après Böcherer, F est dans l'image de ϑ_g si, et seulement si, on a $\mathrm{L}(12-g, \pi_F, \mathrm{St}) \neq 0$ (Remarque VII.2.4). D'après la proposition VIII.6.2, on a $\mathrm{L}(12-g, \pi_F, \mathrm{St}) \neq 0$ si, et seulement si,

$$(2.1) \quad \forall\ 1 \leq j \leq k \text{ tel que } d_j \equiv 0 \bmod 2 \text{ et } d_j > 23 - 2g,\ \ \mathrm{L}(\frac{1}{2}, \pi_j) \neq 0.$$

Si cette condition est satisfaite, la représentation π_F admet donc un ϑ-correspondant π'_F dans $\Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ tel que $(\pi'_F)_\infty = 1$, et

$$\psi(\pi'_F, \mathrm{St}) = \psi(\pi_F, \mathrm{St}) \oplus [23 - 2g]$$

d'après Rallis (Corollaire VII.1.3).

Observation 2. Regardons la table C.5. On constate que pour tout $2 \leq i \leq 23$, il existe un unique $\psi'_i \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g_i+1})$ tel que l'on ait

$$\psi_i = \psi'_i \oplus [23 - 2g_i].$$

Clairement, $(\psi'_i)_\infty$ admet pour valeurs propres les $2g_i+1$ entiers $\pm 11, \pm 10, \ldots,$ $\pm\,(12 - g_i)$ ainsi que 0. Soit $\varpi_i \in \Pi(\mathrm{Sp}_{2g_i})$ l'unique représentation telle que $\psi(\varpi_i, \mathrm{St}) = \psi'_i$ et telle que $(\varpi_i)_\infty \simeq \pi'_{\text{dét}^{12}}$ (la série discrète holomorphe introduite au §VI.3.4). Comme nous l'avons déjà expliqué à plusieurs reprises, la

multiplicité $\mathrm{m}(\varpi_i)$ est non nulle si, et seulement si, il existe une forme propre $F_i \in \mathrm{S}_{12}(\mathrm{Sp}_{2g_i}(\mathbb{Z}))$ telle que $\pi_{F_i} \simeq \varpi_i$ (Corollaire VI.3.7).

Ces deux observations suggèrent la stratégie optimiste suivante pour démontrer le théorème 2.5.

1. Montrer $\mathrm{m}(\varpi_i) \neq 0$ pour tout $2 \leq i \leq 23$.
2. Vérifier, par le critère de Böcherer (2.1), pour tout $1 \leq i \leq 23$, que s'il existe une forme propre $F_i \in \mathrm{S}_{12}(\mathrm{Sp}_{2g_i}(\mathbb{Z}))$ telle que $\pi_{F_i} \simeq \varpi_i$, alors $F_i \in \mathrm{Im}(\vartheta_{g_i})$.

En effet, ceci étant fait, nous en déduisons pour tout $2 \leq i \leq 23$ l'existence d'une représentation dans $\Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ de composante archimédienne triviale et dont le paramètre standard est ψ_i, à savoir un ϑ-correspondant de ϖ_i. L'existence d'une représentation dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ de paramètre standard $\psi_1 = [23] \oplus [1]$ est évidente : la représentation triviale convient (Exemples VI.4.7). Enfin, l'existence d'une représentation dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ de paramètre standard $\psi_{24} = \Delta_{11}[12]$ a déjà été démontrée dans le corollaire VII.3.4 (travaux d'Ikeda et Böcherer).

Vérification du point 2. On constate par inspection des ψ_i' qu'il n'y a rien à vérifier, car aucun entier j ne vérifie $d_j \equiv 0 \bmod 2$ et $d_j > 23 - 2g_i$ (Critère (2.1)), à moins que $i \in \{13, 20, 21, 22, 23\}$ auquel cas le critère s'écrit simplement $\mathrm{L}(\frac{1}{2}, \Delta_{15}) \neq 0$ pour $i = 13$, $\mathrm{L}(\frac{1}{2}, \Delta_{11}) \neq 0$ pour $i \geq 20$. On conclut car ces deux valeurs de fonctions L sont bien non nulles d'après la remarque VII.3.3.

Vérification conjecturale du point 1. La valeur de $\mathrm{m}(\varpi_i)$ est bien entendu déterminée par le théorème VIII.5.2. Pour appliquer ce théorème, il faut savoir d'une part que le morphisme ν_∞ satisfait la conjecture 4.22, et d'autre part vérifier les condition (a) et (b) de son énoncé. La condition (a) est clairement toujours satisfaite, par inspection des ψ_i'. En ce qui concerne la condition (b), nous affirmons qu'elle est également toujours satisfaite. C'est un miracle du même acabit que celui rencontré au §2.10, et que nous pourrions vérifier de la même manière (ou au cas par cas !). Ce n'est en fait pas nécessaire, car d'après la proposition VIII.6.1 (plus exactement d'après la démonstration de cette proposition), cette vérification se déduit formellement de celle effectuée au §2.10 si l'on vérifie que pour tout constituant de ψ_i' de la forme $\pi[d]$ avec $d \equiv 0 \bmod 2$ et $d > 23 - 2g_i$, on a $\varepsilon(\pi) = 1$. Or une inspection immédiate de la table C.5 montre qu'un tel constituant existe uniquement pour les paramètres d'indice $i \in \{13, 20, 21, 22, 23\}$ et que dans tous les cas $\pi = \Delta_{11}$ ou Δ_{15}, de sorte que l'on a bien $\varepsilon(\pi) = 1$. Le fait que l'on retrouve exactement les exceptions que nous avons dû considérer dans la vérification du point 2

n'est bien sûr pas un hasard, comme nous l'avons expliqué au §VIII.6. Ainsi, si pour un i donné nous savons que la conjecture 4.22 vaut pour le ν_∞ associé à ψ_i', on en déduit $\mathrm{m}(\varpi_i) = 1$. $\square$

Remarque 2.12. Hormis le cas $i = 2$ où $\psi_i' = \mathrm{Sym}^2\Delta_{11}$ (et où il est évident que $\mathrm{m}(\varpi_i) = 1$!), le critère "$d_j = 1$ pour tout j" ne s'applique malheureusement jamais. En revanche, on observe que si l'on disposait du cas particulier de la conjecture VIII.4.22 annoncé par Arancibia décrit dans la remarque VIII.4.23, à savoir du cas où "$\pi_j \neq 1 \Rightarrow d_j \leq 4$", on pourrait conclure que $\mathrm{m}(\varpi_i) = 1$ dès que $i \notin \{11, 12, 13, 20, 22, 23\}$. Comme d'autre part, le travail déjà mentionné d'Ikeda [Ike06] assure que $\mathrm{m}(\varpi_i) \neq 0$ dès que $i \notin \{10, 15, 19, 21\}$, cela conduirait à une démonstration inconditionnelle du théorème.

3. Représentations algébriques de poids motivique ≤ 22

3.1. Un énoncé de classification

Le but de cette partie est de démontrer le théorème suivant.

Théorème 3.2. *Soient $n \geq 1$ et $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ algébrique de poids motivique $w \leq 22$. Alors on est dans l'un des cas suivants :*

(i) $n = 1$, $w = 0$ et π est la représentation triviale.

(ii) $n = 2$, $w \in \{11, 15, 17, 19, 21\}$, et π est la représentation Δ_w, engendrée par l'unique forme modulaire parabolique normalisée de poids $w+1$ pour le groupe $\mathrm{SL}_2(\mathbb{Z})$.

(iii) $n = 3$, $w = 22$ et π est le carré symétrique de Δ_{11}.

(iv) $n = 4$ et $\mathrm{Poids}(\pi)$ est de la forme $\{\pm\frac{w}{2}, \pm\frac{v}{2}\}$ avec

$$(w, v) \quad = \quad (19, 7), \quad (21, 5), \quad (21, 9) \quad \text{ou} \quad (21, 13).$$

Dans ce cas, π est l'unique représentation dans $\Pi_{\mathrm{alg}}(\mathrm{PGL}_4)$ de poids $\{\pm\frac{w}{2}, \pm\frac{v}{2}\}$; en particulier, on a $\pi \simeq \pi^\vee$.

(v) $n = 4$, $w = 22$ et $\mathrm{Poids}(\pi) = \{\pm 11, \pm v\}$ avec $v = 4, 5$ ou 6. Dans ce cas, les représentations π et $\pi^\vee$ ne sont pas isomorphes, et ce sont les seules représentations dans $\Pi_{\mathrm{alg}}(\mathrm{PGL}_4)$ de poids $\{\pm 11, \pm v\}$.

De plus, s'il existe des représentations dans $\Pi_{\mathrm{alg}}(\mathrm{PGL}_4)$ de poids respectifs $\{\pm\frac{21}{2}, \pm\frac{9}{2}\}$ et $\{\pm\frac{21}{2}, \pm\frac{13}{2}\}$, alors le cas (v) ne se produit pas.

Soulignons que l'assertion (iv) du théorème affirme seulement l'unicité, mais non l'existence, d'une représentation $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_4)$ dont les poids sont de la forme $\{\pm\frac{w}{2}, \pm\frac{v}{2}\}$ avec (w, v) parcourant la liste des 4 couples de l'énoncé. Cependant nous avons montré dans la Définition-Proposition 1.6, à partir de la formule de Tsushima et des résultats d'Arthur, qu'il existe en effet une telle représentation, que nous avons notée $\Delta_{w,v}$. La raison pour laquelle nous avons formulé ainsi le théorème 3.2 est que sa démonstration, comme nous le verrons, ne nécessite pas de connaître l'existence de ces représentations, et en particulier ne repose pas sur les travaux d'Arthur. Nous en déduisons donc le théorème suivant [2] (théorème F de l'introduction) :

Théorème⋆ 3.3. *Soient $n \geq 1$ et $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ algébrique de poids motivique ≤ 22. Alors π appartient à la liste des 11 représentations suivantes :*

$$1,\ \Delta_{11},\ \Delta_{15},\ \Delta_{17},\ \Delta_{19},\ \Delta_{19,7},\ \Delta_{21},\ \Delta_{21,5},\ \Delta_{21,9},\ \Delta_{21,13}\ \text{ et }\ \mathrm{Sym}^2\Delta_{11}.$$

Comme nous l'avons déjà expliqué dans l'introduction, notre démonstration du théorème 3.2 repose sur un analogue dans le cadre des fonctions L automorphes des *formules explicites* de Riemann et Weil en théorie des nombres premiers. Nous renvoyons aux exposés de Poitou [Poi76a, Poi76b] à ce sujet. Cet analogue a été développé par Mestre [Mes86], puis appliqué par Fermigier aux fonctions $\mathrm{L}(s, \pi)$ pour $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ [Fer96]. Ce dernier en a déduit *loc. cit.* l'annulation de la cohomologie "cuspidale" du groupe $\mathrm{SL}_n(\mathbb{Z})$ à coefficients rationnels quand $n < 24$. Ce résultat a été par la suite étendu à $n < 27$ par Miller [Mil02], inspiré par des travaux de Rudnick et Sarnak [RuS96], en considérant plutôt la fonction $\mathrm{L}(s, \pi \times \pi^\vee)$, qui présente plusieurs avantages de convergence et positivité [3]. Ce sera également notre point de départ. Plus généralement, nous allons examiner en détail les inégalités données par la formule explicite appliquée à la fonction $\mathrm{L}(s, \pi \times \pi')$ pour toute paire de représentations $\{\pi, \pi'\}$ avec $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ et $\pi' \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_{n'})$.

Avant d'entamer ces démonstrations, donnons un corollaire du cas particulier $\mathrm{w}(\pi) = 0$ du Théorème 3.2.

Proposition 3.4. *Supposons que $\mathrm{L}_{\mathbb{Z}}$ est un groupe topologique compact satisfaisant les axiomes (L1) et (L2) introduits en page vii de la préface. Alors $\mathrm{L}_{\mathbb{Z}}$ est connexe.*

2. Mentionnons qu'à notre connaissance, personne n'a encore démontré l'existence d'une représentation $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$, $n \geq 1$, qui ne soit pas autoduale.

3. Dans un contexte proche, l'avantage à considérer ce type de fonctions L avait déjà été observé par Serre [Poi76b, p. 15].

Démonstration. Soit $\psi : \mathrm{L}_{\mathbb{Z}} \to \mathrm{GL}_n(\mathbb{C})$ une représentation continue et irréductible de $\mathrm{L}_{\mathbb{Z}}$. D'après l'axiome (L2), il existe une unique représentation π dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ vérifiant $\mathrm{c}(\pi) = \mathrm{c}(\psi)$ (selon nos conventions, on a $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n) = \Pi_{\mathrm{cusp}}(\mathrm{GL}_n)$). Supposons en outre que l'image de ψ est finie ; on a en particulier $\mathrm{c}_\infty(\psi) = 0$ par définition de Frob_∞ (axiome (L1)). On en déduit $\mathrm{c}_\infty(\pi) = 0$, donc tous les poids de π sont nuls et l'on a $\mathrm{w}(\pi) = 0$. Le théorème 3.2 entraîne $n = 1$ et que π est la représentation triviale. L'axiome (L2) dans le cas $n = 1$ montre que ψ est également la représentation triviale de $\mathrm{L}_{\mathbb{Z}}$. Comme tout groupe fini non trivial admet une représentation irréductible non triviale, nous avons démontré que le groupe compact $\mathrm{L}_{\mathbb{Z}}$ n'admet pas de quotient fini non trivial : c'est un groupe connexe. □

3.5. La formule explicite pour les fonctions L de paires

Les formules explicites dépendent du choix d'une "fonction test". Suivant l'analyse de Poitou et Weil [Po176A, p. 6], nous entendrons par là toute fonction paire $F : \mathbb{R} \to \mathbb{R}$ satisfaisant les axiomes suivants, dans lesquels F_ϵ, pour ϵ réel > 0, désigne la fonction $\mathbb{R} \to \mathbb{R},\ x \mapsto F(x)e^{(\frac{1}{2}+\epsilon)x}$:

(T1) il existe $\epsilon > 0$ tel que F_ϵ soit sommable sur $\mathbb{R}_{>0}$;

(T2) il existe $\epsilon > 0$ tel que F_ϵ est à variation bornée sur $\mathbb{R}$, égale en chaque point à la moyenne de ses limites à droite et à gauche ;

(T3) la fonction $\frac{1}{x}(F(x) - F(0))$ est à variation bornée sur $\mathbb{R} - \{0\}$.

En particulier, toute fonction paire de classe $\mathcal{C}^2$ sur $\mathbb{R}$ et à support compact est une fonction test. Ce sera le cas dans nos applications, où nous prendrons pour F une modification simple de la fonction d'Odlyzko. Dans un premier temps, il sera cependant plus clair de considérer des fonctions tests arbitraires.

Si F est une fonction test, et si $\epsilon > 0$ est tel que F_ϵ est sommable sur $\mathbb{R}$, l'intégrale dépendant du paramètre complexe s définie par

$$\Phi_F(s) = \int_{\mathbb{R}} F(x)e^{(s-\frac{1}{2})x}\mathrm{d}x \tag{3.1}$$

est absolument convergente dans la région $-\epsilon < \mathrm{Re}\ s < 1 + \epsilon$. La fonction $\Phi_F(s)$ est en particulier bien définie et holomorphe dans cette région. La parité de F entraîne l'égalité $\Phi_F(s) = \Phi_F(1-s)$. De plus, la relation $\Phi_F(\overline{s}) = \overline{\Phi_F(s)}$ montre $\Phi_F(s) \in \mathbb{R}$ pour tout réel s tel que $0 \leq s \leq 1$.

On pose

$$\Pi_{\mathrm{alg}} = \coprod_{n\geq 1} \Pi_{\mathrm{alg}}(\mathrm{PGL}_n).$$

Soient $\pi, \pi' \in \Pi_{\mathrm{alg}}$. Ainsi que nous l'avons rappelé au §VIII.2.21, on dispose suivant Jacquet et Shalika [JS81a, Theorem 5.3] d'un produit Eulérien

$$\mathrm{L}(s, \pi \times \pi') = \prod_p \det(1 - p^{-s} \mathrm{c}_p(\pi) \otimes \mathrm{c}_p(\pi'))^{-1}$$

qui est bien défini et absolument convergent pour $\operatorname{Re} s > 1$. De plus, la fonction

$$\xi(s, \pi \times \pi') := \Gamma(s, \mathrm{L}(\pi_\infty) \otimes \mathrm{L}(\pi'_\infty))\, \mathrm{L}(s, \pi \times \pi')$$

admet un prolongement méromorphe à $\mathbb{C}$ tout entier vérifiant l'équation fonctionnelle $\xi(s, \pi \times \pi') = \varepsilon(\pi \times \pi')\, \xi(1 - s, \pi^\vee \times \pi'^\vee)$ avec

$$\varepsilon(\pi \times \pi') = \varepsilon(\mathrm{L}(\pi_\infty) \otimes \mathrm{L}(\pi'_\infty)).$$

En particulier, tous les zéros de ξ sont dans la bande critique $0 \leq \operatorname{Re} s \leq 1$ (Shahidi a même démontré que ces zéros sont dans l'intérieur de cette bande). Enfin, la fonction ξ est holomorphe sur $\mathbb{C} - \{0, 1\}$, et admet un pôle en $s = 1$ si, et seulement si, $\pi' = \pi^\vee$, auquel cas il s'agit d'un pôle simple.

Proposition-Définition 3.6. *Soient $\pi, \pi' \in \Pi_{\mathrm{alg}}$, $\xi(s) = \xi(s, \pi^\vee \times \pi')$, F une fonction test et T un réel > 0. La somme finie*

$$\sum_{\{s \in \mathbb{C},\ |\operatorname{Im} s| < T,\ \xi(s) = 0\}} \Phi_F(s)\ \operatorname{ord}_{z=s} \xi(z)$$

est réelle et admet une limite finie quand $T \to +\infty$; nous noterons $\mathrm{Z}^F(\pi, \pi')$ cette limite.

En effet, cet énoncé est un cas particulier des résultats de Mestre [Mes86, §I], qui généralisent eux-même de manière assez directe ceux de Riemann, Weil, et Poitou [Poi76a]. Supposons $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ et $\pi' \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_{n'})$. Dans les notations de Mestre, on prend $M = M' = nn'$, $c = 0$, $L_1(s) = \mathrm{L}(s, \pi^\vee \times \pi')$, $L_2(s) = \mathrm{L}(s, \pi \times (\pi')^\vee)$, $w = \varepsilon(\pi^\vee \times \pi')$, $\Lambda_1(s) = \xi(s, \pi^\vee \times \pi')$ et $\Lambda_2(s) = \xi(s, \pi \times (\pi')^\vee)$. Par définition, nous incorporons les facteurs qu'il note A^s et B^s, ainsi que ses coefficients a_i, a'_i, b_i, b'_i, dans nos facteurs archimédiens Γ, et il n'y a pas de contribution du conducteur (qui vaut 1 ici). Ceci étant dit, les hypothèses (i), (ii) et (iii) *loc. cit.* découlent de l'équation fonctionnelle et de la finitude du nombre de pôles des Λ_i, qui ont déjà été justifiés ci-dessus. L'hypothèse (iii), à savoir que la fonction ξ diminuée de ses parties singulières est bornée dans toute bande verticale, est un théorème de Gelbart et Shahidi [GSha01, Cor. 2]. Enfin, seule une version affaiblie de sa dernière hypothèse (iv) est satisfaite, à savoir la convergence absolue des produits Eulériens L_1

et L_2 ainsi que leur non-annulation sur $\mathrm{Re}\, s > 1$, mais c'est tout ce dont il a besoin par la suite : voir [Mes86, p. 213-214] et surtout l'argument donné par Poitou [Poi76a, p. 2-3].

La conclusion de cette discussion est que tous les résultats de [Mes86, §I.2] s'appliquent. L'assertion de convergence dans la définition-proposition ci-dessus est notamment justifiée par Mestre page 213. Le fait que la somme finie apparaissant dans la définition-proposition 3.6 est réelle vient du fait que la région $\{s \in \mathbb{C},\ |\mathrm{Im}\, s| < T\}$ est stable par $s \mapsto 1 - \overline{s}$ et des égalités

$$\xi(1-\overline{s}, \pi^\vee \times \pi') \;=\; \varepsilon(\pi^\vee \times \pi')\, \xi(\overline{s}, \pi \times \pi'^\vee) \;=\; \varepsilon(\pi^\vee \times \pi')\, \overline{\xi(s, \pi^\vee \times \pi')}.$$

Mestre établit également *loc. cit.* la formule explicite que nous allons utiliser. C'est le résultat de l'intégration de la 1-forme $\Phi_F(s)\, \mathrm{dlog}\, \xi(s)$ sur le bord du rectangle $\{s \in \mathbb{C},\ -\epsilon \leq \mathrm{Re}\, s \leq 1+\epsilon,\ |\mathrm{Im}\, s| \leq A\}$, A et ϵ étant des réels > 0 convenables, puis d'un passage à la limite $\epsilon \to 0$ et $A \to \infty$. Afin de pouvoir l'énoncer sous une forme agréable, introduisons d'abord certaines quantités préliminaires "locales". L'assertion de convergence dans la définition suivante est justifiée dans [Mes86, p. 213-214] et [Poi76a, p. 2-3].

Proposition-Définition 3.7. *Soient $\pi, \pi' \in \Pi_{\mathrm{alg}}$ et F une fonction test. La somme*

$$\sum_{p,k} F(k\log(p)) \frac{\log(p)}{p^{k/2}}\ \overline{\mathrm{tr}\,(\mathrm{c}_p(\pi)^k)}\ \mathrm{tr}\,(\mathrm{c}_p(\pi')^k)\,,$$

portant sur tous les couples (p,k) avec p un nombre premier et k un entier ≥ 1, est absolument convergente ; nous la notons $\widetilde{\mathrm{B}}_f^F(\pi,\pi')$. On a les relations évidentes $\widetilde{\mathrm{B}}_f^F(\pi,\pi') = \overline{\widetilde{\mathrm{B}}_f^F(\pi',\pi)} = \widetilde{\mathrm{B}}_f^F((\pi')^\vee, \pi^\vee)$. On pose enfin

$$\mathrm{B}_f^F(\pi,\pi') \;:=\; \Re\, \widetilde{\mathrm{B}}_f^F(\pi,\pi').$$

Soit $\mathrm{W}_{\mathbb{R}}^{\mathrm{alg}}$ le quotient du groupe de Weil $\mathrm{W}_{\mathbb{R}}$ par la composante connexe de son centre, à savoir $\mathbb{R}_{>0}$. Soit K_∞ l'anneau de Grothendieck de la catégorie des représentations complexes, continues, et de dimension finie, du groupe $\mathrm{W}_{\mathbb{R}}^{\mathrm{alg}}$. D'après les rappels du §VIII.2.12, c'est le groupe abélien libre sur les (classes des) représentations

$$1, \quad \epsilon_{\mathbb{C}/\mathbb{R}} \quad \text{et} \quad \mathrm{I}_w \ \text{ pour } \ w \in \mathbb{Z}_{>0}.$$

Remarquons que tout élément de K_∞ est égal à son dual, car c'est le cas des classes des trois représentations ci-dessus.

L'application $V \mapsto \Gamma(-,V)$ introduite au §VIII.2.21 s'étend de manière naturelle en un homomorphisme $\Gamma : \mathrm{K}_\infty \to \mathcal{M}(\mathbb{C})^\times$, où $\mathcal{M}(\mathbb{C})^\times$ désigne le groupe multiplicatif du corps $\mathcal{M}(\mathbb{C})$ des fonctions méromorphes sur $\mathbb{C}$. Son image est constituée de fonctions n'ayant ni pôle, ni zéro, dans le demi-plan $\operatorname{Re} s > 0$.

Proposition-Définition 3.8. *Si F est une fonction test, l'application*

$$\mathrm{J}_F : \mathrm{K}_\infty \to \mathbb{R}, \quad V \mapsto -\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\frac{1}{2}} \Phi_F(s)\frac{\Gamma'(s,V)}{\Gamma(s,V)}\mathrm{d}s,$$

est bien définie et $\mathbb{Z}$-linéaire. De plus, on a les identités :

(i) $\mathrm{J}_F(1) = \frac{1}{2}\log(\pi)\, F(0) + \sigma_F(\frac{1}{2},0)$,

(ii) $\mathrm{J}_F(\epsilon_{\mathbb{C}/\mathbb{R}}) = \frac{1}{2}\log(\pi)\, F(0) + \sigma_F(\frac{1}{2},\frac{1}{2})$,

(iii) $\mathrm{J}_F(\mathrm{I}_w) = \log(2\pi)\, F(0) + \sigma_F(1,\frac{w}{2})$ *pour* $w \geq 0$.

où l'on a posé $\sigma_F(a,b) = a\int_0^{+\infty}\left(F(ax)\frac{e^{-(a/2+b)x}}{1-e^{-x}} - F(0)\frac{e^{-x}}{x}\right)\mathrm{d}x$.

Enfin, l'application $\mathrm{K}_\infty \times \mathrm{K}_\infty \to \mathbb{R}$, $(V,W) \mapsto \mathrm{J}_F(V^* \otimes W)$, *est bilinéaire ; nous la noterons* B^F_∞. *La relation évidente* $\mathrm{B}^F_\infty(V,W) = \mathrm{J}_F(V \otimes W)$ *pour tout* $V, W \in \mathrm{K}_\infty$ *montre que* B^F_∞ *est symétrique.*

Démonstration. Notons $\psi \in \mathcal{M}(\mathbb{C})$ la fonction digamma, définie par $\psi(s) = \Gamma'(s)/\Gamma(s)$. Posons également $\psi(s,V) = \frac{\Gamma'(s,V)}{\Gamma(s,V)}$ pour $V \in \mathrm{K}_\infty$. L'application $V \mapsto \psi(-,V)$, $\mathrm{K}_\infty \to \mathcal{M}(\mathbb{C})$, est manifestement $\mathbb{Z}$-linéaire. Suivant la définition des facteurs $\Gamma(s,V)$ rappelée au §VIII.2.21, on a les identités

$$\psi(s,1) = -\frac{1}{2}\log\pi + \frac{1}{2}\psi(\frac{s}{2}) \quad \text{et} \quad \psi(s,\mathrm{I}_w) = -\log(2\pi) + \psi(s+\frac{w}{2})$$

pour tout $w \geq 0$. La fonction F est sommable sur $\mathbb{R}$ d'après (T1), égale en tout point à la moyenne de ses limites à droite et à gauche d'après (T2), et $\frac{F(x)-F(0)}{x}$ est bornée au voisinage de 0 d'après (T3). La formule d'inversion de Fourier est donc valable en $x = 0$, autrement dit l'intégrale $-\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\frac{1}{2}} \Phi_F(s)\mathrm{d}s$ est convergente et vaut $-F(0)$. Il reste à examiner la convergence d'une intégrale de la forme

$$-\frac{a}{2i\pi}\int_{\mathrm{Re}(s)=\frac{1}{2}} \Phi_F(s)\psi(as+b)\mathrm{d}s$$

avec $b \in \mathbb{R}_{\geq 0}$ et $a \in \mathbb{R}_{>0}$. La convergence (simple) de cette intégrale est vérifiée dans [Poi76a, p. 6-04] et [Mes86, Lemme I.2.1] ainsi que l'égalité de sa somme avec l'intégrale (également convergente) $\sigma_F(a,b)$ de l'énoncé. Cela entraîne tous les points de la proposition. □

Nous disposons maintenant de tous les ingrédients nécessaires pour énoncer la formule explicite. Il sera commode d'introduire le groupe abélien libre sur l'ensemble Π_{alg} :

$$\mathrm{K} = \mathbb{Z}[\Pi_{\mathrm{alg}}].$$

Soit F une fonction test. Chacune des trois fonctions $\Pi_{\mathrm{alg}} \times \Pi_{\mathrm{alg}} \to \mathbb{R}$ envoyant respectivement (π, π') sur $\mathrm{Z}^F(\pi, \pi')$, $\mathrm{B}_f^F(\pi, \pi')$ et $\delta_{\pi,\pi'}$ (symbole de Kronecker), s'étend en une application bilinéaire symétrique $\mathrm{K} \times \mathrm{K} \to \mathbb{R}$ associée à F. Nous noterons ces trois formes Z^F, B_f^F et δ respectivement. De plus, l'application $\Pi_{\mathrm{alg}} \to \mathrm{K}_\infty$, $\pi \mapsto \mathrm{L}(\pi_\infty)$, s'étend en un homomorphisme $\mathrm{L} : \mathrm{K} \to \mathrm{K}_\infty$. L'application $\mathrm{K} \times \mathrm{K} \to \mathbb{R}$, $(V, W) \mapsto \mathrm{B}_\infty^F(\mathrm{L}(V), \mathrm{L}(W))$, est donc également bilinéaire et symétrique ; nous nous autoriserons l'abus de langage consistant à la noter également B_∞^F. On pose enfin

$$\mathrm{B}^F = \mathrm{B}_f^F + \mathrm{B}_\infty^F \quad : \quad \mathrm{K} \times \mathrm{K} \to \mathbb{R}.$$

Proposition 3.9. ("Formule explicite") *Pour toute fonction test F, on a l'égalité suivante entre formes bilinéaires* $\mathrm{K} \times \mathrm{K} \to \mathbb{R}$ *:*

$$\mathrm{B}^F + \frac{1}{2}\mathrm{Z}^F = \Phi_F(0)\ \delta.$$

Démonstration. Par bilinéarité, il suffit de montrer cette égalité pour un couple $(\pi, \pi') \in \Pi_{\mathrm{alg}} \times \Pi_{\mathrm{alg}}$. Dans ce cas, la formule donnée par Mestre [Mes86, §I.2] s'écrit, compte tenu de la parité de la fonction F :

$$\mathrm{B}_\infty^F(\pi, \pi') + \mathrm{B}_\infty^F(\pi', \pi) + \widetilde{\mathrm{B}}_f^F(\pi, \pi') + \widetilde{\mathrm{B}}_f^F(\pi', \pi) + \mathrm{Z}^F(\pi, \pi') = \delta_{\pi,\pi'}\,(\Phi_F(0) + \Phi_F(1)).$$

On conclut par les identités $\Phi_F(1) = \Phi_F(0)$, $\mathrm{B}_\infty^F(\pi, \pi') = \mathrm{B}_\infty^F(\pi', \pi)$, et $2\,\mathrm{B}_f^F(\pi, \pi') = \widetilde{\mathrm{B}}_f^F(\pi, \pi') + \widetilde{\mathrm{B}}_f^F(\pi', \pi)$. □

On dira qu'un élément π de K est effectif si c'est une somme finie d'éléments de Π_{alg} (autrement dit, une combinaison linéaire à coefficients ≥ 0). Si π et π' sont effectifs, disons $\pi = \sum_i \pi_i$ et $\pi' = \sum_j \pi'_j$ avec $\pi_i, \pi'_j \in \Pi_{\mathrm{alg}}$, on notera $\xi(s, \pi \times \pi')$ (resp. $\mathrm{L}(s, \pi \times \pi')$), le produit des $\xi(s, \pi_i \times \pi'_j)$ (resp. $\mathrm{L}(s, \pi_i \times \pi'_j)$). Considérons de plus l'assertion suivante portant sur une fonction test F :

(T4) $\Re\ \Phi_F(s)$ est ≥ 0 pour tout $s \in \mathbb{C}$ tel que $0 \leq \mathrm{Re}\, s \leq 1$.

On rappelle que $\Phi_F(s)$ est un nombre réel pour tout réel s dans $[-1, 1]$, en particulier il est ≥ 0 si F satisfait (T4). Dans ce mémoire, nous utiliserons uniquement le corollaire suivant de la formule explicite.

Corollaire 3.10. *Soient F une fonction test et $\pi, \pi' \in \mathrm{K}$ effectifs. On suppose que F satisfait la condition (T4). On a l'inégalité*

$$\mathrm{B}^F(\pi, \pi') \leq \Phi_F(0)\, \delta(\pi, \pi') - \frac{1}{2}\, \Phi_F(\frac{1}{2})\, \mathrm{ord}_{s=\frac{1}{2}} \xi(s, \pi^\vee \times \pi').$$

Démonstration. Sous l'hypothèse (T4) sur F, on a l'inégalité

$$\mathrm{Z}^F(\pi, \pi') = \Re\, \mathrm{Z}^F(\pi, \pi') \geq \Phi_F(\frac{1}{2})\, \mathrm{ord}_{s=\frac{1}{2}} \xi(s, \pi^\vee \times \pi').$$

On conclut par la proposition 3.9. □

Remarque 3.11. Si $V \in \mathrm{K}_\infty$, on constate que la fonction méromorphe $\Gamma(s, V)$ est finie et non nulle en $s = \frac{1}{2}$. On en déduit, pour tous $\pi, \pi' \in \mathrm{K}$ effectifs, l'égalité $\mathrm{ord}_{s=\frac{1}{2}} \xi(s, \pi \times \pi') = \mathrm{ord}_{s=\frac{1}{2}} \mathrm{L}(s, \pi \times \pi')$. Le corollaire ci-dessus vaut donc également en remplaçant $\xi(s, \pi^\vee \times \pi')$ par $\mathrm{L}(s, \pi^\vee \times \pi')$.

L'ordre d'annulation des fonctions $\xi(s, \pi \times \pi')$ en $s = \frac{1}{2}$ est réputé mystérieux. On le minore traditionnellement de la manière suivante. Si $\pi, \pi' \in \Pi_{\mathrm{alg}}$ on pose $\mathrm{e}^\perp(\pi, \pi') = 1$ si π et π' sont toutes deux autoduales et satisfont $\varepsilon(\pi \times \pi') = -1$; sinon on pose $\mathrm{e}^\perp(\pi, \pi') = 0$. La fonction $\mathrm{e}^\perp : \Pi_{\mathrm{alg}} \times \Pi_{\mathrm{alg}} \to \mathbb{Z}$ s'étend en une forme bilinéaire symétrique $\mathrm{e}^\perp : \mathrm{K} \times \mathrm{K} \to \mathbb{Z}$. Ainsi, pour tous $\pi, \pi' \in \mathrm{K}$ effectifs on a l'inégalité $\mathrm{ord}_{s=\frac{1}{2}} \xi(s, \pi \times \pi') \geq \mathrm{e}^\perp(\pi, \pi')$.

Corollaire 3.12. *Soient F une fonction test et $\pi, \pi' \in \mathrm{K}$ effectifs. On suppose que F satisfait (T4) et $F \geq 0$. On pose*

$$\mathrm{C}^F(\pi, \pi') = \Phi_F(0)\, \delta(\pi, \pi') - \frac{1}{2}\, \Phi_F(\frac{1}{2})\, \mathrm{e}^\perp(\pi, \pi') - \mathrm{B}^F_\infty(\pi, \pi').$$

On a les inégalités :

(i) $\mathrm{C}^F(\pi, \pi) \geq 0$. *En particulier, on a* $\mathrm{B}^F_\infty(\pi, \pi) \leq \Phi_F(0)\, \delta(\pi, \pi)$.

(ii) $\mathrm{C}^F(\pi, \pi') + \sqrt{\mathrm{C}^F(\pi, \pi) \mathrm{C}^F(\pi', \pi')} \geq 0$.

Démonstration. Le corollaire 3.10 et la discussion précédente montrent que sous l'hypothèse (T4) sur F on a $\mathrm{B}^F_f(\pi, \pi') \leq \mathrm{C}^F(\pi, \pi')$ pour tous $\pi, \pi' \in \mathrm{K}$ effectifs. Observons que l'hypothèse de positivité de la fonction F entraîne la positivité de la forme bilinéaire B^F_f sur K. En effet, un élément $\varpi \in \mathrm{K} \otimes \mathbb{R}$

peut s'écrire sous la forme $\varpi = \sum_i \lambda_i \pi_i$ où les π_i sont dans Π_{alg} et les λ_i sont dans $\mathbb{R}$. L'identité

$$\mathrm{B}_f^F(\varpi, \varpi) \; = \sum_{p,k} F(k \log p) \, \frac{\log p}{p^{\frac{k}{2}}} \; \mid \sum_i \; \lambda_i \; \mathrm{tr}\, \mathrm{c}(\pi_i)^k \; \mid^2$$

entraîne donc $\mathrm{B}_f^F(\varpi, \varpi) \geq 0$. L'assertion (ii) se déduit de l'inégalité de Cauchy-Schwarz appliquée à B_f^F :

$$|\mathrm{B}_f^F(\pi, \pi')| \leq \sqrt{\mathrm{B}_f^F(\pi, \pi) \, \mathrm{B}_f^F(\pi', \pi')}$$

et de l'inégalité évidente $|\mathrm{B}_f^F(\pi, \pi')| \geq -\mathrm{B}_f^F(\pi, \pi')$. (On prendra garde que la forme bilinéaire C^F est a priori seulement positive sur les éléments effectifs de K, d'où la formulation de l'assertion (ii).) □

Dans [Mil02], l'inégalité (i) du corollaire ci-dessus est exploitée dans le cas particulier $\pi \in \Pi_{\mathrm{alg}}$. Pour un π effectif quelconque elle admet le corollaire 3.14 ci-dessous, d'abord observé par Olivier Taïbi. L'inégalité (ii) semble nouvelle, elle rendra de grands services dans les applications.

Définition 3.13. *Soit* $V \in \mathrm{K}_\infty$. *On note* $\mathrm{m}(V)$ *le nombre de représentations* $\pi \in \Pi_{\mathrm{alg}}$ *satisfaisant* $\mathrm{L}(\pi_\infty) \simeq V$ *; d'après Harish-Chandra on a* $\mathrm{m}(V) < +\infty$ (§IV.3.2). *On note également* $\mathrm{m}^\perp(V)$ *le nombre de représentations* $\pi \in \Pi_{\mathrm{alg}}$ *autoduales et satisfaisant* $\mathrm{L}(\pi_\infty) \simeq V$. *On a l'inégalité* $\mathrm{m}^\perp(V) \leq \mathrm{m}(V)$.

Un élément V de K_∞ sera dit effectif si c'est la classe d'une représentation de dimension finie, continue, et à coefficients dans $\mathbb{C}$, de $\mathrm{W}_{\mathbb{R}}^{\mathrm{alg}}$. Il est évident que si $\mathrm{m}(V) \neq 0$ alors V est effectif.

Corollaire 3.14. (Taïbi) *Soient* $V \in \mathrm{K}_\infty$ *effectif et* F *une fonction test, supposée* ≥ 0 *et satisfaisant l'hypothèse* (T4). *On a l'inégalité*

$$\mathrm{m}(V) \; \mathrm{B}_\infty^F(V, V) \leq \Phi_F(0).$$

Démonstration. Si $\mathrm{m}(V) = 0$ il n'y a rien à démontrer. Supposons donc qu'il existe un entier $r \geq 1$ et des représentations $\pi_1, \ldots, \pi_r \in \Pi_{\mathrm{alg}}$ distinctes telles que $\mathrm{L}((\pi_i)_\infty) \simeq V$ pour tout i. On applique le point (i) du corollaire 3.12 à l'élément $\pi = \pi_1 + \pi_2 + \cdots + \pi_r$ de K. On a d'une part les égalités

$$\mathrm{B}_\infty^F(\pi, \pi) \; = \; \mathrm{B}_\infty^F(rV, rV) \; = \; r^2 \, \mathrm{B}_\infty^F(V, V)$$

et d'autre part $\delta(\pi, \pi) = r$. On en déduit l'inégalité $r^2 \; \mathrm{B}_\infty^F(V, V) \; \leq \; r \, \Phi_F(0)$, et donc $r \, \mathrm{B}_\infty^F(V, V) \leq \Phi_F(0)$. □

Observons que sous l'hypothèse supplémentaire $\mathrm{B}^F_\infty(V,V) > 0$, le corollaire ci-dessus fournit une majoration explicite de $\mathrm{m}(V)$. En particulier, il redémontre le résultat d'Harish-Chandra susmentionné $\mathrm{m}(V) < \infty$ (§IV.3.2).

Corollaire 3.15. *Soient $V, V' \in \mathrm{K}_\infty$ effectifs et F une fonction test ≥ 0 satisfaisant (T4). On suppose $V \neq V'$ et $\mathrm{m}(V)\,\mathrm{m}(V') \neq 0$.*

(i) Si l'on pose $\mathrm{n}(V,V') = \frac{\mathrm{m}^\perp(V)\,\mathrm{m}^\perp(V')}{4\,\mathrm{m}(V)\,\mathrm{m}(V')}(1-\varepsilon(V\otimes V'))$, on a l'inégalité

$$\mathrm{n}(V,V')\,\Phi_F(\frac{1}{2}) + \mathrm{B}^F_\infty(V,V') \leq \sqrt{(\frac{\Phi_F(0)}{\mathrm{m}(V)} - \mathrm{B}^F_\infty(V,V))(\frac{\Phi_F(0)}{\mathrm{m}(V')} - \mathrm{B}^F_\infty(V',V'))},$$

(ii) Si l'on a en outre $\mathrm{m}^\perp(V)\mathrm{m}^\perp(V') \neq 0$, on a également l'inégalité

$$\frac{1-\varepsilon(V\otimes V')}{4}\,\Phi_F(\frac{1}{2}) + \mathrm{B}^F_\infty(V,V') \leq \sqrt{(\frac{\Phi_F(0)}{\mathrm{m}^\perp(V)} - \mathrm{B}^F_\infty(V,V))(\frac{\Phi_F(0)}{\mathrm{m}^\perp(V')} - \mathrm{B}^F_\infty(V',V'))},$$

Démonstration. Soient r, r' des entiers ≥ 1 et des représentations distinctes $\pi_1, \ldots, \pi_r, \pi'_1, \ldots, \pi'_{r'} \in \Pi_{\mathrm{alg}}$ telles que $\mathrm{L}(\pi_i) = V$ pour tout i et $\mathrm{L}(\pi'_j) = V'$ pour tout j. On pose $\pi = \sum_i \pi_i$ et $\pi' = \sum_j \pi'_j$. On a $\delta(\pi,\pi') = 0$ car $V \neq V'$. Notons $s \leq r$ (resp. $s' \leq r'$) le nombre de représentations autoduales parmi les π_i (resp. π'_j). On a l'égalité évidente

$$\mathrm{e}^\perp(\pi,\pi') = s\,s'\,\frac{1-\varepsilon(V\otimes V')}{2}.$$

On a de plus

$$\mathrm{C}^F(\pi,\pi') + \frac{\mathrm{e}^\perp(\pi,\pi')}{2}\,\Phi_F(\frac{1}{2}) = -\,\mathrm{B}^F_\infty(rV, r'V') = -rr'\,\mathrm{B}^F_\infty(V,V').$$

De même, on constate les inégalités $\mathrm{C}^F(\pi,\pi) \leq r\,\Phi_F(0) - r^2\,\mathrm{B}^F_\infty(V,V)$ et $\mathrm{C}^F(\pi',\pi') \leq r'\,\Phi_F(0) - (r')^2\,\mathrm{B}^F_\infty(V',V')$. En divisant par $rr' \neq 0$ l'inégalité donnée par le point (ii) du corollaire 3.12, on en déduit l'inégalité

$$\frac{ss'}{4rr'}(1-\varepsilon(V\otimes V'))\,\Phi_F(\frac{1}{2}) + \mathrm{B}^F_\infty(V,V') \leq \sqrt{(\frac{\Phi_F(0)}{r} - \mathrm{B}^F_\infty(V,V))(\frac{\Phi_F(0)}{r'} - \mathrm{B}^F_\infty(V',V'))}.$$

Cette inégalité est valable pour tout quadruplet d'entiers (r, r', s, s') tels que $1 \leq r \leq \mathrm{m}(V)$, $1 \leq r' \leq \mathrm{m}(V')$, $s \leq r$ et $s' \leq r'$. L'assertion (i) résulte du cas particulier $(r, r', s, s') = (\mathrm{m}(V), \mathrm{m}(V'), \mathrm{m}^\perp(V), \mathrm{m}^\perp(V'))$, et l'assertion (ii) du cas $(r, r', s, s') = (\mathrm{m}(V)^\perp, \mathrm{m}^\perp(V'), \mathrm{m}^\perp(V), \mathrm{m}^\perp(V'))$.

□

Comme nous le verrons, ce corollaire permet typiquement de montrer que si $V \neq V'$, l'existence de certains éléments $\pi \in \Pi_{\mathrm{alg}}$ tels que $\mathrm{L}(\pi_\infty) = V$ entraîne l'inexistence d'éléments $\pi \in \Pi_{\mathrm{alg}}$ tels que $\mathrm{L}(\pi'_\infty) = V'$. Il admet divers raffinements sur lesquels nous reviendrons au §3.29. Terminons par un critère simple bien connu [Poi76a] permettant de construire des fonctions tests satisfaisant (T4) ; nous redonnons l'argument pour le confort du lecteur.

Lemme 3.16. *Soit $g : \mathbb{R} \to \mathbb{R}$ une fonction paire, sommable et de carré sommable. Sa transformée de Fourier $\widehat{g}$ est bien définie et à valeurs réelles sur $\mathbb{R}$. Supposons $\widehat{g} \geq 0$ et considérons la fonction $F : \mathbb{R} \to \mathbb{R}$ définie par*

$$F(x) = \frac{g(x)}{\cosh(x/2)}.$$

Alors $\Phi_F(s)$ est bien définie pour tout $s \in \mathbb{C}$ tel que $0 \leq \mathrm{Re}\, s \leq 1$ (formule (3.1)), et dans cette région on a $\Re\, \Phi_F(s) \geq 0$.

Notre convention pour la transformée de Fourier d'une fonction sommable g est $\widehat{g}(y) = \int_{\mathbb{R}} g(x)\, e^{-2i\pi xy}\, \mathrm{d}y$, où $y \in \mathbb{R}$.

Démonstration. Soit $y \in \mathbb{C}$ tel que $|\mathrm{Im}\ y| < \frac{1}{2}$, on a les égalités

$$\Phi_F(\frac{1}{2} + iy) = 2\pi \int_{\mathbb{R}} g(2\pi x)\, \frac{e^{2i\pi xy}}{\cosh \pi x}\, \mathrm{d}x = \int_{\mathbb{R}} \frac{\widehat{g}(\frac{x}{2\pi})}{\cosh \pi(x-y)}\, \mathrm{d}x.$$

En effet, la première est triviale pour tout $y \in \mathbb{C}$. La seconde est par exemple une application de la formule de Plancherel, les fonctions $x \mapsto g(2\pi x)$ et $x \mapsto \frac{e^{2i\pi xy}}{\cosh \pi x}$ étant sommables et de carré sommable sur $\mathbb{R}$, et du fait que la fonction $\frac{1}{\cosh \pi x}$ est égale à sa transformée de Fourier. On conclut car d'une part on a $\widehat{g}(z) \geq 0$ pour tout $z \in \mathbb{R}$ par hypothèse, et d'autre part on constate l'inégalité $\mathrm{Re}\, \frac{1}{\cosh \pi z} > 0$ pour tout $z \in \mathbb{C}$ tel que $|\mathrm{Im}\, z\,| < \frac{1}{2}$. □

3.17. La fonction d'Odlyzko

Suivant Odlyzko [Poi76a, §3], notons g le double du carré de convolution de la fonction $u : \mathbb{R} \to \mathbb{R}$ définie par $u(x) = \cos(\pi x)$ si $|x| \leq \frac{1}{2}$, et $u(x) = 0$ sinon. Concrètement, la fonction g est nulle hors du segment $[-1, 1]$, et pour $|x| \leq 1$ elle est donnée par la formule

$$g(x) = (1 - |x|) \cos(\pi x) + \frac{1}{\pi} \sin(\pi |x|).$$

On vérifie immédiatement que g est une fonction paire, positive, à support compact, de classe $\mathcal{C}^2$, et que l'on a $g(0) = 1$. Sa transformée de Fourier, à

savoir $2\,\widehat{u}^2$, est manifestement positive, car u est réelle, paire et sommable. En particulier, pour tout $\lambda \in \mathbb{R}_{>0}$ la fonction $\mathrm{F}_\lambda : \mathbb{R} \to \mathbb{R}$ définie par

$$\mathrm{F}_\lambda(x) = g(x/\lambda)/\cosh(x/2)$$

est une fonction test ≥ 0 satisfaisant l'hypothèse (T4) (Lemme 3.16).

Expliquons comment évaluer numériquement la forme forme linéaire $\mathrm{J}_{\mathrm{F}_\lambda}$ sur K_∞. On rappelle que $\psi(z) = \frac{\Gamma'(z)}{\Gamma(z)}$ désigne la fonction digamma. On pose également, respectivement pour $z \in \mathbb{C} - \mathbb{N}$ et $z \in \mathbb{C} - \{\pm i\pi\}$,

$$\phi(z) = \frac{1}{2}\psi(\,\frac{z+1}{2}\,) - \frac{1}{2}\psi(\,\frac{z}{2}\,) \quad \text{et} \quad \mathrm{r}(z) = 2\pi^2 \frac{e^{-z}}{(z^2+\pi^2)^2}.$$

On observera que l'on a la formule $\phi(z) = \sum_{n\geq 0} \frac{(-1)^n}{z+n}$. Nous remercions Henri Cohen de nous avoir mis sur la voie de la proposition suivante.

Proposition 3.18. *Soit λ un nombre réel > 0.*

(i) Pour tout entier $w \geq 0$ on a l'égalité

$$\mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w) = \log\,\pi - \Re\,\psi(b+\frac{i\pi}{2\lambda}) + \frac{1}{\pi}\Im\,\psi(b+\frac{i\pi}{2\lambda}) - \frac{1}{2\lambda}\Re\,\psi'(b+\frac{i\pi}{2\lambda}) + r_1(w,\lambda),$$

avec $b = \frac{1}{2} + \frac{w}{4}$ et $r_1(w,\lambda) = 2\lambda \sum_{n=0}^{\infty} \mathrm{r}(2\lambda(b+n))$.

(ii) De plus, on a l'égalité

$$\mathrm{J}_{\mathrm{F}_\lambda}(1-\epsilon_{\mathbb{C}/\mathbb{R}}) = 1 \,+\, \frac{2\pi}{\lambda}\,\Im\,\phi(1+\frac{i\pi}{\lambda}) \,+\, \frac{2\pi}{\lambda^2}\,\Im\,\phi'(1+\frac{i\pi}{\lambda}) \,+\, r_2(\lambda),$$

avec $r_2(\lambda) = 2\lambda \sum_{n=1}^{\infty} (-1)^{n+1}\, n\, \mathrm{r}(\lambda n)$.

(iii) Enfin, on a $\Phi_{\mathrm{F}_\lambda}(0) = \frac{8}{\pi^2}\lambda$ et

$$\Phi_{\mathrm{F}_\lambda}(\,\frac{1}{2}\,) \;=\; 4\,\Re\,\phi(\,\frac{1}{2}+\frac{i\pi}{\lambda}) \,-\, \frac{4}{\pi}\,\Im\,\phi(\,\frac{1}{2}+\frac{i\pi}{\lambda}) \,+\, \frac{4}{\lambda}\,\Re\,\phi'(\,\frac{1}{2}+\frac{i\pi}{\lambda}) \,+\, r_3(\lambda),$$

avec $r_3(\lambda) = 4\lambda \sum_{n=0}^{\infty} (-1)^n\, \mathrm{r}(\lambda(n+\frac{1}{2}))$.

Démonstration. Si $\alpha > 0$, on pose $h(\alpha) = \int_0^1 g(x)\, e^{-\alpha x}\mathrm{d}x$. En utilisant par exemple la définition $g = 2\,u * u$, on vérifie tout d'abord l'identité $g''(x) + \pi^2 g(x) = 2\pi|\sin \pi x|$ pour $|x| \leq 1$, puis la relation

$$h(\alpha) \;=\; \frac{\alpha}{\alpha^2+\pi^2} + 2\,\pi^2\,\frac{1+e^{-\alpha}}{(\alpha^2+\pi^2)^2} \qquad .$$

On a de plus $\int_0^\infty g(x/\lambda)\, e^{-\alpha x}\, \mathrm{d}x = \lambda\, h(\lambda\, \alpha)$.

Soit $w \geq 0$ un entier ; on pose $b = \frac{1}{2} + \frac{w}{4}$. La proposition 3.8 appliquée à la fonction $F = \mathrm{F}_\lambda$ s'écrit $\mathrm{J}_\lambda(\mathrm{I}_w) = \log(2\pi) + \sigma_{\mathrm{F}_\lambda}(1, \frac{w}{2})$. Des manipulations élémentaires conduisent à la relation

$$\sigma_{\mathrm{F}_\lambda}(1, \frac{w}{2}) = \int_0^\infty \left(\frac{2\, e^{-2bx}}{1 - e^{-2x}} - \frac{e^{-x}}{x} \right) \mathrm{d}x + \int_0^\infty (g(\frac{x}{\lambda}) - 1)\, \frac{2\, e^{-2bx}}{1 - e^{-2x}}\, \mathrm{d}x \quad .$$

Écrivons cette somme sous la forme évidente $\sigma_\lambda(1, \frac{w}{2}) = S_1 + S_2$. La formule de Gauss $\psi(z) = -\int_0^\infty \left(\frac{e^{-zx}}{1-e^{-x}} - \frac{e^{-x}}{x} \right) \mathrm{d}x$, et l'identité $\int_0^\infty \frac{e^{-\alpha x} - e^{-x}}{x} \mathrm{d}x = -\log \alpha$ pour $\alpha > 0$, entraînent l'égalité $S_1 = -\log 2 - \psi(b)$. D'autre part, le développement $\frac{e^{-2bx}}{1-e^{-2x}} = \sum_{n \geq 0} e^{-2(b+n)x}$ conduit à la relation

$$S_2 = 2\lambda \sum_{n=0}^{\infty} \left(h(2\lambda(b+n)) - \frac{1}{2\lambda(b+n)} \right) \quad .$$

On a $h = h_1 + h_2 + \mathrm{r}$ avec $h_1(\alpha) = \frac{\alpha}{\alpha^2 + \pi^2}$ et $h_2(\alpha) = \frac{2\,\pi^2}{(\alpha^2+\pi^2)^2}$. De plus, si u et v sont des réels $\neq 0$ on a les identités $\frac{u}{u^2+v^2} - \frac{1}{u} = \Re\, (\frac{1}{u+vi} - \frac{1}{u})$ et

$$\frac{2v}{(u^2+v^2)^2} = -\frac{1}{v^2}\, \Im\, (\frac{1}{u+vi} - \frac{1}{u}) - \frac{1}{v}\, \Re\, \frac{1}{(u+vi)^2}.$$

Appliquons-les à $v = \frac{\pi}{2\lambda}$ et $u = b + n$ pour tout entier $n \geq 0$ et sommons. La formule $\psi(b) - \psi(b+z) = \sum_{n \geq 0} \frac{1}{b+z+n} - \frac{1}{b+n}$ avec $z = \frac{i\pi}{2\lambda}$ entraîne alors

$$\sum_{n \geq 0} 2\lambda\; h_1(\, 2\lambda(b+n)\,) - \frac{1}{b+n} = \sum_{n \geq 0} \frac{(b+n)}{(b+n)^2 + (\frac{\pi}{2\lambda})^2} - \frac{1}{b+n} = \psi(b) - \Re\, \psi(b + \frac{i\pi}{2\lambda}).$$

De même, compte tenu de l'identité $\psi'(z) = \sum_{n \geq 0} \frac{1}{(z+n)^2}$, on trouve

$$\sum_{n \geq 0} 2\lambda\; h_2(\, 2\lambda(b+n)\,) = \frac{1}{\pi}\, \Im\, \psi(b + \frac{i\pi}{2\lambda}) - \frac{1}{2\lambda} \psi'(b + \frac{i\pi}{2\lambda}).$$

En mettant toutes les formules bout à bout, on obtient l'assertion (i). La démonstration de l'assertion (ii) est similaire. À partir de la proposition 3.8, on commence par établir l'égalité :

$$\mathrm{J}_{\mathrm{F}_\lambda}(1 - \epsilon_{\mathbb{C}/\mathbb{R}}) = 1 + \int_0^\infty \left(g(\frac{x}{2\lambda}) - 1 \right) \frac{e^{-x/2}}{(1 + e^{-x/2})^2}\, \mathrm{d}x \ .$$

Le développement $\frac{e^{-x/2}}{(1+e^{-x/2})^2} = \sum_{n\geq 1} (-1)^{n+1}\, n\, e^{-nx/2}$ permet d'écrire

$$\mathrm{J}_{\mathrm{F}_\lambda}(1-\epsilon_{\mathbb{C}/\mathbb{R}}) \;=\; 1 \,+\, 2 \sum_{n\geq 1} (-1)^{n+1}\, (\lambda n\, h(\lambda n) \;-\; 1).$$

De plus, si u et v sont des réels non nuls on a les identités

$$\frac{u^2}{u^2+v^2} - 1 \;=\; v\,\Im\,\frac{1}{u+vi} \quad \text{et} \quad \frac{2\,u\,v^2}{(u^2+v^2)^2} \;=\; -v\,\Im\,\frac{1}{(u+vi)^2}.$$

En posant $u = n\lambda$ et $v = \frac{\pi}{\lambda}$, et en observant $\phi(z+1) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{z+n}$, on a

$$2 \sum_{n\geq 1} (-1)^{n+1}\, (\lambda n\, h_1(\lambda n) \;-\; 1) \;=\; \frac{2\pi}{\lambda}\,\Im\,\phi(1+\frac{i\pi}{\lambda}),$$

puis $2\sum_{n\geq 1} (-1)^{n+1}\, \lambda n\, h_2(\lambda n) \;=\; \frac{2\pi}{\lambda^2}\,\Im\,\phi'(1+\frac{i\pi}{\lambda})$. Cela démontre le (ii). Il ne reste qu'à vérifier l'assertion (iii). Par définition de F_λ et g, on a les égalités $\Phi_{\mathrm{F}_\lambda}(0) = \int_{\mathbb{R}} g(x/\lambda)\mathrm{d}\,x = 2\lambda\,\widehat{u}(0)^2$; la valeur de $\Phi_{\mathrm{F}_\lambda}(0)$ se déduit donc de la relation immédiate $\widehat{u}(0) = \frac{2}{\pi}$. Pour déterminer $\Phi_{\mathrm{F}_\lambda}(\frac{1}{2})$, on procède comme pour les assertions (i) et (ii) à partir des identités immédiates

$$\Phi_{\mathrm{F}_\lambda}(\frac{1}{2}) = 4\int_0^\infty g(x/\lambda)\frac{e^{-x/2}}{1+e^{-x}}\mathrm{d}x = 4\lambda\sum_{n\geq 0}(-1)^n\, h(\lambda(n+1/2)).$$

□

Commentaires sur les calculs numériques effectués dans les paragraphes qui vont suivre

1) Les formules de la proposition 3.18, bien que peu esthétiques, sont très efficaces pour évaluer numériquement $\mathrm{J}_{\mathrm{F}_\lambda}$ et $\Phi_{\mathrm{F}_\lambda}(\frac{1}{2})$, et ce avec une précision arbitraire. Dans nos applications, nous aurons $0 \leq w \leq 46$ et $\lambda = \log N$ avec $2 \leq N \leq 100$.

2) John L. Spouge a élaboré en 1994 un remarquable algorithme pour déterminer les valeurs des fonctions gamma, ψ (digamma) et ψ' (trigamma). Ces fonctions sont implémentées dans `PARI`. Cependant, Henri Cohen nous a fait savoir que `PARI` utilise pour leur calcul la formule d'Euler-MacLaurin, donc les nombres de Bernoulli, et qu'après le calcul d'une première valeur celui des suivantes est accéléré par le stockage des nombres de Bernoulli.

3) Les trois fonctions $r_1(w,\lambda)$, $r_2(\lambda)$ et $r_3(\lambda)$ qui apparaissent dans l'énoncé 3.18 sont définies comme des sommes de séries ; on estime ci-dessous "les restes" $\sum_{n=N+1}^{\infty}$ de ces séries.

3.1) On a l'inégalité

$$0 \;\leq\; r_1(w,\lambda) - 2\lambda \sum_{n=0}^{N} \mathrm{r}(2\lambda(b+n)) \;\leq\; \frac{2\lambda \mathrm{r}(2\lambda(b+N+1))}{1-e^{-2\lambda}} \qquad ;$$

cette inégalité résulte de ce que l'on a

$$0 \;\leq\; \mathrm{r}(2\lambda(b+n)) \;\leq\; e^{-2\lambda(n-N-1)}\mathrm{r}(2\lambda(b+N+1))$$

pour tout n avec $n \geq N+1$.

3.2) Comme la fonction d'une variable réelle $x \mapsto x\,\mathrm{r}(x)$ est à valeurs positives et décroissante pour $x \geq 0.773$, on a l'inégalité

$$0 \;\leq\; (-1)^N \left(r_2(\lambda) - 2\lambda \sum_{n=1}^{N} (-1)^{n+1} n\,\mathrm{r}(\lambda n) \right) \;\leq\; 2\lambda(N+1)\mathrm{r}(\lambda(N+1)) \qquad ,$$

sous l'hypothèse $\lambda(N+1) \geq 0.773$.

3.3) Comme la fonction d'une variable réelle $x \mapsto \mathrm{r}(x)$ est à valeurs positives et décroissante, on a l'inégalité

$$0 \;\leq\; (-1)^{N+1} \left(r_3(\lambda) - 4\lambda \sum_{n=0}^{N} (-1)^n \mathrm{r}(\lambda(n+\frac{1}{2})) \right) \;\leq\; 4\lambda \mathrm{r}(\lambda(N+\frac{3}{2})) \qquad .$$

4) Les calculs effectués à l'aide des formules de la proposition 3.18 sont confirmés, avec une précision arbitraire, par les routines d'intégration numérique de `PARI`.

5) La fonction $w \mapsto \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$, λ fixé, est décroissante. On s'en convainc en invoquant le point (iii) de la proposition-définition 3.8 qui montre que sous les hypothèses $F \geq 0$ et $w' \geq w$ la différence $\mathrm{J}_F(\mathrm{I}_w) - \mathrm{J}_F(\mathrm{I}_{w'})$ est l'intégrale sur $[0,+\infty[$ d'une fonction positive ou nulle.

De même, la fonction $\lambda \mapsto \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$, w fixé, est croissante. En effet, comme la fonction d'Odlyzko est décroissante sur $[0,+\infty[$, le point (iii) de la proposition-définition 3.8 montre que sous l'hypothèse $\lambda \leq \lambda'$ la différence $\mathrm{J}_{\mathrm{F}_{\lambda'}}(\mathrm{I}_w) - \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$ est l'intégrale sur $[0,+\infty[$ d'une fonction positive ou nulle (on observera que l'on a $\mathrm{F}_\lambda(0) = 1$ pour tout λ).

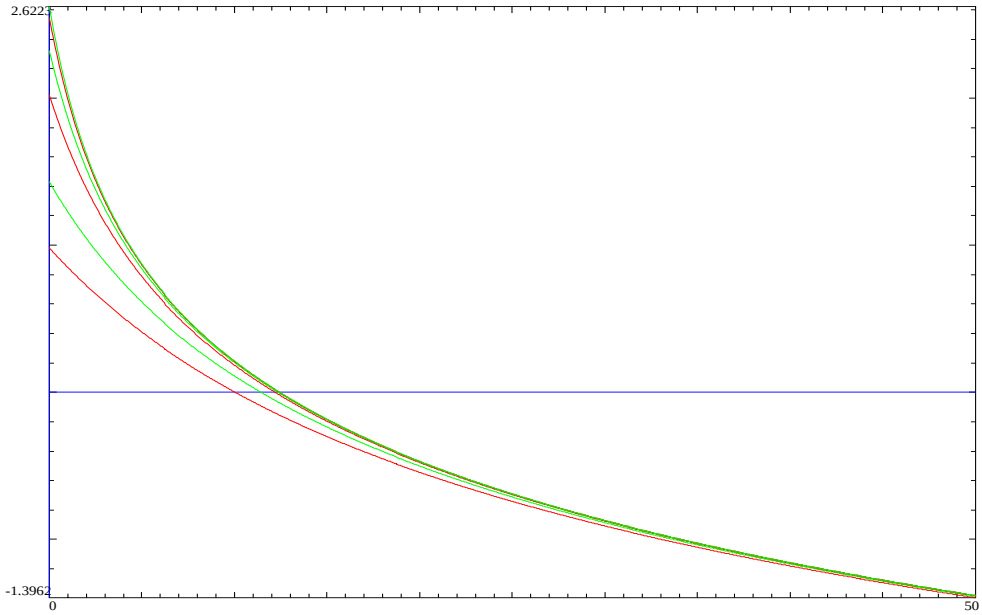

FIGURE IX.1 – Graphe de la fonction $w \mapsto \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$ sur l'intervalle $0 \leq w \leq 50$, pour les paramètres $\lambda = \log 2$, $\log 3$, $\log 8$, $\log 20, \log 60$ et $\log 100$.

Ce qui précéde implique que l'on l'encadrement $-1.40 \leq \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w) \leq 2.63$ pour $\log 2 \leq \lambda \leq \log 100$ et $0 \leq w \leq 50$. On trace ci-contre le graphe de la fonction $w \mapsto \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$ pour quelques valeurs du paramètre λ.

6) Dans l'appendice de [MES86] Mestre décrit un calcul de $\sigma_{\mathrm{F}_\lambda}(1, \frac{1}{2})$ (autrement dit $\mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_1) - \log 2\pi$) pour $\lambda < \pi$ par une méthode totalement différente de la nôtre ; la restriction $\lambda < \pi$ tient à ce que Mestre utilise implicitement le développement en série entière de la fonction holomorphe $\frac{z}{e^z - 1}$ dans le disque $|z| < 2\pi$.

3.19. Début de démonstration du théorème 3.2 : cas $w \leq 20$

Pour tout entier $w \geq 0$, on considère le sous-groupe de K_∞ défini de la manière suivante :

$$\mathrm{K}_\infty^{\leq w} = \begin{cases} \left(\bigoplus_{1\leq j\leq w/2} \mathbb{Z}\,\mathrm{I}_{2j}\right) \oplus \mathbb{Z}\,1 \oplus \mathbb{Z}\,\epsilon_{\mathbb{C}/\mathbb{R}}, & \text{si } w \equiv 0 \bmod 2, \\ \bigoplus_{1\leq j\leq \frac{w+1}{2}} \mathbb{Z}\,\mathrm{I}_{2j-1}\,, & \text{si } w \equiv 1 \bmod 2. \end{cases}$$

L'intérêt de cette définition est que si $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ est de poids motivique w, on a $\mathrm{L}(\pi_\infty) \in \mathrm{K}_\infty^{\leq w}$ (Proposition VIII.2.13). On dispose de deux autres contraintes simples sur $\mathrm{L}(\pi_\infty)$. D'une part, c'est un élément effectif de K_∞. D'autre part, on a la relation $\det \mathrm{L}(\pi_\infty) = 1$. On rappelle l'identité $\det \mathrm{I}_v = \epsilon_{\mathbb{C}/\mathbb{R}}^{v+1}$ pour tout $v \geq 0$.

Le principe général de la démonstration va consister à montrer que sous une hypothèse convenable sur π_∞, il n'existe pas – ou peu – de représentations $\pi \in \Pi_{\mathrm{alg}}$ de poids motivique ≤ 22, et ce à l'aide des inégalités données par la proposition 3.9 appliquée aux fonctions tests introduites au §3.17. Dans toute cette partie, λ désignera donc un nombre réel > 0, et l'on considère la fonction test associée F_λ définie au §3.17. Dans la démonstration, nous ferons un usage systématique de la forme bilinéaire $\mathrm{B}_\infty^{\mathrm{F}_\lambda}$ sur K_∞ introduite au §3.5. Nous aurons notamment besoin d'évaluer explicitement cette forme bilinéaire, ce que nous ferons bien entendu à l'aide de l'ordinateur, en utilisant les formules décrites au §3.17. Nous renvoyons le lecteur à la feuille de calculs [CL `PARI`] donnée en annexe pour une justification des calculs numériques que nous ferons ci-dessous. Afin d'acquérir une intuition sur la méthode, nous allons commencer par démontrer le cas $n = 2$ du théorème. La représentation triviale étant le seul élément de $\Pi(\mathrm{PGL}_1) = \Pi_{\mathrm{cusp}}(\mathrm{PGL}_1)$, observons qu'il n'y a rien à démontrer pour $n = 1$!

Cas $n = 2$ ou $w \leq 10$

Supposons donnée une représentation $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_2)$ de poids motivique w. La condition $\det \mathrm{L}(\pi_\infty) = 1$ montre qu'il y a deux cas : soit w est impair et $\mathrm{L}(\pi_\infty) = \mathrm{I}_w$, soit $w = 0$ et l'on a $\mathrm{L}(\pi_\infty) = 2 \cdot 1$ ou $\mathrm{L}(\pi_\infty) = 2 \cdot \epsilon_{\mathbb{C}/\mathbb{R}}$.

Si w est impair, la proposition 1.5 assure que π est la représentation engendrée par une unique forme modulaire propre et normalisée de poids $w+1$ pour le groupe $\mathrm{SL}_2(\mathbb{Z})$; réciproquement, toute telle forme engendre bien évidemment un tel π. Autrement dit, compte tenu de la définition §3.13 nous avons pour tout w impair ≥ 1 l'égalité :

$$\mathrm{m}(\mathrm{I}_w) = \dim \mathrm{S}_{w+1}(\mathrm{SL}_2(\mathbb{Z}))$$

Ainsi, le cas particulier $n = 2$ et poids motivique $\neq 0$ du théorème 3.2 est conséquence de la description bien connue de $\mathrm{S}_{w+1}(\mathrm{SL}_2(\mathbb{Z}))$ [Ser70, Ch. VII]. De telles descriptions de $\Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ n'existant pas en dimension $n > 2$, il y a un intérêt à expliquer comment procéder autrement, si possible. Dans ce qui suit, on se propose de démontrer différemment que $\mathrm{S}_{w+1}(\mathrm{SL}_2(\mathbb{Z}))$ est nul si $w < 11$ ou $w = 13$, et de dimension ≤ 1 si $15 \leq w \leq 21$, à l'aide du corollaire 3.10.

La fonction F_λ étant continue et à support dans $[-\lambda, \lambda]$, observons que pour tous $\pi, \pi' \in \Pi_{\mathrm{alg}}$ on a

$$\widetilde{\mathrm{B}}_f^{\mathrm{F}_\lambda}(\pi, \pi') = \sum_{p^k < e^\lambda} \mathrm{F}_\lambda(k \log p) \frac{\log p}{p^{k/2}} \ \overline{\mathrm{tr}\,(\mathrm{c}_p(\pi)^k)} \ \mathrm{tr}\,(\mathrm{c}_p(\pi')^k). \tag{3.2}$$

En particulier, on constate $\mathrm{B}_f^{\mathrm{F}_\lambda} = 0$, i.e. $\mathrm{B}^{\mathrm{F}_\lambda} = \mathrm{B}_\infty^{\mathrm{F}_\lambda}$, pour $\lambda \leq \log 2$. On considère maintenant $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_2)$ de poids motivique impair w et $\pi' = 1 \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_1)$, auquel cas on a $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(\pi, 1) = \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_w)$. L'inégalité du corollaire 3.10 entraîne donc en particulier

$$\mathrm{J}_{\mathrm{F}_{\log 2}}(\mathrm{I}_w) \leq 0.$$

La table IX.3 donne l'évaluation numérique à 10^{-2} près de $\mathrm{J}_{\mathrm{F}_{\log 2}}(\mathrm{I}_w)$, pour $1 \leq w \leq 21$ impair. Elle contredit l'inégalité ci-dessus si $w < 11$: la représentation π n'existe pas. Soulignons que cet argument n'est pas nouveau : c'est par exemple exactement la méthode utilisée par Mestre dans [Mes86]. Sa précision est assez étonnante, puisque l'on sait bien que l'on a $\mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z})) \neq 0$. Nous verrons plus loin de nombreux autres exemples de la précision fascinante des formules explicites.

w	1	3	5	7	9	11	13	15	17	19	21
$\mathrm{J}_{\mathrm{F}_{\log 2}}(\mathrm{I}_w)$	0.85	0.61	0.41	0.23	0.07	−0.06	−0.19	−0.30	−0.40	−0.50	−0.59

Table IX.3 – Valeurs à 10^{-2} près de $\mathrm{J}_{\mathrm{F}_{\log 2}}(\mathrm{I}_w)$ pour $1 \leq w \leq 21$ impair.

Comme le remarque essentiellement Mestre [Mes86, Remarque 1 §III], l'argument précédent est de portée plus vaste : si $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ est de poids motivique ≤ 10, alors $n = 1$ et π est la représentation triviale. En effet, si $\pi \neq 1$ on a l'inégalité $\mathrm{B}_\infty^{\mathrm{F}_{\log 2}}(\pi, 1) \leq 0$ alors que l'on vérifie numériquement $\mathrm{B}_\infty^{\mathrm{F}_{\log 2}}(V, 1) = \mathrm{J}_{\mathrm{F}_{\log 2}}(V) > 0.02$ pour $V = 1, \epsilon_{\mathbb{C}/\mathbb{R}}$ et I_w pour $w < 11$.

Expliquons maintenant comment aller plus loin dans le cas $n = 2$, à commencer par éliminer le cas $w = 13$. Comme tout élément de $\Pi(\mathrm{PGL}_2)$, la

représentation π est autoduale ; on a donc $\mathrm{L}(s,\pi) = \varepsilon(\pi)\mathrm{L}(1-s,\pi)$ avec $\varepsilon(\pi) = \varepsilon(\mathrm{I}_w) = i^{w+1}$. Ce facteur epsilon vaut -1 si $w \equiv 1 \bmod 4$. D'après le corollaire 3.10, on doit donc avoir

$$\mathrm{J}_{\mathrm{F}_{\log 2}}(\mathrm{I}_w) \leq -\frac{1}{2}\Phi_{\mathrm{F}_{\log 2}}(\,\frac{1}{2}\,)$$

pour $w \equiv 1 \bmod 4$. Une évaluation numérique montre que le nombre $\frac{1}{2}\Phi_{\mathrm{F}_{\log 2}}(\,\frac{1}{2}\,)$ vaut 0.28 à 10^{-2} près. La table précédente montre donc également que π n'existe pas pour $w = 13$.

Montrons maintenant $\mathrm{m}(\mathrm{I}_w) \leq 1$ pour $w \leq 21$. On a

$$\mathrm{m}(w)\ \mathrm{B}_\infty^{\mathrm{F}_\lambda}(\mathrm{I}_w,\mathrm{I}_w)\ \leq \Phi_{\mathrm{F}_\lambda}(0) \quad \text{(on rappelle } \Phi_{\mathrm{F}_\lambda}(0) = \frac{8}{\pi^2}\,\lambda\ )$$

pour tout $\lambda > 0$ d'après le corollaire 3.14. D'autre part, on a

$$\mathrm{B}_\infty^{\mathrm{F}_\lambda}(\mathrm{I}_w,\mathrm{I}_w)\ =\ \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_{2w}) + \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_0)$$

d'après la relation $\mathrm{I}_u \otimes \mathrm{I}_v = \mathrm{I}_{u+v} + \mathrm{I}_{|u-v|}$. L'inégalité ci-dessus s'avère remarquablement bonne expérimentalement pour des petites valeurs de w. Par exemple, lorsque $\lambda = \log 8$ on vérifie numériquement $\mathrm{m}(\mathrm{I}_{11}) \leq 1.17$, $\mathrm{m}(\mathrm{I}_{15}) \leq 1.48$, $\mathrm{m}(\mathrm{I}_{17}) \leq 1.66$, $\mathrm{m}(\mathrm{I}_{19}) \leq 1.86$ et $\mathrm{m}(\mathrm{I}_{21}) \leq 2.08$. On en déduit les inégalités annoncées $\mathrm{m}(\mathrm{I}_w) \leq 1$ pour $w \leq 19$, ainsi que $\mathrm{m}(\mathrm{I}_{21}) \leq 2$. Cette dernière égalité ne semble toutefois pas améliorable en considérant simplement d'autres valeurs de λ.

Pour conclure $\mathrm{m}(\mathrm{I}_{21}) \leq 1$ nous allons utiliser le corollaire 3.15 (ii) appliqué à $V = 1$ et $V' = \mathrm{I}_{21}$. On effet, on a $\mathrm{m}(1) = \mathrm{m}^\perp(1) = 1$, $\mathrm{m}(\mathrm{I}_{21}) = \mathrm{m}^\perp(\mathrm{I}_{21})$, et $\varepsilon(\mathrm{I}_{21}) = -1$. On en déduit pour tout $\lambda > 0$ l'inégalité

$$\frac{1}{2}\,\Phi_{\mathrm{F}_\lambda}(\frac{1}{2})\ + \mathrm{J}_{\mathrm{F}_\lambda}(\mathrm{I}_{21})\ \leq \sqrt{(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{J}_{\mathrm{F}_\lambda}(1))\,(\,\frac{\Phi_{\mathrm{F}_\lambda}(0)}{\mathrm{m}(\mathrm{I}_{21})} - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(\mathrm{I}_{21},\mathrm{I}_{21}))}.$$

Mais pour $\lambda = \log 6$ on vérifie qu'à 10^{-2} près le terme de gauche vaut 0.17, alors que celui de droite vaut 0.13 si $\mathrm{m}(\mathrm{I}_{21}) = 2$ (et 0.51 si $\mathrm{m}(\mathrm{I}_{21}) = 1$!). $\square$

Cas w impair ≤ 19

Notre but dans ce qui suit est de démontrer que si $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ est de poids motivique ≤ 19, et si $n > 2$, alors $n = 4$ et π est l'unique représentation autoduale telle que $\mathrm{L}(\pi_\infty) = \mathrm{I}_{19} \oplus \mathrm{I}_{17}$. Notre point de départ est le résultat suivant.

Lemme 3.20. *Si $\lambda = \log 9$, la restriction de $\mathrm{B}_\infty^{\mathrm{F}_\lambda}$ à $\mathrm{K}_\infty^{\leq 19}$ est définie positive.*

Si $w \geq 0$, nous noterons $\mathrm{Gram}(w, \lambda)$ la matrice de Gram de la forme bilinéaire $\mathrm{B}_\infty^{\mathrm{F}_\lambda}$ sur $\mathrm{K}_\infty^{\leq w}$ dans la $\mathbb{Z}$-base naturelle définissant $\mathrm{K}_\infty^{\leq w}$, à savoir :

– dans le cas où w est impair, les I_v avec $1 \leq v \leq w$ et v impair,

– dans le cas où w est pair, les représentations 1, $\epsilon_{\mathbb{C}/\mathbb{R}}$ et I_v avec $0 \leq v \leq w$.

Démonstration. Soit $B = \mathrm{Gram}(19, \log 9)$. Les formules de la proposition 3.18 (et le logiciel `PARI`) permettent de calculer les coefficients de B, et de $\mathrm{Gram}(w, \lambda)$ en général, avec une précision théoriquement arbitraire (dans la feuille de calculs [CL `PARI`] fournie, plus de 20 chiffres significatifs), et l'on constate que B est bien définie positive. L'argument que nous dégageons ci-dessous montre que nous n'avons besoin en fait que de très peu de chiffres significatifs ; cet argument sera surtout utile dans la démonstration du lemme 3.22, où il s'agira de déterminer les vecteurs $v \in \mathrm{K}_\infty^{\leq 19}$ tels que $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(v, v)$ est inférieur à une certaine constante.

On constate d'abord numériquement que tous les coefficients de B sont de valeur absolue dans l'intervalle $]0.01, 3.48[$. Soit $A \in 10^{-4}\,\mathrm{M}_{10}(\mathbb{Z})$ la matrice symétrique obtenue en arrondissant l'approximation de B donnée par l'ordinateur à l'élément le plus proche de $10^{-4}\,\mathbb{Z}$, de sorte que la matrice $A - B$ ait tous ses coefficients $\leq 10^{-4}$ en valeur absolue. Un calcul exact fait par l'ordinateur démontre que A est définie positive (il suffit d'appliquer le critère de Sylvester). Soit $||.||$ la norme sur $\mathrm{M}_n(\mathbb{R})$ subordonnée à la norme $\sup_i |x_i|$ sur $\mathbb{R}^n$, de sorte que $||(m_{i,j})|| = \sup_i \sum_j |m_{i,j}|$. On constate $||A^{-1}|| \leq 3.23$ et l'on a de plus $||A - B|| \leq 10 \cdot 10^{-4} = 10^{-3}$. Cela entraîne que le rayon spectral de $A^{-1}(A - B)$ est ≤ 0.00323, et en particulier que B est définie positive d'après le lemme 3.21. □

Lemme 3.21. *Soient V un $\mathbb{R}$-espace vectoriel de dimension finie, b_1, b_2 deux formes bilinéaires symétriques sur V, $e = (e_1, \ldots, e_n)$ une base de V, et M_i la matrice de Gram de b_i dans la base e. On suppose b_2 définie positive. Pour tout $x \in V$ on a l'inégalité*

$$|b_1(x, x) - b_2(x, x)| \;\leq\; \rho(M_2^{-1}(M_1 - M_2))\, b_2(x, x),$$

où $\rho(M)$ désigne le rayon spectral de la matrice M. Si l'on a de plus l'inégalité $\rho(M_2^{-1}(M_1 - M_2)) < 1$ alors b_1 est définie positive, et on a pour tout $x \in V$

$$b_2(x, x) \leq (1 - \rho(M_2^{-1}(M_1 - M_2)))^{-1}\, b_1(x, x).$$

Démonstration. C'est une conséquence classique de la diagonalisablilité des endomorphismes autoadjoints d'un espace euclidien. □

Lemme 3.22. *Soit* $V \in \mathrm{K}_\infty^{\leq 19}$ *effectif et tel que* $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V,V) \leq \frac{8\log 9}{\pi^2}$, *alors :*

(i) soit $V = \mathrm{I}_w$ *avec* $9 \leq w \leq 19$,

(ii) soit $V = \mathrm{I}_{19} + \mathrm{I}_v$ *avec* $5 \leq v \leq 13$.

Démonstration. Le lemme 3.20 assure qu'il n'existe qu'un nombre fini d'éléments non nuls V dans le "réseau" $\mathrm{K}_\infty^{\leq 19}$ tels que $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V,V) \leq \frac{8\log 9}{\pi^2}$. Il ne reste qu'à les énumérer, ce que l'on va faire en utilisant l'algorithme de Fincke et Pohst [FP85] implémenté dans `PARI` (commande `qfminim`). Pour ne pas à avoir à justifier les erreurs d'arrondis sur l'algorithme sus-cité, il est commode de réutiliser l'approximation $A \in 10^{-4}\,\mathrm{M}_{10}(\mathbb{Z})$ de $\mathrm{Gram}(19, \log 9)$ introduite dans la démonstration du lemme 3.20. Soit $\mathrm{q}_A : \mathbb{Z}^{10} \to \frac{1}{10^4}\mathbb{Z}$ la forme quadratique définie positive $x \mapsto {}^{\mathrm{t}}xAx$. Si $V \in \mathrm{K}_\infty$ vérifie $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V,V) \leq \frac{8\log 9}{\pi^2}$, alors ses coordonnées $(x_1, x_3, \ldots, x_{19})$ dans la base $\mathrm{I}_1, \ldots, \mathrm{I}_{19}$ vérifient

$$10^4\,\mathrm{q}_A(x_1, \ldots, x_{19}) \leq 10^4\,(1 - 0.00323)^{-1} \cdot \frac{8\log 9}{\pi^2} < 17868$$

d'après le lemme 3.21. L'algorithme de Fincke et Pohst assure qu'il existe exactement 24 couples $\pm(x_i) \in \mathbb{Z}^{10}$ vérifiant cette inégalité, et nous en donne la liste. On ne retient bien entendu parmi ceux-ci que les éléments $x = (x_i)$ appartenant à $\mathbb{N}^{10}$ (correspondant à des V effectifs), il ne reste que 11 tels éléments, listés dans l'énoncé. □

Remarque 3.23. Précisons que 9 n'est pas le plus petit entier $m \geq 2$ tel que $\mathrm{Gram}(19, \log m)$ soit définie positive (et encore moins le seul !). Par exemple tout entier $5 \leq m \leq 100$ conviendrait. Néanmoins, ce choix $\log(9)$, obtenu par tâtonnement, a l'avantage de minimiser la taille de la liste obtenue dans l'énoncé du lemme 3.22.

Supposons maintenant que $\pi \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_n)$ est de poids motivique impair $w \leq 19$, et posons $V = \mathrm{L}(\pi_\infty) \in \mathrm{K}_\infty^{\leq 19}$. Le corollaire 3.12 (i) montre que l'on a $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V,V) \leq \frac{8\log 9}{\pi^2}$, de sorte que V est dans la liste donnée dans le lemme ci-dessus. On peut supposer $n = \dim V > 2$, car le cas $n = 2$ a déjà été traité plus haut. On en déduit $n = 4$, $w = 19$ et $V = \mathrm{I}_{19} + \mathrm{I}_v$ avec $5 \leq v \leq 13$ et v impair. On veut montrer $v = 7$ et l'unicité de la représentation π. Démontrons d'abord que π est unique si elle existe.

Lemme 3.24. *Pour tout* $v \in \{5, 7, 9, 11, 13\}$ *on a* $\mathrm{m}(\mathrm{I}_{19} + \mathrm{I}_v) \leq 1$.

Démonstration. On applique le corollaire 3.14. Il suffit de voir que pour $V = \mathrm{I}_{19} + \mathrm{I}_v$, avec v comme dans l'énoncé, on a

$$\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V, V) > \frac{1}{2}\,\frac{8\log 9}{\pi^2}.$$

Mais un calcul numérique montre qu'à 10^{-2} près on a $\frac{1}{2}\,\frac{8\log 9}{\pi^2} \simeq 0.89$ alors que le terme de gauche de l'inégalité ci-dessus vaut 1.65, 1.47, 1.42, 1.49 ou 1.70 lorsque v vaut respectivement $5, 7, 9, 11$ ou 13. □

Lemme 3.25. *Soit $V \in \mathrm{K}_\infty$. Supposons qu'il existe une unique représentation $\pi \in \Pi_{\mathrm{alg}}$ telle que $\mathrm{L}(\pi_\infty) = V$. Alors π est autoduale. Plus généralement, on a $\mathrm{m}(V) \equiv \mathrm{m}^\perp(V) \bmod 2$.*

Démonstration. En effet, si $\pi \in \Pi_{\mathrm{alg}}$ on a également $\pi^\vee \in \Pi_{\mathrm{alg}}$, ainsi que les égalités $\mathrm{L}((\pi^\vee)_\infty) = \mathrm{L}(\pi_\infty)^* = \mathrm{L}(\pi_\infty)$. □

Pour achever la démonstration du théorème 3.2 dans le cas w impair ≤ 19, il reste à démontrer qu'il n'existe pas de représentation autoduale $\pi \in \Pi_{\mathrm{alg}}$ telle que $\mathrm{L}(\pi_\infty) = \mathrm{I}_{19} + \mathrm{I}_v$ avec $v \in \{5, 9, 11, 13\}$. Une première manière de procéder serait d'utiliser la proposition 1.4 (iii) ainsi que la table IX.1 (cette table contient les renseignements requis car $19 - v \geq 6$ dans tous les cas). Ce n'est toutefois pas nécessaire, car nous allons voir que cela se déduit du corollaire 3.15 et de l'existence des représentations $1, \Delta_{11}$ et Δ_{15}. Pour usage futur, explicitons le critère suivant.

Scholie 3.26. *Soient $V, V' \in \mathrm{K}_\infty$ et λ un réel > 0. On pose*

$$\mathrm{t}(V, V', \lambda) = \sqrt{|(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V))(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V', V'))|} + \frac{\varepsilon(V \otimes V') - 1}{4}\,\Phi_{\mathrm{F}_\lambda}(\tfrac{1}{2}) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V')$$

Supposons que V et V' sont distincts, effectifs, et vérifient $\mathrm{m}^\perp(V) \geq 1$ et $\mathrm{m}^\perp(V') \geq 1$. Alors on a $\mathrm{t}(V, V', \lambda) \geq 0$. En particulier, si $\mathrm{m}(V) = \mathrm{m}(V') = 1$ on a $\mathrm{t}(V, V', \lambda) \geq 0$.

Démonstration. La première assertion est une conséquence immédiate du point (ii) du corollaire 3.15. La seconde découle de la première et du lemme 3.25. □

v \ π'	1	Δ_{11}	Δ_{15}	Δ_{17}	Δ_{19}	Δ_{21}
13	0.141	0.074	-0.006	0.166	0.088	0.990
11	0.697	-0.492	0.396	0.498	0.376	1.251
9	-0.094	-0.046	0.636	0.689	0.536	1.388
7	0.308	0.223	0.762	0.778	0.597	1.430
5	-0.660	0.359	0.771	0.751	0.546	1.357

TABLE IX.4 – Valeur à 10^{-3} près de $\mathrm{t}(\mathrm{I}_{19}+\mathrm{I}_v, \mathrm{L}(\pi'_\infty), \log 5)$.

Nous savons que l'on a $\mathrm{m}(V)=1$ pour $V=1$ ou $V=\mathrm{L}((\Delta_w)_\infty)$ pour $w \leq 21$. Observons la table IX.4. On constate que si $v \neq 7$, il existe toujours une représentation $\pi' \in \{1, \Delta_{11}, \Delta_{15}\}$ telle que $\mathrm{t}(\mathrm{I}_{19}+\mathrm{I}_v, \mathrm{L}(\pi'_\infty), \log 5) < 0$. Par le scholie 3.26, cela démontre $\mathrm{m}(\mathrm{I}_{19}+\mathrm{I}_v) \neq 1$, et conclut donc la démonstration. $\square$

Remarque 3.27. Le paramètre $\lambda = \log 5$ a été choisi par tâtonnement. Une variation de ce paramètre montre que l'existence d'une représentation dans le cas $v=7$ paraît assez miraculeuse de ce point de vue. La propriété qui semble importante est que les écarts successifs entre les 4 poids, à savoir $\frac{19-v}{2}, v$ et $\frac{19-v}{2}$, sont presque égaux pour $v=7$.

CAS w PAIR ≤ 20

On procède de manière strictement similaire au cas w impair ≤ 19, c'est pourquoi nous donnerons moins de détails.

Lemme 3.28. *La restriction de* $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}$ *à* $\mathrm{K}_\infty^{\leq 20}$ *est définie positive. Soit* $V \in \mathrm{K}_\infty^{\leq 20}$ *effectif, de déterminant* 1*, et vérifiant* $\mathrm{B}_\infty^{\mathrm{F}_{\log 9}}(V,V) \leq \Phi_{\mathrm{F}_{\log 9}}(0)$*, alors :*

(i) soit $V=1$*,*

(ii) soit $V = \mathrm{I}_w + \epsilon_{\mathbb{C}/\mathbb{R}}$ *avec* $w = 18$ *ou* 20*,*

(iii) soit $V = \mathrm{I}_w + \mathrm{I}_v$ *avec soit* $w=18$ *et* $8 \leq v \leq 10$*, soit* $w=20$ *et* $4 \leq v \leq 14$*,*

(iv) soit $V = \mathrm{I}_{20} + \mathrm{I}_v + 1$ *avec* $10 \leq v \leq 16$*.*

De plus, on a $\mathrm{m}(V) \leq 1$*.*

Démonstration. Les deux premières assertions se déduisent d'une étude de la matrice $\mathrm{Gram}(20, \log 9)$ analogue à celle conduisant aux démonstrations des lemmes 3.20 et 3.22 : voir la feuille de calculs en annexe [CL `PARI`]. Pour les 15 éléments V de l'énoncé, on vérifie que l'on a $\mathrm{m}(V) \leq 1.6$ à l'aide du corollaire 3.14 appliqué à $\lambda = \log 9$, d'où la dernière assertion. $\square$

Il en résulte que si $\pi \in \Pi_{\mathrm{alg}}$ est de poids motivique pair ≤ 20, alors $V = \mathrm{L}(\pi_\infty)$ est dans la liste ci-dessus, $\mathrm{m}(V) \leq 1$ et π est autoduale. On élimine les possibilités

$$V = \mathrm{I}_{18} + \mathrm{I}_{10}, \quad \mathrm{I}_{20} + \mathrm{I}_{10} + 1 \quad \text{ou} \quad \mathrm{I}_{20} + \mathrm{I}_{16} + 1$$

à l'aide du critère $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V) \leq \Phi_{\mathrm{F}_\lambda}(0)$ en prenant respectivement $\lambda = \log 10$, $\log 16$ et $\log 16$. Mentionnons que si $V = \mathrm{I}_{18} + \mathrm{I}_{10}$ et $\lambda = \log 10$, la quantité $\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V)$ vaut -0.00012 à 10^{-5} près, ce qui passe assez juste !

Il reste à montrer que π n'existe pas si $V \neq 1$. Par chance, nous y parvenons à l'aide du scholie 3.26, appliqué dans les cas particuliers indiqués dans la table IX.5. Cela termine la démonstration du théorème 3.2 lorsque le poids motivique w est pair ≤ 20.

V	π'	V	π'	V	π'
$\mathrm{I}_{18} + \epsilon_{\mathbb{C}/\mathbb{R}}$	1	$\mathrm{I}_{20} + \mathrm{I}_{12}$	Δ_{15}	$\mathrm{I}_{20} + \mathrm{I}_4$	1
$\mathrm{I}_{20} + \epsilon_{\mathbb{C}/\mathbb{R}}$	1	$\mathrm{I}_{20} + \mathrm{I}_{10}$	1	$\mathrm{I}_{20} + \mathrm{I}_{14} + 1$	Δ_{15}
$\mathrm{I}_{18} + \mathrm{I}_8$	Δ_{11}	$\mathrm{I}_{20} + \mathrm{I}_8$	1	$\mathrm{I}_{20} + \mathrm{I}_{12} + 1$	1
$\mathrm{I}_{20} + \mathrm{I}_{14}$	Δ_{15}	$\mathrm{I}_{20} + \mathrm{I}_6$	Δ_{11}		

TABLE IX.5 – Des couples (V, π') vérifiant $\mathrm{t}(V, \mathrm{L}(\pi'_\infty), \log 5) < -0.05$.

3.29. Interlude : un critère géométrique

Lemme 3.30. *Soient E un espace euclidien, $m \geq 1$ un entier, $x_0, x_1, \ldots, x_m$ des éléments de E, et $C_0, C_1, \ldots, C_m$ des nombres réels. On suppose que pour tout $i = 0, \ldots, m$ on a l'inégalité $x_0 \cdot x_i \leq C_i$. Alors :*

(i) On a $C_0 \geq 0$ et, pour tout $i = 1, \ldots, m$, $C_i + \sqrt{C_0\,(x_i \cdot x_i)} \geq 0$.

Soient $G = (x_i \cdot x_j)_{1 \leq i,j, \leq m} \in \mathrm{M}_m(\mathbb{R})$ la matrice de Gram des vecteurs $x_1, \ldots, x_m$ et C le vecteur colonne $(C_i)_{1 \leq i \leq m} \in \mathbb{R}^m$. On suppose $\mathrm{dét}(G) \neq 0$, i.e. que les vecteurs $x_1, \ldots, x_m$ sont linéairement indépendants. Alors l'une des deux assertions suivantes est vérifiée :

(ii) au moins une des coordonnées du vecteur $G^{-1}C$ est > 0.

(ii)' on a l'inégalité (entre nombres réels) ${}^{\mathrm{t}}C\, G^{-1}\, C \;\leq\; C_0$.

Démonstration. L'inégalité $C_0 \geq 0$ est évidente. De plus, pour $i = 1, \ldots, m$ l'inégalité de Cauchy-Schwarz donne

$$C_i \geq x_0 \cdot x_i \geq -|x_0 \cdot x_i| \geq -\sqrt{(x_0 \cdot x_0)(x_i \cdot x_i)} \geq -\sqrt{C_0 \;\; x_i \cdot x_i}.$$

Vérifions la seconde assertion. Soit $(x_i^*)_{1 \leq i \leq m}$ la base duale de $(x_i)_{1 \leq i \leq m}$ dans l'espace euclidien $F = \mathrm{Vect}_{\mathbb{R}}(x_1, \ldots, x_m)$. Soit $H = (h_{i,j}) \in \mathrm{M}_m(\mathbb{R})$ la matrice définie par les égalités $x_j^* = \sum_{i=1}^m h_{i,j} x_i$ pour $j = 1, \ldots, m$. Par définition de la base duale, H est également la matrice de Gram $(x_i^* \cdot x_j^*)$ et on a la relation $H = G^{-1}$. Ainsi, les coefficients du vecteur $G^{-1}\, C = H\, C$ ne sont autres que les produits scalaires $x_i^* \cdot v$, $i = 1, \ldots, m$, avec

$$v \;:=\; \sum_{j=1}^m C_j\, x_j^*.$$

Supposons que l'assertion (ii) n'est pas satisfaite, i.e. $x_i^* \cdot v \leq 0$ pour tout $i = 1, \ldots, m$. Nous allons voir que l'on a $x_0 \cdot x_0 \geq v \cdot v$, ce qui est l'assertion (ii)'. Le vecteur x_0 s'écrit de manière unique sous la forme $x_0 = v - \sum_{i=1}^m t_i x_i^* + w$ avec $w \in F^\perp$ et $t_i \in \mathbb{R}$ pour $i = 1, \ldots, m$. Si $i = 1, \ldots, m$, la condition $x_0 \cdot x_i \leq C_i$ équivaut à $t_i \geq 0$. Posons $\|x\|^2 = x \cdot x$ pour $x \in E$. On conclut en contemplant l'égalité suivante :

$$\|x_0\|^2 \;=\; \|v\|^2 \;-\; 2 \sum_{i=1}^m t_i \; x_i^* \cdot v \;+\; \|w - \sum_{i=1}^m t_i\, x_i^*\|^2.$$

□

Remarque 3.31. L'interprétation géométrique du lemme ci-dessus est la suivante. Par hypothèses, le point x_0 est dans l'intersection de la boule B de centre 0 et de rayon $\sqrt{C_0}$, et du "polyèdre" P intersection des m demi-espaces $x \cdot x_i \leq C_i$ pour $i = 1, \ldots, m$. L'assertion (i) affirme que chacun de ces demi-espaces rencontre B, une condition nécessaire évidente ! La quantité ${}^{\mathrm{t}}C\, G^{-1}\, C$ de l'énoncé est le carré de la distance à l'origine de l'espace affine $\{x \in V \mid \; x \cdot x_i = C_i, \;\; i = 1 \ldots m\}$, soit encore $v + F^\perp$ dans les notations de la démonstration. Si (et seulement si) la condition (ii) n'est pas satisfaite, cette distance est également la distance de P à l'origine, d'où le résultat.

Le corollaire 3.10 montre que les paramètres de Satake d'une représentation $\pi \in \Pi_{\mathrm{alg}}$ telle que $\mathrm{L}(\pi_\infty) = V$ sont soumis à un ensemble de contraintes rentrant dans le cadre du lemme précédent. Pour mettre ceci en place, il sera commode de noter $\mathrm{Q} \subset \mathbb{N}$ le sous-ensemble des puissances des nombres premiers ; tout $q \in \mathrm{Q}$ s'écrit donc de manière unique sous la forme $q = p^k$ avec p premier et k un entier ≥ 1. Si $\pi \in \Pi(\mathrm{PGL}_n)$ et si $q \in \mathrm{Q}$ on lui associe le nombre complexe

$$x_q(\pi) = \mathrm{tr}\ \mathrm{c}_p(\pi)^k \in \mathbb{C},$$

où l'on a écrit $q = p^k$ avec p premier et $k \geq 1$. Si π est autoduale et dans Π_{alg} on a même $x_q(\pi) \in \mathbb{R}$ d'après la proposition VIII.2.2. Fixons λ un réel > 0, et posons

$$\mathrm{Q}_\lambda = \{q \in \mathrm{Q},\ \ q < e^\lambda\} \quad \text{et} \quad \mathrm{E}_\lambda = \prod_{q \in \mathrm{Q}_\lambda} \mathbb{C}.$$

On munit le $\mathbb{R}$-espace vectoriel sous-jacent à E_λ d'une structure d'espace euclidien au moyen du produit scalaire

$$(x_q) \cdot (y_q) = \sum_{q \in \mathrm{Q}_\lambda} \mathrm{F}_\lambda(\log q)\ \frac{\log p}{\sqrt{q}}\ \Re\, \overline{x}_q\, y_q,$$

où dans cette somme p désigne le diviseur premier de q. Pour tout entier $n \geq 1$ et tout $\pi \in \Pi(\mathrm{PGL}_n)$ on dispose d'un vecteur

$$x_\lambda(\pi) := (x_q(\pi))_q \in \mathrm{E}_\lambda.$$

Par définition de $\mathrm{B}_f^{\mathrm{F}_\lambda}$ (Proposition-Définition 3.7), on a

$$\mathrm{B}_f^{\mathrm{F}_\lambda}(\pi, \pi') = x_\lambda(\pi) \cdot x_\lambda(\pi')$$

pour tous $\pi, \pi' \in \Pi_{\mathrm{alg}}$.

Notons $\Pi_{\mathrm{alg}}^\perp \subset \Pi_{\mathrm{alg}}$ le sous-ensemble des représentations autoduales. Pour ne pas multiplier les énoncés, et étant donné les applications que nous avons en vue, nous restreindrons l'analyse ci-dessous aux éléments de $\Pi_{\mathrm{alg}}^\perp$. Fixons $\pi_0 \in \Pi_{\mathrm{alg}}^\perp$ et posons $V_0 = \mathrm{L}((\pi_0)_\infty)$. La proposition 3.10 entraîne le système d'inégalités suivantes :

$$(3.3) \qquad \begin{cases} x_\lambda(\pi_0) \cdot x_\lambda(\pi_0) \leq\ \Phi_{\mathrm{F}_\lambda}(0)\ -\ \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V_0, V_0), \\ \qquad\qquad \text{et} \quad \forall \pi \in \Pi_{\mathrm{alg}}^\perp - \{\pi_0\}, \\ x_\lambda(\pi_0) \cdot x_\lambda(\pi)\ \leq\ -\ \frac{1-\varepsilon(V_0 \otimes \mathrm{L}(\pi_\infty))}{4}\ \Phi_\lambda(\frac{1}{2})\ -\ \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V_0, \mathrm{L}(\pi_\infty)). \end{cases}$$

Nous sommes donc manifestement dans les hypothèses du lemme 3.30, il entraîne immédiatement le scholie suivant.

Scholie 3.32. *Soient* $V_0 \in \mathrm{K}_\infty$, λ *un réel* > 0, $m \geq 1$ *un entier, et* $\pi_1, \dots, \pi_m$ *des éléments distincts de* $\Pi_{\mathrm{alg}}^{\perp}$. *On pose* $C_0 = \Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V_0, V_0)$,

$$C_i = -\frac{1 - \varepsilon(V_0 \otimes \mathrm{L}((\pi_i)_\infty))}{4}\, \Phi_\lambda(\frac{1}{2}) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V_0, \mathrm{L}((\pi_i)_\infty))$$

pour $i = 1, \dots, m$, *et* $C = (C_i) \in \mathbb{R}^m$. *On suppose que la matrice de* $\mathrm{M}_m(\mathbb{R})$

$$G = (x_\lambda(\pi_i) \cdot x_\lambda(\pi_j))_{1 \leq i,j \leq m}$$

est inversible, que les coordonnées du vecteur $G^{-1}\, C$ *sont toutes* < 0, *et que le réel* $C_0 - C^t\, G^{-1}\, C$ *est* < 0.

Si $\pi \in \Pi_{\mathrm{alg}}^{\perp}$ *vérifie* $\mathrm{L}(\pi_\infty) = V_0$, *alors il existe* $1 \leq i \leq m$ *tel que* $\pi = \pi_i$. *En particulier, si* $\mathrm{L}((\pi_i)_\infty) \neq V_0$ *pour tout* i *alors* $\mathrm{m}^{\perp}(V_0) = 0$.

Dans la suite, nous allons appliquer ce critère aux éléments π_i de l'ensemble

$$\mathcal{R} = \{1, \Delta_{11}, \Delta_{15}, \Delta_{17}, \Delta_{19}, \Delta_{21}, \mathrm{Sym}^2\Delta_{11}\} \subset \Pi_{\mathrm{alg}}^{\perp}.$$

Les vecteurs $x_\lambda(\pi)$, pour $\pi \in \mathcal{R}$ et λ raisonnable, sont considérés comme connus. Par exemple on a $x_\lambda(1) = (1, 1, 1, \dots)$ et

$$\begin{aligned} x_\lambda(\Delta_{11}) &= (\tau(2)\, 2^{-\frac{11}{2}},\ \tau(3)\, 3^{-\frac{11}{2}},\ (\tau(4) - 2^{11})\, 4^{-\frac{11}{2}},\ \dots) \\ &\simeq (-0.530,\ 0.599,\ -1.719,\ \dots). \end{aligned}$$

En guise d'application, démontrons le résultat suivant, dont nous aurons besoin par la suite.

Lemme 3.33. *Supposons que* $V \in \mathrm{K}_\infty$ *appartienne à la liste des* 8 *éléments*

$$\mathrm{I}_{21} + \mathrm{I}_{17} + \mathrm{I}_7,\quad \mathrm{I}_{22} + \mathrm{I}_4,\quad \mathrm{I}_{22} + \mathrm{I}_{12},\quad \mathrm{I}_{22} + \mathrm{I}_{16} + 1,\quad \mathrm{I}_{22} + \mathrm{I}_{12} + 1,$$

$$\mathrm{I}_{22} + \mathrm{I}_{16} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}},\quad \mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}},\quad \mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{14} + \mathrm{I}_4.$$

Alors on a $\mathrm{m}^{\perp}(V) = 0$.

Démonstration. On applique le scholie 3.32 avec $m = 2$ et en prenant pour V_0, $\{\pi_1, \pi_2\}$, λ chacun des triplets indiqués dans le tableau IX.6. On vérifie au cas par cas que les hypothèses du scholie sont bien satisfaites (voir la feuille de calculs [CL `PARI`]). □

V_0	$\{\pi_1, \pi_2\}$	λ	V_0	$\{\pi_1, \pi_2\}$	λ
$\mathrm{I}_{21} + \mathrm{I}_{17} + \mathrm{I}_7$	$\{\Delta_{15}, \Delta_{17}\}$	log 14	$\mathrm{I}_{22} + \mathrm{I}_4$	$\{1, \Delta_{21}\}$	log 7
$\mathrm{I}_{22} + \mathrm{I}_{12}$	$\{\Delta_{11}, \Delta_{15}\}$	log 5	$\mathrm{I}_{22} + \mathrm{I}_{16} + 1$	$\{1, \Delta_{17}\}$	log 8
$\mathrm{I}_{22} + \mathrm{I}_{12} + 1$	$\{1, \Delta_{11}\}$	log 5	$\mathrm{I}_{22} + \mathrm{I}_{16} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}}$	$\{\Delta_{11}, \Delta_{15}\}$	log 9
$\mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}}$	$\{\Delta_{19}, \mathrm{Sym}^2\, \Delta_{11}\}$	log 38	$\mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{14} + \mathrm{I}_4$	$\{1, \Delta_{21}\}$	log 40

TABLE IX.6 – Des triplets $(V_0, \{\pi_1, \pi_2\}, \lambda)$ vérifiant les hypothèses du scholie 3.3.

3.34. Fin de la démonstration du théorème 3.2 : cas des poids motiviques 21 et 22.

Lemme 3.35. *Soit $V \in \mathrm{K}_\infty^{\leq 21}$ tel que $V - \mathrm{I}_{21}$ est effectif, non nul, et tel que $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V) \leq \Phi_\lambda(0)$ pour $\lambda = \log 28$. Alors V est l'un des 26 éléments suivants :*

(i) $\mathrm{I}_{21} + \mathrm{I}_v$ *avec* $17 \geq v \geq 3$,

(ii) $\mathrm{I}_{21} + \mathrm{I}_v + \mathrm{I}_u$ *avec* $19 \geq v \geq 13$, $9 \geq u \geq 3$, *et* $(v, u) \neq (13, 9)$, *ou avec* $(v, u) = (17, 11)$,

(iii) $\mathrm{I}_{21} + \mathrm{I}_{19} + \mathrm{I}_{13} + \mathrm{I}_v$ *avec* $5 \geq v \geq 3$.

De plus, on a $\mathrm{m}(V) \leq 1$.

Démonstration. La première assertion se déduit d'une étude de la matrice (définie positive !) $\mathrm{Gram}(21, \log 28)$ analogue à celle conduisant aux démonstrations des lemmes 3.20 et 3.22 : voir la feuille de calculs en annexe. Pour les 26 éléments V de l'énoncé, on vérifie que l'on a $\mathrm{m}(V) < 1.8$ à l'aide du corollaire 3.14 appliqué à $\lambda = \log 28$, d'où la dernière assertion. □

Lemme 3.36. *Soit $V \in \mathrm{K}_\infty$ l'un des 26 éléments listés dans l'énoncé du lemme 3.35. On suppose* $\mathrm{t}(V, \mathrm{L}(\pi_\infty), \log 27) > 0$ *pour tout* $\pi \in \mathcal{R}$ (voir le Scholie 3.26 et le §3.29). *Alors V est l'un des éléments* $\mathrm{I}_{21} + \mathrm{I}_5$, $\mathrm{I}_{21} + \mathrm{I}_9$, $\mathrm{I}_{21} + \mathrm{I}_{13}$ ou $\mathrm{I}_{21} + \mathrm{I}_{17} + \mathrm{I}_7$.

Démonstration. C'est un simple calcul numérique pour lequel nous renvoyons à la fiche de calculs. □

Pour démontrer le cas $w = 21$ du théorème 3.2, il ne reste donc qu'à montrer que l'on a $\mathrm{m}^\perp(\mathrm{I}_{21} + \mathrm{I}_{17} + \mathrm{I}_7) = 0$. Mais cela a déjà été démontré dans le lemme 3.33. Cela termine la démonstration du théorème 3.2 dans le cas $w = 21$. □

Lemme 3.37. *Soit* $V \in \mathrm{K}_\infty^{\leq 22}$. *On suppose* $V - \mathrm{I}_{22}$ *effectif et l'inégalité* $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V) \leq \Phi_\lambda(0)$ *satisfaite pour* $\lambda = \log 80$.

(i) On a $\mathrm{m}(V) \leq 1$, *sauf si* V *est parmi les éléments suivants*

$$\mathrm{I}_{22} + \mathrm{I}_{12}, \quad \mathrm{I}_{22} + \mathrm{I}_{10}, \quad \mathrm{I}_{22} + \mathrm{I}_{8},$$

auquel cas on a seulement $\mathrm{m}(V) \leq 2$.

(ii) Supposons de plus $V \neq \mathrm{I}_{22} + \epsilon_{\mathbb{C}/\mathbb{R}}$ *et l'inégalité* $\mathrm{t}(V, \mathrm{L}(\pi_\infty), \log 77) > 0$ *satisfaite pour tout* $\pi \in \mathcal{R}$. *Alors* V *appartient à la liste des* 8 *représentations suivantes :*

$$\left\{ \begin{array}{c} \mathrm{I}_{22} + \mathrm{I}_{12}, \quad \mathrm{I}_{22} + \mathrm{I}_{8}, \quad \mathrm{I}_{22} + \mathrm{I}_{4}, \quad \mathrm{I}_{22} + \mathrm{I}_{16} + 1, \quad \mathrm{I}_{22} + \mathrm{I}_{12} + 1, \\ \\ \mathrm{I}_{22} + \mathrm{I}_{16} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}}, \quad \mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{10} + \epsilon_{\mathbb{C}/\mathbb{R}}, \quad \mathrm{I}_{22} + \mathrm{I}_{20} + \mathrm{I}_{14} + \mathrm{I}_{4}. \end{array} \right. \tag{3.4}$$

Démonstration. On vérifie tout d'abord que la matrice $B = \mathrm{Gram}(22, \log 80)$ est définie positive par la même méthode que celle employée dans la démonstration du lemme 3.20 : voir la feuille de calculs en annexe, dans laquelle on étudie la matrice symétrique $10^6\, A$ obtenue en arrondissant à l'entier le plus proche tous les coefficients de la matrice $10^6\, B$.

On procède ensuite comme dans la démonstration du lemme 3.22. L'algorithme `qfminim` de `PARI` appliqué à $10^6 A \in \mathrm{M}_{12}(\mathbb{Z})$ renvoie un ensemble de 701 couples $\pm V$ contenant tous les éléments $V \in \mathrm{K}_\infty^{\leq 22}$ vérifiant $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V) \leq \Phi_\lambda(0)$ pour $\lambda = \log 80$. Si l'on ne retient dans cet ensemble que le sous-ensemble, noté $\mathcal{L}$, constitué des V tels que $V - \mathrm{I}_{22}$ est effectif et vérifiant $\operatorname{dét} V = 1$, il ne reste "plus que" 158 possibilités pour V, autrement dit nous avons $|\mathcal{L}| = 158$.

Nous déterminons ensuite le sous-ensemble des $V \in \mathcal{L}$ vérifiant de plus $0 \leq 2\,\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V) \leq \Phi_\lambda(0)$ pour $\lambda = \log 77$: on constate qu'il ne reste que les trois éléments de la forme $\mathrm{I}_{22} + \mathrm{I}_v$ avec $v = 12, 10$ ou 8. Comme dans chacun de ces cas on vérifie d'autre part l'inégalité $3\,\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V) > \Phi_\lambda(0)$ (toujours pour $\lambda = \log 77$), le corollaire 3.14 démontre la première assertion.

Pour démontrer la seconde assertion, nous calculons simplement les $|\mathcal{L}| \cdot |\mathcal{R}| = 1106$ quantités $\mathrm{t}(V, \mathrm{L}(\pi_\infty), \log 77)$, avec $V \in \mathcal{L}$ et $\pi \in \mathcal{R}$. Nous renvoyons à la feuille de calculs pour la justification des résultats. □

Démonstration. (Fin de la démonstration du théorème 3.2) Soit $\pi \in \Pi_{\mathrm{alg}}$ de poids motivique 22. On pose $V = \mathrm{L}(\pi_\infty)$. L'élément $V - \mathrm{I}_{22}$ est effectif et l'on a $\mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V) \leq \Phi_{\mathrm{F}_\lambda}(0)$ pour tout $\lambda > 0$ d'après le corollaire 3.12 (i).

Supposons d'abord π autoduale, en particulier $\mathrm{m}^{\perp}(V) \geq 1$. Le scholie 3.26 et le lemme 3.37 (ii) montrent que soit $V = \mathrm{I}_{22} + \epsilon_{\mathbb{C}/\mathbb{R}}$, soit V est dans la liste (3.4) ci-dessus. De plus, on constate l'inégalité

$$\mathrm{t}(\mathrm{I}_{22} + \mathrm{I}_8, \mathrm{I}_{11}, \log 5) < 0$$

de sorte que l'on a également $V \neq \mathrm{I}_{22} + \mathrm{I}_8$. Mais d'après le lemme 3.33, pour les 7 éléments W restants de la liste (3.4) on a $\mathrm{m}^{\perp}(W) = 0$. En conclusion, on a $V = \mathrm{I}_{22} + \epsilon_{\mathbb{C}/\mathbb{R}}$. Mais le lemme 3.37 (i) entraîne $\mathrm{m}(V) \leq 1$, et donc $\mathrm{m}^{\perp}(V) = 1$ et $\pi = \mathrm{Sym}^2\Delta_{11}$.

Supposons maintenant que π n'est pas autoduale. D'après le lemme 3.37 (i) on a donc $\mathrm{m}(V) = 2$ et $V = \mathrm{I}_{22} + \mathrm{I}_v$ avec $v \in \{8, 10, 12\}$. En particulier, les deux représentations $\varpi \in \Pi_{\mathrm{alg}}$ vérifiant $\mathrm{L}(\varpi_\infty) = V$ sont π et $\pi^\vee$.

Pour conclure, il suffit de démontrer que l'égalité $\mathrm{m}(\mathrm{I}_{22} + \mathrm{I}_v) = 2$ pour $v = 8$ (resp. 10, 12) entraîne $\mathrm{m}(\mathrm{I}_{21} + \mathrm{I}_u) = 0$ pour $u = 9$ (resp. 9, 13). Soient (v, u) l'un des trois couples $(8, 9)$, $(10, 9)$ ou $(12, 13)$, $V = \mathrm{I}_{22} + \mathrm{I}_v$ et $V' = \mathrm{I}_{21} + \mathrm{I}_u$. D'après le corollaire 3.15 (i), il suffit de vérifier qu'il existe $\lambda > 0$ tel que l'on ait l'inégalité

$$\sqrt{(\frac{\Phi_{\mathrm{F}_\lambda}(0)}{2} - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V))(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V', V'))} \; - \; \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V, V') < 0.$$

Mais on vérifie que pour $\lambda = \log 22$, et disons à 10^{-2} près, le terme de gauche vaut respectivement -0.14, -0.03 et -0.23 quand (v, u) vaut $(8, 9)$, $(10, 9)$ et $(12, 13)$. $\square$

3.38. Compléments

Le premier complément concerne l'ordre d'annulation en $s = \frac{1}{2}$ de $\mathrm{L}(s, \pi)$ lorsque $\pi \in \Pi_{\mathrm{alg}}$ est de poids motivique ≤ 22 (comparer avec la remarque VII.3.3).

Proposition 3.39. *Soit $\pi \in \Pi_{\mathrm{alg}}^{\perp}$ de poids motivique ≤ 22. On a*

$$\mathrm{ord}_{s=\frac{1}{2}} \mathrm{L}(s, \pi) \;=\; \begin{cases} 0 & \text{si} \quad \varepsilon(\pi) = 1, \\ 1 & \text{sinon.} \end{cases} \tag{3.5}$$

De plus on a $\varepsilon(\pi) = -1$ si, et seulement, si $\pi = \Delta_{17}$ ou $\pi = \Delta_{21}$.

Démonstration. Posons $r = \mathrm{ord}_{s=\frac{1}{2}} \mathrm{L}(s, \pi)$, ou ce qui revient au même $r = \mathrm{ord}_{s=\frac{1}{2}} \xi(s, \pi)$ d'après la remarque suivant le corollaire 3.10. L'équation

fonctionnelle $\xi(s,\pi) = \varepsilon(\pi)\,\xi(1-s,\pi)$ montre que r est pair si $\varepsilon(\pi) = 1$, et impair sinon. Il suffit donc de montrer $r < 2$. On peut supposer $\pi \neq 1$ car on a $\varepsilon(1) = 1$ et $\zeta(\frac{1}{2}) \neq 0$. Un argument similaire à celui donné dans la démonstration du corollaire 3.12 (ii), appliqué à π et 1, montre que sous l'hypothèse $r \geq 2$ on a l'inégalité

$$(3.6)\quad -\Phi_{\mathrm{F}_\lambda}(\frac{1}{2}) - \mathrm{J}_{\mathrm{F}_\lambda}(V) + \sqrt{(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{J}_{\mathrm{F}_\lambda}(1))(\Phi_{\mathrm{F}_\lambda}(0) - \mathrm{B}_\infty^{\mathrm{F}_\lambda}(V,V))} \geq 0$$

pour tout $\lambda > 0$: il suffit de minorer $\mathrm{ord}_{s=1/2}\,\xi(s,\pi)$ par 2 plutôt que par $\mathrm{e}^\perp(\pi,1)$. Mais lorsque V vaut respectivement

$$\mathrm{I}_{11},\ \mathrm{I}_{15},\ \mathrm{I}_{17},\ \mathrm{I}_{19},\ \mathrm{I}_{21},\ \mathrm{I}_{19}+\mathrm{I}_7,\ \mathrm{I}_{21}+\mathrm{I}_5,\ \mathrm{I}_{21}+\mathrm{I}_9,\ \mathrm{I}_{21}+\mathrm{I}_{13},\ \mathrm{I}_{22}+\epsilon_{\mathbb{C}/\mathbb{R}},$$

et disons $\lambda = \log 4$, on vérifie que le terme de gauche de (3.6) vaut respectivement -1.07, -0.64, -0.49, -0.35, -0.23, -0.79, -0.86, -0.35, -0.05, -0.82 à 10^{-2} près. La première assertion de la proposition découle donc du théorème 3.2. On observe que dans la liste 10 des éléments V ci-dessus, on a $\varepsilon(V) = 1$ sauf pour $V = \mathrm{I}_{17}$ et I_{21} ; cela termine la démonstration. □

Une conséquence très simple, mais surprenante, du théorème 3.2 est le fait qu'il n'existe qu'un nombre fini de $\pi \in \Pi_{\mathrm{alg}}$ telles que $\mathrm{w}(\pi) \leq 22$. Un retour sur notre démonstration montre que cette assertion de finitude, qui est en fait notre point de départ, est conséquence de la propriété suivante : si l'on a $w \leq 22$, il existe des réels $\lambda > 0$ tels que la restriction de la forme bilinéaire symétrique $\mathrm{B}_\infty^{\mathrm{F}_\lambda}$ à $\mathrm{K}_\infty^{\leq w}$ est définie positive (Lemmes 3.20, 3.28, 3.35 et 3.37). Il se trouve que cette propriété persiste pour $w = 23$ (mais cesse d'être vraie pour $w > 23$!).

Proposition 3.40. *Il n'existe qu'un nombre fini de représentations dans* Π_{alg} *de poids motivique* ≤ 23.

Démonstration. Un simple calcul montre en effet que $\mathrm{Gram}(23, 9.74)$ est définie positive. □

Nous reportons à un travail ultérieur l'étude détaillée des représentations dans Π_{alg} dont le poids motivique est ≥ 23, qui nous entraînerait ici trop loin de nos préoccupations. Mentionnons toutefois deux travaux en relation avec ces questions. Dans [CR12], les auteurs démontrent en supposant la conjecture VIII.4.25 une formule explicite et calculable pour $\mathrm{m}^\perp(V)$ lorsque :

– V est *sans multiplicité*, c'est-à-dire que ses coefficients dans la base $1, \epsilon_{\mathbb{C}/\mathbb{R}}, \{\mathrm{I}_w, w > 0\}$ sont tous dans $\{0, 1\}$.

– $\dim V \leq 8$, les résultats n'étant que partiels pour $\dim V = 7$.

Dans un remarquable tour de force [TAI14], Taïbi a ensuite redémontré ces formules en supposant uniquement la conjecture VIII.4.22, et surtout, il les a étendues au cas plus général $\dim V \leq 14$. Ses résultats sont même indépendants de toute conjecture si V a ses poids "assez écartés". [4]

Revenons au cas du poids motivique 23 et admettons la conjecture 4.22. La théorie des formes modulaires montre bien entendu l'égalité $\mathrm{m}(\mathrm{I}_{23}) = 2$. Considérons ensuite $V \in \mathrm{K}_\infty$ sans multiplicité tel que $V - \mathrm{I}_{23}$ est effectif et vérifie $\mathrm{m}^\perp(V) \geq 1$. La théorie des formes de Siegel de genre 2, et la formule de Tsushima (voir la remarque 3.41), montrent que si $\dim V = 2$ on a $\mathrm{m}(V) = 1$ et $V - \mathrm{I}_{23} \in \{I_7, \ \mathrm{I}_9, \ \mathrm{I}_{13}\}$. Les calculs de [CR12, Cor. I.1.5], basés sur l'étude des invariants polynomiaux du groupe orthogonal du réseau E_7, montrent de plus que si $6 \leq \dim V \leq 8$ alors on a $\dim V = 6$, $\mathrm{m}^\perp(V) = 1$ et $V - \mathrm{I}_{23}$ parcourt la liste suivante :

$$\mathrm{I}_{13} + \mathrm{I}_5, \ \mathrm{I}_{15} + \mathrm{I}_3, \ \mathrm{I}_{15} + \mathrm{I}_7, \ \mathrm{I}_{17} + \mathrm{I}_5, \ \mathrm{I}_{17} + \mathrm{I}_9, \ \mathrm{I}_{19} + \mathrm{I}_3, \ \mathrm{I}_{19} + \mathrm{I}_{11}.$$

Enfin, les résultats sus-cités de Taïbi montrent que si $8 < \dim V \leq 14$ alors $\dim V = 10$, $\mathrm{m}^\perp(V) = 1$ et $V = \mathrm{I}_{23} + \mathrm{I}_{21} + \mathrm{I}_{17} + \mathrm{I}_{11} + \mathrm{I}_3$. Cela fait en tout 13 représentations dans Π_{alg} de poids motivique 23, la question restante est de savoir s'il y en a d'autres. Mentionnons également que nous ne connaissons que trois $\pi \in \Pi_{\mathrm{alg}}$ de poids motivique 24, de dimensions respectives 7, 8 et 8. Celui de dimension 7 vérifie $\mathrm{L}(\pi_\infty) = \epsilon_{\mathbb{C}/\mathbb{R}} \oplus \bigoplus_{i=1}^3 \mathrm{I}_{8i}$ et il est relié à la trialité et au groupe G_2 [CR12, Cor. I.1.10].

Remarque 3.41. Un cas particulier très simple des formules de Taïbi est que la formule donnée par Tsushima [TSU83] pour calculer $\dim \mathrm{S}_{j,k}$ quand $k \geq 5$ est plus généralement valable pour $k \geq 3$ (§IX.1), à l'exception du cas $(j,k) = (0,3)$. Une inspection de ses valeurs montre notamment l'annulation $\dim \mathrm{S}_{j,k} = 0$ quand $k = 3, 4$ et $j + 2k - 3 \leq 21$. Une seconde démonstration de cette annulation est fournie par le théorème 3.2 et la proposition 1.4.

4. Précisons cette notion. Supposons V effectif, disons de dimension $n = \dim V$, et notons $\lambda_1, \ldots, \lambda_n$ le multi-ensemble de n nombres complexes associés à $V_{|\mathbb{C}^*}$ comme dans l'assertion de compatibilité de la paramétrisation de Langlands au caractère infinitésimal §VIII.2.12 (iii). On peut supposer $\lambda_i \in \frac{1}{2}\mathbb{Z}$ pour tout i et $\lambda_i - \lambda_j \in \mathbb{Z}$ pour tout i, j. Si les λ_i sont entiers, on dit que V a ses poids assez écartés si l'on a l'inégalité $|\lambda_i - \lambda_j| \neq 1$ pour tout $1 \leq i, j \leq n$. Si les λ_i sont dans $\frac{1}{2}\mathbb{Z} - \mathbb{Z}$, on demande $\lambda_{n/2} > 1$ ainsi que pour tout entier $3 \leq i \leq n/2$ l'inégalité $\lambda_{i-2} > \lambda_i + 2$.

4. Démonstration du théorème E

4.1. Une nouvelle démonstration du théorème A

Commençons par donner une nouvelle démonstration du théorème A, en utilisant une méthode qui se généralisera à la dimension 24. On rappelle que l'on a $|\mathrm{X}_{16}| = 2$ et que l'opérateur de Hecke T_2 admet des valeurs propres distinctes sur $\mathbb{Z}[\mathrm{X}_{16}]$ (Corollaire II.3.6, §III.3.1). En particulier, il existe exactement deux représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{16})$ telles que π_∞ est la représentation triviale de $\mathrm{O}_{16}(\mathbb{R})$. Nous avons déjà expliqué au §V.2 que la proposition suivante entraîne le théorème A ; nous avons d'ailleurs déjà donné une première démonstration de cette proposition au corollaire VII.2.6 (ii).

Proposition* **4.2.** *Les paramètres standards $\psi(\pi, \mathrm{St})$ des deux représentations $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{16})$ telles que π_∞ est la représentation triviale sont* $[15] \oplus [1]$ *et* $\Delta_{11}[4] \oplus [7] \oplus [1]$.

Démonstration. D'après l'exemple donné à la fin du §VI.4.7, nous savons que la représentation triviale $1 \in \Pi_{\mathrm{disc}}(\mathrm{O}_{16})$ satisfait

$$\psi(1, \mathrm{St}) = [15] \oplus [1].$$

Il s'agit donc de montrer que si π désigne la représentation non triviale de $\Pi_{\mathrm{disc}}(\mathrm{O}_{16})$ telle que π_∞ est triviale, alors $\psi(\pi, \mathrm{St}) = \Delta_{11}[4] \oplus [7] \oplus [1]$. Ajoutons que l'on a $\psi(\pi, \mathrm{St}) \neq \psi(1, \mathrm{St})$. Il y a une raison générale à cela, mais une manière de le voir ici est d'utiliser que les deux valeurs propres de T_2 agissant sur $\mathbb{Z}[\mathrm{X}_{16}]$, à savoir $\quad 2^7 \operatorname{tr} \psi(\pi, \mathrm{St})_2 \quad$ et $\quad 2^7 \operatorname{tr} \psi(1, \mathrm{St})_2 \quad$ (Formule VI.(2.5)), sont distinctes.

D'après la proposition V.2.1, la représentation π admet un ϑ-correspondant en genre $1 \leq g \leq 4$. Étant donné l'inégalité $16 > 2\,g$, le théorème VIII.1.1 d'Arthur et le corollaire VII.1.3 montrent que le couple (π, St) vérifie la conjecture d'Arthur-Langlands. Autrement dit, il existe un entier $k \geq 1$, et pour $i = 1, \ldots, k$ des représentations $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ et des entiers $d_i \geq 1$, tels que

$$\psi(\pi, \mathrm{St}) \;=\; \oplus_{i=1}^{k} \pi_i[d_i].$$

L'hypothèse sur π_∞ impose que les valeurs propres de $\mathrm{St}\,\mathrm{c}_\infty(\pi)$ sont les 14 entiers $\pm 7, \pm 6, \ldots, \pm 1$, ainsi que 0 avec multiplicité 2. On en déduit que les π_i sont algébriques (Proposition VIII.2.8), de poids motivique vérifiant $\frac{\mathrm{w}(\pi_i)+d_i-1}{2} \leq 7$. En particulier, on a $\mathrm{w}(\pi_i) \leq 14$ pour tout i.

D'après le théorème 3.2, pour tout $i = 1, \ldots, k$ on a $\pi_i = 1$ ou $\pi_i = \Delta_{11}$. De plus, les poids de Δ_{11} sont $\pm\frac{11}{2}$. En considérant la valeur propre ± 7, qui ne

peut qu' "appartenir" à un constituant de la forme $\Delta_{11}[4]$ ou $[15]$, on constate que les seules possibilités pour $\psi(\pi, \mathrm{St})$ sont les deux de l'énoncé. On peut aussi invoquer à ce stade l'égalité $\Psi_{16} = \{ [15] \oplus [1],\ \Delta_{11}[4] \oplus [7] \oplus [1] \}$ qui a été vérifiée au cours de la démonstration de la proposition 2.2. Cela termine la démonstration (et redémontre même la conjecture de Witt $g = 4$!). $\square$

4.3. Démonstration du théorème E

Théorème[⋆] **4.4.** *Les éléments $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$ tels que ψ_∞ admette pour valeurs propres simples les entiers $\pm 11, \pm 10, \ldots, \pm 1$, ainsi que 0 pour valeur propre double, sont exactement les 24 paramètres de la table I.2.*

Démonstration. En effet, soit $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$ tel que ψ_∞ vérifie la propriété de l'énoncé. Écrivons $\psi = \oplus_{i=1}^{k} \pi_i[d_i]$ avec $\pi_i \in \Pi_{\mathrm{alg}}(\mathrm{PGL}_{n_i})$ pour tout entier $1 \leq i \leq k$. Soit i un tel entier. La condition sur ψ_∞ entraîne $\frac{\mathrm{w}(\pi_i)+d_i-1}{2} \leq 11$, puis l'inégalité $\mathrm{w}(\pi_i) \leq 22$. D'après le théorème 3.2, pour tout entier i la représentation π_i est donc dans l'ensemble Π introduit juste avant l'énoncé de la proposition 2.2. On conclut par cette proposition. $\square$

Démonstration. (Démonstration du théorème E) Reprenons les notations du §2.4 : on dispose notamment de 24 éléments $\psi_i \in \mathcal{X}(\mathrm{SO}_{24})$, $i = 1, \ldots, 24$, distincts d'après Nebe et Venkov, et nous devons démontrer que ce sont les éléments de la table I.2. Comme cette table a également exactement 24 éléments, et étant donné le théorème 4.4, il ne reste qu'à démontrer que l'on a $\psi_i \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$ pour tout i.

Nous savons déjà, suivant Ikeda et Böcherer, que l'on a $\psi_{24} = \Delta_{11}[12]$ (Corollaire IV.3.4, voir aussi le début de la démonstration de la proposition 5.1). Soit $1 \leq i \leq 23$ et soit $\psi_i' \in \mathcal{X}(\mathrm{SL}_{2g_i+1})$ le paramètre standard du ϑ-correspondant dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g_i})$ de π_i (les notations π_i et g_i sont rappelées au §2.4). D'après le lemme 2.9 on a $g_i \leq 11$, de sorte que d'après Rallis (Corollaire VII.1.3) on a l'identité

$$\psi_i = \psi_i' \oplus [23 - 2g_i].$$

D'après le théorème VIII.1.1 d'Arthur, on a $\psi_i' \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g_i+1})$. Cela entraîne $\psi_i \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$ et conclut la démonstration. $\square$

Remarque 4.5. Dans la démonstration ci-dessus, il a été commode de traiter à part le cas du paramètre $\Delta_{11}[12]$, ce qui a été possible grâce à [Ike01] et [BFW98]. Un examen de la démonstration que nous donnerons du théorème 5.2 montrerait en fait que l'on peut se passer de ces deux références, et utiliser simplement le résultat d'Erokhin [Ero79].

5. Formes de Siegel de poids ≤ 12

Le but de cette partie est d'étudier l'espace $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$, avec $g \geq 1$ arbitraire et $k \leq 12$. Il s'agira en premier lieu de déterminer sa dimension, puis de décrire, pour toute forme $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ propre pour l'action de $\mathrm{H}(\mathrm{Sp}_{2g})$, le paramètre standard $\psi(\pi_F, \mathrm{St})$ de la représentation $\pi_F \in \Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ engendrée par F. Pour faire court, nous dirons simplement que $\psi(\pi_F, \mathrm{St})$ est *le paramètre standard de la forme propre* F.

La question de déterminer la dimension de $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ a fait l'objet de travaux de nombreux auteurs, dans divers cas particuliers. Nous renvoyons par exemple aux articles de Poor et Yuen [PY96, PY07], et à celui de Nebe et Venkov [NV01], pour une discussion des dimensions qui étaient connues avant ce travail et l'article récent [Tai14]. Rappelons que le cas $g = 1$ est classique, et que dans les cas $g = 2$ et 3 une formule pour $\dim \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ valable pour tout $k > g$ a été respectivement démontrée par Igusa [Igu62] et Tsuyumine [Tsuy86]. La situation pour $g > 3$ est longtemps restée très partielle, au sens où $\dim \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ n'avait pu être déterminé que pour un petit nombre (fini !) de couples (g, k) avec $g > 3$, $k \geq 0$ et $gk \equiv 0 \bmod 2$. Elle a substantiellement évoluée récemment avec l'algorithme de Taïbi [Tai14], qui a aboutit à une formule concrète pour $\dim \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ valable pour tout $k > g$ et tout $g \leq 7$; cette formule est toutefois encore conditionnelle à la conjecture VIII.4.22, du moins au moment où nous écrivons ces lignes !

La méthode que nous allons utiliser est largement indépendante de celles des auteurs sus-cités. En particulier, elle n'utilise aucun des calculs mentionnés ci-dessus en genre $g > 2$, et donne donc des nouvelles démonstrations des cas précédemment connus en ces genres. Dans l'esprit, elle est proche de la démonstration par Duke et Imamoğlu [DI98] de l'annulation $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ pour tout $g \geq 1$ et tout $k \leq 6$. En effet, notre démonstration et la leur ont de commun l'utilisation des "formules explicites" (au sens du §IX.3). Duke et Imamoğlu les appliquent à la fonction L standard d'une forme de Siegel propre, en se basant sur les travaux de Böcherer et Mizumoto rappelés au §VIII.7, alors que nous les avons appliquées aux fonctions L de paires de représentations automorphes cuspidales de groupes linéaires (Jacquet, Piatetski-Shapiro, Shalika). Notre approche est bien sûr permise par le théorème d'Arthur VIII.1.1. Sous cet angle, l'ingrédient crucial des démonstrations qui vont suivre devient le théorème 3.2.

Rappelons enfin l'annulation très utile $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ si $k < g/2$, d'après la théorie des formes singulières de Freitag, Resnikoff et Weissauer [vdG08, §14]. En particulier, si $k \leq 12$ nous pouvons supposer $g \leq 24$, de sorte qu'il n'y a en réalité qu'un nombre fini de couples (k, g) à considérer.

5.1. Formes de poids 12 et démonstration du théorème D de l'introduction

Rappelons que l'on dispose pour tout $g \geq 1$ d'une application linéaire $\vartheta_g : \mathbb{C}[\mathrm{X}_{24}] \longrightarrow \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$, ainsi que de $\vartheta_0 : \mathbb{C}[\mathrm{X}_{24}] \to \mathbb{C}$ (§V.1).

Théorème* **5.2.** *(i) La dimension des espaces* $\mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *avec* $g \leq 12$ *est donnée par la table :*

g	1	2	3	4	5	6	7	8	9	10	11	12
$\dim \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$	1	1	1	2	2	3	3	4	2	2	1	1

En particulier, $\bigoplus_{1\leq g\leq 12} \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *est de dimension* 23.

(ii) Pour tout $1 \leq g \leq 12$*, l'application* $\vartheta_g : \mathbb{C}[\mathrm{X}_{24}] \to \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ *induit un isomorphisme* $\mathrm{Ker}\,\vartheta_{g-1}/\mathrm{Ker}\,\vartheta_g \xrightarrow{\sim} \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$.

(iii) Il existe exactement 23 *représentations dans les* $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$*, avec* $1 \leq g \leq 12$*, qui sont engendrées par une forme de Siegel propre de poids* 12*. Elles ont pour paramètres standards ceux de la table C.1.*

Démonstration. Nous allons commencer par établir un lemme préliminaire expliquant le contenu de la table C.1. Rappelons l'ensemble

$$\Pi = \{\mathrm{Sym}^2\Delta_{11}, \Delta_{21,13}, \Delta_{21,9}, \Delta_{21,5}, \Delta_{21}, \Delta_{19,7}, \Delta_{19}, \Delta_{17}, \Delta_{15}, \Delta_{11}, 1\}, \tag{5.1}$$

introduit avant l'énoncé de la proposition 2.2. Considérons, pour $1 \leq g \leq 12$, l'ensemble Φ_g de tous les éléments $\phi \in \mathcal{X}(\mathrm{SL}_{2g+1})$ tels que :

(a) ϕ_∞ admet pour valeurs propres les $2g+1$ entiers 0 et $\pm(12-j)$ avec $j = 1, \ldots, g$.

(b) il existe $r \geq 1$, des entiers $d_1, \ldots, d_r \geq 1$, et des représentations $\pi_1, \ldots, \pi_r \in \Pi$, tels que $\phi = \oplus_{i=1}^r \pi_i[d_i]$.

Si $1 \leq g \leq 12$ et $\phi \in \Phi_g$, nous dirons que ϕ *satisfait la condition* (C) si dans sa décomposition (b) ci-dessus, il n'existe pas d'entier $1 \leq i \leq r$ vérifiant $\pi_i = 1$ et $d_i > 1$, et s'il existe au plus un entier i tel que $\pi_i = 1$. La condition (C) est toujours satisfaite si $g < 11$, car dans ce cas 1 n'est pas valeur propre de ϕ_∞ et 0 en est valeur propre simple.

Lemme 5.3. *L'ensemble des éléments de* $\coprod_{1\leq g\leq 12} \Phi_g$ *satisfaisant la condition* (C) *est exactement l'ensemble des paramètres réunis dans la table C.1.*

Démonstration. C'est un exercice de combinatoire du même acabit que celui effectué dans la démonstration de la proposition 2.2. On peut le déduire de cette proposition de la manière suivante.

Soit $\phi \in \Phi_g$ avec $g \leq 11$. D'après la proposition 2.2, $\phi \oplus [23-2g]$ est un élément de la table I.2. La propriété $\phi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1})$, la condition (C), et le théorème de Jacquet-Shalika (Proposition VI.4.5), déterminent alors uniquement ϕ. C'est ainsi que nous avons en fait défini les 22 éléments de la table C.1 correspondants aux genres $g < 12$.

Il ne reste qu'à voir que le seul élément $\phi \in \Phi_{12}$ satisfaisant (C) est $\Delta_{11}[12] \oplus [1]$. Pour cela, écrivons $\phi = \oplus_{i=1}^r \pi_i[d_i]$ avec $\pi_i \in \Pi$ pour tout i. Par la condition (C), il existe au plus un entier i tel que $\pi_i = 1$. La valeur propre 11 de ϕ_∞ étant simple, il existe également au plus un entier i tel que $\pi_i = \mathrm{Sym}^2\Delta_{11}$. Comme 0 est valeur propre triple de ϕ_∞, le lemme 2.3 (i) montre qu'il existe un entier i tel que $\pi_i = \Delta_{11}$ et $d_i = 12$. La seule possibilité est alors $\phi = \Delta_{11}[12] \oplus [1]$. □

Ce lemme préliminaire étant établi, considérons $F \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$ avec $1 \leq g \leq 12$ et $\psi \in \mathcal{X}(\mathrm{SL}_{2g+1})$ son paramètre standard. D'après le corollaire VI.3.6, ψ_∞ admet pour valeurs propres les $2g+1$ entiers $\pm 11, \pm 10, \ldots, \pm(12-g)$ et 0. Toutes ces valeurs propres sont simples, hormis la valeur propre 0 pour $g = 12$ qui est de multiplicité 3. D'après le théorème 1.1 d'Arthur, on peut écrire

$$\psi = \oplus_{i=1}^r \pi_i[d_i] \tag{5.2}$$

avec $d_i \geq 1$ et $\pi_i \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_{n_i})$ pour $i = 1, \ldots, r$. On observe que les π_i sont algébriques de poids motivique ≤ 22. D'après le théorème 3.2, on en déduit que pour tout i la représentation π_i est dans l'ensemble Π. Autrement dit, on a $\psi \in \Phi_g$.

Lemme* **5.4.** *Soient $1 \leq g \leq 12$, $F \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre et ψ le paramètre standard de F. Alors $\psi \in \Phi_g$ et ψ vérifie la condition* (C).

Démonstration. Nous venons de vérifier $\psi \in \Phi_g$. La condition (C) étant automatique quand $g \leq 10$, on peut supposer $g \geq 11$. On écrit $\psi = \oplus_{i=1}^r \pi_i[d_i]$ avec $\pi_i \in \Pi$ pour tout i.

Cas $g = 11$. Si $g = 11$ alors 0 est valeur propre simple de ψ_∞. Nous pouvons donc supposer, quitte à réindexer les π_i, que l'on a[5] $\pi_r = 1$ et

5. Le lecteur ayant digéré les considérations du chapitre VIII remarquera que cette hypothèse est en contradiction avec la conjecture VIII.4.22, par exemple d'après le théorème VIII.5.2 ; nous allons en effet aboutir à une contradiction, mais en utilisant plutôt les résultats du §VIII.7.

$d_r > 1$. Posons

$$g' = \frac{23 - d_r}{2}.$$

C'est un entier vérifiant $0 \leq g' \leq 10$ car d_r est impair > 1. Ainsi, soit on a $\psi = [23]$, soit $d_r < 23$ et ψ s'écrit sous la forme $\psi' \oplus [d_r]$ avec $\psi' \oplus [1] \in \Phi_{g'}$. L'inégalité $g' \leq 10$ assure que $\psi' \oplus [1]$ satisfait (C) : c'est l'un des 12 éléments de la table C.1 contenant [1] et vérifiant $g' \leq 10$ (Lemme 5.3). Il y a donc en tout 13 possibilités pour ψ, et il reste à démontrer qu'aucune d'entre elles n'est possible. D'après la proposition VIII.7.1 appliquée à la forme F (cas $k = g+1$), il suffit pour cela de vérifier que l'on a $\delta(\pi_F, \frac{d_r+1}{2}) = 0$ dans chacun des cas, dans les notations *loc. cit.* (voir la formule (7.1)). C'est évident si $\psi = [23]$. Dans les autres cas, on conclut par le lemme 5.5 ci-dessous et la relation $d_r + 1 = 24 - 2g'$.

Cas $g = 12$. On procède de manière similaire en genre $g = 12$. Supposons en effet que ψ ne satisfait pas la condition (C). Nous affirmons que l'un des π_i vaut $\mathrm{Sym}^2\Delta_{11}$ et que deux des π_i valent 1. En effet, ψ_∞ admet 0 pour valeur propre triple, et les entiers $\pm 1, \ldots, \pm 11$ pour valeurs propres simples. Si $(\pi_i[d_i])_\infty$, pour $i = 1, \ldots, r$, admet la valeur propre 0, le lemme 2.3 (i) montre que l'on a soit $\pi_i = \mathrm{Sym}^2\Delta_{11}$ et $d_i = 1$, soit $\pi_i = \Delta_{11}$ et $d_i = 12$, soit $\pi_i = 1$. Le second cas est exclu car il entraîne $\psi = \Delta_{11}[12] \oplus [1]$, qui vérifie (C). La valeur propre 11 de ψ_∞ étant simple, cela démontre l'affirmation plus haut.

Ainsi, on a $r \geq 3$ et quitte à réindexer les π_i on peut supposer que l'on a $\pi_1 = \mathrm{Sym}^2\Delta_{11}$, $\pi_r = \pi_{r-1} = 1$, $d_{r-1} = 1$ et $d_r > 1$ (d'après le théorème d'Arthur VIII.2.4, on rappelle qu'on ne peut avoir $d_r = d_{r-1} = 1$). En particulier, si l'on pose à nouveau $g' = \frac{23-d_r}{2}$, on a

$$\psi = \psi' \oplus [1] \oplus [d_r]$$

avec $\psi' \in \Phi_{g'}$ contenant $\mathrm{Sym}^2\Delta_{11}$. L'inégalité $d_r \geq 3$, *i.e.* $g' \leq 10$, montre que ψ' vérifie la condition (C) : il est dans la table C.1 par le lemme 5.3. On constate par inspection qu'il y a 9 possibilités pour ψ', et donc pour ψ.

On exclut ensuite chacune de ces 9 possibilités en utilisant la proposition VIII.7.1 appliquée à F (cas $k = g$). Cette proposition s'applique encore à cause du lemme 5.5, qui contredit l'inégalité $\delta(\pi_F, \frac{d_r+1}{2}) > 0$ (observer la relation $d_r + 1 = 24 - 2g'$). Cela termine la démonstration du lemme 5.4. $\square$

Lemme 5.5. *Soient $1 \leq g' \leq 10$ et $\phi \in \Phi_{g'}$. Écrivons $\phi = \oplus_{i=1}^s \varpi_i[q_i]$. Alors on a $\mathrm{L}(\frac{1}{2}, \varpi_i) \neq 0$ pour tout $1 \leq i \leq s$ tel que $q_i \geq 24 - 2g'$ et $\pi_i \neq 1$.*

Démonstration. Seuls les ϕ de la table C.1 contenant un facteur de la forme $\Delta_{17}[d]$ (resp. $\Delta_{21}[2]$) méritent une attention d'après la proposition 3.39. On conclut car on observe par inspection que l'on a toujours $24 - 2g' > d$ (resp. $g' \leq 10$). $\square$

Terminons la démonstration du théorème. Pour cela, vérifions tout d'abord l'assertion (ii), à savoir que pour tout $g = 1, \ldots, 12$, l'injection

$$\operatorname{Ker} \vartheta_{g-1} / \operatorname{Ker} \vartheta_g \to \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z})),$$

induite par ϑ_g, est surjective. Il s'agit de voir que si $g \leq 12$, toute forme propre $F \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est dans l'image de ϑ_g. Les deux lemmes ci-dessus assurent que son paramètre standard $\psi(\pi_F, \mathrm{St})$ est dans la table C.1. On conclut en constatant que dans tous les cas le critère de Böcherer s'applique : cela a d'ailleurs déjà été justifié lors de la vérification du point 2 dans le §2.11. L'assertion (ii) est donc démontrée.

Observons maintenant que si $g \leq 12$ et si $G, H \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ sont deux formes propres pour $\mathrm{H}(\mathrm{Sp}_{2g})$ telles que $\psi(\pi_G, \mathrm{St}) = \psi(\pi_H, \mathrm{St})$, alors G et H sont proportionnelles. En effet, le paragraphe précédent assure qu'il existe $G', H' \in \mathbb{C}[\mathrm{X}_{24}]$ tels que $\vartheta_g(G') = G$ et $\vartheta_g(H') = H$. Les formes G et H étant propre, la relation de commutation d'Eichler (Proposition V.1.1) assure que l'on peut supposer que G' et H' sont propres pour T_2. Mais cette même relation et l'identité $\psi(\pi_G, \mathrm{St}) = \psi(\pi_H, \mathrm{St})$ imposent que G' et H' ont même valeur propre de T_2 : elles sont donc proportionnelles d'après le calcul de Nebe et Venkov, et donc G et H sont proportionnelles.

Soit Φ l'ensemble des paramètres ϕ de la table C.1 tels qu'il existe une forme propre $G \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ satisfaisant $\phi = \psi(\pi_G, \mathrm{St})$ (l'entier g étant bien sûr uniquement déterminé par ϕ). Le paragraphe précédent démontre $|\Phi| = \sum_{g=1}^{12} \dim \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$. L'assertion (ii) du théorème entraîne alors

$$|\Phi| = \sum_{g=1}^{12} \dim(\operatorname{Ker} \vartheta_{g-1} / \operatorname{Ker} \vartheta_g) = \dim(\operatorname{Ker} \vartheta_0) - \dim(\operatorname{Ker} \vartheta_{12}) = 23,$$

la dernière égalité provenant du résultat d'Erokhin $\operatorname{Ker} \vartheta_{12} = 0$ [Ero79]. Comme il n'y a que 23 paramètres dans la table C.1, Φ est l'ensemble de tous les paramètres de cette table, ce qui démontre les assertions (i) et (iii) du théorème (et justifie la remarque 4.5). $\square$

Proposition 5.6. *Si $g > 12$ et $g \neq 24$ alors on a $\mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$.*

Démonstration. Les auteurs s'excusent du manque d'élégance de la démonstration qui va suivre. Une raison à cela est que l'on ne dispose pas des outils adéquats pour la traiter, à savoir dans l'idéal d'un analogue du théorème VIII.5.2 dans le cas où l'élément ψ_∞ considéré *loc. cit.* n'a pas toutes ses valeurs propres distinctes. À la place, nous utiliserons de manière ad hoc le substitut très partiel fourni par la proposition VIII.7.3.

Il s'agit de démontrer qu'il n'existe pas de forme $F \in \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ propre pour $\mathrm{Sp}_{2g}(\mathbb{Z})$ pour $24 > g > 12$. Supposons donc qu'il existe une telle forme et notons ψ son paramètre standard. Les valeurs propres de ψ_∞ sont les $2g+1$ entiers 0 et $\pm(12-j)$ pour $1 \leq j \leq g$. D'après un argument déjà utilisé, le théorème d'Arthur, l'inégalité $g < 24$, et le théorème 3.2, montrent que l'on a $\psi = \oplus_{i=1}^r \pi_i[d_i]$ avec $\pi_i \in \Pi$ pour $i = 1, \ldots, r$ (l'ensemble Π étant défini par la formule (5.1)). Il sera commode de noter $\mathcal{X}_\Pi(\mathrm{SL}_n)$ l'ensemble des éléments de $\mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$ qui sont somme directe (au sens du §VI.4.4) d'éléments de la forme $\varpi[d]$ avec $\varpi \in \Pi$ et $d \geq 1$; on pose aussi $\mathcal{X}_\Pi = \coprod_{n\geq 1} \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_n)$.

La première assertion du lemme 2.3 montre que l'hypothèse (7.3) de la proposition VIII.7.3 est satisfaite, ainsi donc que ses conclusions. Conformément à l'énoncé de cette proposition, nous posons $I = \{i,\ \pi_i = 1\}$, $I' = \{i \in I, d_i = 1\}$, ainsi que $d = \mathrm{Max}\{d_i, i \in I\}$ si $I \neq \emptyset$. Nous allons d'abord démontrer les deux propriétés suivantes :

(1) $\pi_i[d_i] \neq \Delta_{11}[12]$ pour tout $i = 1, \ldots, r$.

(2) $\pi_i \neq \mathrm{Sym}^2\Delta_{11}$ pour tout $i = 1, \ldots, r$.

Commençons par une observation. Soit $\pi \in \Pi$ vérifiant $\mathrm{L}(\frac{1}{2}, \pi) = 0$. D'après la proposition 3.39 on a $\pi \in \{\Delta_{17}, \Delta_{21}\}$ et $\mathrm{ord}_{s=\frac{1}{2}} \mathrm{L}(s, \pi) = 1$. En particulier, si $\mathrm{L}(\frac{1}{2}, \pi_i) = 0$ on constate que $\pi_i[d_i]$ est dans l'ensemble

$$\Psi_0 \ = \ \{\Delta_{17}[2],\ \Delta_{17}[4],\ \Delta_{17}[6],\ \Delta_{21}[2]\ \}.$$

Il sera utile d'avoir sous les yeux les valeurs propres de ϕ_∞ pour $\phi \in \Psi_0$: elles sont données dans la table IX.7 ci-contre. Chacun de ces éléments de Ψ_0 apparaissant au plus avec multiplicité 1 dans l'écriture de ψ d'après Arthur, on constate par exemple $\delta(\pi_F, a) \leq 4 - a$ pour tout entier $1 \leq a \leq 4$.

ϕ	$\Delta_{17}[2]$	$\Delta_{17}[4]$	$\Delta_{17}[6]$	$\Delta_{21}[2]$
E	$\{9, 8\}$	$\{10, 9, 8, 7\}$	$\{11, 10, 9, 8, 7, 6\}$	$\{11, 10\}$

TABLE IX.7 – Ensemble E des valeurs propres ≥ 0 de ϕ_∞ pour $\phi \in \Psi_0$.

Démonstration de l'assertion (1). Supposons que l'un des $\pi_i[d_i]$, avec $i = 1, \ldots, r$, soit égal à $\Delta_{11}[12]$. On a donc une décomposition de la forme $\psi = \Delta_{11}[12] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$. Observons que ψ'_∞ a pour valeurs propres (simples) les entiers $\pm(g-12), \ldots, \pm 1$ et 0. La contemplation de la table IX.7 montre donc : $\delta(\pi_F, 1) = 0$ si $g - 12 < 9$, $\delta(\pi_F, 1) \leq 1$ si $g < 23$, et $\delta(\pi_F, 1) \leq 2$ dans tous les cas.

Si l'on a $I = I'$, l'assertion (e) de la proposition VIII.7.3 entraîne $\delta(\pi_F, 1) \geq g - 14$. On en déduit $g \leq 16$ et $\psi' = [2g - 23]$, car $\psi' \in \mathcal{X}_\Pi$, ce qui contredit $I = I'$ et $g > 12$. On a donc $I' = \emptyset$, $|I| = 1$, et aussi $\frac{d-1}{2} \leq g - 12$ car $[d]$ est un constituant de ψ'. L'assertion (d) de la proposition VIII.7.3 entraîne d'autre part $\frac{d+1}{4} \geq g - 12 - \delta(\pi_F, 1) \geq g - 14$. On en tire successivement $g \leq 17$, $\delta(\pi_F, 1) = 0$, $g = 13$ et $\psi' = [3]$. La formule VIII.(7.4) s'écrit dans ce cas $\xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) = \xi_{\mathrm{B}}(s, \pi_F, \mathrm{St})$. Une considération de l'ordre d'annulation en $s = 1$ de ces fonctions conduit à une contradiction : la non-annulation de $\mathrm{L}(\frac{1}{2}, \Delta_{11})$ montre $\mathrm{ord}_{s=1}\, \xi_{\mathrm{A}}(s, \pi_F, \mathrm{St}) = -2$, mais d'après Mizumoto (§VIII.7) nous avons aussi $\mathrm{ord}_{s=1}\, \xi_{\mathrm{B}}(s, \pi_F, \mathrm{St}) \geq -1$.

Démonstration de l'assertion (2). Supposons maintenant qu'il existe un entier i tel que $\pi_i = \mathrm{Sym}^2\Delta_{11}$. Dans ce cas, on a $d_i = 1$ et il n'existe donc d'après Arthur qu'un seul tel entier i. D'après l'assertion (1) et le lemme 2.3 (i), on a $|I| = 2$, et donc $d \geq 3$. Si l'on a $I' \neq \emptyset$, la considération de la valeur propre double 1 de ψ_∞ et le lemme 2.3 (ii) montrent que l'on a une décomposition $\psi = \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10] \oplus [1] \oplus [d] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$. En particulier, on a $\frac{d-1}{2} \leq g - 12$ et $\delta(\pi_F, 1) \leq 2$. La proposition VIII.7.3 (c) entraîne $\frac{d+1}{4} \geq g - 13$, puis $g \leq 15$. Les valeurs propres de ψ'_∞ sont donc parmi $\pm 3, \pm 2, \pm 1$, ce qui contredit $\psi' \in \mathcal{X}_\Pi$. Au final, nous avons donc $I' = \emptyset$, $|I| = 2$, $d \geq 5$ et $\frac{d+1}{2} \geq g - 9 - \delta(\pi_F, 1)$ d'après le point (b) *loc. cit.*

Supposons $\delta(\pi_F, \frac{d+1}{2}) > 0$. La description de Ψ_0 montre que cela entraîne $d = 5$ et que l'on a une décomposition de la forme $\psi = \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[6] \oplus [5] \oplus [3] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$. En particulier, on a $g = 23$ et $\delta(\pi_F, 1) \geq 11$, ce qui est absurde. On a donc $\delta(\pi_F, 1) \geq 2$ d'après le second point du (b) de la proposition *loc. cit.* .

Supposons enfin que ψ "contienne" un élément $\phi \in \Psi_0$ tel que 11 est valeur propre de ϕ_∞. Dans ce cas, on a $g = 23$ et $\frac{d-1}{2} \leq 10$. L'inégalité $\frac{d+1}{2} \geq g - 9 - \delta(\pi_F, 1)$ donne alors $\delta(\pi_F, 1) \geq 3$. Par inspection de la table IX.7 cela force $\frac{d-1}{2} \leq 7$, puis $\delta(\pi_F, 1) \geq 6$, ce qui est absurde. Ainsi, la seule possibilité restante est celle d'une décomposition de la forme $\psi = \mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[2] \oplus \Delta_{17}[4] \oplus [d] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$. Dans ce cas, on a les inégalités $g - 12 \geq 9$ et $\frac{d-1}{2} \leq 7$. Elles entraînent $\delta(\pi_F, 1) \geq 4$: une contradiction.

Fin de la démonstration. La conclusion des assertions (1) et (2), compte tenu du lemme 2.3 (i), est que l'on a $|I| = 3$ et $|I'| = 1$. Supposons $\delta(\pi_F, \frac{d+1}{2}) > 0$. Cela entraîne $d = 5$ et que l'on a une décomposition de la forme $\psi = \Delta_{17}[6] \oplus [5] \oplus [3] \oplus [1] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$. De plus, on dispose de l'inégalité $\delta(\pi_F, 1) \geq g - 11$ donnée par la proposition VIII.7.3 (a). On en tire $g \leq 14$, ce qui entraîne $g = 14$, et $\delta(\pi_F, 1) = 3$: c'est absurde étant donné la description de Ψ_0. En conclusion, la seconde assertion de la proposition VIII.7.3 (a) entraîne $\delta(\pi_F, 1) = 3$. Un examen de la table IX.7 montre que l'on a une décomposition de la forme $\psi = \Delta_{21}[2] \oplus \Delta_{17}[2] \oplus \psi'$ avec $\psi' \in \mathcal{X}_\Pi$ et que l'élément ψ'_∞ admet les valeurs propres $\pm 10, \pm 9$ et ± 8. En particulier, on a $g - 12 \geq 10$ et $\frac{d-1}{2} \leq 7$. Mais l'assertion (a) *loc. cit.* montre ausi $\frac{d+1}{2} \geq g - 11 \geq 11$, qui entraîne $d \geq 23$, ce qui est absurde. □

Corollaire 5.7. *Soit $1 \leq g \leq 23$. L'application $\vartheta_g : \mathbb{C}[\mathrm{X}_{24}] \to \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est surjective, et la dimension de $\mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est donnée par la table :*

g	1	2	3	4	5	6	7	8	9	10	11	≥ 12
$\dim \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$	2	3	4	6	8	11	14	18	20	22	23	24

Démonstration. On procède par récurrence sur l'entier g. Le résultat est bien connu si $g = 1$. Si $g > 1$ on rappelle que l'on dispose de l'opérateur de Siegel $\Phi_g : \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z})) \longrightarrow \mathrm{M}_{12}(\mathrm{Sp}_{2g-2}(\mathbb{Z}))$; il vérifie la relation $\Phi_g \circ \vartheta_g = \vartheta_{g-1}$. Par hypothèse de récurrence, l'application $\Phi_g \circ \vartheta_g$ est donc surjective. Mais l'application ϑ_g : Ker $\vartheta_{g-1} \to \mathrm{S}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est également surjective si $g \leq 12$ d'après l'assertion (ii) du théorème 5.2, ainsi que si $12 < g \leq 23$ d'après la proposition 5.6. Cela démontre la surjectivité de ϑ_g et Φ_g. □

Remarque 5.8. Il n'est pas vrai que toute forme de Siegel parabolique de poids 16 pour $\mathrm{Sp}_{2g}(\mathbb{Z})$ est une combinaison linéaire de séries thêta d'éléments de X_{32}, comme le démontre le corollaire VII.3.5 (le contre-exemple donné étant en genre $g = 14$).

5.9. Formes de poids ≤ 11

Théorème[⋆] **5.10.** *Soient $k, g \in \mathbb{Z}$ tels que $k \leq 11$ et $g \geq 1$. Alors on a $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$, à moins que l'on ne soit dans l'un des cas suivants :*

(i) $k = 8$ *et* $g = 4$. *Dans ce cas* $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ *est de dimension* 1, *engendré par la forme de Schottky, de paramètre standard* $\Delta_{11}[4] \oplus [1]$.

(ii) $k = 10$ *et* $g = 2$. *Dans ce cas* $\mathrm{S}_{10}(\mathrm{Sp}_4(\mathbb{Z}))$ *est de dimension* 1, *engendré par la forme de Saito-Kurorawa* F_{10}, *de paramètre standard* $\Delta_{17}[2] \oplus [1]$.

(iii) $k = 10$ *et* $g = 4$. *Dans ce cas* $\mathrm{S}_{10}(\mathrm{Sp}_8(\mathbb{Z}))$ *est de dimension* 1, *engendré par la forme d'Ikeda de paramètre standard* $\Delta_{15}[4] \oplus [1]$.

(iv) $k = 10$ *et* $g = 6$. *Dans ce cas* $\mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z}))$ *est de dimension* 1, *engendré par une forme de paramètre standard* $\Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1]$.

(v) $k = 10$ *et* $g = 8$. *Dans ce cas* $\mathrm{S}_{10}(\mathrm{Sp}_{16}(\mathbb{Z}))$ *est de dimension* 1, *engendré par la forme d'Ikeda de paramètre standard* $\Delta_{11}[8] \oplus [1]$.

(vi) $k = 11$ *et* $g = 6$. *Dans ce cas toute forme propre de* $\mathrm{S}_{11}(\mathrm{Sp}_{12}(\mathbb{Z}))$ *a pour paramètre standard* $\Delta_{17}[4] \oplus \Delta_{11}[2] \oplus [1]$. *De plus, si l'on admet la conjecture VIII.4.22, on a* $\mathrm{S}_{11}(\mathrm{Sp}_{12}(\mathbb{Z})) = 0$.

Observons que le cas particulier $g = 2$ du théorème ci-dessus se déduit du travail d'Igusa [Igu62], qui montre que $\mathrm{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$ est nul si $k \leq 11$, de dimension 1 et engendré par F_{10} si $k = 10$: voir le §IX.1. Rappelons aussi que l'annulation $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ pour tout $g \geq 1$ et tout $k \leq 6$ et due à Duke et Imamoğlu [DI98].

Démonstration. Soient $k \leq 11$ et $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ une forme propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$, de représentation engendrée $\pi_F \in \Pi_{\mathrm{disc}}(\mathrm{Sp}_{2g})$, et de paramètre standard $\psi = \psi(\pi_F, \mathrm{St}) = \oplus_{i=1}^r \pi_i[d_i]$ d'après Arthur. D'après la théorie des formes singulières, on a $g \leq 2k$. Rappelons que $\psi(\pi_F, \mathrm{St})_\infty$ admet pour valeurs propres les $2g+1$ entiers 0 et $\pm(k-j), j = 1, \ldots, g$ d'après le corollaire VI.3.6. Les représentations π_i sont donc algébriques de poids motivique ≤ 20, sauf peut-être si $g = 2k = 22$ auquel cas l'une d'entre elles peut être de poids motivique 21 ou 22 (les autres étant de poids motivique ≤ 20). Supposons dans un premier temps $(g, k) \neq (22, 11)$. Le théorème 3.2 assure que les π_i sont parmi l'ensemble

$$\Pi = \{1, \Delta_{11}, \Delta_{15}, \Delta_{17}, \Delta_{19}, \Delta_{19,7}\}.$$

Il s'ensuit que ψ est une somme, sans multiplicités d'après Arthur [Art13, Thm. 1.5.2], d'éléments de la forme $[m]$ avec $m \geq 1$ impair, ou de l'ensemble

$$\Psi := \{\Delta_w[d] \mid d \equiv 0 \bmod 2, w + d - 1 \leq 20\} \coprod \{\Delta_{19,7}[2]\}.$$

Lemme* **5.11.** *Si $F \in \mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est une forme propre avec $k \leq 11$ et $g \geq 1$ alors on a $k > g$. De plus, si $\psi = \oplus_{i=1}^{k} \pi_i[d_i]$ désigne le paramètre standard de F, il existe un unique $i \in \{1, \ldots, r\}$ tel que $\pi_i = 1$, et l'on a $d_i = 1$.*

Admettons temporairement ce lemme et poursuivons la démonstration. On observera que son énoncé est évident sous l'hypothèse $k > g + 1$, qui est un cas déjà suffisament intéressant. On a donc $k > g$ et ψ est une somme sans multiplicités de $[1]$ et d'éléments de Ψ. Nous nous sommes ainsi ramenés à un assez petit nombre de possibilités à étudier, ce que nous ferons au cas par cas.

Cas $k \leq 6$. Dans ce cas, on a $\mathrm{w}(\pi_i) \leq 10$ pour tout i, et donc $\psi = [1]$ et la forme F n'existe pas !

Cas $k = 7$. Dans ce cas, on a $\mathrm{w}(\pi_i) \leq 11$, et donc $\pi_i \in \{\Delta_{11}, 1\}$, pour tout i. La seule possibilité est $\psi = \Delta_{11}[2] \oplus [1]$, en particulier $g = 2$, un cas que nous avons déjà traité : la forme F n'existe pas non plus car d'après Igusa on a l'annulation $\dim \mathrm{S}_7(\mathrm{Sp}_4(\mathbb{Z})) = 0$.

Cas $k = 8$. La seule possibilité est $\psi = \Delta_{11}[4] \oplus [1]$. En particulier, $g = 8$ et $F \in \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. Observons incidemment que si l'on applique notre raisonnement au cas où $F = J = \vartheta_4(\mathrm{E}_8 \oplus \mathrm{E}_8) - \vartheta_4(\mathrm{E}_{16})$ est la forme de Schottky (voir le §V.2), nous obtenons une nouvelle démonstration du fait que le paramètre standard de la représentation engendrée par J est $\Delta_{11}[4] \oplus [1]$ (corollaire VII.2.6 (i)), puisque c'est l'unique paramètre possible.

Pour conclure la démonstration du théorème 5.10 pour $k = 8$, il suffit d'invoquer le fait que $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ est de dimension 1 (et engendré par la forme de Schottky) d'après un résultat de Poor et Yuen [PY96] déjà mentionné au §V.2. Donnons un autre argument. Observons que F est dans l'image de l'application linéaire $\vartheta_4 : \mathbb{C}[\mathrm{X}_{16}] \longrightarrow \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$. En effet, le critère de Böcherer s'applique puisque la fonction

$$\mathrm{L}(s, \pi_F, \mathrm{St}) = \zeta(s) \prod_{i=0}^{3} \mathrm{L}(s + i - 3/2, \Delta_{11})$$

ne s'annule pas en $s = 4$ (§VII.2.4). Comme $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ est engendré par des formes propres, cela montre $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})) \subset \mathrm{Im}\, \vartheta_4$. Cela conclut car il est évident que $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})) \cap \mathrm{Im}\, \vartheta_4$ est engendré par J (§V.2). Soulignons que cet argument pour démontrer $\dim \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})) = 1$ n'est pas nouveau : il avait déjà été observé par Duke et Imamoğlu dans [DI98], qui ont pu démontrer

que $\mathrm{L}(s, \pi_F, \mathrm{St})$ admet nécessairement un pôle simple en $s = 1$, sans toutefois pouvoir en déduire directement la forme exacte à priori du paramètre ψ.

Donnons enfin un troisième argument pour démontrer que $\mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z}))$ est de dimension 1. En effet, c'est une conséquence immédiate de notre analyse ci-dessus et du résultat général suivant d'Ikeda, précisant son propre théorème VII.3.1, qui s'avèrera bien utile dans la suite de cette démonstration (voir aussi l'exemple VIII.5.3).

Lemme 5.12. [Ike13, Thm. 7.1, §15] *Soient m et g des entiers pairs, ainsi que $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ la représentation engendrée par une forme propre de poids m pour $\mathrm{SL}_2(\mathbb{Z})$. Il existe une forme $G \in \mathrm{S}_{\frac{m+g}{2}}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ propre pour $\mathrm{H}(\mathrm{Sp}_{2g})$ et telle que $\psi(\pi_G, \mathrm{St}) = \pi[g] \oplus [1]$ si, et seulement si, $m \equiv g \bmod 4$. De plus, si cette condition est satisfaite alors la forme G est unique à un scalaire près.*

Cas $k = 9$. On trouve cette fois-ci trois possibilités pour ψ, correspondant respectivement à des genres $2, 4$ et 6. Celle de genre 2 est $\psi = \Delta_{15}[2] \oplus [1]$, qui ne se produit pas car $\dim \mathrm{S}_9(\mathrm{Sp}_4(\mathbb{Z})) = 0$ d'après Igusa. La seconde est

$$\psi = \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [1],$$

pour laquelle $g = 4$. Considérons l'application linéaire (§V.4.1)

$$\vartheta_{5,4} : \mathrm{M}_{\mathrm{H}_{5,4}(\mathbb{R}^8)}(\mathrm{O}_8) \to \mathrm{S}_9(\mathrm{Sp}_8(\mathbb{Z})).$$

Comme on a $\mathrm{L}(\frac{1}{2}, \Delta_w) \neq 0$ pour $w = 11, 15$, le produit $\zeta(s) \prod_{i=0}^{1} \mathrm{L}(s + i - \frac{1}{2}, \Delta_{11})\mathrm{L}(s + i - \frac{1}{2}, \Delta_{15})$ admet un pôle simple en $s = 1$, de sorte que le critère de Böcherer s'applique et montre que $\vartheta_{5,4}$ est surjective. Pour éliminer ce second cas, il suffit donc de montrer $\mathrm{M}_{\mathrm{H}_{5,4}(\mathbb{R}^8)}(\mathrm{O}_8) = 0$. Mais cette annulation est conséquence des tables de [CR12, §2] ; nous avons d'ailleurs déjà rencontré cette propriété au §VII.4. Une manière plus directe de l'obtenir et de constater que par trialité (§V.4.14), on a pour tout entier $d \geq 0$ pair l'égalité

$$\dim \mathrm{M}_{\mathrm{H}_{d,1}(\mathbb{R}^8)}(\mathrm{SO}_8) = \dim \mathrm{M}_{\mathrm{H}_{d/2,4}(\mathbb{R}^8)}(\mathrm{O}_8). \tag{5.3}$$

On conclut alors car $\mathrm{M}_{\mathrm{H}_{10,1}(\mathbb{R}^8)}(\mathrm{SO}_8) = 0$ d'après le lemme V.4.2.

Pour se rassurer, vérifions que ce dernier raisonnement est cohérent avec la formule du théorème 5.2, autrement dit, que la formule de multiplicité d'Arthur suggère bien que $\Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [1]$ n'est pas le paramètre standard d'une forme de Siegel. Mais cela vient de ce que dans les notations de ce théorème, on a $\chi(s_2) = -1$ et $\varepsilon(\Delta_{15} \times \Delta_{11}) = \varepsilon(\Delta_{11}) = 1$.

La dernière possibilité est $\psi = \Delta_{11}[6] \oplus [1]$, pour laquelle $g = 6$. Mais elle ne se produit pas d'après Ikeda car $6 \not\equiv 12 \bmod 4$ (Lemme 5.12).

Cas $k = 10$. On trouve cette fois-ci quatre possibilités pour ψ, correspondant respectivement à des genres $2, 4, 6$ et 8, à savoir

$$\Delta_{17}[2] \oplus [1], \Delta_{15}[4] \oplus [1], \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1], \Delta_{11}[8] \oplus [1].$$

Ils sont tous traités par le lemme 5.12, sauf celui de genre 6, à savoir $\psi = \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1]$. Cela démontre les assertions (ii) à (v) du théorème, excepté le fait que $\dim \mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z})) = 1$ dans le (iv).

Démontrons maintenant cette assertion. Nous avons vu ci-dessus que toute forme propre de $\mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z}))$ a pour paramètre standard $\Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1]$. Une inspection de la formule de multiplicité d'Arthur suggère qu'une telle forme existe et a multiplicité 1. Procédons autrement. Combiné au critère de Böcherer, cette propriété montre aussi que l'application linéaire

$$\vartheta_{2,6} : \mathrm{M}_{\mathrm{H}_{2,6}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \to \mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z}))$$

est surjective. Pour conclure, il suffit donc de montrer $\dim \mathrm{M}_{\mathrm{H}_{2,6}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 1$ et $\vartheta_{2,6} \neq 0$. Mais l'assertion de dimension découle du (i) du corollaire 5.14. La vérification de la non-nullité de $\vartheta_{2,6}$ sera reportée à la fin du paragraphe pour ne pas interrompre le fil de cette démonstration.

Cas $k = 11$. Ce cas est déjà relativement fastidieux. On trouve cette fois-ci 8 paramètres ψ possibles : 1 en genre 2, 2 en genre 4, 2 en genre 6, 2 en genre 8 et 1 en genre 10.

Les deux paramètres de genre 4 sont $\Delta_{17}[4] \oplus [1]$ et $\Delta_{19}[2] \oplus \Delta_{15}[2] \oplus [1]$. Le premier ne se produit pas d'après Ikeda (Lemme 5.12). Considérons l'application $\vartheta_{7,4} : \mathrm{M}_{\mathrm{H}_{7,4}(\mathbb{R}^8)}(\mathrm{O}_8) \to \mathrm{S}_{11}(\mathrm{Sp}_8(\mathbb{Z}))$. Le critère de Böcherer montre alors que $\vartheta_{7,4}$ est surjective. Nous allons voir qu'elle est nulle, ce qui montrera que le cas $\psi = \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus [1]$ ne se produit pas non plus. Observons pour cela que la relation (5.3) assure $\dim \mathrm{M}_{\mathrm{H}_{7,4}(\mathbb{R}^8)}(\mathrm{O}_8) = 1$, étant donné $\dim \mathrm{M}_{\mathrm{H}_{14,1}(\mathbb{R}^8)}(\mathrm{SO}_8) = 1$ (Lemme V.4.2). D'après le théorème VII.2.1, on sait qu'il existe une forme propre $G \in \mathrm{M}_{\mathrm{H}_{7,4}(\mathbb{R}^8)}(\mathrm{O}_8)$ engendrant une représentation dans $\Pi_{\mathrm{disc}}(\mathrm{O}_8)$ de paramètre standard $\Delta_{17}[4]$; on a donc $\mathrm{M}_{\mathrm{H}_{7,4}(\mathbb{R}^8)}(\mathrm{O}_8) = \mathbb{C}G$. Il suffit alors de prouver $\vartheta_{7,4}(G) = 0$. Si cette forme est non nulle, les relations d'Eichler-Rallis montrent que $\vartheta_{7,4}(G)$ est propre et de paramètre standard $\Delta_{17}[4] \oplus [1]$ (Corollaire VII.1.3), ce qui contredit le lemme 5.12 (ainsi que le critère de Böcherer !).

Les deux paramètres possibles de genre 6 sont $\Delta_{15}[6] \oplus [1]$ et $\Delta_{17}[4] \oplus \Delta_{11}[2] \oplus [1]$. Le premier est encore exclu par Ikeda (Lemme 5.12). Le second ne devrait pas se produire d'après la formule de multiplicité d'Arthur. En effet, dans les notations du théorème 5.2) on a $\chi(s_2) = -1$ et $\varepsilon(\Delta_{11} \times \Delta_{17})^2 \varepsilon(\Delta_{11}) = 1$. Cependant, nous ne voyons pas comment l'éliminer directement, ce qui explique le point (vi) de l'énoncé du théorème. Observons que l'on ne tire rien cette fois-ci de l'application $\vartheta_{3,6} : \mathrm{M}_{\mathrm{H}_{3,6}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \to \mathrm{S}_{11}(\mathrm{Sp}_{12}(\mathbb{Z}))$, car le critère de Böcherer montre $\vartheta_{3,6} = 0$ (en fait on a $\mathrm{M}_{\mathrm{H}_{3,6}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 0$ d'après le lemme 5.14).

Les deux paramètres possibles de genre 8 sont $\Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [1]$ et $\Delta_{19}[2] \oplus \Delta_{11}[6] \oplus [1]$. Le critère de Böcherer montre alors que l'application

$$\vartheta_{3,8} : \mathrm{M}_{\mathrm{H}_{3,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \to \mathrm{S}_{11}(\mathrm{Sp}_{16}(\mathbb{Z}))$$

est surjective, comme on le vérifie immédiatement à l'aide de la proposition 3.39. On en déduit $\mathrm{S}_{11}(\mathrm{Sp}_{16}(\mathbb{Z})) = 0$ car on a $\mathrm{M}_{\mathrm{H}_{3,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 0$ d'après le lemme 5.14 (ii).

Le dernier paramètre, de genre 10, est $\Delta_{11}[10] \oplus [1]$, mais il n'apparaît pas d'après le lemme 5.12, ce qui conclut la démonstration du théorème. Il ne reste qu'à démontrer le lemme 5.11. $\square$

Démonstration. (Démonstration du lemme 5.11) Supposons $k \leq g$ et posons $I = \{i, \pi_i = 1\}$. Supposons de plus $(k, g) \neq (11, 22)$ pour commencer. L'analyse précédant l'énoncé du lemme montre $\psi = \oplus_{i=1}^{r} \pi_i[d_i]$, où pour tout entier i, soit $\pi_i[d_i]$ appartient à l'ensemble Ψ introduit *loc. cit.*, soit $\pi_i = 1$. Le lemme 2.3 montre $|I| = 3$ et que l'hypothèse (7.3) de l'énoncé de la proposition VIII.7.3 est satisfaite. En particulier, les conclusions du point (a) de cette proposition affirment que l'on a soit $\delta(\pi_F, 1) > 2 - \nu$, où $\nu \in \{0, 1\}$ est tel que $\nu \equiv k \bmod 2$, soit $\delta(\pi_F, 3) > 0$.

D'après la proposition 3.39, la quantité $\delta(\pi_F, a)$ est le nombre de constituants de ψ de la forme $\Delta_{17}[d']$ avec $d' \geq 2a$. Si un tel constituant est dans Ψ, cela force $d \in \{2, 4\}$, ce qui montre $\delta(\pi_F, 3) = 0$ et $\delta(\pi_F, 1) \leq 2$ dans tous les cas. La seule possibilité est donc $\delta(\pi_F, 1) = 2$, $\nu = 1$ (i.e. k impair), et

$$\psi = \Delta_{17}[2] \oplus \Delta_{17}[4] \oplus \phi,$$

où ϕ est une somme sans multiplicités d'éléments de $\Psi \coprod \{[m], m \geq 1\}$. En particulier, 10 (resp. 9) est valeur propre (resp. valeur propre double) de ψ_∞. Comme k est impair cela entraîne $k = 11$ et $20 \leq g \leq 22$. Comme il n'y a pas de forme de Siegel non nulle de poids et genre tous deux impairs, et

puisqu'on a supposé $(k,g) \neq (11,22)$, la seule possibilité est $g = 20$. Le point (a) de la proposition VIII.7.3 entraîne alors que $[d]$ est un constituant de ϕ avec $d \geq 21$, ce qui est absurde car les valeur propres de ϕ_∞ sont de valeur absolue ≤ 7.

Nous avons donc démontré $k > g$. En particulier, il existe un unique entier i tel que $\pi_i = 1$, et il ne reste qu'à montrer $d_i = 1$. C'est évident si $k > g+1$, et l'on peut donc supposer que $k = g+1$. La proposition VIII.7.1 entraîne

$$\delta(\pi_F, \frac{d_i+1}{2}) > 0. \tag{5.4}$$

Mais un argument similaire à celui donné ci-dessus montre $\delta(\pi_F, 2) = 0$ si $k > g$, et donc $d_i = 1$, à moins que l'on ne soit dans le cas particulier $\psi = \Delta_{17}[4] \oplus \phi$, ϕ étant la somme de $[d_i]$ et d'éléments de Ψ. Dans ce cas, on a $k = 11$ et $g = 10$, de sorte que ϕ_∞ admet pour valeurs propres 0 et les entiers $\pm j$ avec $1 \leq j \leq 6$. Une inspection des éléments de Ψ montre que cela force $\phi = \Delta_{11}[2] \oplus [9]$ ou $\phi = [13]$. En particulier, on a $d_i \geq 9$, et la formule (5.4) contredit $\delta(\pi_F, 3) = 0$.

Il ne reste qu'à exclure la possibilité $(k,g) = (11,22)$. Le théorème 3.2 entraîne dans ce cas que chacun des π_i est dans l'ensemble

$$\{1, \Delta_{11}, \Delta_{15}, \Delta_{17}, \Delta_{19}, \Delta_{21}, \Delta_{19,7}, \Delta_{21,5}, \Delta_{21,9}, \Delta_{21,13}, \mathrm{Sym}^2\Delta_{11}\}. \tag{5.5}$$

Nous allons encore appliquer la proposition VIII.7.3, dont les hypothèses sont satisfaites grâce au lemme 2.3. Si l'on pose $I' = \{i \in I, d_i = 1\}$, on a donc

$$\sum_{i \in I - I'} [\frac{d_i+1}{4}] \geq 9 - \delta(\pi_F, 1) + |I'| + 2|I - I'|. \tag{5.6}$$

D'après la proposition 3.39, si pour un entier $1 \leq i \leq r$ on a $\mathrm{L}(\frac{1}{2}, \pi_i) = 0$ et $d_i \equiv 0 \bmod 2$, alors on a $\pi_i \in \{\Delta_{17}, \Delta_{21}\}$ et $\mathrm{ord}_{s=1/2}\mathrm{L}(s, \pi_i) = 1$. Étant donné que ψ_∞ admet la valeur propre 11 (resp. 9) avec multiplicité 1 (resp. 2), cela montre l'inégalité $\delta(\pi_F, 1) \leq 3$.

Supposons $\delta(\pi_F, 1) = 3$. Dans ce cas un examen de la table IX.7 montre que l'on a une décomposition $\psi = \Delta_{21}[2] \oplus \Delta_{17}[4] \oplus \Delta_{17}[2] \oplus \phi$ où ϕ est une somme sans multiplicités d'éléments de $\Psi \coprod \{[m], m \geq 1\}$, et ϕ_∞ a ses valeurs propres ≤ 7 en valeur absolue. Le lemme 2.3 entraîne $|I| = 3$ et si l'on pose $d = \mathrm{Max}\{d_i, i \in I\}$ on a donc $\frac{d-1}{2} \leq 7$, alors que l'inégalité (5.6) entraîne $\frac{d+1}{2} > 11$, ce qui est absurde.

On a donc $\delta(\pi_F, 1) \leq 2$, de sorte que le membre de droite de l'inégalité (5.6) est ≥ 7. Cela entraîne $I \neq I'$. Mieux, sous l'hypothèse $I - I' = \{j\}$

on obtient $\frac{d_j+1}{4} \geq 8$, et donc $d_j \geq 31$: c'est absurde car on a trivialement $d_i \leq 23$ si $i \in I$. Ainsi l'ensemble $I - I'$ a deux éléments $\{a, b\}$, avec disons $1 < d_a < d_b$. L'inégalité (5.6) entraîne $\frac{d_b+1}{2} > 11 + |I'|$, qui s'écrit aussi $d_b > 21 + 2|I'|$. Or on a évidemment $d_b \leq 23$ et $d_i \equiv 1 \bmod 2$ pour $i \in I$. Cela impose $d_b = 23$ et $|I'| = 1$. On en déduit $d_a \geq 23$ en utilisant à nouveau (5.6), ce qui contredit $d_a < d_b$. □

Proposition 5.13. *Soit $L \subset \mathbb{R}^{16}$ un réseau unimodulaire pair. On note V_λ la représentation irréductible de $\mathrm{SO}(\mathbb{R}^{16})$ de plus haut poids*

$$\lambda = m_1\varepsilon_1 + m_2\varepsilon_2 + \cdots + m_8\varepsilon_8, \quad \text{avec} \quad m_1 \geq m_2 \geq \cdots \geq m_8 \geq 0$$

(§VI.4.3), et $V_\lambda^{\mathrm{SO}(L)} \subset V_\lambda$ le sous-espace des invariants par le groupe fini $\mathrm{SO}(L) \subset \mathrm{SO}(\mathbb{R}^{16})$. On suppose $m_1 \leq 4$.

(i) Si $L \simeq \mathrm{E}_{16}$, alors $V_\lambda^{\mathrm{SO}(L)} = 0$, à mois que λ ne soit égal à 0 ou de la forme $4(\sum_{i=1}^k \varepsilon_i)$ avec $1 \leq k \leq 8$, auxquels cas $\dim V_\lambda^{\mathrm{SO}(L)} = 1$.

(ii) Si $L \simeq \mathrm{E}_8 \oplus \mathrm{E}_8$, alors les couples $(\lambda, \dim V_\lambda^{\mathrm{SO}(L)})$ tels que $V_\lambda^{\mathrm{SO}(L)} \neq 0$ sont donnés par la table C.6.

Démonstration. Il s'agit d'un calcul basé sur la formule du caractère de Weyl, à la manière de ceux effectués dans [CR12, §2]. Nous remercions Olivier Taïbi de nous avoir fait bénéficier de son propre algorithme, plus rapide que celui utilisé *loc. cit.*, pour l'évaluation finale. Il nécessite, comme travail préliminaire, une énumération des polynômes caractéristiques des éléments de $\mathrm{SO}(L)$, ainsi que leurs multiplicités. Nous renvoyons à la feuille de calculs [CL `PARI`] pour une justification des affirmations qui vont suivre.

Dans le cas du réseau $L = \mathrm{E}_{16}$, on a $\mathrm{O}(L) = \mathrm{W}(\mathbf{D}_{16}) \simeq \{\pm 1\}^{15} \ltimes \mathfrak{S}_{16}$, et l'énumération ne pose pas de difficulté à l'aide de l'ordinateur (si l'on se restreint aux éléments de déterminant 1, on trouve par exemple 823 polynômes). Dans le cas du réseau $L = \mathrm{E}_8 \oplus \mathrm{E}_8$, le groupe $\mathrm{O}(L)$ est le produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathrm{O}(\mathrm{E}_8)^2$ induit par l'échange des deux facteurs. Les polynômes caractéristiques des classes de conjugaison d'éléments de $\mathrm{O}(\mathrm{E}_8) = \mathrm{W}(\mathbf{E}_8)$, ainsi que les cardinaux de ces classes, ont été déterminés par Carter [Car72, Table 11]. Cela permet de conclure, en observant que le déterminant d'une matrice par blocs de la forme $\begin{bmatrix} X\,\mathrm{I}_m & g \\ h & X\,\mathrm{I}_m \end{bmatrix}$, avec $g, h \in \mathrm{M}_m$ et X une indéterminée, vaut $\det(X^2\mathrm{I}_m - gh)$. Après calcul, on trouve par exemple 1544 polynômes caractéristiques pour $\mathrm{SO}(\mathrm{E}_8 \oplus \mathrm{E}_8)$.

Mentionnons qu'avec un peu de patience, qui à ce stade manque aux auteurs, il devrait être également possible de démontrer "à la main" la proposition ! □

Corollaire 5.14. *(i) On a les égalités*

$$\dim \mathrm{M}_{\mathrm{H}_{2,6}(\mathbb{R}^{16})}(\mathrm{SO}_{16}) = \dim \mathrm{M}_{\mathrm{H}_{2,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 1.$$

(ii) Pour tout entier $1 \leq g \leq 8$*, on a* $\mathrm{M}_{\mathrm{H}_{3,g}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 0$.

Démonstration. On rappelle que si U est une représentation de $\mathrm{O}_n(\mathbb{R})$, dont on note U' la restriction à $\mathrm{SO}_n(\mathbb{R})$, alors $\mathrm{M}_U(\mathrm{O}_n)$ est un sous-espace de $\mathrm{M}_{U'}(\mathrm{SO}_n)$ (c'est l'application res introduite au §IV.4.4). De plus, la formule IV.(4.1) entraîne l'égalité

$$\dim \mathrm{M}_{U'}(\mathrm{SO}_n) = \dim(U'^{\mathrm{SO}(\mathrm{E}_{16})}) + \dim(U'^{\mathrm{SO}(\mathrm{E}_8 \oplus \mathrm{E}_8)}).$$

Si $g < r$, la représentation irréductible $\mathrm{H}_{d,g}(\mathbb{R}^{2r})$ de $\mathrm{O}(\mathbb{R}^{2r})$ reste irréductible quand on la restreint à $\mathrm{SO}(\mathbb{R}^{2r})$; si $g = r$ elle se décompose en une somme de représentations non isomorphes $\mathrm{H}_{d,g}(\mathbb{R}^{2r})^{\pm}$, conjuguées sous l'action extérieure de $\mathrm{O}(\mathbb{R}^{2r})$ (§V.4.14). On rappelle que d'après la formule V.(4.1), le plus haut poids de $\mathrm{H}_{d,g}(\mathbb{R}^{2r})$ est $d \sum_{i=1}^{g} \varepsilon_i$ si $g < r$, et que ceux de $\mathrm{H}_{d,g}(\mathbb{R}^{2g})^{\pm}$ sont $d(\pm\varepsilon_g + \sum_{i=1}^{g-1} \varepsilon_i)$. Le (ii) découle alors de la proposition 5.13, car les deux dimensions en question sont nulles pour les poids de la forme $3(\sum_{i=1}^{g} \varepsilon_i)$, $g \geq 1$. Le (i) se démontre de la même manière, les invariants non nuls provenant seulement de $\mathrm{E}_8 \oplus \mathrm{E}_8$, en observant l'isomorphisme

$$\mathrm{M}_{\mathrm{H}_{d,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \simeq \mathrm{M}_{\mathrm{H}_{d,8}(\mathbb{R}^{16})^{\pm}}(\mathrm{SO}_{16})$$

(c'est l'application ind du §IV.4.4). □

Pour terminer ce paragraphe, disons un mot sur la construction par série thêta d'un élément de $\mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z}))$. Partons du réseau $L = \mathrm{E}_8 \oplus \mathrm{E}_8$ de $\mathbb{R}^8 \oplus \mathbb{R}^8$. Soient $e = (e_1, \ldots, e_6)$ un sextuplet d'éléments de $L \otimes \mathbb{C}$ engendrant un sous-espace isotrope de dimension 6, ainsi que $P_e(v_1, \ldots, v_6) = \text{dét}\,[e_i \cdot v_j]_{1 \leq i,j \leq 6}$, de sorte que $P_e^2 \in \mathrm{H}_{2,6}(L \otimes \mathbb{R})$. Soient $Q \subset L$ un réseau de rang 6 et $v_1, \ldots, v_6$ une $\mathbb{Z}$-base de Q. Pour des raisons semblables à celles évoquées au §V.4.21, l'élément $P_e(v_1, \ldots, v_6)^2$ ne dépend pas du choix de la $\mathbb{Z}$-base v_i de Q, et peut donc être noté $P_e(Q)^2$. Le coefficient de Fourier de $\vartheta_{2,6}(\mathrm{E}_8 \oplus \mathrm{E}_8, P_e^2)$ correspondant à la matrice de Gram d'une $\mathbb{Z}$-base de Q est alors donné par la formule

$$\mathrm{c}_Q(P_e^2) = |\mathrm{O}(Q)| \sum_{M \subset \mathrm{E}_8 \oplus \mathrm{E}_8} P_e(M)^2,$$

la somme portant sur les sous-réseaux M isométriques à Q. Nous allons appliquer ceci au cas particulier où $Q \simeq \mathrm{Q}(R)$ avec $R = \mathbf{D}_6$ ou $R = \mathbf{E}_6$. On

posera $\mathrm{E}_6 := \mathrm{Q}(\mathbf{E}_6)$. On observe tout d'abord que si un tel sous-réseau est dans $\mathrm{E}_8 \oplus \mathrm{E}_8$, il est nécessairement inclus dans l'un des deux facteurs E_8. De plus, il n'est pas difficile de démontrer que les sous-réseaux de E_8 isométriques à D_6 (resp. E_6) sont exactement les orthogonaux des sous-réseaux de E_8 isométriques à $\mathrm{A}_1 \oplus \mathrm{A}_1$ (resp. A_2), ils sont donc aisés à énumérer à l'aide de l'ordinateur (voir la feuille de calculs [CL `PARI`]).

Terminons par une application numérique. Notons $\varepsilon_1, \ldots, \varepsilon_8$ la base canonique du premier facteur $\mathbb{R}^8$, $\varepsilon'_1, \ldots, \varepsilon'_8$ celle du second, et prenons $e = (\varepsilon_j + i\varepsilon'_j)_{1 \leq j \leq 6}$. La première observation ci-dessus assure que si $Q \simeq \mathrm{D}_6, \mathrm{E}_6$ alors $\mathrm{c}_Q(P_e^2) = 2|\mathrm{O}(Q)| \sum_{M \subset \mathrm{E}_8 \oplus 0} P_e(M)^2$, la somme portant cette fois-ci sur les sous-réseaux du premier facteur E_8 isométriques à Q. La seconde observation permet d'évaluer cette somme. L'ordinateur nous donne [CL `PARI`]

$$\frac{\mathrm{c}_{\mathrm{E}_6}(P_e^2)}{2|\mathrm{O}(\mathrm{E}_6)|} = 120 \quad \text{et} \quad \frac{\mathrm{c}_{\mathrm{D}_6}(P_e^2)}{2|\mathrm{O}(\mathrm{D}_6)|} = 540.$$

En particulier, ces deux coefficients sont non nuls et on constate

$$\frac{\mathrm{c}_{\mathrm{D}_6}(P_e^2)}{\mathrm{c}_{\mathrm{E}_6}(P_e^2)} = 2.$$

Le corollaire qui suit fournit au final un procédé concret de construction de toutes les formes de Siegel de poids ≤ 11 par séries thêta.

Corollaire* **5.15.** *Les applications $\vartheta_{d,g}$ induisent des isomorphismes entres espaces de dimension* 1 *:*

$$\vartheta_{4,4} : \mathrm{M}_{\mathrm{H}_{4,4}(\mathbb{R}^8)}(\mathrm{O}_8) \xrightarrow{\sim} \mathrm{S}_8(\mathrm{Sp}_8(\mathbb{Z})), \quad \vartheta_{6,2} : \mathrm{M}_{\mathrm{H}_{6,2}(\mathbb{R}^8)}(\mathrm{O}_8) \xrightarrow{\sim} \mathrm{S}_{10}(\mathrm{Sp}_4(\mathbb{Z})),$$

$$\vartheta_{6,4} : \mathrm{M}_{\mathrm{H}_{6,4}(\mathbb{R}^8)}(\mathrm{O}_8) \xrightarrow{\sim} \mathrm{S}_{10}(\mathrm{Sp}_8(\mathbb{Z})), \quad \vartheta_{2,6} : \mathrm{M}_{\mathrm{H}_{2,6}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \xrightarrow{\sim} \mathrm{S}_{10}(\mathrm{Sp}_{12}(\mathbb{Z})),$$

$$\vartheta_{2,8} : \mathrm{M}_{\mathrm{H}_{2,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) \xrightarrow{\sim} \mathrm{S}_{10}(\mathrm{Sp}_{16}(\mathbb{Z})).$$

Démonstration. L'assertion sur $\vartheta_{4,4}$ est la proposition V.4.22, et celle sur $\vartheta_{6,4}$ est de même contenue dans la table V.3. L'assertion sur $\vartheta_{6,2}$ est un cas particulier de la proposition 1.2. Celle sur $\vartheta_{2,6}$ résulte de la discussion précédant l'énoncé du corollaire. Enfin, l'assertion sur $\vartheta_{2,8}$ se déduit de $\dim \mathrm{M}_{\mathrm{H}_{2,8}(\mathbb{R}^{16})}(\mathrm{O}_{16}) = 1$ (Lemme 5.14 (i)) et du critère de Böcherer, puisque l'on a $\mathrm{L}(\frac{1}{2}, \Delta_{11}) \neq 0$. $\square$

6. Vers une nouvelle démonstration de l'égalité $|\mathrm{X}_{24}| = 24$

L'intérêt du théorème suivant réside dans le fait que sa démonstration n'utilise aucun calcul appartenant à la théorie des réseaux unimodulaires. En particulier, elle n'utilise pas bien entendu la détermination par Niemeier de X_{24}. En revanche, elle repose sur la théorie d'Arthur et le théorème 3.2. On rappelle que les ensembles X_n et $\widetilde{\mathrm{X}}_n$ ont été introduits au §IV.1.2.

Théorème 6.1. *Admettons les conjectures* VIII.1.2 *et* VIII.4.25*. Alors on a les égalités*

$$|\mathrm{X}_{24}| = 24 \qquad \textit{et} \qquad |\widetilde{\mathrm{X}}_{24}| = 25.$$

Démonstration. Démontrons d'abord l'égalité $|\widetilde{\mathrm{X}}_{24}| = 25$. Soit π un élément de $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$. D'après la conjecture VIII.1.2, on a $\psi(\pi, \mathrm{St}) \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$. Si l'on suppose de plus la représentation π_∞ triviale, le théorème 4.4 entraîne que $\psi(\pi, \mathrm{St})$ est l'un des paramètres listés dans la table I.2. La relation

$$|\widetilde{\mathrm{X}}_{24}| \;=\; \dim \mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$$

montre qu'il ne reste qu'à déterminer, pour chacun des paramètres ψ de cette table, la somme m_ψ des multiplicités des représentations $\pi' \in \Pi(\mathrm{SO}_{24})$ telles que $\pi'_\infty = 1$ et $\psi(\pi', \mathrm{St}) = \psi$. D'après la conjecture VIII.4.25, on a toujours $m_\psi \in \{0, 1, 2\}$, sa valeur exacte pouvant être déterminée à l'aide des formulaires donnés au §VIII.5 ; en l'occurence, nous allons utiliser ici le théorème VIII.5.8. Cette détermination des 24 entiers m_ψ, essentiellement faite au "cas par cas", a déjà été menée à bien au §2.10. La conclusion de l'analyse *loc. cit.* est la suivante : si $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{24})$ est l'un des éléments listés dans la table I.2 alors

(a) soit $\psi \neq \Delta_{11}[12]$ et l'on a $m_\psi = 1$,

(b) soit $\psi = \Delta_{11}[12]$ et l'on a $m_\psi = 2$. Dans ce cas, il existe exactement deux représentations distinctes π', π'' dans $\Pi_{\mathrm{disc}}(\mathrm{SO}_{24})$ vérifiant $\psi(\pi', \mathrm{St}) = \psi(\pi'', \mathrm{St}) = \psi$, et l'on a $\mathrm{m}(\pi') = \mathrm{m}(\pi'') = 1$ et $\pi'' = S(\pi')$ au sens de la remarque VIII.5.9.

On a bien démontré $|\widetilde{\mathrm{X}}_{24}| = 23 + 2 = 25$. Montrons enfin $|\mathrm{X}_{24}| = 24$. On part de l'égalité $\dim \mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24}) = |\mathrm{X}_{24}|$. On rappelle que le groupe à deux éléments $\mathrm{O}_{24}(\mathbb{Q})/\mathrm{SO}_{24}(\mathbb{Q}) = \langle s \rangle$ agit sur $\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$ avec pour sous-espace fixe $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24})$ (voir l'exemple IV.4.6). Soit $f' \in \mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$ une fonction propre sous $\mathrm{H}(\mathrm{SO}_{24})$ engendrant la représentation π' introduite dans le point (b) ci-dessus. L'assertion $S(\pi') \neq \pi'$ montre que la droite $\mathbb{C}f'$ n'est pas stable par l'action de l'élément s, et entraîne que le sous-espace vectoriel

$$V := \langle f, sf \rangle \subset \mathrm{M}_{\mathbb{C}}(\mathrm{SO}_{24})$$

est de dimension 2 et vérifie $\dim(\mathrm{M}_{\mathbb{C}}(\mathrm{O}_{24}) \cap V) = 1$ (ce fait a d'ailleurs déjà été exploité dans la démonstration de la proposition VII.5.1). On en déduit d'une part l'inégalité $|\mathrm{X}_{24}| < 25$ et d'autre part l'existence d'une représentation $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\psi(\pi, \mathrm{St}) = \Delta_{11}[12]$.

Pour conclure $|\mathrm{X}_{24}| = 24$, il suffit de montrer que pour chacun des 23 éléments $\psi \neq \Delta_{11}[12]$ listés dans la table I.2, il existe une représentation $\pi \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telle que $\psi(\pi, \mathrm{St}) = \psi$. C'est évident dans le cas particulier $\psi = [23] \oplus [1]$, qui correspond à la représentation triviale (Exemples VI.4.7). Pour les autres, l'argument que nous proposons est assez indirect. Il consiste à appliquer verbatim la méthode du §2.11. Elle se résume ainsi : on observe d'abord que ψ s'écrit de manière unique sous la forme $\psi' \oplus [23 - 2g]$ avec $1 \leq g < 12$ et $\psi' \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2g+1})$, puis on utilise la conjecture VIII.4.25 pour vérifier (au cas pas cas !) que ψ' est le paramètre standard d'une forme modulaire de Siegel parabolique, propre, de poids 12, pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, et enfin on vérifie que cette forme modulaire est une combinaison linéaire de séries thêta d'éléments de X_{24} à l'aide du critère de Böcherer. Aucun de ces arguments n'utilise la détermination de X_{24}. Cela conclut la démonstration. □

7. Quelques éléments de $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ pour $n = 15, 17$ et 23

Théorème* **7.1.** *Soit n un entier impair ≥ 1. Les éléments $\psi \in \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{n-1})$ tels que la classe de conjugaison ψ_∞ admette pour valeurs propres les $n-1$ demi-entiers $\pm\frac{n-2}{2}, \pm\frac{n-4}{2}, \ldots, \pm\frac{1}{2}$ sont les suivants :*

(i) l'unique élément $[n-1]$ si $n \leq 11$,

(ii) $[12]$ et $\Delta_{11} \oplus [10]$ si $n = 13$,

(iii) $[14]$ et $\Delta_{11}[3] \oplus [8]$ si $n = 15$,

(iv) $[16]$, $\Delta_{15} \oplus [14]$, $\Delta_{15} \oplus \Delta_{11}[3] \oplus [8]$ et $\Delta_{11}[5] \oplus [6]$ si $n = 17$,

(v) les 32 paramètres listés dans la table C.7 si $n = 23$.

Démonstration. Il s'agit d'une conséquence du théorème 3.2, dont la démonstration est similaire à celles du théorème 4.4 et de la proposition 2.2. Mentionnons que les cas $n = 19$ et 21, bien que non explicités dans l'énoncé, se déduisent immédiatement également de cette méthode, et même de la table C.7. □

Ce théorème a des conséquences sur la classification des $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ vérifiant $\pi_\infty = 1$ si n est impair, les valeurs propres de $\mathrm{St}\,\mathrm{c}_\infty(\pi) \subset \mathfrak{sl}_{n-1}(\mathbb{C})$ étant dans ce cas les $n-1$ demi-entiers $\pm\frac{n-2}{2}, \pm\frac{n-4}{2}, \ldots, \pm\frac{1}{2}$.

Théorème 7.2. *Admettons la conjecture VIII.1.2. Les paramètres standards* $\psi(\pi, \mathrm{St})$ *des représentations* $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ *telles que* $\pi_\infty = 1$ *sont :*

(i) $[14]$ et $\Delta_{11}[3] \oplus [8]$ *si* $n = 15$,

(ii) $[16]$, $\Delta_{15} \oplus [14]$, $\Delta_{15} \oplus \Delta_{11}[3] \oplus [8]$ et $\Delta_{11}[5] \oplus [6]$ *si* $n = 17$.

Démonstration. Sous l'hypothèse $n = 15$ ou $n = 17$, on rappelle que la dimension $\dim \mathrm{M}_{\mathbb{C}}(\mathrm{SO}_n) = |\mathrm{X}_n|$ vaut respectivement 2 et 4 d'après le corollaire IV.1.11. L'opérateur T_2 de $\mathbb{C}[\mathrm{X}_n]$ est déterminé dans l'appendice B §5. Dans les deux cas ses valeurs propres sont bien compatibles avec le théorème ci-dessus ; la chose qui importera ici est qu'elles soient distinctes. Ainsi, si $n = 15$ (resp. $n = 17$) il existe exactement 2 (resp. 4) éléments de $\Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ vérifiant $\pi_\infty = 1$, chacun ayant multiplicité 1. L'entier n étant impair, les paramètres standards $\psi(\pi, \mathrm{St})$ de ces éléments sont évidemment distincts. D'après la conjecture VIII.1.2, ces paramètres satisfont les hypothèses du théorème 7.1. Mais d'après les conclusions de ce théorème, il n'existe que 2 paramètres possibles pour $n = 15$, et 4 pour $n = 17$, ce qui termine la démonstration. □

Théorème 7.3. *Admettons la conjecture* VIII.4.25. *Les paramètres standards* $\psi(\pi, \mathrm{St})$ *des représentations* $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_{23})$ *telles que* $\pi_\infty = 1$ *sont les* 32 *éléments listés dans la table C.7 si* $n = 23$.

Démonstration. On rappelle l'égalité $|\mathrm{X}_{23}| = 32$ (Corollaire IV.1.11). Soient ψ l'un des 32 éléments de la table C.7 et $\pi \in \Pi(\mathrm{SO}_{23})$ l'unique représentation telle que $\psi(\pi, \mathrm{St}) = \psi$. Il s'agit de démontrer que la multiplicité de π est non nulle. D'après la conjecture VIII.4.25, il suffit pour cela d'appliquer la formule de multiplicité d'Arthur sous sa forme donnée par le Théorème VIII.5.6. Il s'agit d'une étude au cas par cas, que l'on peut légèrement simplifier en dégageant des critères du même type que ceux donnés au §VIII.5.7 dans le cas $n \equiv 0 \bmod 8$, ce que nous laissons en exercice au lecteur car les raisonnements sont très similaires à ceux étudiés en détail *loc. cit.* On constate au final, ô miracle, que l'on a bien $\mathrm{m}(\pi) = 1$, quel que soit l'élément ψ choisi initialement. □

Remarque 7.4. (i) Le théorème 7.3 a été étendu à la dimension 25 dans [CR12, Thm. 1.14]. Les 121 paramètres en question font intervenir notamment les 7 représentations dans $\Pi_{\mathrm{alg}}(\mathrm{PGL}_6)$ de poids motivique 23 mentionnées au §3.38.

(ii) Un argument semblable à celui de la démonstration du théorème 6.1 permet de redémontrer, à partir du théorème 3.2 et conditionnellement aux conjectures VIII.1.2 et VIII.4.25, mais sans aucun calcul appartenant à la théorie des réseaux euclidiens, les égalités $|\mathrm{X}_7| = |\mathrm{X}_9| = 1$, $|\mathrm{X}_{15}| = 2$, $|\mathrm{X}_{17}| = 4$ et $|\mathrm{X}_{23}| = 32$.

Terminons par une curieuse observation. Pour tout entier $n \leq 24$ tel que $n \equiv -1, 0, 1 \bmod 8$, nous avons décrit dans ce mémoire le sous-ensemble

$$\Phi_n \subset \mathcal{X}(\mathrm{SL}_{2[\frac{n}{2}]})$$

constitué des éléments de la forme $\psi(\pi, \mathrm{St})$ avec $\pi \in \Pi_{\mathrm{disc}}(\mathrm{SO}_n)$ tel que $\pi_\infty = 1$. Par exemple Φ_{24} et Φ_{25} sont respectivement donnés par les tables I.2 et C.7. Cette description est encore conditionnelle quand n impair, auquel cas elle s'étend même à $n = 25$ d'après la remarque 7.4 (i), mais là n'est pas la question dans cette discussion, où nous serions prêts volontiers à admettre la conjecture VIII.4.25. Considérons le second problème, en apparence assez différent, de déterminer le sous-ensemble

$$\Phi'_n \subset \mathcal{X}_{\mathrm{AL}}(\mathrm{SL}_{2[\frac{n}{2}]})$$

constitué de tous les ψ tels que ψ_∞ est le caractère infinitésimal de la représentation triviale de $\mathrm{SO}_n(\mathbb{R})$ (une condition simple sur ses valeurs propres). La théorie d'Arthur assure d'abord $\Phi_n \subset \Phi'_n$; elle donne aussi un critère explicite, la "formule de multiplicité d'Arthur", permettant de déterminer si un élément $\psi \in \Phi'_n$ donné est dans Φ_n : ce sont les formules VIII.5.6 et VIII.5.8. Mais le théorème 3.2 permet de déterminer Φ'_n pour tout $n \leq 24$. La propriété miraculeuse, vérifiée dans tous les cas, est alors l'égalité

$$\Phi_n = \Phi'_n, \quad \forall\, n \leq 24. \tag{7.1}$$

Il est même concevable que cette égalité s'étende à $n = 25$. Concrètement, cela signifie que pour $n \leq 24$ et tout $\psi \in \Phi'_n$, la formule de multiplicité d'Arthur appliquée à ψ conduit toujours à une multiplicité non nulle. Il serait intéressant de trouver une raison plus profonde à ce phénomène.

On pourrait espérer que l'égalité (7.1) se produise pour tout $n \equiv -1, 0, 1 \bmod 8$, du moins si l'on remplace Φ'_n par son sous-ensemble constitué des ψ tels que $\psi_p = \psi_p^{-1}$ pour tout p. Il n'en est rien. En effet, la formule de multiplicité d'Arthur montre que si $n = 32$, le paramètre $\Delta_{17}[14] \oplus [3] \oplus [1]$ de Φ'_{32} ne doit pas appartenir à Φ_{32}. De même, l'élément $\Delta_{17}[13] \oplus [4]$ de Φ'_{31} ne doit pas appartenir à Φ_{31}. Si $\mathrm{S}_{14}(\mathrm{SL}_2(\mathbb{Z}))$ n'était pas nul, de tels exemples existeraient également en dimensions 23 et 24.

X. Applications

1. 24 représentations galoisiennes ℓ-adiques

Rappelons que l'espace vectoriel $\mathbb{Q}[\mathrm{X}_{24}]$ admet une $\mathbb{Q}$-base $\mathrm{v}_1, \ldots, \mathrm{v}_{24}$ constituée de vecteurs propres communs à tous les éléments de $\mathrm{H}(\mathrm{O}_{24})$ (§IX.2). Chacun de ces vecteurs v_i engendre une représentation automorphe $\pi_i \in \Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ dont le paramètre standard $\psi(\pi_i, \mathrm{St})$ est déterminé par le théorème* 2.5 (Table C.5). En particulier, le couple (π_i, St) satisfait la conjecture d'Arthur-Langlands, de sorte que le corollaire VIII.2.19 s'applique, et lui associe des représentations ℓ-adiques de dimension 24 du groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Dans ce qui suit, nous allons préciser l'énoncé obtenu.

Si p est un nombre premier et $1 \leq i \leq 24$, nous notons $\lambda_i(p) \in \mathbb{Z}$ la valeur propre de T_p sur le vecteur v_i. D'après la formule VI.(2.5), on a $\lambda_i(p) = p^{11} \operatorname{trace} \mathrm{St}(\mathrm{c}_p(\pi_i))$. Plus généralement, le lemme suivant montre que le polynôme $\operatorname{dét}(t - p^{11} \mathrm{St}(\mathrm{c}_p(\pi_i)))$ est à coefficients entiers, chacun de ses coefficients pouvant être vu comme la valeur propre d'un opérateur de Hecke bien choisi dans $\mathrm{H}(\mathrm{O}_{24})$.

Lemme 1.1. *Soient G un $\mathbb{Z}_p$-groupe semi-simple déployé, λ un poids dominant de $\widehat{G}$, V_λ la représentation irréductible de $\widehat{G}$ associée, et ρ la demi-somme des racines positives de $G_{\mathbb{C}}$. Pour tout entier $m \geq 1$, il existe un unique élément $T \in \mathrm{H}(G)$ tel que pour tout $c \in \widehat{G}_{\mathrm{ss}}$, on ait*

$$p^{m\langle\lambda,\rho\rangle} \operatorname{trace}(c \,|\, \Lambda^m V_\lambda) = \operatorname{tr}(c)(\mathrm{Sat}(T)).$$

De plus, si $G = \mathrm{SO}_n$ et si la représentation V_λ s'étend à $\mathrm{O}_n(\mathbb{C})$, par exemple si $V = \mathrm{St}$, alors T appartient au sous-anneau $\mathrm{H}(\mathrm{O}_n) \subset \mathrm{H}(\mathrm{SO}_n)$.

Démonstration. L'existence et unicité d'un élément $T \in \mathrm{H}(G) \otimes \mathbb{Z}[p^{-\frac{1}{2}}]$ tel que $\mathrm{Sat}(T) = p^{m\langle\lambda,\rho\rangle}[\Lambda^m V_\lambda]$ est conséquence immédiate de l'isomorphisme de Satake (§VI.2.1). Il s'agit donc de voir que $T \in \mathrm{H}(G)$. Rappelons que l'on a

$$p^{\langle\rho,\mu\rangle}[V_\mu] \in \mathrm{Sat}(\mathrm{H}(G))$$

pour tout poids dominant μ de $\widehat{G}$, d'après la formule VI.(2.4). Le cas $m = 1$ suit immédiatement. Si $m \geq 1$ est quelconque, on observe que les constituants irréductibles de $\Lambda^m V_\lambda$, qui sont de la forme V_μ où μ est un poids dominant de $\widehat{G}$, vérifient $\mu \leq m\lambda$ (§VI.1.4). En effet, cette inégalité vaut plus généralement pour tous les poids μ de $V_\lambda^{\otimes m}$, et $\Lambda^m V_\lambda$ est un quotient de ce dernier. On conclut la première assertion du lemme car pour un tel μ, $\langle \rho, m\lambda - \mu \rangle$ est un entier ≥ 0.

Pour vérifier la seconde assertion, concernant $G = \mathrm{SO}_n$, il d'observer que si V_λ se prolonge à $\mathrm{O}_n(\mathbb{C}) \supset \widehat{G} = \mathrm{SO}_n(\mathbb{C})$, alors il en va de même de $\Lambda^m V_\lambda$. La relation VI.(2.2) montre alors que l'élément $T \in \mathrm{H}(\mathrm{SO}_n)$ défini ci-dessus appartient à $\mathrm{H}(\mathrm{O}_n)$. $\square$

Remarque 1.2. Il est en général difficile de déterminer explicitement l'opérateur T donné par le lemme ci-dessus, disons en terme de la $\mathbb{Z}$-base des c_μ (§VI.2.5), et ce même dans le cas particulier du groupe $G = \mathrm{SO}_n$ et de la représentation standard $V_\lambda = \mathrm{St}$ de $\widehat{G}$. Dans ce cas, on a toutefois déjà dit que $T = \mathrm{T}_p$ pour $m = 1$, et l'on a de plus $T = p\,\mathrm{T}_{p,p} + p^{n/2-1} + \sum_{i=0}^{n/2-2} p^{2i+1}$ pour $m = 2$ (Formule VI.(2.6)).

Nous avons rappelé au §VIII.2 l'existence et quelques propriétés des représentations galoisiennes $\rho_{\pi,\iota}$ associées à une représentation automorphe algébrique, autoduale, régulière $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$ et à un plongement $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$, où $\overline{\mathbb{Q}}_\ell$ désigne une clôture algébrique de $\mathbb{Q}_\ell$. La représentation galoisienne $\rho_{\pi,\iota}$ est continue, semi-simple, non ramifiée hors de ℓ, et sa classe d'isomorphisme est uniquement déterminée par la relation

$$\text{dét}(t - \rho_{\pi,\iota}(\mathrm{Frob}_p)) = \iota(\text{dét}(t - \mathrm{c}_p(\pi) p^{\frac{\mathrm{w}(\pi)}{2}})) \tag{1.1}$$

pour tout premier $p \neq \ell$ (l'assertion d'unicité étant conséquence du théorème de Cebotarev). Si le polynôme $\text{dét}(t - \mathrm{c}_p(\pi) p^{\frac{\mathrm{w}(\pi)}{2}})$ est dans $\mathbb{Q}[t]$ pour tout premier p, la représentation galoisienne $\rho_{\pi,\iota}$ dépend uniquement de ℓ, et non du choix de ι ; elle sera simplement notée $\rho_{\pi,\ell}$.

Les représentations automorphes π d'intérêt ici seront les Δ_w et les $\Delta_{w,v}$, et dans ces cas les représentations galoisiennes $\rho_{\pi,\iota}$ (satisfaisant les conditions (i) et (ii) du théorème VIII.2.17) ont été respectivement construites par Deligne [Del71] (généralisant une construction antérieure d'Eichler, Shimura, Kuga et Sato [KS65]) et Weissauer [Weis05] (voir aussi les travaux antérieurs de Chai-Faltings [CF90] et Taylor [Tay91]).

Lorsque π est engendrée par une forme modulaire $f = q + a_2 q^2 + \ldots$ dans $\mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ qui est propre pour les opérateurs de Hecke, la relation (1.1) se

réduit à la relation bien connue $\text{dét}(t - \rho_{\pi,\iota}(\text{Frob}_p)) = t^2 - \iota(a_p)t + p^{k-1}$. Ce polynôme est à coefficients entiers si $k \leq 22$ (car la forme f l'est) ; il est par ailleurs bien connu que $\rho_{\pi,\ell}$ peut dans ce cas être choisie à coefficients dans le corps $\mathbb{Q}_\ell$.

Lorsque π est l'une des 4 représentations $\Delta_{w,v}$ définie au §IX.1, rappelons que le membre de droite de l'égalité (1.1) s'écrit aussi

$$t^4 - \tau_{j,k}(p)\, t^3 + \frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2}\, t^2 - \tau_{j,k}(p)\, p^{j+2k-3}\, t \, + \, p^{2j+4k-6},$$

où $(j,k) = (v-1, (w-v)/2+2)$ (Formule IX.(1.3)). Là encore, ce polynôme est à coefficients rationnels, et même entiers d'après la proposition IX.1.9.

Théorème[*] **1.3.** *Soient $i = 1, \ldots, 24$, ℓ un nombre premier et $\overline{\mathbb{Q}}_\ell$ une clôture algébrique de $\mathbb{Q}_\ell$. Il existe une représentation continue et semi-simple $\rho_{i,\ell}$: $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_{24}(\overline{\mathbb{Q}}_\ell)$, unique à isomorphisme près, qui est non ramifiée hors de ℓ et telle que pour tout premier $p \neq \ell$ on ait l'égalité dans $\mathbb{Z}[t]$*

$$\text{dét}(t - \rho_{i,\ell}(\text{Frob}_p)) = \text{dét}(t - p^{11}\, \text{St}(\text{c}_p(\pi_i))). \tag{1.2}$$

En particulier, on a $\lambda_i(p) = \text{trace}\, \rho_{i,\ell}(\text{Frob}_p)$ pour tout premier $p \neq \ell$.

Démonstration. Soit $i = 1, \ldots, 24$. Le théorème IX.2.5 affirme que $\psi(\pi_i, \text{St})$ est de la forme $\oplus_{j=1}^k \varpi_j[d_j]$, où les ϖ_j sont parmi les représentations automorphes 1, Δ_w, $\Delta_{w,v}$, et $\text{Sym}^2\Delta_{11}$. L'existence de $\rho_{i,\ell}$ en découle en posant

$$\rho_{i,\ell} = \bigoplus_{j=1}^{k} \rho_{\varpi_j,\ell} \otimes (\oplus_{m=0}^{d_j-1} \omega_\ell^m) \otimes \omega_\ell^{\frac{22-\text{w}(\varpi_j)+1-d_j}{2}}, \tag{1.3}$$

la notation $\rho_{\varpi_j,\ell}$ étant introduite quelques lignes plus haut. L'assertion d'unicité est conséquence du théorème de Cebotarev. Bien entendu, lorsque ϖ_j est la représentation automorphe triviale dans $\Pi_{\text{cusp}}(\text{PGL}_1)$, $\rho_{\varpi_j,\ell}$ désigne la représentation galoisienne triviale (de dimension 1). De plus, on peut prendre pour $\rho_{\text{Sym}^2\Delta_{11},\ell}$ la représentation $\text{Sym}^2\rho_{\Delta_{11},\ell}$. □

Remarque 1.4. En suivant la construction de Weissauer [Weis05], il devrait être possible de montrer que les représentations $\rho_{\Delta_{w,v},\ell}$, ainsi donc que les $\rho_{i,\ell}$, sont définies sur $\mathbb{Q}_\ell$, puisque $\dim \text{S}_{j,k} = 1$ pour les 4 couples (j,k) correspondants (§IX.1.1).

Il serait intéressant d'étudier en détail les images des représentations galoisiennes $\rho_{\Delta_{w,v},\ell}$, à la manière des travaux de Serre et Swinnerton-Dyer sur les représentations $\rho_{\Delta_w,\ell}$ [Sw72]. Nous nous contenterons au §X.4 de démontrer quelques congruences satisfaites par ces représentations, dans l'esprit de la congruence de Ramanujan.

Corollaire* **1.5.** *Soient $i = 1, \ldots, 24$ et ℓ un nombre premier. Il existe une représentation continue et semi-simple $\overline{\rho}_{i,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_{24}(\mathbb{F}_\ell)$, unique à isomorphisme près, qui est non ramifiée hors de ℓ et telle que pour tout premier $p \neq \ell$ on ait la congruence*

$$\text{dét}(t - \overline{\rho}_{i,\ell}(\mathrm{Frob}_p)) \equiv \text{dét}(t - p^{11}\,\mathrm{St}(\mathrm{c}_p(\pi_i))) \bmod \ell. \tag{1.4}$$

En particulier, on a $\lambda_i(p) \equiv \mathrm{trace}\,\overline{\rho}_{i,\ell}(\mathrm{Frob}_p) \bmod \ell$ pour tout premier $p \neq \ell$.

L'assertion d'unicité est conséquence du théorème de Cebotarev et d'un résultat classique de Brauer-Nesbitt [1]. L'existence de $\overline{\rho}_{i,\ell}$ se déduit de celle de $\rho_{i,\ell}$ par un procédé général standard, rappelé ci-dessous.

Fixons une clôture algébrique $\overline{\mathbb{Q}}_\ell$ (resp. $\overline{\mathbb{F}}_\ell$) de $\mathbb{Q}_\ell$ (resp. $\mathbb{F}_\ell$), ainsi qu'un morphisme d'anneaux $\mathcal{O} \to \overline{\mathbb{F}}_\ell$, où $\mathcal{O} \subset \overline{\mathbb{Q}}_\ell$ désigne la clôture intégrale de $\mathbb{Z}_\ell$. Soient G un groupe profini et $\rho : G \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ une représentation continue. On démontre que :

(i) $\text{dét}(t - \rho(g)) \in \mathcal{O}[t]$ pour tout $g \in G$,

(ii) il existe une représentation continue semi-simple $\overline{\rho} : G \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$, unique à isomorphisme près, telle que pour tout $g \in G$, le polynôme caractéristique $\text{dét}(t - \overline{\rho}(g))$ est l'image de $\text{dét}(t - \rho(g)) \in \mathcal{O}[t]$ dans $\overline{\mathbb{F}}_\ell[t]$.

(iii) si de plus $\text{dét}(t - \rho(g)) \in \mathbb{Q}_\ell[t]$ pour tout $g \in G$, alors $\overline{\rho}$ peut être choisie à coefficients dans $\mathbb{F}_\ell$, et sa classe d'isomorphisme ne dépend pas du choix du morphisme $\mathcal{O} \to \overline{\mathbb{F}}_\ell$.

On dit alors que $\overline{\rho}$ est "la" représentation résiduelle de ρ. Cette construction (le point (iii) inclus) s'applique aux $\rho_{i,\ell}$, ainsi qu'aux représentations de la forme $\rho_{\pi,\ell}$ introduites plus haut ; elle donne lieu à des représentations résiduelles $\overline{\rho}_{i,\ell}$ et $\overline{\rho}_{\pi,\ell}$ à coefficients dans $\mathbb{F}_\ell$. Bien entendu, la relation (1.3) induit une décomposition similaire

$$\overline{\rho}_{i,\ell} \simeq \bigoplus_{j=1}^{k} \overline{\rho}_{\varpi_j,\ell} \otimes (\oplus_{m=0}^{d_j-1} \overline{\omega_\ell}^{\,m}) \otimes \overline{\omega_\ell}^{\,\frac{22-\mathrm{w}(\varpi_j)+1-d_j}{2}}. \tag{1.5}$$

1. Rappelons l'énoncé de ce dernier. Soient G un groupe, k un corps, ainsi que $\rho_1, \rho_2 : G \to \mathrm{GL}_m(k)$ deux représentations semi-simples. Les représentations ρ_1 et ρ_2 sont isomorphes si, et seulement si, $\text{dét}(t - \rho_1(g)) = \text{dét}(t - \rho_2(g))$ pour tout $g \in G$.

Indiquons brièvement comment l'on démontre les points (i), (ii) et (iii). Une application classique du lemme de Baire assure d'abord que $\rho(G) \subset \mathrm{GL}_n(F)$ où $F \subset \overline{\mathbb{Q}}_\ell$ est une extension finie de $\mathbb{Q}_\ell$. Quitte à conjuguer ρ par un élément de $\mathrm{GL}_n(F)$, la compacité de $\rho(G)$ permet de supposer que $\rho(G) \subset \mathrm{GL}_n(\mathcal{O}_F)$ où $\mathcal{O}_F = \mathcal{O} \cap F$. Le (i) suit. En composant par le morphisme d'anneaux $\mathcal{O} \to \overline{\mathbb{F}}_\ell$, il en résulte une représentation continue $G \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$. Pour démontrer le point (ii) il suffit de prendre pour $\overline{\rho}$ une semi-simplifiée de cette dernière représentation. L'assertion d'unicité, ainsi que la dernière assertion du (iii), découlent du résultat de Brauer-Nesbitt. L'obstruction de Schur étant triviale sur les corps finis, on en déduit la première assertion du (iii) (voir [Tay91, Lemma 2]).

Remarque 1.6. Soit $\rho = \rho_{\Delta_{w,v},\ell}$. Nous avons déjà observé au §VIII.2.16, formule VIII.(2.1), que l'on dispose d'un isomorphisme $\rho^* \simeq \rho \otimes \omega_\ell^{-w}$. Mieux, d'après [BC11, Corollary 1.3], il existe un accouplement non dégénéré, alterné, et $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-équivariant $\rho \otimes \rho \to \omega_\ell^w$ (voir aussi [Weis05]). Il n'est pas difficile d'en déduire l'existence d'un accouplement non dégénéré, alterné, et $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-équivariant, $\overline{\rho} \otimes \overline{\rho} \to \overline{\omega_\ell}^{\,w}$.

2. Retour sur les p-voisins des réseaux de Niemeier

On numérote $\mathrm{L}_1, \mathrm{L}_2, \ldots, \mathrm{L}_{24}$ les 24 réseaux de Niemeier (ou plutôt leurs classes d'isomorphisme) suivant la convention de Conway et Sloane [CS99, Chap. 16, Table 16.1] (les entiers $1, 2, \ldots, 24$ remplaçant les lettres grecques $\alpha, \beta, \ldots, \omega$). On a donc $\mathrm{R}(\mathrm{L}_i) = \mathbf{R}_i$ pour $i \leq 23$ (voir II.3) et L_{24} est le réseau de Leech que nous avons aussi noté Leech en III.4.

Soit p un nombre premier ; nous notons encore T_p la matrice de l'opérateur de Hecke $\mathrm{T}_p : \mathbb{Z}[\mathrm{X}_{24}] \to \mathbb{Z}[\mathrm{X}_{24}]$ dans la base $(\mathrm{L}_1, \mathrm{L}_2, \ldots, \mathrm{L}_{24})$.

Comme nous l'avons déjà dit Nebe et Venkov ont déterminé T_2 et constaté que les valeurs propres de cet opérateur sont entières et distinctes. On les note

$$\lambda_1 > \lambda_2 > \ldots > \lambda_{24} \qquad .$$

On note v_j, $1 \leq j \leq 24$, un vecteur propre associé à λ_j dont les coordonnées, dans la base évoquée plus haut, sont entières et premières entre elles (un tel vecteur propre est déterminé au signe près) ; on note V la matrice à 24 lignes et colonnes dont la j-ième colonne est la colonne des cordonnées de v_j.

On note $\lambda_j(p)$ l'entier défini par l'égalité $\mathrm{T}_p \mathrm{v}_j = \lambda_j(p) \mathrm{v}_j$ (se rappeler que T_2 et T_p commutent) ; on a donc par définition $\lambda_j(2) = \lambda_j$.

On pose $\theta_1(p) = \tau_{12}(p)(= \tau(p))$, $\theta_2(p) = \tau_{16}(p)$, $\theta_3(p) = \tau_{18}(p)$, $\theta_4(p) = \tau_{20}(p)$, $\theta_5(p) = \tau_{22}(p)$; en clair, on note $\theta_r(p)$ le p-ième coefficient de Fourier de la forme modulaire (pour $\mathrm{SL}_2(\mathbb{Z})$) parabolique normalisée respectivement de poids $12, 16, 18, 20, 22$ pour $r = 1, 2, 3, 4, 5$. On pose $\theta_6(p) = (\theta_1(p))^2 - p^{11}$ ($\theta_6(p) = p^{11}\,\mathrm{tr}(\mathrm{Sym}^2 \mathrm{c}_p(\Delta_{11}))$).

On pose enfin $\theta_7(p) = \tau_{6,8}(p)$, $\theta_8(p) = \tau_{8,8}(p)$, $\theta_9(p) = \tau_{12,6}(p)$, $\theta_{10}(p) = \tau_{4,10}(p)$.

D'après le théorème 2.5 du chapitre IX et la formule (2.5) du chapitre VI, il existe des polynômes $\mathrm{C}_{j,r}$ de $\mathbb{Z}[X]$, $1 \leq j \leq 24$, $0 \leq r \leq 10$, uniquement déterminés, tels que l'on a

$$\lambda_j(p) \;=\; \mathrm{C}_{j,0}(p) + \sum_{r=1}^{10} \mathrm{C}_{j,r}(p)\,\theta_r(p) \tag{2.1}$$

pour tout nombre premier p.

Rappelons la valeur de quelques-uns des polynômes $\mathrm{C}_{j,r}$.

On a $\mathrm{C}_{1,0} = \sum_{k=0}^{k=22} X^k + X^{11}$ et $\mathrm{C}_{1,r} = 0$ pour $r \geq 1$, en clair on a $\lambda_1(p) = \mathrm{c}_{24}(p) := \sum_{k=0}^{k=22} p^k + p^{11}$ (voir III.2.4 et III.2.1).

On a $\mathrm{C}_{2,0} = \sum_{k=1}^{k=21} X^k$, $\mathrm{C}_{2,6} = 1$ et $\mathrm{C}_{2,r} = 0$ pour $r \neq 0, 6$.

Pour $r \geq 7$ la valeur des polynômes $\mathrm{C}_{j,r}$ est la suivante :
– $\mathrm{C}_{j,7} = 0$ pour $j \neq 19$ et $\mathrm{C}_{19,7} = X(X+1)$;
– $\mathrm{C}_{j,8} = 0$ pour $j \neq 15$ et $\mathrm{C}_{15,8} = X + 1$;
– $\mathrm{C}_{j,9} = 0$ pour $j \neq 10$ et $\mathrm{C}_{10,9} = X + 1$;
– $\mathrm{C}_{j,10} = 0$ pour $j \neq 21$ et $\mathrm{C}_{21,10} = X + 1$.

En contemplant la formule

$$\mathrm{T}_p \;=\; \mathrm{V}\ \mathrm{diag}(\lambda_1(p), \lambda_2(p), \ldots, \lambda_{24}(p))\ \mathrm{V}^{-1} \tag{2.2}$$

(la notation $\mathrm{diag}(\lambda_1(p), \lambda_2(p), \ldots, \lambda_{24}(p))$ désignant la matrice diagonale dont les coefficients diagonaux sont les $\lambda_j(p)$) on obtient l'énoncé suivant :

Théorème 2.1. *Soient L et L' deux réseaux unimodulaires pairs de dimension 24. Il existe des polynômes $\mathrm{P}_r(L, L'; X)$ de $\mathbb{Q}[X]$, $0 \leq r \leq 10$, uniquement déterminés en fonction des classes d'isomorphismes de L et L', tels que l'on a*

$$\mathrm{N}_p(L, L') \;=\; \mathrm{P}_0(L, L'; p) + \sum_{r=1}^{10} \mathrm{P}_r(L, L'; p)\,\theta_r(p)$$

pour tout nombre premier p.

Remarque. Par définition, on a pour tout r avec $0 \leq r \leq 10$, l'égalité suivante de matrices, à 24 lignes et colonnes, à coefficients dans $\mathbb{Q}[X]$:

$$[\,\mathrm{P}_r(\mathrm{L}_j, \mathrm{L}_i; X)\,] \;=\; \mathrm{V}\ \mathrm{diag}(\mathrm{C}_{1,r}(X), \mathrm{C}_{2,r}(X), \ldots, \mathrm{C}_{24,r}(X))\ \mathrm{V}^{-1} \qquad ;$$

comme les colonnes de V sont deux à deux orthogonales pour le produit scalaire de matrice $\mathrm{diag}(|\mathrm{O}(\mathrm{L}_1)|, |\mathrm{O}(\mathrm{L}_2)|, \ldots, |\mathrm{O}(\mathrm{L}_{24})|)$ (Proposition III.2.3) cette égalité montre que l'on a

$$\frac{1}{|\mathrm{O}(L)|}\ \mathrm{P}_r(L, L'; X) \;=\; \frac{1}{|\mathrm{O}(L')|}\ \mathrm{P}_r(L', L; X)$$

pour tout r, L et L' (ce qui est bien sûr compatible avec le scholie III.1.7).

On note Proj_1 le projecteur orthogonal, pour le produit scalaire introduit en III.2.3, de $\mathbb{Q}[\mathrm{X}_{24}]$ sur la droite engendrée par v_1. On note w le vecteur $\sum_{x \in \mathrm{X}_{24}} \frac{1}{|\mathrm{O}(x)|} x$ de de $\mathbb{Q}[\mathrm{X}_{24}]$; il résulte de III.2.4 que le vecteur v_1 est colinéaire au vecteur w. Soit y un élément de X_{24} ; les égalités $\mathrm{w}.y = 1$ et $\mathrm{w}.\mathrm{w} = \sum_{x \in \mathrm{X}_{24}} \frac{1}{|\mathrm{O}(x)|}$ entraînent :

$$\mathrm{Proj}_1(y) \;=\; \frac{\mathrm{w}}{\sum_{x \in \mathrm{X}_{24}} \frac{1}{|\mathrm{O}(x)|}} \;=\; \sum_{x \in \mathrm{X}_{24}} \mu(x)\, x$$

en posant

$$\mu(x) \;=\; \frac{\frac{1}{|\mathrm{O}(x)|}}{\sum_{x \in \mathrm{X}_{24}} \frac{1}{|\mathrm{O}(x)|}} \qquad .$$

On observera que $\mu(x)$ est le quotient de la masse de x par la masse du genre des réseaux unimodulaires pairs de dimension 24, masses au sens de Minkowski-Siegel : $\sum_{x \in \mathrm{X}_{24}} \mu(x)\delta_x$ est *la mesure de probalité de Minkowski-Siegel* sur l'ensemble X_{24}.

Théorème 2.2. *Lorsque le nombre premier p tend vers l'infini, on a*

$$\mathrm{T}_p \;=\; p^{22}\ \mathrm{Proj}_1 \;+\; \mathrm{O}(p^{21})$$

(la notation $\mathrm{O}(-)$ qui apparaît ci-dessus est la notation de Landau... et n'a pas de rapport avec les groupes orthogonaux !).

Démonstration. Compte tenu de III.2.3, on a $\mathrm{T}_p = \sum_{j=1}^{24} \lambda_j(p)\mathrm{Proj}_j$, Proj_j étant le projecteur orthogonal de $\mathbb{Q}[\mathrm{X}_{24}]$ sur la droite engendrée par v_j. Or on a $\lambda_1(p) = p^{22} + \mathrm{O}(p^{21})$ et les inégalités de Ramanujan pour les θ_r impliquent $\lambda_j(p) = \mathrm{O}(p^{21})$ pour $j \geq 2$. Rappelons ce que sont ces inégalités. On a

$|\tau_k(p)| \leq 2p^{\frac{k-1}{2}}$ pour $k = 12, 16, 18, 20, 22$, $|\tau(p)^2 - p^{11}| \leq 3p^{11}$, $|\tau_{6,8}(p)| \leq 4p^{\frac{19}{2}}$ et $\tau_{j,k}(p)| \leq 4p^{\frac{21}{2}}$ pour $(j,k) = (8,8), (12,6), (4,10)$. Les 5 premières inégalités sont dues à Deligne [DEL71], les 4 dernières à Weissauer [WEIS05] (la 6-ième est conséquence de la première !) ; pour une discussion générale concernant ce type d'inégalité voir §VIII.2.16. □

Scholie 2.3. *Soient x et y deux éléments de X_{24} ; on a*

$$\frac{\mathrm{N}_p(x,y)}{\mathrm{c}_{24}(p)} \;=\; \mu(y) \;+\; \mathrm{O}(\frac{1}{p})$$

lorsque p tend vers l'infini.

Commentaires. Soient L un réseau unimodulaire pair de dimension 24 et y un élément de X_{24}. Le quotient

$$\frac{\mathrm{N}_p([L],y)}{\mathrm{c}_{24}(p)} \;=\; \frac{\mathrm{N}_p([L],y)}{|\mathrm{C}_L(\mathbb{F}_p)|}$$

est la proportion des points c de la quadrique $\mathrm{C}_L(\mathbb{F}_p)$ tels que la classe d'isomorphisme du p-voisin de L associé à c (voir II.1.5) est y. Le scholie 2.3 dit que cette proportion tend (en p^{-1}) vers $\mu(y)$ quand p tend vers l'infini.

Remarque. La mesure de probabilité de Minkowski-Siegel sur X_{24} est très loin d'être uniforme. On a par exemple $\mu([\mathrm{E}_{24}]) \approx 2.42 \times 10^{-17}$ (c'est le minimum de la fonction μ sur X_{24}), $\mu([\mathrm{L}_{21}]) \approx 0.426$ (c'est le maximum) et $\mu([\mathrm{L}_{20}]) + \mu([\mathrm{L}_{21}]) + \mu([\mathrm{L}_{22}]) \approx 0.906$.

Remarque. On constate en inspectant les égalités (2.1) que les inégalités de Ramanujan donnent $\lambda_j(p) = \mathrm{C}_{0,j}(p) + \mathrm{O}(p^{\frac{33}{2}})$ pour tout j. On en déduit comme précédemment des estimations de la forme

$$\frac{\mathrm{N}_p(x,y)}{\mathrm{c}_{24}(p)} \;=\; \mu(y)\;\Big(\,1 + \sum_{n=1}^{5} \kappa_n(x,y)\,\frac{1}{p^n} \;+\; \mathrm{O}(p^{-\frac{11}{2}})\,\Big) \qquad ;$$

le lien entre le vecteur propre v_2 et les séries thêta de genre 1 des réseaux unimodulaires pair de dimension 24 permet d'expliciter $\kappa_1(x,y)$:

$$\kappa_1(x,y) \;=\; \frac{37092156523}{34673184000}\;\big(\,\mathrm{h}(x) - \frac{2730}{691}\,\big)\;\big(\,\mathrm{h}(y) - \frac{2730}{691}\,\big) \qquad .$$

Donnons quelques précisions sur le lien évoqué ci-dessus entre v_2 et séries thêta de genre 1 ; ces précisions sont en fait un développement du deuxième commentaire qui suit la table V.1.

D'une part le théorème V.5.1 montre que le diagramme

$$\begin{array}{ccc} \mathbb{C}[\mathrm{X}_{24}] & \xrightarrow{\vartheta_1} & \mathrm{M}_{12}(\mathrm{SL}_2(\mathbb{Z})) \\ {\scriptstyle \mathrm{T}_p}\Big\downarrow & & \Big\downarrow{\scriptstyle p\,\frac{p^{21}-1}{p-1}+\mathrm{T}(p^2)} \\ \mathbb{C}[\mathrm{X}_{24}] & \xrightarrow{\vartheta_1} & \mathrm{M}_{12}(\mathrm{SL}_2(\mathbb{Z})) \end{array}$$

est commutatif (relation d'Eichler). D'autre part $\{\mathbb{E}_{12}, \Delta\}$ est une base du $\mathbb{C}$-espace vectoriel $\mathrm{M}_{12}(\mathrm{SL}_2(\mathbb{Z}))$, propre pour les opérateurs de Hecke ; on a en particulier $\mathrm{T}(p^2)\,(\Delta) = \tau(p^2)\,\Delta = (\tau(p)^2 - p^{11})\,\Delta$. Soient $\mathrm{coord}_\Delta : \mathrm{M}_{12}(\mathrm{SL}_2(\mathbb{Z})) \to \mathbb{C}$ la forme linéaire coordonnée "d'indice Δ" définie par cette base et $\eta : \mathbb{C}[\mathrm{X}_{24}] \to \mathbb{C}$ la forme linéaire composée $\mathrm{coord}_\Delta \circ \vartheta_1$; il résulte de ce qui précède que η est vecteur propre de l'endomorphisme T_p^* de $(\mathbb{C}[\mathrm{X}_{24}])^*$, pour la valeur propre $\sum_{k=1}^{21} p^k + (\tau(p)^2 - p^{11}) = \lambda_2(p)$. On vérifie facilement que l'on a

$$\eta(x) \;=\; |\mathrm{R}(x)| - \frac{65520}{691} \;=\; 24\;(\,\mathrm{h}(x) - \frac{2730}{691}\,)$$

pour tout x dans X_{24} (voir par exemple [Ser70, §6.6, formule (108)]). Comme en II.2 (Proposition 2.4), il en résulte que le vecteur

$$\sum_{x\in \mathrm{X}_{24}} \frac{1}{|\mathrm{O}(x)|}\,(\,\mathrm{h}(x) - \frac{2730}{691}\,)\;x$$

est vecteur propre de l'endomorphisme T_p de $\mathbb{C}[\mathrm{X}_{24}]$, pour la valeur propre $\lambda_2(p)$.

Sur le diamètre du graphe des p-voisins en dimension 24

La formule du théorème 2.1 montre que si l'on a $\mathrm{N}_p(L, L') = 0$ alors on a

$$\mathrm{P}_0(L, L'; p)^{\,2} \;=\; (\sum_{r=1}^{10} \mathrm{P}_r(L, L'; p)\,\theta_r(p)\,)^2 \qquad .$$

D'après l'inégalité de Schwarz on a

$$(\sum_{r=1}^{10} \mathrm{P}_r(L, L'; p)\,\theta_r(p)\,)^2 \;\le\; (\sum_{r=1}^{10} \gamma_r\,\mathrm{P}_r(L, L'; p)^2\,)\;(\sum_{r=1}^{10} \gamma_r^{-1}\,\theta_r(p)^2\,)$$

pour tout 10-uple $(\gamma_1, \gamma_2, \ldots, \gamma_{10})$ de nombres réels strictement positifs. En prenant

$$(\gamma_1, \gamma_2, \ldots, \gamma_{10}) = (4p^{11}, 4p^{15}, 4p^{17}, 4p^{19}, 4p^{21}, 9p^{22}, 16p^{19}, 16p^{21}, 16p^{21}, 16p^{21})$$

on obtient, compte tenu des inégalités de Ramanujan, l'inégalité

$$(\sum_{r=1}^{10} \mathrm{P}_r(L, L'; p)\,\theta_r(p)\,)^2 \;\le\; 10\;(\sum_{r=1}^{10} \gamma_r\,\mathrm{P}_r(L, L'; p)^2\,) \qquad .$$

On pose

$$(\Gamma_1(X), \Gamma_2(X), \ldots, \Gamma_{10}(X)) = (4X^{11}, 4X^{15}, \ldots, 16X^{21})$$

et

$$\mathrm{Q}(L, L'; X) \;=\; \mathrm{P}_0(L, L'; X)^{\,2} - 10\,(\sum_{r=1}^{10} \Gamma_r(X)\,\mathrm{P}_r(L, L'; X)^2\,) \qquad ;$$

on constate que $\mathrm{Q}(L, L'; X)$ est un polynôme de $\mathbb{Q}[X]$ dont le monôme de plus haut degré est $\mu(L')^2\,X^{44}$. On observera que la remarque qui suit le théorème 2.1 implique l'égalité $\mu(L)^2\,\mathrm{Q}(L, L'; X) = \mu(L')^2\,\mathrm{Q}(L', L; X)$. On note $\rho(L, L')$ la plus grande racine réelle du polynôme $\mathrm{Q}(L, L'; X)$ (on pourrait convenir que l'on a $\rho(L, L') = -\infty$ si $\mathrm{Q}(L, L'; X)$ n'a pas de racine réelle mais ce polynôme a en fait toujours des racines réelles) ; on note enfin $\mathrm{p}(L, L')$ le plus petit nombre premier strictement plus grand que $\rho(L, L')$. On a tout fait pour avoir $\mathrm{N}_p(L, L') > 0$ pour $p \geq \mathrm{p}(L, L')$.

Exemple. Le 24-uple $(\rho(\mathrm{L}_i, \mathrm{Leech}))_{1 \leq i \leq 24}$ est approximativement le suivant :

$$(46.77, 30.11, 30.88, 23.97, 21.71, 17.80, 17.59, 15.63, 13.72, 12.00, 11.27,$$
$$12.14, 9.36, 9.58, 8.48, 7.03, 6.19, 5.21, 5.86, 4.12, 3.10, 2.13, 1.37, 1.68)\ .$$

On constate par inspection que pour tout réseau de Niemeier L le nombre premier $\mathrm{p}(L, \mathrm{Leech})$ est le plus petit nombre premier supérieur ou égal au nombre de Coxeter $\mathrm{h}(L)$. Cette inspection et la proposition III.4.1.1 montrent que l'énoncé "$\mathrm{N}_p(L, L') > 0$ pour $p \geq \mathrm{p}(L, L')$" est optimal pour $L' = \mathrm{Leech}$.

On constate, également par inspection, que l'on a

$$\rho(L, L') \;\leq\; \rho(\mathrm{E}_{24}, \mathrm{Leech}) \;< 47$$

pour tous réseaux de Niemeier L et L'. On voit donc que le graphe des p-voisins en dimension 24 est le graphe complet d'ensemble de sommets X_{24} pour $p \geq 47$. Comme nous avons calculé les $\tau_{j,k}(p)$ pour $p \leq 43$ (et même $p \leq 113$, voir le prochain paragraphe), nous sommes maintenant en mesure de déterminer le diamètre du graphe des p-voisins en dimension 24 ; voici le résultat :

Théorème 2.4. *Soit p un nombre premier. Le diamètre du graphe $\mathrm{K}_{24}(p)$ est le suivant : 5 pour $p = 2$, 4 pour $p = 3$, 3 pour $p = 5$, 2 pour $7 \leq p \leq 43$ et 1 pour $p \geq 47$.*

3. Détermination des $\tau_{j,k}(q)$ pour de petites valeurs de q

Les $\tau_{j,k}(q)$ en question, $q = p^n$ avec p premier et $n \geq 1$ entier, sont définis en IX.1.7 ; on a vu que la détermination des $\tau_{j,k}(p^n)$ pour $n > 2$ se ramène à celle des $\tau_{j,k}(p^n)$ pour $n = 1, 2$. Les valeurs des $\tau_{j,k}(p)$ pour $p \leq 113$ sont rassemblées dans la table C.3, celles des $\tau_{j,k}(p^2)$ pour $p \leq 29$ dans la table C.4.

3.1. Détermination des $\tau_{j,k}(p)$ pour $p \leq 113$

Les entiers $\theta_r(p)$, $r \leq 6$, ne sont pas difficiles à calculer (au moins pour un nombre premier dont la taille n'est pas déraisonnable !). Par contre, comme nous l'avons déjà dit, les tables pour les $\theta_r(p)$, $r \geq 7$, sont assez courtes. Nous nous proposons de montrer que la théorie développée dans ce mémoire et les informations que nous avons collectées en III.4 sur la dernière colonne de T_p (c'est-à-dire sur les nombres de voisins $\mathrm{N}_p(L, \mathrm{Leech})$ pour L un réseau unimodulaire pair de dimension 24 représentant 2) permettent de déterminer ces $\theta_r(p)$ pour $p \leq 113$. Les formules (2.1) et (2.2) (ou ce qui revient au même le théorème 2.1), et la détermination de $\tau_{6,8}(p)$, $\tau_{8,8}(p)$, $\tau_{12,6}(p)$ et $\tau_{4,10}(p)$ pour $p \leq 113$ permettent d'expliciter l'opérateur de Hecke $\mathrm{T}_p : \mathbb{Z}[\mathrm{X}_{24}] \to \mathbb{Z}[\mathrm{X}_{24}]$ pour $p \leq 113$.

On écrit $\mathrm{N}_p(L, L') = \mathrm{N}_p^1(L, L') + \mathrm{N}_p^2(L, L')$ avec

$$\mathrm{N}_p^1(L, L') \;=\; \mathrm{P}_0(L, L'; p) + \sum_{r=1}^{6} \mathrm{P}_r(L, L'; p)\, \theta_r(p)$$

(c'est le terme “aisément calculable”) et

$$\mathrm{N}_p^2(L, L') \;=\; \sum_{r=7}^{10} \mathrm{P}_r(L, L'; p)\, \theta_r(p)$$

(c'est le terme “mystérieux”). Compte tenu de ce que l'on a rappelé plus haut sur les polynômes $\mathrm{C}_{j,r}$, $j \geq 1, r \geq 7$, qui interviennent dans l'expression des $\lambda_j(p)$, on a

$$\mathrm{N}_p^2(L, L') \;=\; \mathrm{c}_7(L, L')\, p(p+1)\, \theta_7(p) + \sum_{r=8}^{10} \mathrm{c}_r(L, L')\, (p+1)\, \theta_r(p) \quad , \tag{3.1}$$

les $\mathrm{c}_r(L, L')$, $r \geq 7$, désignant des nombres rationnels déterminés en fonction des classes d'isomorphisme des réseaux L et L'.

On voit donc que si l'on connaît les entiers $\mathrm{N}_p(L, L')$ pour quatre couples (L, L') (dont les orbites sous l'action de $\mathfrak{S}_2$ par échange des facteurs sont distinctes) alors on peut espérer déterminer les $\theta_r(p)$ pour $r \geq 7$ en résolvant un système linéaire.

Ci-après, on prend pour L' le réseau de Leech et pour L les quatre réseaux de Niemeier avec racines dont le nombre de Coxeter est le plus grand : $\mathrm{L}_1 := \mathrm{E}_{24}$ $(h = 46)$, $\mathrm{L}_2 := \mathrm{E}_{16} \oplus \mathrm{E}_8$ $(h = 30)$, $\mathrm{L}_3 := \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8$ $(h = 30)$ et $\mathrm{L}_4 := \mathrm{A}_{24}^+$ $(h = 25)$.

Les quatre égalités $\mathrm{N}_p^2(\mathrm{L}_i, \mathrm{Leech}) = \sum_{r=7}^{10} \mathrm{P}_r(\mathrm{L}_i, \mathrm{Leech}; p)\, \theta_r(p)$, $i = 1, 2, 3, 4$, peuvent encore s'écrire

$$\mathrm{A}(p) \begin{bmatrix} \theta_7(p) \\ \theta_8(p) \\ \theta_9(p) \\ \theta_{10}(p) \end{bmatrix} = \mathrm{B}(p) \qquad , \tag{3.2}$$

$\mathrm{A}(p)$ désignant la matrice 4×4 produit de la matrice

$$\mathrm{a} := \begin{bmatrix} \frac{-20360704}{297} & \frac{31085824}{1495} & \frac{210852224}{15795} & \frac{182174720}{9963} \\ \frac{-1048320}{2057} & \frac{110194560}{116909} & \frac{901568}{2223} & \frac{-15608320}{77121} \\ \frac{16329600}{22627} & \frac{16092820800}{16717987} & \frac{12615840}{35321} & \frac{27014400}{94259} \\ \frac{994175}{4752} & \frac{-36575}{208} & \frac{37053115}{202176} & \frac{-4447625}{79704} \end{bmatrix} \tag{3.3}$$

et de la matrice diagonale $\mathrm{diag}(p(p+1), p+1, p+1, p+1)$, et $\mathrm{B}(p)$ la matrice colonne

$$\begin{bmatrix} \mathrm{N}_p(\mathrm{E}_{24}, \mathrm{Leech}) - \mathrm{N}_p^1(\mathrm{E}_{24}, \mathrm{Leech}) \\ \mathrm{N}_p(\mathrm{E}_{16} \oplus \mathrm{E}_8, \mathrm{Leech}) - \mathrm{N}_p^1(\mathrm{E}_{16} \oplus \mathrm{E}_8, \mathrm{Leech}) \\ \mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{Leech}) - \mathrm{N}_p^1(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{Leech}) \\ \mathrm{N}_p(\mathrm{A}_{24}^+, \mathrm{Leech}) - \mathrm{N}_p^1(\mathrm{A}_{24}^+, \mathrm{Leech}) \end{bmatrix} .$$

On constate que l'on dét $\mathrm{a} \neq 0$ (merci `PARI`) ; le système linéaire (3.2) permet donc de déterminer les $\theta_r(p)$, $r \geq 7$, si l'on connaît les entiers $\mathrm{N}_p(\mathrm{L}_i, \mathrm{Leech})$ pour $i = 1, 2, 3, 4$.

Les cas $p \leq 23$

Soit L un réseau unimodulaire pair de dimension 24 avec racines. La proposition III.4.1.1 dit que l'on a $\mathrm{N}_p(L, \mathrm{Leech}) = 0$ pour $p < \mathrm{h}(L)$. On a donc en particulier $\mathrm{N}_p(\mathrm{L}_i, \mathrm{Leech}) = 0$ pour $i = 1, 2, 3, 4$: le système linéaire (3.2) permet de déterminer les $\theta_r(p)$, $r \geq 7$, pour $p \leq 23$.

Les cas $p = 29$ *et* $p = 31$

On a calculé $\mathrm{N}_p(\mathrm{A}_{24}^+, \mathrm{Leech})$ en III.4.3 pour $p = 29$ et $p = 31$. D'après III.4.1.1, on a $\mathrm{N}_{29}(L, \mathrm{Leech}) = 0$ pour $L = \mathrm{E}_{24}, \mathrm{E}_{16} \oplus \mathrm{E}_8, \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8$ et $\mathrm{N}_{31}(L, \mathrm{Leech}) = 0$ pour $L = \mathrm{E}_{24}$; d'autre part le point (d) de III.4.2.10 donne la valeur de $\mathrm{N}_{31}(L, \mathrm{Leech})$ pour $L = \mathrm{E}_{16} \oplus \mathrm{E}_8, \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8$. Le système linéaire (3.2) permet encore de déterminer les $\theta_r(p)$, $r \geq 7$, pour $p = 29$ et $p = 31$.

Les cas $p = 3$ *et* $7 \leq p \leq 59$

Le calcul de $\mathrm{N}_{31}(\mathrm{A}_{24}^+, \mathrm{Leech})$, évoqué ci-dessus, bien qu'élémentaire est assez acrobatique. Nous proposons ci-après une méthode, loin d'être aussi élémentaire mais autrement plus efficace, pour déterminer les entiers $\mathrm{N}_p(L, \mathrm{Leech})$, L désignant un réseau de Niemeier avec racines, lorsque p n'est "pas trop grand en fonction de L", au moins si p ne divise pas l'indice, noté $\mathrm{g}(L)$ en III.4, du sous-module de L engendré par ses racines. Cette méthode est fondée sur les deux observations suivantes :

– Soit p un nombre premier qui ne divise pas $\mathrm{g}(L)$. L'énoncé III.4.3.3 dit que $\mathrm{N}_p(L, \mathrm{Leech})$ appartient à une progression arithmétique (contenant 0) de raison

$$\mathrm{pas}(L; p) \ := \ \frac{|\mathrm{W}(L)|}{\mathrm{p.g.c.d.}(p-1, 24\mathrm{h}(L), |\mathrm{W}(L)|)} \qquad .$$

– Soient L et L' deux réseaux unimodulaires pairs de dimension 24. Les inégalités de Ramanujan pour les $\theta_r(p)$, $r \geq 7$, fournissent un encadrement

$$\mathrm{N}_p^{\inf}(L, L') \ \leq \ \mathrm{N}_p(L, L') \ \leq \ \mathrm{N}_p^{\sup}(L, L')$$

dont la largeur est $2\mathrm{K}(L, L')(p+1)p^{\frac{21}{2}}$ avec $\mathrm{K}(L, L') := 4 \sum_{r=7}^{10} |\mathrm{c}_r(L, L')|$ (notations de (3.1)).

On prend pour L un réseau de Niemeier avec racines avec $\mathrm{g}(L)$ non divisible par p et pour L' le réseau de Leech. Si la largeur en question est strictement inférieure à $\mathrm{pas}(L; p)$ alors $\mathrm{N}_p(L, \mathrm{Leech})$ est déterminé.

Détaillons un peu.

On a $|\theta_7(p)| \leq 4p^{\frac{19}{2}}$ et $|\theta_r(p)| \leq 4p^{\frac{21}{2}}$ pour $r = 8, 9, 10$. On en déduit l'inégalité

$$|\mathrm{N}_p^2(L, L')| \ \leq \ \mathrm{K}(L, L')\,(p+1)\,p^{\frac{21}{2}} \qquad .$$

On pose

$$\mathrm{N}_p^{\mathrm{inf}}(L, L') \ = \ \mathrm{N}_p^1(L, L') - \mathrm{K}(L, L')\,(p+1)\,p^{\frac{21}{2}} \qquad ,$$

$$\mathrm{N}_p^{\mathrm{sup}}(L, L') \ = \ \mathrm{N}_p^1(L, L') + \mathrm{K}(L, L')\,(p+1)\,p^{\frac{21}{2}} \qquad .$$

Rappelons que nous avons noté $\mathrm{n}_p(L)$ l'entier défini par l'égalité $\mathrm{N}_p(L, \mathrm{Leech}) = \mathrm{n}_p(L)\,\mathrm{pas}(L; p)$. On pose

$$\nu_p^{\mathrm{inf}}(L) \ = \ \frac{\mathrm{N}_p^{\mathrm{inf}}(L, \mathrm{Leech})}{\mathrm{pas}(L; p)} \qquad , \qquad \nu_p^{\mathrm{sup}}(L) \ = \ \frac{\mathrm{N}_p^{\mathrm{sup}}(L, \mathrm{Leech})}{\mathrm{pas}(L; p)} \qquad ;$$

on a donc l'encadrement $\nu_p^{\mathrm{inf}}(L) \leq \mathrm{n}_p(L) \leq \nu_p^{\mathrm{sup}}(L)$.

Exemples. On illustre par quelques exemples l'efficacité de cet encadrement :

– On a $\nu_3^{\mathrm{inf}}(\mathrm{L}_{23}) \approx 0.99953$ et $\nu_3^{\mathrm{sup}}(\mathrm{L}_{23}) \approx 1.00041$; on en déduit $\mathrm{n}_3(\mathrm{L}_{23}) = 1$ et $\mathrm{N}_3(\mathrm{L}_{23}, \mathrm{Leech}) = 8388608$ en accord avec le point (d) de III.4.2.10.

– On a $\nu_{31}^{\mathrm{inf}}(\mathrm{A}_{24}^+) \approx 275.99920$ et $\nu_{31}^{\mathrm{sup}}(\mathrm{A}_{24}^+) \approx 276.00061$; on en déduit $\mathrm{n}_{31}(\mathrm{A}_{24}^+) = 276$ et $\mathrm{N}_{31}(\mathrm{A}_{24}^+, \mathrm{Leech}) = 1427031323986450710528000 00$, en accord avec le calcul effectué en III.4.3.

– On constate que l'on a $\nu_p^{\mathrm{sup}}(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8) < 8 \times 10^{-6}$ pour $p \leq 29$; on a donc $\mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{Leech}) = 0$ pour $p \leq 29$, en accord avec III.4.1.1.

– On a $\nu_{47}^{\mathrm{inf}}(\mathrm{E}_{24}) \approx 0.99992$ et $\nu_{47}^{\mathrm{sup}}(\mathrm{E}_{24}) \approx 1.00006$; on en déduit $\mathrm{n}_{47}(\mathrm{E}_{24}) = 1$ et $\mathrm{N}_{47}(\mathrm{E}_{24}, \mathrm{Leech}) = 1131456179644927440637132 80000$, en accord avec le point (d) de III.4.2.10.

On pose $\mathrm{n}_p^{\mathrm{inf}}(L) = \lceil \nu_p^{\mathrm{inf}}(L) \rceil$ et $\mathrm{n}_p^{\mathrm{sup}}(L) = \lfloor \nu_p^{\mathrm{sup}}(L) \rfloor$. Rappelons la notation : soit ν un nombre réel ; $\lceil \nu \rceil$ est le plus petit entier n avec $\nu \leq n$ et $\lfloor \nu \rfloor$ le plus grand entier n avec $n \leq \nu$. On a donc par définition l'encadrement

$$\mathrm{n}_p^{\mathrm{inf}}(L) \ \leq \ \mathrm{n}_p(L) \ \leq \ \mathrm{n}_p^{\mathrm{sup}}(L) \qquad .$$

On note $\mathrm{e}_p(L)$ l'entier naturel $\mathrm{n}_p^{\mathrm{sup}}(L) - \mathrm{n}_p^{\mathrm{inf}}(L)$. Si l'on a $\mathrm{e}_p(L) = 0$ alors $\mathrm{N}_p(L, \mathrm{Leech})$ est déterminé : $\mathrm{N}_p(L, \mathrm{Leech}) = \mathrm{n}_p^{\mathrm{inf}}(L)\,\mathrm{pas}(L; p)$.

Exemple. On prend $L = \mathrm{E}_{24}$. Comme l'on a $\mathrm{g}(\mathrm{E}_{24}) = 2$, il faut supposer $p \geq 3$ pour que la théorie précédente s'applique. `PARI` nous dit que $\mathrm{e}_p(\mathrm{E}_{24})$ est nul pour pour $3 \leq p \leq 131$. L'entier $\mathrm{N}_p(\mathrm{E}_{24}, \mathrm{Leech})$ est déterminé pour ces nombres premiers, on a par exemple (pour le plaisir enfantin d'écrire un très gros nombre entier !) :

$$\mathrm{N}_{131}(\mathrm{E}_{24}, \mathrm{Leech}) \;=\; 1236254480530019921169523818786874982400 00 \quad .$$

On considère maintenant le quadruplet

$$\underline{\mathrm{e}}_p \;:=\; (\mathrm{e}_p(\mathrm{E}_{24}), \mathrm{e}_p(\mathrm{E}_{16} \oplus \mathrm{E}_8), \mathrm{e}_p(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8), \mathrm{e}_p(\mathrm{A}_{24}^+)) \qquad ;$$

comme l'on a $(\mathrm{g}(\mathrm{E}_{24}), \mathrm{g}(\mathrm{E}_{16} \oplus \mathrm{E}_8), \mathrm{g}(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8), \mathrm{g}(\mathrm{A}_{24}^+)) = (2, 2, 1, 5)$ on suppose $p \neq 2, 5$. `PARI` nous dit que l'on a $\underline{\mathrm{e}}_p = (0, 0, 0, 0)$ pour $p = 3$ et $7 \leq p \leq 59$. Les entiers $\mathrm{N}_p(\mathrm{L}_i, \mathrm{Leech})$ sont déterminés pour ces nombres premiers et $i = 1, 2, 3, 4$; du coup le système linéaire (3.2) permet de calculer les $\theta_r(p)$, $r \geq 7$, pour les nombres premiers en question.

Les cas $61 \leq p \leq 107$

Pour $61 \leq p \leq 107$, on n'a plus $\underline{\mathrm{e}}_p = (0, 0, 0, 0)$; on va montrer cependant que l'on peut encore déterminer les $\theta_r(p)$, $r \geq 7$. La méthode est décrite ci-après. On pose $\mathrm{n}_p(\mathrm{L}_i) = \mathrm{n}_p^{\inf}(\mathrm{L}_i) + x_i$, $1 \leq i \leq 4$; (x_1, x_2, x_3, x_4) est donc un quadruplet d'entiers naturels qu'il s'agit de déterminer. Ce quadruplet est soumis aux contraintes suivantes, numérotées (1), (2), (3), (4) :

(1) On a les inégalités $0 \leq x_i \leq \mathrm{e}_p(\mathrm{L}_i)$, $1 \leq i \leq 4$.

(2) Le quadruplet (x_1, x_2, x_3, x_4) vérifie des congruences affines modulo p ou modulo des diviseurs de $p+1$. Détaillons un peu. La relation (3.2) peut être écrite sous la forme suivante :

$$\begin{bmatrix} p(p+1)\,\theta_7(p) \\ (p+1)\,\theta_8(p) \\ (p+1)\,\theta_9(p) \\ (p+1)\,\theta_{10}(p) \end{bmatrix} \;=\; \mathrm{F}(p) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \mathrm{G}(p) \qquad , \tag{3.4}$$

$\mathrm{F}(p)$ désignant la matrice carrée $a^{-1}\,\mathrm{diag}(\mathrm{pas}(\mathrm{L}_1; p), \ldots, \mathrm{pas}(\mathrm{L}_4; p))$ et $\mathrm{G}(p)$ la matrice colonne $a^{-1}\,\mathrm{B}^{\inf}(p)$ avec

$$\mathrm{B}^{\inf}(p) \;:=\; \begin{bmatrix} \mathrm{n}_p^{\inf}(\mathrm{L}_1)\,\mathrm{pas}(\mathrm{L}_1; p) - \mathrm{N}_p^1(\mathrm{L}_1, \mathrm{Leech}) \\ \mathrm{n}_p^{\inf}(\mathrm{L}_2)\,\mathrm{pas}(\mathrm{L}_2; p) - \mathrm{N}_p^1(\mathrm{L}_2, \mathrm{Leech}) \\ \mathrm{n}_p^{\inf}(\mathrm{L}_3)\,\mathrm{pas}(\mathrm{L}_3; p) - \mathrm{N}_p^1(\mathrm{L}_3, \mathrm{Leech}) \\ \mathrm{n}_p^{\inf}(\mathrm{L}_4)\,\mathrm{pas}(\mathrm{L}_4; p) - \mathrm{N}_p^1(\mathrm{L}_4, \mathrm{Leech}) \end{bmatrix} \qquad .$$

La matrice $\mathrm{F}(p)$ est à coefficients entiers pour $p \not\equiv 1 \bmod 23$. Expliquons pourquoi. Comme dans la remarque qui suit III.4.3.3 on écrit $\mathrm{pas}(\mathrm{L}_i; p) = \mathrm{pas}_1(\mathrm{L}_i)\mathrm{pas}_2(\mathrm{L}_i; p)$. On constate que la matrice

$$a^{-1}\,\mathrm{diag}(\mathrm{pas}_1(\mathrm{L}_1), \ldots, \mathrm{pas}_1(\mathrm{L}_4))\,\mathrm{diag}(23, 1, 1, 1)$$

(qui est indépendante de p) est à coefficients entiers ; or, par définition même, 23 divise l'entier $\mathrm{pas}_2(\mathrm{E}_{24}; p)$ pour $p \not\equiv 1 \bmod 23$. On observera que si $\mathrm{F}(p)$ est à coefficients entiers alors, compte tenu de (3.4) il est de même pour $\mathrm{G}(p)$. Le fait que $\mathrm{F}(p)$, $\mathrm{G}(p)$ sont à coefficients entiers et que les $\theta_r(p)$, $r \geq 7$, sont entiers conduit aux congruences évoquées plus haut.

(3) Soient $\theta_r(p; X_1, X_2, X_3, X_4)$, $7 \leq r \leq 10$, les quatre polynômes affines de $\mathbb{Q}[X_1, X_2, X_3, X_4]$ définis par

$$\begin{bmatrix} \theta_7(p; X_1, X_2, X_3, X_4) \\ \theta_8(p; X_1, X_2, X_3, X_4) \\ \theta_9(p; X_1, X_2, X_3, X_4) \\ \theta_{10}(p; X_1, X_2, X_3, X_4) \end{bmatrix} := \mathrm{diag}(p(p+1), p+1, p+1, p+1)^{-1}(\mathrm{F}(p) \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} + \mathrm{G}(p))$$

(la notation est étrange... mais transparente, on observera que la condition (2) équivaut au fait que $\theta_r(p; x_1, x_2, x_3, x_4)$ est entier pour $7 \leq r \leq 10$). Soit $\mathrm{T}_p(X_1, X_2, X_3, X_4)$ la matrice obtenue en substituant dans (2.2) aux $\theta_r(p)$, $r \leq 7$, les $\theta_r(p; X_1, X_2, X_3, X_4)$; $\mathrm{T}_p(X_1, X_2, X_3, X_4)$ est donc une matrice à 24 lignes et 24 colonnes dont les coefficients sont des polynômes affines de $\mathbb{Q}[X_1, X_2, X_3, X_4]$ telle que l'on a $\mathrm{T}_p(x_1, x_2, x_3, x_4) = \mathrm{T}_p$. On note $\mathrm{N}_p(\mathrm{L}_i, \mathrm{L}_j; X_1, X_2, X_3, X_4)$ le coefficient d'indice (j, i) de $\mathrm{T}_p(X_1, X_2, X_3, X_4)$ et on pose, pour $i \leq 23$,

$$\mathrm{n}_p(\mathrm{L}_i; X_1, X_2, X_3, X_4) \;:=\; \frac{\mathrm{N}_p(\mathrm{L}_i, \mathrm{Leech}; X_1, X_2, X_3, X_4)}{\mathrm{pas}(\mathrm{L}_i; p)}$$

(on a donc, par construction, $\mathrm{n}_p(\mathrm{L}_i; X_1, X_2, X_3, X_4) = X_i + \mathrm{n}_p^{\mathrm{inf}}(\mathrm{L}_i)$ pour $i \leq 4$). On a par exemple

$$\mathrm{n}_p(\mathrm{L}_5; X_1, X_2, X_3, X_4) \;=\; \sum_{i=1}^{4} \alpha_i \gamma_i(p)\, X_i + \beta(p)$$

avec

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (-1472, -\frac{41}{8}, \frac{119}{16}, \frac{281}{256})$$
$$\gamma_i(p) = \frac{\mathrm{p.g.c.d.}(p-1, 24\mathrm{h}(\mathrm{L}_5))}{\mathrm{p.g.c.d.}(p-1, 24\mathrm{h}(\mathrm{L}_i))} \quad , \quad \beta(p) = \frac{\mathrm{N}_p^1(\mathrm{L}_5, \mathrm{Leech})}{\mathrm{pas}(\mathrm{L}_i; p)} \quad .$$

D'après III.4.3.3, $\mathrm{n}_p(\mathrm{L}_5; x_1, x_2, x_3, x_4) = \mathrm{n}_p(\mathrm{L}_5)$ est entier ; on en déduit que le quadruplet (x_1, x_2, x_3, x_p) vérifie une congruence affine modulo un entier explicite dépendant de p, disons $\mathrm{m}(p)$. Précisons un peu. On constate que le dénominateur commun des rationnels $\alpha_i \gamma_i(p)$ (mis sous forme irréductible) est $\mathrm{m}(p)$, la fonction $p \mapsto \mathrm{m}(p)$ pour $61 \leq p \leq 113$ étant donnée par le tableau suivant (on a rajouté les valeurs de $\mathrm{m}(p)$ pour $p = 109$ et $p = 113$ en vue d'une future application)

p	61	67	71	73	79	83	89	97	101	103	107	109	113
m	1280	256	1280	768	256	256	256	128	6400	256	256	768	128

.

On en déduit que $\mathrm{m}(p)\beta(p)$ est entier et la congruence évoquée plus haut.

On observe que la valuation 2-adique de $\mathrm{v}_2(\gamma_i(p))$ est nulle pour $i = 1, 2, 3$ et que l'on a $\mathrm{v}_2(\gamma_4(p)) = 0$ pour $\mathrm{v}_2(p-1) \leq 3$, $\mathrm{v}_2(\gamma_4(p)) = 1$ pour $\mathrm{v}_2(p-1) \geq 4$. On déduit, en contemplant le quadruplet $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, que la congruence que l'on vient de dégager détermine la classe de x_4 modulo 16 pour $p \neq 97, 113$ (et $61 \leq p \leq 113$) et modulo 8 pour $p = 97, 113$. La valeur de x_4 modulo 16 pour $61 \leq p \leq 113$ est donnée par le tableau suivant

p	61	67	71	73	79	83	89	97	101	103	107	109	113
x_4 mod 16	3	0	2	11	7	3	2	0 ou 8	5	4	5	0	0 ou 8

.

Cette forme faible de la contrainte (3) sera notée (3_4) ci-après.

(4) On doit avoir $|\theta_7(p; x_1, x_2, x_3, x_4)| \leq 4p^{\frac{19}{2}}$ et $|\theta_r(p; x_1, x_2, x_3, x_4)| \leq 4p^{\frac{21}{2}}$ pour $r = 8, 9, 10$.

Le cas $p = 61$

On a $\underline{\mathrm{e}}_{61} = (0, 0, 0, 5)$. La contrainte (3_4) détermine le quadruplet cherché : $(x_1, x_2, x_3, x_4) = (0, 0, 0, 3)$.

Le cas $p = 67$

On a $\underline{\mathrm{e}}_{67} = (0, 0, 0, 1)$. La contrainte (3_4) détermine le quadruplet cherché : $(x_1, x_2, x_3, x_4) = (0, 0, 0, 0)$.

Le cas $p = 71$

On a $\underline{\mathrm{e}}_{71} = (0, 0, 0, 6)$. La contrainte (3_4) détermine le quadruplet cherché : $(x_1, x_2, x_3, x_4) = (0, 0, 0, 2)$.

Le cas $p = 73$

On a $\underline{\mathrm{e}}_{73} = (0, 6, 9, 20)$. La contrainte (2) donne notamment $(x_1, x_2, x_3, x_4) \equiv (0, 3, 5, 11) \bmod 37$. Le quadruplet cherché est $(0, 3, 5, 11)$.

Le cas $p = 79$

On a $\underline{e}_{79} = (0, 0, 1, 12)$. La contrainte (2) donne $2x_3 + x_4 \equiv 9 \bmod 79$; l'encadrement $0 \leq 2x_3 + x_4 \leq 14$ force $2x_3 + x_4 = 9$. La contrainte (3_4) détermine alors le quadruplet cherché : $(x_1, x_2, x_3, x_4) = (0, 0, 1, 7)$.

Le cas $p = 83$

On a $\underline{e}_{83} = (0, 0, 0, 6)$. La contrainte (3_4) détermine le quadruplet cherché : $(x_1, x_2, x_3, x_4) = (0, 0, 0, 3)$.

Le cas $p = 89$

On a $\underline{e}_{89} = (0, 6, 10, 67)$. La contrainte (2) donne $-2x_2 - 7x_3 + x_4 + 7 \equiv 0 \bmod 89$; l'encadrement $-75 \leq -2x_2 - 7x_3 + x_4 - 7 \leq 74$ force $x_4 = 2x_2 + 7x_3 - 7$. La contrainte (3) donne $10x_2 + 3x_3 - 45 \equiv 0 \bmod 256$; le même argument que précédemment montre que l'on a $10x_2 + 3x_3 - 45 = 0$. En particulier x_2 est divisible par 3. L'encadrement $0 \leq x_3 \leq 10$ force alors $x_2 = 3$. Le quadruplet cherché est $(0, 3, 5, 34)$.

Le cas $p = 97$

On a $\underline{e}_{97} = (0, 117, 187, 548)$. L'ordinateur dit que les quadruplets satisfaisant (1), (2), et (3) sont $(0, 22, 63, 432)$ et $(0, 71, 105, 272)$ (on peut aider l'ordinateur en observant que (2) implique $(x_2, x_3) \equiv (1, 0) \bmod 7$ et que (3_4) dit que x_4 est divisible par 8). Le premier ne passe pas le "test de Ramanujan" (la contrainte (4)) : $(x_1, x_2, x_3, x_4) = (0, 71, 105, 272)$.

Le cas $p = 101$

On a $\underline{e}_{101} = (0, 78, 124, 3643)$. L'ordinateur dit que le seul quadruplet satisfaisant (1), (2) et (3) est $(0, 30, 63, 2149)$.

Le cas $p = 103$

On a $\underline{e}_{103} = (0, 29, 46, 273)$. L'ordinateur dit que les quadruplets satisfaisant (1), (2) et (3) sont $(0, 7, 46, 196)$, $(0, 15, 27, 148)$ et $(0, 23, 8, 100)$. Le premier et le troisième ne passent pas le test de Ramanujan : $(x_1, x_2, x_3, x_4) = (0, 15, 27, 148)$.

Le cas $p = 107$

On a $\underline{e}_{107} = (0, 14, 23, 141)$. L'ordinateur dit que le seul quadruplet satisfaisant (1), (2) et (3) est $(0, 7, 10, 53)$.

Les cas $p = 109$ et $p = 113$

Une conséquence inattendue du théorème 4.4, que nous démontrerons dans le prochain paragraphe en faisant appel à la théorie des représentations galoisiennes, est que le quadruplet (x_1, x_2, x_3, x_4), introduit lors de l'étude des cas $61 \leq p \leq 107$, vérifie des congruences affines modulo des diviseurs de $p + 1$ dont certaines peuvent être "indépendantes" des congruences de la contrainte (2). Ces contraites supplémentaires permettent de déterminer le quadruplet (x_1, x_2, x_3, x_4) pour $p = 109$ et $p = 113$.

Le cas $p = 109$

On a $\underline{e}_{109} = (0, 337, 538, 1049)$. L'ordinateur dit qu'il existe 208 quadruplets satisfaisant les contraintes (1), (2) et (3) et que parmi ceux-ci 12 satisfont la contrainte (4). On note $\underline{x}^{(1)}, \underline{x}^{(2)}, \ldots, \underline{x}^{(12)}$ ces 12 quadruplets d'entiers naturels ; on suppose, pour fixer les idées, que l'on a $\underline{x}^{(1)} < \underline{x}^{(2)} < \ldots < \underline{x}^{(12)}$ pour l'ordre lexicographique. Pour $k = 1, 2, \ldots, 12$, on vérifie que $\mathrm{T}_{109}(\underline{x}^{(k)})$ est à coefficients entiers et que $\mathrm{n}_{109}(\mathrm{L}_i; \underline{x}^{(k)})$ est aussi entier pour $6 \leq i \leq 23$ (nous avons tout fait pour que $\mathrm{n}_{109}(\mathrm{L}_i; \underline{x}^{(k)})$ soit entier pour $1 \leq i \leq 5$).

Ce qui précède montre que la méthode qui nous a permis de déterminer $\tau_{6,8}(p)$, $\tau_{8,8}(p)$, $\tau_{12,6}(p)$ et $\tau_{4,10}(p)$ pour $p \leq 107$ est en échec pour $p = 109$.

On parvient cependant à lever l'indétermination évoquée ci-dessus de la façon suivante. On contemple la suite de quadruplets d'entiers relatifs

$$(\theta_7(109; \underline{x}^{(k)}) \, , \, \theta_8(109; \underline{x}^{(k)}) \, , \, \theta_9(109; \underline{x}^{(k)}) \, , \, \theta_{10}(109; \underline{x}^{(k)}) \,)_{k=1,2,\ldots,12} \qquad .$$

Par chance, un seul de ces quadruplets, à savoir le 5-ième, vérifie la congruence imposée par le point (12) du théorème 4.4 (le quadruplet en question est d'ailleurs celui qui était le plus probable "au sens de Sato-Tate"). On observera que le point (12) du théorème 4.4 est une congruence modulo 11 et que 11 divise $109 + 1$!

On peut paraphraser ainsi ce qui précède. En plus des contraintes (1), (2), (3) et (4), les entiers naturels $x_i := \mathrm{n}_{109}(\mathrm{L}_i) - \mathrm{n}^{\mathrm{inf}}_{109}(\mathrm{L}_i)$, $i = 1, 2, 3, 4$, sont soumis à la contrainte, disons (2-supp), imposée par le point (12) du théorème 4.4. Il n'est pas difficile d'expliciter (2-supp), il s'agit de la congruence

$$x_1 + x_2 + 6x_3 + x_4 + 2 \;\equiv\; 0 \mod 11 \qquad .$$

Un seul quadruplet (x_1, x_2, x_3, x_4) satisfait les contraintes (1), (2), (2-supp), (3) et (4) : le quadruplet $(0, 138, 284, 576)$.

Le cas $p = 113$

On a $\underline{e}_{113} = (0, 227, 361, 1058)$. On considère cette fois les points (3) et (4) du théorème 4.4 (parce que 19 divise $113 + 1$). Ces deux points imposent au quadruplet (x_1, x_2, x_3, x_4) une contrainte, disons (2-supp), constituée de deux congruences affines modulo 19 ; on constate que celles-ci sont indépendantes des deux congruences affines modulo 19 qui apparaissent dans la contrainte (2). Du coup, le quadruplet (x_1, x_2, x_3, x_4) est déterminé modulo 19 ; on trouve :

$$(x_1, x_2, x_3, x_4) \equiv (0, 6, 3, 16) \mod 19$$

(la présence du 0 en première position au second membre est rassurante !). L'ordinateur montre ensuite qu'il n'existe que deux quadruplets satisfaisant les contraintes (1), (2), (2-supp) et (3) : $(0, 120, 155, 396)$ et $(0, 177, 326, 244)$. Le second ne passe pas le test de Ramanujan. Les entiers $\tau_{6,8}(113)$, $\tau_{8,8}(113)$, $\tau_{12,6}(113)$ et $\tau_{4,10}(113)$ et l'endomorphisme T_{113} de $\mathbb{Z}[\mathrm{X}_{24}]$ sont donc déterminés.

On trouve par exemple

$$\mathrm{N}_{113}(\mathrm{L}_{12}, \mathrm{L}_{21}) = 633323838523478069636624166862873752207360000$$

(c'est le plus grand nombre de p-voisins, p premier, parmi ceux que nous avons pu calculer).

Le cas $p = 127$

Les méthodes qui nous ont permis de déterminer $\tau_{6,8}(p)$, $\tau_{8,8}(p)$, $\tau_{12,6}(p)$ et $\tau_{4,10}(p)$ pour $p \leq 113$ sont en échec pour $p = 127$. Nous expliquons pourquoi ci-après (en petits caractères).

– L'ordinateur dit qu'il existe 3329 quadruplets satisfaisant les contraintes (1), (2), (3) et (4), disons $\underline{x}^{(1)}, \underline{x}^{(2)}, \ldots, \underline{x}^{(3329)}$. Pour $k = 1, 2, \ldots, 3329$, on vérifie que $\mathrm{T}_{127}(\underline{x}^{(k)})$ est à coefficients entiers et que $\mathrm{n}_{127}(\mathrm{L}_i; \underline{x}^{(k)})$ est aussi entier pour $6 \leq i \leq 23$.

– Le seul nombre premier qui divise $127+1$ est 2 et l'on constate que les entiers $\theta_r(127; \underline{x}^{(k)})$, $7 \leq r \leq 10$, $1 \leq k \leq 3329$, sont tous pairs, en accord avec la congruence (12) du théorème 4.4. En fait, en contemplant les quatre polynômes affines $\theta_r(127; X_1, X_2, X_3, X_4)$, $7 \leq r \leq 10$, on constate que l'on a $\theta_7(127; \underline{x}) \equiv 134400 \bmod 2^{18}$, $\theta_8(127; \underline{x}) \equiv 3840 \bmod 2^{13}$, $\theta_9(127; \underline{x}) \equiv -3840 \bmod 2^{13}$ et $\theta_{10}(127; \underline{x}) \equiv 256 \bmod 2^{10}$ pour tout $\underline{x}$ dans $\mathbb{Z}^4$.

3.2. Détermination des $\tau_{j,k}(p^2)$ pour $p \leq 29$

On note, ci-dessous, respectivement $\varpi_1, \varpi_2, \ldots, \varpi_{10}$ les représentations automorphes Δ_{11}, Δ_{15}, Δ_{17}, Δ_{19}, Δ_{21}, $\mathrm{Sym}^2\Delta_{11}$, $\Delta_{19,7}$, $\Delta_{21,9}$, $\Delta_{21,13}$ et $\Delta_{21,5}$

(voir §VII.3, §VI.4.7, définition 1.6). La représentation ϖ_r est donc dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ pour $r \leq 5$, dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_3)$ pour $r = 6$ et dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_4)$ pour $r \geq 7$.

Soit p un nombre premier, les entiers $\theta_r(p)$, $1 \leq r \leq 10$, que nous avons introduits au paragraphe 2 vérifient par définition la relation

$$\theta_r(p) \;=\; p^{\frac{\mathrm{w}(\varpi_r)}{2}} \,\mathrm{trace}\, \mathrm{c}_p(\varpi_r) \qquad .$$

(Voir §VI.4.1, §VIII.2.6 ; on rappelle que $\mathrm{w}(\pi)$ désigne le poids motivique d'une représentation automorphe algébrique π dans $\Pi_{\mathrm{cusp}}(\mathrm{PGL}_n)$, ici l'indice w pour $\pi = \Delta_w$ ou $\Delta_{w,v}$.)

On pose pareillement

$$\theta_r(p^2) \;:=\; p^{\mathrm{w}(\varpi_r)} \,\mathrm{trace}\,(\mathrm{c}_p(\varpi_r)^2) \qquad .$$

Pour $r \geq 7$, la définition ci-dessus est en accord avec celle que nous avons choisie en IX.1.7 : $\theta_7(p^2) = \tau_{6,8}(p^2)$, $\theta_8(p^2) = \tau_{8,8}(p^2)$, $\theta_9(p^2) = \tau_{12,6}(p^2)$ et $\theta_9(p^2) = \tau_{4,10}(p^2)$.

Par contre, on prendra garde que, pour $r = 1, 2, 3, 4, 5$, $\theta_i(p^2)$ n'est pas la valeur en p^2 des fonctions arithmétiques $\tau_{12}, \tau_{16}, \tau_{18}, \tau_{20}, \tau_{22}$; on a en fait $\theta_1(p^2) = \tau_{12}(p)^2 - 2p^{11}$, $\theta_2(p^2) = \tau_{16}(p)^2 - 2p^{15}$, $\theta_3(p^2) = \tau_{18}(p)^2 - 2p^{17}$, $\theta_4(p^2) = \tau_{20}(p)^2 - 2p^{19}$ et $\theta_5(p^2) = \tau_{22}(p)^2 - 2p^{21}$. Enfin, on vérifie aisément que l'on a $\theta_6(p^2) = \tau_{12}(p)^4 - 4p^{11}\tau_{12}(p)^2 + 3p^{22}$.

Soit V_{St} la représentation standard de $\mathrm{SO}_n(\mathbb{C})$. Pour p un nombre premier, on note $\mathrm{T}_p^{\psi^2}$ l'opérateur de Hecke dans $\mathrm{H}_p(\mathrm{O}_n)$ défini, *via* l'isomorphisme de Satake, par la formule

$$p^{2-n}\,\mathrm{Sat}(\mathrm{T}_p^{\psi^2}) \;=\; \psi^2\,[\mathrm{V}_{\mathrm{St}}] \;:=\; [\mathrm{V}_{\mathrm{St}} \otimes \mathrm{V}_{\mathrm{St}}] - 2\,[\Lambda^2 \mathrm{V}_{\mathrm{St}}]$$

(voir §VI.2.1). L'intégralité de cet opérateur découle du lemme 1.1 ; en fait on a dans le cas présent

$$\mathrm{T}_p^{\psi^2} \;=\; \mathrm{T}_p^2 - 2p\mathrm{T}_{p,p} - 2p\,(\sum_{i=0}^{\frac{n}{2}-2} p^{2i} + p^{\frac{n}{2}-2}) \tag{3.5}$$

d'après les formules VI.(2.5) et VI.(2.6).

On suppose maintenant $n = 24$ et on note $\lambda_j^{\psi^2}(p)$ la valeur propre de $\mathrm{T}_p^{\psi^2}$ sur le vecteur v_j de $\mathbb{Z}[\mathrm{X}_{24}]$, $1 \leq j \leq 24$; on a tout fait pour avoir

$$\lambda_j^{\psi^2}(p) \;=\; p^{22}\,\mathrm{trace}\,\mathrm{St}(\mathrm{c}_p(\pi_j)^2) \;=\; \mathrm{C}_{j,0}(p^2) + \sum_{r=1}^{10} \mathrm{C}_{j,r}(p^2)\,\theta_r(p^2) \qquad ,$$

les polynômes $\mathrm{C}_{j,r}$ de $\mathbb{Z}[X]$ étant ceux introduits au paragraphe 2.

On revient au cas général. La formule

$$(p+1)\,\mathrm{T}_{p,p} \;=\; \mathrm{T}_p^2 - \mathrm{T}_{p^2} - \frac{(p^{\frac{n}{2}}-1)(p^{\frac{n}{2}-1}+1)}{(p-1)}$$

de l'exemple VI.2.11 et la formule (3.5), montrent que l'opérateur T_{p^2} s'exprime en fonction de $\mathrm{T}_p^{\psi^2}$ et T_p^2 :

$$\mathrm{T}_{p^2} \;=\; \frac{p+1}{2p}\,\mathrm{T}_p^{\psi^2} + \frac{p-1}{2p}\,\mathrm{T}_p^2 \;- p^{n-2} + p^{\frac{n}{2}-2} \qquad . \tag{3.6}$$

Comme l'on a déterminé les $\tau_{j,k}(p)$ pour $p \leq 113$ en 3.1, les considérations ci-dessus montrent que la détermination des $\tau_{j,k}(p^2)$ avec $p \leq 29$ se ramène à celle des nombres de voisins $\mathrm{N}_{p^2}(\mathrm{L}_i, \mathrm{Leech})$ pour $i \leq 4$ et $p \leq 29$ (on rappelle que l'on a posé $\mathrm{E}_{24} = \mathrm{L}_1$, $\mathrm{E}_{16} \oplus \mathrm{E}_8 = \mathrm{L}_2$, $\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{E}_8 = \mathrm{L}_3$ et $\mathrm{A}_{24}^+ = \mathrm{L}_4$) ; en effet, le système qui exprime les $\mathrm{N}_{p^2}(\mathrm{L}_i, \mathrm{Leech})$ en fonction des "inconnues" $\tau_{j,k}(p^2)$ est toujours un système de Cramer parce que la matrice a de (3.3) est inversible. On détermine ces nombres de voisins ci-après.

Les cas $p \leq 3$

On a $\mathrm{N}_{p^2}(\mathrm{L}_i, \mathrm{Leech}) = 0$ pour $i \leq 4$ et $p = 2, 3$ d'après la proposition III.4.1.1.

Le cas $p = 5$

On a encore $\mathrm{N}_{25}(\mathrm{L}_i, \mathrm{Leech}) = 0$ pour $i \leq 3$ d'après la proposition III.4.1.1 ; le point (d) du théorème III.4.2.10 donne la valeur de $\mathrm{N}_{25}(\mathrm{L}_4, \mathrm{Leech})$.

Le cas $p = 7$

On adapte la méthode utilisée précédemment pour déterminer $\mathrm{N}_p(\mathrm{L}_i, \mathrm{Leech})$, $i = 1, 2, 3, 4$, dans les cas $7 \leq p \leq 59$.

La proposition III.4.3.1, dont on reprend les notations, doit être modifiée comme suit :

Proposition 8.2.1 *Soient L un réseau de Niemeier avec racines et p un nombre premier qui ne divise pas l'indice de Q dans L ; soit S le stabilisateur, pour l'action de W, d'un élément de $\mathrm{P}_L^{\text{rég}}(\mathbb{Z}/p^2)$.*

(a) *Le groupe S s'identifie à un sous-groupe de $(\mathbb{Z}/p^2)^\times$.*

(b) *Soit S^p l'image de S par l'endomorphisme $x \mapsto x^p$ du groupe $(\mathbb{Z}/p^2)^\times$; l'action de S^p sur R (induite par celle de W) est libre.*

Du coup, le scholie-définition III.4.3.3 doit être modifié comme suit :

Scholie-Définition 8.2.2 *Soient L un réseau de Niemeier avec racines et p un nombre premier ; on note* $\mathrm{pas}(L;p^2)$ *l'entier défini par*

$$\mathrm{pas}(L;p^2) \ := \ \frac{|\mathrm{W}(L)|}{\mathrm{p.g.c.d.}\,(p(p-1)\,,\,24p\mathrm{h}(L)\,,\,|\mathrm{W}(L)|)} \qquad .$$

Si p ne divise pas l'indice de Q dans L, alors $\mathrm{N}_{p^2}(L,\mathrm{Leech})$ *est divisible par* $\mathrm{pas}(L;p^2)$ *; on note dans ce cas* $\mathrm{n}_{p^2}(L)$ *l'entier défini par*

$$\mathrm{N}_{p^2}(L,\mathrm{Leech}) \ = \ \mathrm{n}_{p^2}(L)\ \mathrm{pas}(L;p^2) \qquad .$$

On procède ensuite comme lorsque l'on a déterminé $\mathrm{N}_p(\mathrm{L}_i,\mathrm{Leech})$ pour $i = 1,2,3,4$ et $7 \leq p \leq 59$. *Mutatis mutandis*, on définit des entiers $\mathrm{n}_{p^2}^{\inf}(L)$ et $\mathrm{n}_{p^2}^{\sup}(L)$, "aisément calculables", tels que l'on a l'encadrement

$$\mathrm{n}_{p^2}^{\inf}(L) \ \leq \ \mathrm{n}_{p^2}(L) \ \leq \ \mathrm{n}_{p^2}^{\sup}(L) \qquad .$$

Précisons un peu. Pour obtenir cet encadrement on contemple l'expression (3.6) de T_{p^2} en fonction de T_p et $\mathrm{T}_p^{\psi^2}$ obtenue plus haut, on utilise la détermination de T_p pour $p \leq 113$ et les inégalités de Ramanujan pour les $\tau_{j,k}(p^2)$, à savoir $|\tau_{6,8}(p^2)| \leq 4\,p^{19}$, $|\tau_{8,8}(p^2)| \leq 4\,p^{21}$, $|\tau_{12,6}(p^2)| \leq 4\,p^{21}$ et $|\tau_{4,10}(p^2)| \leq 4\,p^{21}$ (pour des inégalités de Ramanujan plus fines voir (3.8)).

On constate que l'on a $\mathrm{n}_{49}^{\inf}(\mathrm{L}_i) = \mathrm{n}_{49}^{\sup}(\mathrm{L}_i)$ pour $i = 1,2,3,4$; on en déduit la détermination de $\mathrm{N}_{49}(\mathrm{L}_i,\mathrm{Leech})$ pour $i = 1,2,3,4$.

Remarque. On constate que l'on a $\mathrm{n}_9(\mathrm{L}_{16}) = 1$; l'énoncé 8.2.2 est donc, en un certain sens, optimal.

Les cas $11 \leq p \leq 29$

On adapte cette fois la méthode utilisée pour déterminer $\mathrm{N}_p(\mathrm{L}_i,\mathrm{Leech})$, $i = 1,2,3,4$, dans les cas $61 \leq p \leq 107$.

On pose $x_i = \mathrm{n}_{p^2}(\mathrm{L}_i) - \mathrm{n}_{p^2}^{\inf}(\mathrm{L}_i)$; il s'agit à nouveau de déterminer le quadruplet d'entiers naturels (x_1,x_2,x_3,x_4).

On pose $\mathrm{e}_{p^2}(\mathrm{L}_i) := \mathrm{n}_{p^2}^{\sup}(\mathrm{L}_i) - \mathrm{n}_{p^2}^{\inf}(\mathrm{L}_i)$, $1 \leq i \leq 23$, et

$$\underline{\mathrm{e}}_{p^2} \ := \ (\mathrm{e}_{p^2}(\mathrm{L}_1),\mathrm{e}_{p^2}(\mathrm{L}_2),\mathrm{e}_{p^2}(\mathrm{L}_3),\mathrm{e}_{p^2}(\mathrm{L}_4)) \qquad .$$

On a donc, par définition même, les inégalités

$$(1) \qquad x_1 \leq \mathrm{e}_{p^2}(\mathrm{L}_1) \ \ , \ \ x_2 \leq \mathrm{e}_{p^2}(\mathrm{L}_2) \ \ , \ \ x_3 \leq \mathrm{e}_{p^2}(\mathrm{L}_3) \ \ , \ \ x_4 \leq \mathrm{e}_{p^2}(\mathrm{L}_4) \ \ .$$

Le cas $p = 11$

On calcule tout d'abord $\underline{e}_{11^2}$; on trouve $\underline{e}_{11^2} = (1, 1868, 270, 17436)$.

On exprime ensuite les entiers $\tau_{j,k}(11^2)$ en fonction des "inconnues" x_1, x_2, x_3, x_4 ; on trouve (le calcul utilise la détermination que nous avons déjà faite de T_{11}) :

$$\begin{bmatrix} \tau_{6,8}(11^2) \\ \tau_{8,8}(11^2) \\ \tau_{12,6}(11^2) \\ \tau_{4,10}(11^2) \end{bmatrix} = \frac{A}{61} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \frac{B}{61} \quad ,$$

A et B désignant deux matrices explicites à coefficients entiers, respectivement de taille $(4, 4)$ et $(4, 1)$ (l'apparition du nombre premier 61 est due au fait que 61 divise $11^2 + 1$).

On constate que la réduction modulo 61 de la matrice A est inversible ; on peut donc calculer la réduction modulo 61 du quadruplet (x_1, x_2, x_3, x_4), on trouve :

$$(2) \qquad (x_1, x_2, x_3, x_4) \equiv (1, 52, 25, 15) \mod 61$$

(on observera que cette congruence force déjà $x_1 = 1$).

On exprime également les entiers $\mathrm{n}_{11^2}(\mathrm{L}_i)$, $5 \leq i \leq 23$, en fonction de x_1, x_2, x_3, x_4, on trouve :

$$\mathrm{n}_{11^2}(\mathrm{L}_i) = a_{i,1}x_1 + a_{i,2}x_2 + a_{i,3}x_3 + a_{i,4}x_4 + b_i$$

avec $a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4}, b_i$ des nombres rationnels. Cette égalité montre que le quadruplet (x_1, x_2, x_3, x_4) satisfait une certaine congruence affine (éventuellement triviale) modulo le p.p.c.m. des dénominateurs des $a_{i,j}$, $1 \leq j \leq 4$; on note (3) l'ensemble de ces nouvelles congruences.

L'ordinateur dit que les seuls quadruplets vérifiant (1), (2) et (3) sont :

$$(1, 662, 269, 6481) \quad , \quad (1, 1333, 147, 6481) \quad , \quad (1, 1333, 208, 17217) \quad .$$

On constate enfin que le premier et le troisième quadruplet ne passent pas le test de Ramanujan. Les $\tau_{j,k}(11^2)$ sont déterminés.

Méthode alternative

D'après la proposition IX.1.9, le coefficient de t^2 dans le polynôme caractéristique $\mathrm{dét}(t - p^{\frac{\mathrm{w}(\varpi_i)}{2}} \mathrm{c}_p(\varpi_i))$, pour $i = 7, 8, 9, 10$ est respectivement divisible par p^6, p^6, p^4, p^8, c'est-à-dire que l'on a la congruence

$$(3.7) \qquad \tau_{j,k}(p)^2 \equiv \tau_{j,k}(p^2) \mod 2p^{k-2} \quad .$$

On pose $\varepsilon_{j,k}(p) := \frac{\tau_{j,k}(p)^2 - \tau_{j,k}(p^2)}{2}$ et on exprime ces $\varepsilon_{j,k}(p)$ en fonction du quadruplet d'entiers naturels $(x_i)_{1\leq i\leq 4} := (\mathrm{n}_{p^2}(\mathrm{L}_i) - \mathrm{n}^{\inf}_{p^2}(\mathrm{L}_i))$ (on suppose que les $\tau_{j,k}(p)$ sont connus, ce qui est le cas pour les nombres premiers qui nous intéressent ici) ; on obtient une expression de la forme

$$\begin{bmatrix} \varepsilon_{6,8}(p) \\ \varepsilon_{8,8}(p) \\ \varepsilon_{12,6}(p) \\ \varepsilon_{4,10}(p) \end{bmatrix} = \mathrm{E}(p) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \mathrm{H}(p)$$

avec $\mathrm{E}(p)$ et $\mathrm{H}(p)$ deux matrices à coefficients rationnels respectivement de taille $(4,4)$ et $(4,1)$. Le fait que les $\varepsilon_{j,k}(p)$ sont entiers et satisfont les congruences (3.7) impose une contrainte au quadruplet (x_1, x_2, x_3, x_4) que nous notons (2-bis).

Pour $p = 11$, on constate qu'il existe un seul quadruplet qui satisfait les contraintes (1) et (2-bis) à savoir $(1, 1333, 147, 6481)$.

Les cas $p = 13$, $p = 17$ et $p = 19$

On a :

- $\underline{\mathrm{e}}_{13^2} = (655, 121728, 14943, 1135678)$;
- $\underline{\mathrm{e}}_{17^2} = (536541, 5855913, 9346120, 46438144)$;
- $\underline{\mathrm{e}}_{19^2} = (2884703, 84510145, 134879385, 4993470088)$.

On constate à nouveau que dans les trois cas il existe un seul quadruplet (x_1, x_2, x_3, x_4) qui satisfait les contraintes (1) et (2-bis) à savoir :

- $(453, 50943, 3642, 439453)$ pour $p = 13$;
- $(217661, 1571118, 3271290, 261210371)$ pour $p = 17$;
- $(964326, 29790571, 55543719, 3055506804)$ pour $p = 19$.

Le cas $p = 23$

On a $\underline{\mathrm{e}}_{23^2} = (93365728, 753181406, 1202088152, 161617609778)$. Cette fois il existe deux quadruplets qui satisfont (1) et (2-bis). Le seul à passer le test de Ramanujan est $(52157635, 398996852, 418588772, 78467649933)$.

Le cas $p = 29$

On a $\underline{\mathrm{e}}_{29^2} = (1662796593, 308516971151, 492397438725, 2878328193860)$. Il existe 156 quadruplets qui satisfont (1) et (2-bis). Parmi ceux-ci, il n'y en a que 6 qui passent le test de Ramanujan.

Pour effectuer la sélection ultime on procède comme dans le cas $p = 11$, première méthode. On exprime $\mathrm{n}_{29^2}(\mathrm{L}_5)$ en fonction de (x_1, x_2, x_3, x_4) et on

observe que l'intégralité de $\mathrm{n}_{29^2}(\mathrm{L}_5)$ implique que le quadruplet (x_1, x_2, x_3, x_4) satisfait une certaine congruence modulo 256, disons (3). On constate que (3) n'est satisfaite que par un seul des 6 quadruplets ci-dessus à savoir

$$(773950187, 87165709281, 106617389411, 1454026724829)$$

(en fait ce quadruplet est le seul à satisfaire à la fois (1) et (3)).

Remarque. La détermination des $\tau_{j,k}(p^2)$ pour $p \leq 29$ permet d'expliciter l'opérateur de Hecke $\mathrm{T}_{p^2} : \mathbb{Z}[\mathrm{X}_{24}] \to \mathbb{Z}[\mathrm{X}_{24}]$ pour $p \leq 29$. On trouve par exemple

$$\mathrm{N}_{29^2}(\mathrm{E}_{24}, \mathrm{L}_{21}) \;=\; 97878474318706056157360008133508687530518943031243877384192000 00$$

(approximativement 0.98×10^{64}, record battu !).

Le cas $p = 31$

La méthode que nous avons employée pour $11 \leq p \leq 29$ est en échec pour $p = 31$. Nous expliquons pourquoi ci-après (en petits caractères).

Cette méthode peut être décrite de la façon suivante. On pose $\mathrm{n}_{p^2}(\mathrm{L}_i) = \mathrm{n}_{p^2}^{\mathrm{inf}}(\mathrm{L}_i) + x_i$, avec $x_i \in \mathbb{Z}$, pour $i = 1, 2, 3, 4$; on pose $\underline{x} = (x_1, x_2, x_3, x_4)$, $\underline{x}$ est donc *a priori* un élément de $\mathbb{Z}^4 \subset \mathbb{R}^4$.

Les inégalités de Ramanujan vérifiées par les $\tau_{j,k}(p^2)$ disent que $\underline{x}$ appartient à un parallélotope, disons Par_p, de l'espace affine $\mathbb{R}^4$; la définition des entiers $\mathrm{n}_{p^2}^{\mathrm{inf}}(\mathrm{L}_i)$ et $\mathrm{n}_{p^2}^{\mathrm{sup}}(\mathrm{L}_i)$ est telle que la condition $\underline{x} \in \mathrm{Par}_p$ implique l'encadrement $0 \leq x_i \leq \mathrm{e}_{p^2}(\mathrm{L}_i)$. Le fait que les $\varepsilon_{j,k}(p)$ sont des entiers, que ces entiers vérifient les congruences (3.7) et enfin que les $\mathrm{n}_{p^2}(\mathrm{L}_i)$ sont des entiers pour $5 \leq i \leq 23$ (ces $\mathrm{n}_{p^2}(\mathrm{L}_i)$ s'expriment comme des fonctions affines de $\underline{x}$ à coefficients rationnels) font que $\underline{x}$ appartient à un translaté, disons Γ_p^{aff}, d'un réseau, disons Γ_p, de l'espace vectoriel $\mathbb{R}^4$, contenant $\mathbb{Z}^4$.

On considère le quotient

$$\phi(p) \;:=\; \frac{\mathrm{volume}\,(\mathrm{Par}_p)}{\mathrm{covolume}\,(\Gamma_p)}$$

(volume et covolume pour la mesure de Lebesgue). La différence essentielle entre les cas $p = 29$ et $p = 31$ est la suivante : on a $\phi(29) \approx 0.02409$ et $\phi(31) \approx 31918.2436$. Dans le premier cas nous avons pu montrer que l'intersection $\Gamma_{29}^{\mathrm{aff}} \cap \mathrm{Par}_{29}$ contient un seul point et déterminer ce point. Dans le second, le calcul de $\phi(31)$ indique, heuristiquement, que le nombre de points de $\Gamma_{31}^{\mathrm{aff}} \cap \mathrm{Par}_{31}$ est de l'ordre 32000 ; en fait ce nombre de points est 31995.

Le lecteur diligent objectera que nous avons été un peu paresseux en ce qui concerne les inégalités de Ramanujan. En effet, nous avons simplement utilisé le fait que, pour $7 \leq r \leq 10$, $\theta_r(p^2)$ est somme de quatre nombres complexes de module $p^{\mathrm{w}(\varpi_r)}$ (on rappelle

que $\theta_7, \theta_8, \theta_9, \theta_{10}$ est une notation alternative pour $\tau_{6,8}, \tau_{8,8}, \tau_{12,6}, \tau_{4,10}$). Or nous connaissons ici les $\theta_r(p)$, $7 \leq r \leq 10$; le fait que les racines dans $\mathbb{C}$ du polynôme caractéristique $\text{dét}(t - p^{\frac{\mathrm{w}(\varpi_r)}{2}}\, \mathrm{c}_p(\varpi_r))$ sont de module $p^{\frac{\mathrm{w}(\varpi_r)}{2}}$ équivaut aux inégalités

$$(3.8) \qquad -4\, p^{\mathrm{w}(\varpi_r)} + \frac{\theta_r(p)^2}{2} \;\leq\; \theta_r(p^2) \;\leq\; (2\, p^{\frac{\mathrm{w}(\varpi_r)}{2}} - |\theta_r(p)|)^2 \qquad .$$

Ces inégalités montrent que le point $\underline{x}$ appartient à un parallélotope, disons $\mathrm{Par}_p^{\mathrm{slim}}$, contenu dans Par_p. On a

$$\frac{\text{volume}\,(\mathrm{Par}_p^{\mathrm{slim}})}{\text{volume}\,(\mathrm{Par}_p)} \;=\; \prod_{r=7}^{10} \left(1 - \frac{|\theta_r(p)|}{4p^{\frac{\mathrm{w}(\varpi_r)}{2}}}\right)^2 \qquad .$$

Pour $p = 31$, ce rapport est approximativement 0.2115 et le cardinal de $\Gamma_{31}^{\mathrm{aff}} \cap \mathrm{Par}_{31}^{\mathrm{slim}}$ est 6735.

4. Congruences à la Harder

Ce paragraphe se compose de trois parties.

Dans la première, très élémentaire, on exploite l'observation suivante : le seul fait que les endomorphismes T_p de $\mathbb{Z}[\mathrm{X}_{24}]$, p premier, aient (après extension des scalaires à $\mathbb{Q}$) une base de vecteurs propres commune, à savoir celle de T_2, entraîne que les $\lambda_j(p)$ vérifient de nombreuses congruences. On obtient par exemple la congruence suivante :

$$(p+1)\;(\tau_{4,10}(p) - \tau_{22}(p) - p^{13} - p^8) \;\equiv\; 0 \mod 41 \qquad .$$

Dans la deuxième partie, plus subtile, "on divise par $p+1$" certaines des congruences obtenues dans la première en faisant notamment appel à la théorie des représentations galoisiennes. On démontre par exemple que l'on a la congruence

$$\tau_{4,10}(p) \;\equiv\; \tau_{22}(p) + p^{13} + p^8 \mod 41$$

conjecturée par Günter Harder [Har08]. Dans la troisième partie on analyse la forme que peut prendre *a priori* une décomposition en irréductibles de la représentation ℓ-adique résiduelle associée à un $\tau_{j,k}$. On déduit de cette analyse, et des calculs que l'on a faits au paragraphe 3, que certaines d'entre elles sont irréductibles ce qui explique pourquoi les $\tau_{j,k}$ correspondants n'apparaissent pas dans les congruences dégagées dans la deuxième partie.

Sur certaines congruences vérifiées par les $\lambda_j(p)$

On contemple à nouveau la formule (2.2) :

$$\mathrm{T}_p \;=\; \mathrm{V}\ \mathrm{diag}(\lambda_1(p), \lambda_2(p), \ldots, \lambda_{24}(p))\ \mathrm{V}^{-1} \qquad .$$

La matrice V ci-dessus est à coefficients entiers mais ce n'est pas le cas de la matrice V^{-1}. En effet `PARI` nous dit que l'on a

$$\begin{aligned} |\,\text{dét}\,\mathrm{V}| \;=\; & 2^{220}\,.\,3^{85}\,.\,5^{35}\,.\,7^{23}\,.\,11^{9}\,.\,13^{10}\,.\,17^{3}\,.\,19^{2}\,.\,23^{2}\,. \\ & 41\,.\,131\,.\,283^{2}\,.\,593\,.\,617^{2}\,.\,691^{10}\,.\,3617^{4}\,.\,43867^{3} \quad ; \end{aligned}$$

`PARI` nous dit également que le plus petit des entiers $d > 0$ tels que $d\,\mathrm{V}^{-1}$ est à coefficients entiers est

$$\begin{aligned} \mathrm{D} \;:=\; & 2^{21}\,.\,3^{10}\,.\,5^{5}\,.\,7^{2}\,.\,11^{3}\,.\,13^{2}\,.\,17\,.\,19\,.\,23^{2}\,. \\ & 41\,.\,131\,.\,283\,.\,593\,.\,617\,.\,691^{2}\,.\,3617\,.\,43867 \qquad . \end{aligned}$$

On voit donc que pour que la matrice T_p soit à coefficient entiers, il faut que de nombreuses congruences modulo des diviseurs de D, impliquant les valeurs propres $\lambda_j(p)$, soient vérifiées. La matrice V en main (merci Nebe-Venkov), l'obtention de ces congruences ne fait intervenir que la théorie des modules sur les anneaux principaux. L'expression (2.1) des $\lambda_j(p)$ en fonction de $\tau_{12}(p)$, $\tau_{16}(p)$, $\tau_{18}(p)$, $\tau_{20}(p)$, $\tau_{22}(p)$, $\tau_{6,8}(p)$, $\tau_{8,8}(p)$, $\tau_{12,6}(p)$ et $\tau_{4,10}(p)$ donne alors des congruences concernant ces fonctions arithmétiques.

La théorie des modules sur les anneaux principaux nous dit qu'il existe deux matrices R et S de $\mathrm{GL}_{24}(\mathbb{Z})$, et des entiers strictement positifs, $\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_{24}$, avec d_j divisant d_i pour $j > i$, tels que l'on a

$$\mathrm{V} \;=\; \mathrm{R}\ \mathrm{diag}(\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_{24})\ \mathrm{S}^{-1}$$

(on observera que l'on a $\mathrm{d}_1 = \mathrm{D}$ et $\prod_i \mathrm{d}_i = |\,\text{dét}\,\mathrm{V}|$).

Les deux conditions suivantes sont équivalentes :

– La matrice $\mathrm{V}\,\mathrm{diag}(\lambda_1(p), \lambda_2(p), \ldots, \lambda_{24}(p))\,\mathrm{V}^{-1}$ est à coefficient entiers.

– La matrice

$$\mathrm{diag}(\mathrm{d}_1, \ldots, \mathrm{d}_{24})\,\mathrm{S}^{-1}\,\mathrm{diag}(\lambda_1(p), \lambda_2(p), \ldots, \lambda_{24}(p))\,\mathrm{S}\,\mathrm{diag}(\mathrm{d}_1^{-1}, \ldots, \mathrm{d}_{24}^{-1})$$

est à coefficient entiers.

Soit k un entier avec $1 \leq k \leq 24$; on pose

$$\mathrm{E}_k \;:=\; \mathrm{S}^{-1}\,\mathrm{diag}(\delta_{k,1}, \delta_{k,2}, \ldots, \delta_{k,24})\,\mathrm{S}$$

($\delta_{-,-}$ est le symbole de Kronecker) et on note $\mathrm{e}_{i,j,k}$ le coefficient d'indice (i, j) de la matrice E_k (les $\mathrm{e}_{i,j,k}$ sont des entiers "universels", déterminés par V et un choix du couple (R, S)). La seconde condition ci-dessus est encore équivalente à la suivante :

– Pour tout couple (i,j) avec $i > j$ on a la congruence

$$\sum_{k=1}^{24} \mathrm{e}_{i,j,k}\, \lambda_k(p) \;\equiv\; 0 \mod \frac{\mathrm{d}_j}{\mathrm{d}_i} \qquad . \tag{4.1}$$

Conceptualisons un peu ce qui précède.

On observe tout d'abord que la seule propriété de T_p que nous ayons utilisée ci-dessus est que les v_j, $1 \leq j \leq 24$, sont tous des vecteurs propres de T_p. Soient U un endomorphisme de $\mathbb{Z}[\mathrm{X}_{24}]$ vérifiant cette propriété et $\lambda_j(U)$, $1 \leq j \leq 24$, l'entier défini par l'égalité $U(\mathrm{v}_j) = \lambda_j(U)\,\mathrm{v}_j$; alors pour tout couple (i,j) avec $i > j$ on a la congruence

$$\sum_{k=1}^{24} \mathrm{e}_{i,j,k}\, \lambda_k(U) \;\equiv\; 0 \mod \frac{\mathrm{d}_j}{\mathrm{d}_i} \qquad . \tag{4.2}$$

On note C le sous-anneau de $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{X}_{24}])$ constitué des endomorphismes U considérés ci-dessus ; les applications $\lambda_j : \mathrm{C} \to \mathbb{Z}\,,\, U \mapsto \lambda_j(U)$ sont des homomorphismes d'anneaux dont le produit, disons $\underline{\lambda}$,

$$\mathrm{C} \to \mathbb{Z}^{24} \qquad , \qquad U \mapsto (\lambda_1(U), \lambda_2(U), \ldots, \lambda_{24}(U))$$

est un homomorphisme d'anneaux injectif (ce qui montre en particulier que l'anneau C est commutatif). L'image de $\underline{\lambda}$ est le sous-anneau de $\mathbb{Z}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant

$$\sum_{k=1}^{24} \mathrm{e}_{i,j,k}\, x_k \;\equiv\; 0 \mod \frac{\mathrm{d}_j}{\mathrm{d}_i}$$

pour tout couple (i,j) avec $i > j$.

Remarques

1) Puisque les coefficients de V sont premiers entre eux on a $\mathrm{d}_{24} = 1$ (en fait on a $\mathrm{d}_j = 1$ pour $j \geq 21$).

2) Posons $\underline{\mathrm{d}} := (\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_{24})$ et notons $\Gamma(\underline{\mathrm{d}})$ le sous-groupe de $\mathrm{GL}_{24}(\mathbb{Z})$ intersection dans $\mathrm{GL}_{24}(\mathbb{Q})$ de $\mathrm{GL}_{24}(\mathbb{Z})$ et $\mathrm{diag}(\underline{\mathrm{d}})\,\mathrm{GL}_{24}(\mathbb{Z})\,\mathrm{diag}(\underline{\mathrm{d}})^{-1}$. On constate que la classe de S dans l'ensemble fini $\mathrm{GL}_{24}(\mathbb{Z})/\Gamma(\underline{\mathrm{d}})$ ne dépend que de V et que l'on peut définir le sous-anneau C de $\mathbb{Z}^{24}$ en termes du 24-uple $\underline{\mathrm{d}}$ et de cette classe.

3) Soit ℓ un nombre premier, alors les homomorphismes d'anneaux $\mathrm{C} \to \mathbb{Z}/\ell$, considérés comme des éléments du $\mathbb{Z}/\ell$-espace vectoriel $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{C}, \mathbb{Z}/\ell)$, sont linéairement indépendants ("indépendance des caractères"). Si la valuation ℓ-adique de D est 1, en clair si ℓ appartient à la liste

$$\{17, 19, 41, 131, 283, 593, 617, 3617, 43867\} \qquad ,$$

alors $\mathbb{Z}_{(\ell)} \otimes_{\mathbb{Z}} \operatorname{coker} \underline{\lambda}$ est annulé par la multiplication par ℓ. L'observation précédente montre dans ce cas qu'il existe une relation d'équivalence sur $\{1, 2, \ldots, 24\}$, disons $\mathcal{R}_\ell$, uniquement déterminée, telle que $\mathbb{Z}_{(\ell)} \otimes_{\mathbb{Z}} \mathrm{C}$ est le sous-anneau de $\mathbb{Z}_{(\ell)}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant les congruences $x_i \equiv x_j \bmod \ell$ pour $i \mathcal{R}_\ell j$. Nous verrons par exemple ci-après que $\mathbb{Z}_{(41)} \otimes_{\mathbb{Z}} \mathrm{C}$ est le sous-anneau de $\mathbb{Z}_{(41)}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant $x_{18} \equiv x_{21} \bmod 41$.

On peut déterminer en toute généralité la classe d'isomorphisme du $(\mathbb{Z}/\mathrm{D})$-module $\operatorname{coker} \underline{\lambda}$ à l'aide des "routines" d'algèbre linéaire de `PARI` (`mathnf`, `mathnfmod` et `matsnf`). On a effectué le calcul en considérant C comme le sous-module de $\mathbb{Z}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ tels que la matrice $\sum_j x_j \mathrm{Proj}_j$ est à coefficients entiers (la notation Proj_j est introduite dans la démonstration de 2.2). On donne le résultat ci-après :

Proposition 4.1. *Soit ℓ un nombre premier qui divise* D*, en clair un élément de la liste*

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 41, 131, 283, 593, 617, 691, 3617, 43867\} \qquad ;$$

on a des isomorphismes de la forme

$$\mathbb{Z}_{(\ell)} \otimes_{\mathbb{Z}} \operatorname{coker}(\underline{\lambda} : \mathrm{C} \to \mathbb{Z}^{24}) \ \simeq \ \mathbb{Z}/\ell^{\mathrm{e}_{\ell,1}} \times \mathbb{Z}/\ell^{\mathrm{e}_{\ell,1}} \times \ldots \times \mathbb{Z}/\ell^{\mathrm{e}_{\ell,\mathrm{r}_\ell}} \qquad ,$$

$\mathrm{e}_\ell := (\mathrm{e}_{\ell,1}, \mathrm{e}_{\ell,2}, \ldots, \mathrm{e}_{\ell,\mathrm{r}_\ell})$ *désignant la suite finie décroissante d'entiers naturels non nuls explicitée ci-dessous :*

- $\mathrm{e}_2 = (21, 19, 17, 17, 15, 15, 14, 14, 12, 12, 11, 10, 9, 9, 9, 8, 8, 7, 6, 6, 3, 1)$ *;*
- $\mathrm{e}_3 = (10, 9, 9, 7, 7, 6, 5, 5, 5, 5, 5, 5, 5, 5, 4, 4, 4, 3, 3, 3, 2, 1)$ *;*
- $\mathrm{e}_5 = (5, 5, 3, 3, 3, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1)$ *;*
- $\mathrm{e}_7 = (2, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$ *;*
- $\mathrm{e}_{11} = (3, 2, 1, 1, 1, 1, 1)$ *;*
- $\mathrm{e}_{13} = (2, 2, 1, 1, 1, 1, 1, 1, 1)$ *;*
- $\mathrm{e}_{17} = (1, 1, 1)$ *;*

– $\mathrm{e}_{19} = (1,1)$;
– $\mathrm{e}_{23} = (2)$;
– $\mathrm{e}_{41} = (1)$;
– $\mathrm{e}_{131} = (1)$;
– $\mathrm{e}_{283} = (1,1)$;
– $\mathrm{e}_{593} = (1)$;
– $\mathrm{e}_{617} = (1,1)$;
– $\mathrm{e}_{691} = (2,1,1,1,1,1,1,1,1)$;
– $\mathrm{e}_{3617} = (1,1,1,1)$;
– $\mathrm{e}_{43867} = (1,1,1)$.

On décrit maintenant deux généralisations des congruences (4.2) (et (4.1)).

1) Les congruences (4.2) font, *a priori*, intervenir simultanément les 24 valeurs propres $\lambda_j(U)$. Soit J un sous-ensemble arbitraire de $\{1,2,\ldots,24\}$; nous décrivons ci-après un algorithme à celui qui conduit à (4.2) pour obtenir des congruences faisant intervenir seulement les $\lambda_j(U)$ avec j dans J.

On note respectivement M_J et L_J, le sous-module de $\mathbb{Z}[\mathrm{X}_{24}]$ engendré par les v_j avec $j \in J$ et l'intersection dans $\mathbb{Q}[\mathrm{X}_{24}]$ de $\mathbb{Q}\otimes_{\mathbb{Z}}\mathrm{M}_J$ et $\mathbb{Z}[\mathrm{X}_{24}]$. Toujours d'après la théorie des modules sur les anneaux principaux, il existe :
– une $J\times J$ matrice $\mathrm{S}_J = [\mathrm{s}_{J,i,j}]_{(i,j)\in J\times J}$, à coefficients entiers, inversible avec S_J^{-1} également à coefficients entiers,
– des entiers strictement positifs $\mathrm{d}_{J,i}$, $i \in J$, avec $\mathrm{d}_{J,j}$ divisant $\mathrm{d}_{J,i}$ pour $i < j$, tels que l'ensemble

$$\{\, \frac{1}{d_{J,j}} \sum_{i\in J} \mathrm{s}_{J,i,j}\, \mathrm{v}_i \,\}_{j\in J}$$

est une base de L_J (si bien que le quotient $\mathrm{L}_J/\mathrm{M}_J$ est isomorphe à la somme directe $\bigoplus_{j\in J}\mathbb{Z}/\mathrm{d}_{J,j}$).

Soit (i,j,k) un élément de $J\times J\times J$; on note $\mathrm{e}_{J,i,j,k}$ le coefficient d'indice (i,j) de la matrice $\mathrm{S}_J^{-1}\,\mathrm{diag}((\delta_{k,i})_{i\in J})\,\mathrm{S}_J$. Pour tout couple (i,j) avec $i > j$ on a la congruence

$$\sum_{k\in J} \mathrm{e}_{J,i,j,k}\,\lambda_k(U) \;\equiv\; 0 \mod \frac{\mathrm{d}_{J,j}}{\mathrm{d}_{J,i}} \tag{4.3}$$

(on observera que la somme $\sum_{k\in J}\mathrm{e}_{J,i,j,k}$ est nulle).

2) Soit m un diviseur de D ; on note $\mathbb{Z}_{(m)}$ le localisé de $\mathbb{Z}$ obtenu en inversant les éléments premiers à m. On obtient des congruences modulo des diviseurs

d'une puissance de m (et de D) en remplaçant dans le point 1 ci-dessus l'anneau principal $\mathbb{Z}$ par l'anneau principal $\mathbb{Z}_{(m)}$.

On considère enfin un cas particulier de ce qui précède.

On note $\mathcal{V}$ l'ensemble $\{\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_{24}\}$. Soit $\mathcal{W}$ un sous-ensemble de $\mathcal{V}$; on note $\mathrm{J}(\mathcal{W})$ le sous-ensemble de $\{1, 2, \ldots, 24\}$ constitué des j avec $\mathrm{v}_j \in \mathcal{W}$.

Soient m un diviseur de D et $\rho_m : \mathbb{Z}[\mathrm{X}_{24}] \to (\mathbb{Z}/m)[\mathrm{X}_{24}]$ l'homomorphisme de réduction modulo m. Soit $\mathcal{W}$ un sous-ensemble de $\mathcal{V}$. Supposons tout d'abord m premier. Si le système de vecteurs $\rho_m(\mathcal{W})$ est lié et si $\mathcal{W}$ est minimal parmi les sous-ensembles de $\mathcal{V}$ avec cette propriété alors, pour tout v dans $\mathcal{W}$, $\rho_m(\mathcal{W} - \{v\})$ est une base du sous-espace vectoriel engendré par $\rho_m(\mathcal{W})$. Supposons maintenant que m est un diviseur quelconque de D, nous dirons plus généralement que $\mathcal{W}$ est *m-lié minimal* si le sous-module de $(\mathbb{Z}/m)[\mathrm{X}_{24}]$ engendré par $\rho_m(\mathcal{W})$ est un $(\mathbb{Z}/m)$-module libre et si $\rho_m(\mathcal{W} - \{v\})$ en est une base pour tout v dans $\mathcal{W}$. Si $\mathcal{W}$ est m-lié minimal alors le $\mathbb{Z}_{(m)}$-module $\mathbb{Z}_{(m)} \otimes_{\mathbb{Z}} (\mathrm{L}_{\mathrm{J}(\mathcal{W})}/\mathrm{M}_{\mathrm{J}(\mathcal{W})})$ est isomorphe à $\mathbb{Z}/\widetilde{m}$ avec $\widetilde{m}$ un multiple de m qui divise une puissance de m. Le point 2 ci-dessus fournit des congruences modulo $\widetilde{m}$ et *a fortiori* modulo m :

Proposition 4.2. *Soit U un endomorphisme de $\mathbb{Z}[\mathrm{X}_{24}]$ qui admet les v_j, $1 \leq j \leq 24$, pour vecteurs propres. Soient m un diviseur de D et $\mathcal{W}$ un sous-ensemble m-lié minimal de $\mathcal{V}$. Alors on a les congruences*

$$\lambda_i(U) \equiv \lambda_j(U) \mod m$$

pour tous i et j dans $\mathrm{J}(\mathcal{W})$.

Pour le confort du lecteur nous donnons une démonstration *ab initio* de l'énoncé ci-dessus :

Démonstration. Par définition, on dispose d'une relation de dépendance de la forme $\sum_{v \in \mathcal{W}} \mu_v \, \rho_m(v) = 0$ avec $\mu_v \in (\mathbb{Z}/m)^\times$ et si $\sum_{v \in \mathcal{W}} \mu'_v \, \rho_m(v) = 0$ est une autre relation de dépendance alors on a $\frac{\mu'_v}{\mu_v} = \frac{\mu'_w}{\mu_w}$ pour tous v et w dans $\mathcal{W}$. La proposition en résulte. $\square$

Il est clair que le cardinal d'un sous-ensemble m-lié minimal de $\mathcal{V}$ est supérieur ou égal à 2. La proposition suivante, que l'on vérifie par inspection, dit que l'on a souvent l'égalité, au moins si m est premier.

Proposition 4.3. *Soient ℓ un diviseur premier de D différent de $3, 5, 7, 11$ et $\mathcal{W}$ un sous-ensemble ℓ-lié minimal de $\mathcal{V}$. Alors le cardinal de $\mathcal{W}$ est 2.*

Remarque. Soit $\mathrm{P}_{\mathrm{X}_{24}}$ le $\mathbb{Z}$-schéma dont les A-points (A anneau commutatif unitaire) sont les facteurs directs de rang 1 de $A[\mathrm{X}_{24}]$ ($\mathrm{P}_{\mathrm{X}_{24}}$ est donc un avatar de l'espace projectif P^{23}). On dispose d'un sous-ensemble canonique de $\mathrm{P}_{\mathrm{X}_{24}}(\mathbb{Q}) = \mathrm{P}_{\mathrm{X}_{24}}(\mathbb{Z})$, à savoir l'ensemble des classes des v_j ; on le note $[\mathcal{V}]$. La proposition ci-dessus dit que cet ensemble à 24 éléments est très loin d'être "générique". En effet, elle montre que pour les ℓ qui apparaissent dans son énoncé, les points de $\rho_\ell([\mathcal{V}])$ sont "projectivement indépendants".

Exemples

Le cas $m = 43867$

Les sous-ensembles m-liés minimaux de $\mathcal{V}$ sont $\{\mathrm{v}_1, \mathrm{v}_{11}\}$, $\{\mathrm{v}_2, \mathrm{v}_8\}$ et $\{\mathrm{v}_3, \mathrm{v}_6\}$. En prenant $U = \mathrm{T}_p$, p premier, dans la proposition 4.2 on obtient les congruences modulo 43867 :

$$\lambda_1(p) \equiv \lambda_{11}(p) \quad , \quad \lambda_2(p) \equiv \lambda_8(p) \quad , \quad \lambda_3(p) \equiv \lambda_6(p) \quad . \tag{4.4}$$

On on constate que l'on a

– $\lambda_{11}(p) - \lambda_1(p) = (p^5 + p^4 + p^3 + p^2 + p + 1)\ (\tau_{18}(p) - p^{17} - 1)$,

– $\lambda_8(p) - \lambda_2(p) = (p^4 + p^3 + p^2 + p)\ (\tau_{18}(p) - p^{17} - 1)$,

– $\lambda_6(p) - \lambda_3(p) = (p^3 + p^2)\ (\tau_{18}(p) - p^{17} - 1)$.

Comme le p.g.c.d. des polynômes $X^5+X^4+X^3+X^2+X+1$, $X^4+X^3+X^2+X$ et $X^3 + X^2$ est $X + 1$, on voit que (4.4) implique la congruence

$$(p + 1)\ (\tau_{18}(p) - p^{17} - 1) \equiv 0 \mod 43867 \quad . \tag{4.5}$$

Cette congruence est plus faible que la congruence bien connue (voir par exemple [Sw72])

$$\tau_{18}(p) - p^{17} - 1 \equiv 0 \mod 43867 \tag{4.6}$$

(on notera quand même que (4.5) implique (4.6) pour $p \not\equiv -1 \bmod 43867$!). Nous expliquerons cependant, au cours de la démonstration du théorème 4.4, comment l'intervention de la théorie des représentations galoisiennes et une version plus élaborée de la proposition 4.2 (Proposition 4.5) permettent d'obtenir (4.6) (ce qui fournit une démonstration bien compliquée de cette congruence !).

Remarque. La proposition 4.1 dit que l'on a $\mathbb{Z}_{(43867)} \otimes_{\mathbb{Z}} \operatorname{coker} \underline{\lambda} \approx (\mathbb{Z}/43867)^3$; ce qui précède montre en fait que $\mathbb{Z}_{(43867)} \otimes_{\mathbb{Z}} \mathrm{C}$ est le sous-anneau de $\mathbb{Z}_{(43867)}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant $x_1 \equiv x_{11}$, $x_2 \equiv x_8$ et $x_3 \equiv x_6$ modulo 43867.

Le cas $m = 3617$

Les sous-ensembles m-liés minimaux de $\mathcal{V}$ sont $\{\mathrm{v}_1, \mathrm{v}_{13}\}$, $\{\mathrm{v}_2, \mathrm{v}_{12}\}$, $\{\mathrm{v}_3, \mathrm{v}_9\}$ et $\{\mathrm{v}_4, \mathrm{v}_7\}$. On obtient cette fois les congruences modulo 3617 :

$$\lambda_1(p) \equiv \lambda_{13}(p) \ , \ \lambda_2(p) \equiv \lambda_{12}(p) \ , \ \lambda_3(p) \equiv \lambda_9(p) \ , \ \lambda_4(p) \equiv \lambda_7(p) \ .$$

Comme précédemment, on constate que les congruences ci-dessus impliquent la congruence

$$(p+1)\ (\tau_{16}(p) - p^{15} - 1) \ \equiv \ 0 \mod 3617 \qquad .$$

Le cas $m = 691$

Les sous-ensembles m-liés minimaux sont de cardinal 2 et au nombre de 12. La considération des deux ensembles m-liés minimaux $\{\mathrm{v}_1, \mathrm{v}_{24}\}$ et $\{\mathrm{v}_2, \mathrm{v}_{23}\}$ conduit à la congruence

$$(p+1)\ (\tau_{12}(p) - p^{11} - 1) \ \equiv \ 0 \mod 691 \qquad .$$

Le cas $m = 283.617$

Les sous-ensembles m-liés minimaux sont $\{\mathrm{v}_1, \mathrm{v}_5\}$ et $\{\mathrm{v}_2, \mathrm{v}_4\}$. On obtient cette fois la congruence

$$(p+1)\ (\tau_{20}(p) - p^{19} - 1) \ \equiv \ 0 \mod 283.617 \qquad .$$

Le cas $m = 131.593$

Le seul sous-ensemble m-lié minimal est dans ce cas $\{\mathrm{v}_1, \mathrm{v}_3\}$. Comme l'on a l'égalité $\lambda_3(p) - \lambda_1(p) = (p+1)(\tau_{22}(p) - p^{21} - 1)$, on obtient la congruence

$$(p+1)\ (\tau_{22}(p) - p^{21} - 1) \ \equiv \ 0 \mod 131.593 \qquad .$$

Le cas $m = 41$

Le seul sous-ensemble m-lié minimal est $\{\mathrm{v}_{18}, \mathrm{v}_{21}\}$. Comme l'on a l'égalité $\lambda_{21}(p) - \lambda_{18}(p) = (p+1)(\tau_{4,10}(p) - \tau_{22}(p) - p^{13} - p^8)$, on obtient la congruence

$$(p+1)\ (\tau_{4,10}(p) - \tau_{22}(p) - p^{13} - p^8) \ \equiv \ 0 \mod 41 \qquad . \tag{4.7}$$

Comme nous l'avons déjà dit, nous verrons que la théorie des représentations galoisiennes permet de montrer que l'on a en fait

$$\tau_{4,10}(p) - \tau_{22}(p) - p^{13} - p^8 \ \equiv \ 0 \mod 41 \qquad , \tag{4.8}$$

congruence conjecturée par G. Harder [Har08].

Le sous-ensemble $\{\mathrm{v}_{18}, \mathrm{v}_{21}\}$ est m-lié minimal pour $m = 2^4.3.41$ si bien que la congruence (4.7) se raffine en

$$(p+1)\ (\tau_{4,10}(p) - \tau_{22}(p) - p^{13} - p^8)\ \equiv\ 0 \mod 2^4.3.41 \qquad .$$

Remarque. Compte tenu de la proposition 4.1, ce qui précède montre que $\mathbb{Z}_{(41)} \otimes_{\mathbb{Z}} \mathrm{C}$ est le sous-anneau de $\mathbb{Z}_{(41)}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant $x_{18} \equiv x_{21} \bmod 41$.

Le cas $m = 23$

Le seul sous-ensemble m-lié minimal est $\{\mathrm{v}_{13}, \mathrm{v}_{15}\}$; en fait $\{\mathrm{v}_{13}, \mathrm{v}_{15}\}$ est $\widetilde{m}$-lié minimal avec $\widetilde{m} = 23^2$. On obtient cette fois la congruence

$$(p+1)\ (\,\tau_{8,8}(p) - (p^6+1)\tau_{16}(p)\,)\ \equiv\ 0 \mod 23^2 \qquad . \tag{4.9}$$

Là encore nous verrons plus tard que l'on a en fait

$$\tau_{8,8}(p) - (p^6+1)\tau_{16}(p)\ \equiv\ 0 \mod 23^2 \qquad .$$

Par le même argument que précédemment, la congruence (4.9) se raffine en

$$(p+1)\ (\,\tau_{8,8}(p) - (p^6+1)\tau_{16}(p)\,)\ \equiv\ 0 \mod 2^3.3^2.23^2 \qquad .$$

Remarque. Compte tenu de la proposition 4.1, ce qui précède montre que $\mathbb{Z}_{(23)} \otimes_{\mathbb{Z}} \mathrm{C}$ est le sous-anneau de $\mathbb{Z}_{(23)}^{24}$ constitué des 24-uples $(x_1, x_2, \ldots, x_{24})$ vérifiant $x_{13} \equiv x_{15} \bmod 23^2$.

Le cas $m = 19$

Les sous-ensembles m-liés minimaux sont $\{\mathrm{v}_9, \mathrm{v}_{10}\}$ et $\{\mathrm{v}_{21}, \mathrm{v}_{22}\}$.

La considération de $\{\mathrm{v}_9, \mathrm{v}_{10}\}$ donne

$$(p+1)\ (\,\tau_{12,6}(p) - (p^4+p^2)\tau_{16}(p) + p^2\tau_{18}(p) - \tau_{22}(p)\,) \equiv 0 \mod 19 \quad . \tag{4.10}$$

Comme $\{\mathrm{v}_9, \mathrm{v}_{10}\}$ est m-lié minimal pour $m = 2^4.19$ on a aussi

$$(p+1)\ (\,\tau_{12,6}(p) - (p^4+p^2)\tau_{16}(p) + p^2\tau_{18}(p) - \tau_{22}(p)\,) \equiv 0 \mod 2^4.19\ .$$

La considération de $\{\mathrm{v}_{21}, \mathrm{v}_{22}\}$ donne

$$(p+1)\ (\,\tau_{4,10}(p) - (p^8+p^2)\tau_{12}(p) + p^2\tau_{18}(p) - \tau_{22}(p)\,) \equiv 0 \mod 19 \quad .$$

Comme $\{v_{21}, v_{22}\}$ est m-lié minimal pour $m = 2^4.3^2.19$ on a aussi

$$(p+1)\ (\tau_{4,10}(p) - (p^8+p^2)\tau_{12}(p) + p^2\tau_{18}(p) - \tau_{22}(p)\ ) \equiv 0 \bmod 2^4.3^2.19\ .$$

Le cas $m = 17$

Les sous-ensembles m-liés minimaux sont $\{v_5, v_9\}$, $\{v_{15}, v_{17}\}$ et$\{v_{19}, v_{20}\}$. Les congruences associées respectivement à ces paires sont :

$$(4.11)\quad (p+1)((p^4+p^2)\tau_{16}(p)-(p^2+1)\tau_{20}(p)+\tau_{22}(p)-p^{17}-p^4) \equiv 0 \mod 17\ ;$$

(4.12)
$$(p+1)(\tau_{8,8}(p)-(p^6+p^4)\tau_{12}(p)+(p^4+p^2)\tau_{16}(p)-(p^2+1)\tau_{20}(p)) \equiv 0 \bmod 17\ ;$$

$$(4.13)\quad (p+1)(\tau_{6,8}(p) - (p^6+p^2)\tau_{12}(p) + p^2\tau_{16}(p) - \tau_{20}(p)) \equiv 0 \mod 17\ .$$

Le cas $m = 13$

Les sous-ensembles m-liés minimaux sont de cardinal 2 et au nombre de 12. La considération des ensembles m-liés minimaux $\{v_6, v_{10}\}$, $\{v_9, v_{15}\}$, $\{v_{10}, v_{11}\}$, $\{v_{15}, v_{17}\}$ et $\{v_{15}, v_{18}\}$ conduit respectivement aux congruences suivantes :

$$(4.14)\qquad (p+1)(\tau_{12,6}(p) - \tau_{22}(p) - p^{17} - p^4) \equiv 0 \mod 13\ ;$$

$$(4.15)\qquad (p+1)(\tau_{8,8}(p) - \tau_{22}(p) - p^{15} - p^6) \equiv 0 \mod 13\ ;$$

$$(4.16)\qquad (p+1)(\tau_{12,6}(p) - (p^4+1)\tau_{18}(p)) \equiv 0 \mod 13\ ;$$

$$(p+1)(\tau_{8,8}(p)-(p^6+p^4)\tau_{12}(p)+(p^4+p^2)\tau_{16}(p)-(p^2+1)\tau_{20}(p)) \equiv 0 \bmod 13\,;$$

$$(p+1)(\tau_{8,8}(p)-(p^6+p^4)\tau_{12}(p)+(p^4+p^2)\tau_{16}(p)-p^2\tau_{18}(p)-\tau_{22}(p)) \equiv 0 \bmod 13.$$

En fait, $\{v_{10}, v_{11}\}$ est m-lié pour $m = 2^5.7.13$ si bien que la congruence (4.16) se raffine en

$$(4.17)\qquad (p+1)(\tau_{12,6}(p) - (p^4+1)\tau_{18}(p)) \equiv 0 \mod 2^5.7.13\ .$$

Le cas $m = 11$

Les sous-ensembles m-liés minimaux sont $\{v_5, v_{13}\}$, $\{v_{10}, v_{15}\}$, $\{v_{14}, v_{16}\}$, $\{v_{14}, v_{19}\}$, $\{v_{16}, v_{19}\}$, $\{v_{17}, v_{21}\}$ et $\{v_7, v_8, v_{12}\}$ (observer que ce dernier a 3 éléments !).

En prenant $\mathcal{W} = \{\mathrm{v}_7, \mathrm{v}_8, \mathrm{v}_{12}\}$ dans la proposition 4.2 on obtient

$$\lambda_7(p) \equiv \lambda_8(p) \equiv \lambda_{12}(p) \mod 11 \quad .$$

En prenant $\mathcal{W} = \{\mathrm{v}_{14}, \mathrm{v}_{16}\}$, $\mathcal{W} = \{\mathrm{v}_{14}, \mathrm{v}_{19}\}$ et $\mathcal{W} = \{\mathrm{v}_{17}, \mathrm{v}_{21}\}$ dans cette proposition, on obtient respectivement

$$\lambda_{14}(p) \equiv \lambda_{16}(p) \bmod 11 \ ; \ \lambda_{14}(p) \equiv \lambda_{19}(p) \bmod 11^2 \ ; \ \lambda_{17}(p) \equiv \lambda_{21}(p) \bmod 11^2 \, .$$

La deuxième congruence ci-dessus s'écrit encore

$$p\,(p+1)\,(\tau_{6,8}(p) - \tau_{20}(p) - p^{13} - p^6) \equiv 0 \mod 11^2 \quad ,$$

congruence qui par inspection du cas $p = 11$ implique la suivante

$$(p+1)\,(\tau_{6,8}(p) - \tau_{20}(p) - p^{13} - p^6) \equiv 0 \mod 11^2 \quad . \tag{4.18}$$

La troisième s'écrit encore

$$(p+1)\,(\tau_{4,10}(p) - (p^2+1)\,\tau_{20}(p) + p^2\,\tau_{18}(p) - p^{13} - p^8) \equiv 0 \mod 11^2 \quad . \tag{4.19}$$

Exemples de spécialisations de la congruence (4.3) *qui échappent à la proposition 4.2*

– Comme les deux ensembles $\{\mathrm{v}_9, \mathrm{v}_{15}\}$, $\{\mathrm{v}_{15}, \mathrm{v}_{17}\}$ et $\{\mathrm{v}_{17}, \mathrm{v}_{18}\}$ sont 13-liés minimaux, on a $\lambda_9(p) \equiv \lambda_{15}(p) \bmod 13$, $\lambda_{15}(p) \equiv \lambda_{17}(p) \bmod 13$ et $\lambda_{17}(p) \equiv \lambda_{18}(p) \bmod 13$ (la première et la deuxième congruences ont été exploitées ci-dessus, la troisième ne l'a pas été car elle ne fait pas intervenir les $\tau_{j,k}$). On va analyser ce que donne la congruence (4.3) pour $J = \{9, 15, 17, 18\}$ (et $(i, j) = (4, 1)$).

On obtient (merci `PARI`) :

$$\begin{aligned} 2407302\,\lambda_9(p) - 513085\,\lambda_{15}(p) - 482792\,\lambda_{17}(p) - 1411425\,\lambda_{18}(p) \\ \equiv 0 \mod 2^8.3^2.13^2.17 \end{aligned}$$

et *a fortiori*

$$\lambda_9(p) + 64\,\lambda_{15}(p) - 89\,\lambda_{17}(p) + 24\,\lambda_{18}(p) \equiv 0 \mod 13^2 \quad .$$

On a

$$\begin{aligned} \lambda_9(p) + 64\,\lambda_{15}(p) - 89\,\lambda_{17}(p) + 24\,\lambda_{18}(p) \ = \\ \lambda_9(p) - \lambda_{15}(p) + 2\,\lambda_{17}(p) - 2\,\lambda_{18}(p) \\ - 65\,(\lambda_{17}(p) - \lambda_{15}(p)) + 26\,(\lambda_{18}(p) - \lambda_{17}(p)) \quad . \end{aligned}$$

Comme les deux différences $\lambda_{17}(p) - \lambda_{15}(p)$ et $\lambda_{18}(p) - \lambda_{17}(p)$ sont divisibles par 13, on obtient au bout du compte la congruence

$$\lambda_9(p) - \lambda_{15}(p) + 2\,\lambda_{17}(p) - 2\,\lambda_{18}(p) \;\equiv\; 0 \mod 13^2$$

soit encore

$$(p+1)(\tau_{8,8}(p) + 2p^2\,\tau_{18}(p) - 2\,(p^2+1)\,\tau_{20}(p) + \tau_{22}(p) - p^{15} - p^6) \equiv 0 \bmod 13^2.$$

Remarque. L'ordinateur dit que l'on a en fait

$$\lambda_9(p) - \lambda_{15}(p) + 2\,\lambda_{17}(p) - 2\,\lambda_{18}(p) \;\equiv\; 0 \mod 2^4.3^2.5.13^2$$

pour $p \leq 113$ (rappelons que nous avons calculé les $\tau_{j,k}(p)$ pour $p \leq 113$). On peut montrer que l'on a

$$\lambda_9(p) - \lambda_{15}(p) + 2\,\lambda_{17}(p) - 2\,\lambda_{18}(p) \;\equiv\; 0 \mod 5$$

pour tout p de la façon ci-après. On constate que $\{\mathrm{v}_9, \mathrm{v}_{14}, \mathrm{v}_{15}\}$ et $\{\mathrm{v}_6, \mathrm{v}_{17}, \mathrm{v}_{18}\}$ sont respectivement 25-lié minimal et 5-lié minimal ; on a donc en particulier $\lambda_9(p) \equiv \lambda_{15}(p) \bmod 25$ et $\lambda_{17}(p) \equiv \lambda_{18}(p) \bmod 5$.

– On a vu plus haut que l'on a les congruences $\lambda_{14}(p) \equiv \lambda_{19}(p) \bmod 11^2$ et $\lambda_{14}(p) \equiv \lambda_{16}(p) \bmod 11$; on a donc aussi

$$\lambda_{19}(p) - \lambda_{14}(p) + 22\,(\lambda_{16}(p) - \lambda_{14}(p)) \;\equiv\; 0 \mod 11^2 \qquad .$$

La congruence (4.3) pour $J = \{14, 16, 19\}$ (et $(i,j) = (3,1)$) permet de montrer, par la même méthode que ci-dessus, que l'on a en fait

$$\lambda_{19}(p) - \lambda_{14}(p) + 22\,(\lambda_{16}(p) - \lambda_{14}(p)) \;\equiv\; 0 \mod 11^3 \qquad .$$

– En prenant $J = \{1, 2, 23, 24\}$ (et $(i,j) = (4,1)$) on obtient cette fois

$$\lambda_1(p) - \lambda_2(p) + 2\,\lambda_{23}(p) - 2\,\lambda_{24}(p) \;\equiv\; 0 \mod 691^2 \qquad ;$$

cette congruence n'est pas très surprenante car le premier membre est égal à $(\tau(p) - p^{11} - 1)^2$!

Où l'on explique comment la théorie des représentations galoisiennes permet de "diviser par $p+1$" certaines des congruences précédentes

Théorème[*] **4.4.** *Pour tout nombre premier p, les congruences suivantes sont vérifiées :*

(1) $\tau_{4,10}(p) \equiv \tau_{22}(p) + p^{13} + p^8 \mod 41$ (conjecture de Harder [Har08]) ;
(2) $\tau_{8,8}(p) \equiv (p^6+1)\,\tau_{16}(p) \mod 23^2$;
(3) $\tau_{12,6}(p) \equiv (p^4+p^2)\,\tau_{16}(p) \mod 19$;
(4) $\tau_{4,10}(p) \equiv (p^8+p^2)\,\tau_{12}(p) \mod 19$;
(5) $\tau_{6,8}(p) \equiv (p^6+p^2)\,\tau_{12}(p) \mod 17$;
(6) $\tau_{8,8}(p) \equiv (p^6+p^4)\,\tau_{12}(p) \mod 17$;
(7) $\tau_{8,8}(p) \equiv p^8+p^6+p^3+p \mod 13$;
(8) $\tau_{12,6}(p) \equiv p^8+p^5+p^4+p \mod 13$;
(9) $\tau_{6,8}(p) \equiv p^8+p^6+p^3+p \mod 11$;
(10) $\tau_{6,8}(p) \equiv \tau_{20}(p) + p^{13} + p^6 \mod 11^2$;
(11) $\tau_{4,10}(p) \equiv p^{10}+p^8+p^3+p \mod 11$;
(12) $\tau_{8,8}(p) \equiv \tau_{12,6}(p) \mod 11$;
(13) $\tau_{12,6}(p) \equiv p^5+p^4+p^2+p \mod 7$;
(14) $p\tau_{6,8}(p) \equiv \tau_{8,8}(p) \equiv \tau_{4,10}(p) \mod 7$;
(15) $\tau_{8,8}(p) \equiv 2\,(p^3+p^2) \mod 5$;
(16) $\tau_{6,8,}(p) \equiv \tau_{12,6}(p) \equiv \tau_{4,10}(p) \equiv p^4+p^3+p^2+p \mod 5$;
(17) $\tau_{j,k}(p) \equiv 2\,(p^2+p) \mod 3$;
(18) $\tau_{j,k}(p) \equiv 0 \mod 2$.

Démonstration de la congruence (1)

Nous avons montré plus haut que l'on a $\lambda_{18}(p) \equiv \lambda_{21}(p) \bmod 41$ à l'aide de la proposition 4.2 et constaté en invoquant le théorème 2.5 (le résultat principal du mémoire !) que l'on a

$$\lambda_{21}(p) - \lambda_{18}(p) \;=\; (p+1)\,(\,\tau_{4,10}(p) - (\tau_{22}(p) + p^{13} + p^8)\,) \qquad .$$

Nous en avons déduit la congruence (4.7) qu'il nous faut maintenant "diviser par $p+1$". Pour cela nous allons faire intervenir les 24 représentations galoisiennes ℓ-adiques $\rho_{i,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{24}(\overline{\mathbb{Q}}_\ell)$ semi-simples, non ramifiées hors de ℓ, introduites dans le premier paragraphe (avec ici $\ell = 41$), caractérisées par les égalités $\lambda_i(p) = \mathrm{trace}\,\rho_{i,\ell}(\mathrm{Frob}_p)$ pour tout $p \neq \ell$.

On a vu aussi, dans ce même paragraphe, que le polynôme caractéristique de $\rho_{i,\ell}(\mathrm{Frob}_p)$ est à coefficients entiers (et indépendant de ℓ) et qu'il existe une représentation continue et semi-simple $\overline{\rho}_{i,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{24}(\mathbb{F}_\ell)$, unique à isomorphisme près, qui est non ramifiée hors de ℓ et telle que le polynôme caractéristique de $\overline{\rho}_{i,\ell}(\mathrm{Frob}_p)$ est la réduction modulo ℓ du polynôme caractéristique de $\rho_{i,\ell}(\mathrm{Frob}_p)$. Le lemme 1.1 et la proposition 4.2 impliquent l'énoncé suivant :

Proposition 4.5. *Soient m un diviseur de D, ℓ un diviseur premier de m, et $\mathcal{W}$ un sous-ensemble m-lié minimal de $\mathcal{V}$. Alors on a la congruence*

$$\text{dét}(t - \rho_{i,\ell}(\gamma)) \;\equiv\; \text{dét}(t - \rho_{j,\ell}(\gamma)) \mod m\,\mathbb{Z}_\ell$$

pour tous i, j avec $\mathrm{v}_i, \mathrm{v}_j$ dans $\mathcal{W}$ et tout γ dans $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. En particulier, les représentations $\overline{\rho}_{i,\ell}$ et $\overline{\rho}_{j,\ell}$ sont isomorphes.

En prenant $m = \ell = 41$ et $\mathcal{W} = \{\mathrm{v}_{18}, \mathrm{v}_{21}\}$ dans la proposition ci-dessus on obtient $\overline{\rho}_{18,41} \simeq \overline{\rho}_{21,41}$. Pour obtenir une équation dont l'aspect soit similaire à celui de (4.7) on introduit le formalisme ci-après.

Soit ℓ un nombre premier ; on note A_ℓ l'anneau de Grothendieck des représentations continues de dimension finie, à coefficients dans $\mathbb{F}_\ell$, de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, disons non ramifiées hors de ℓ. On a donc, par définition même, $\overline{\rho}_{21,41} - \overline{\rho}_{18,41} = 0$ dans A_{41}.

Les représentations ℓ-adiques notées $\rho_{\Delta_w,\ell}$, $w = 11, 15, 17, 19, 21$, et $\rho_{\Delta_{w,v},\ell}$, $(w, v) = (19, 7), (21, 9), (21, 13), (21, 5)$, dans la démonstration du théorème 1.3, seront ici notées respectivement $\mathrm{r}_{i;\ell}$, $i = 12, 16, 18, 20, 22$, et $\mathrm{r}_{j,k;\ell}$, $(j, k) = (6, 8), (8, 8), (12, 6), (4, 10)$. Avec cette notation on a $\tau_i(p) = \mathrm{trace}\,\mathrm{r}_{i;\ell}(\mathrm{Frob}_p)$ et $\tau_{j,k}(p) = \mathrm{trace}\,\mathrm{r}_{j,k;\ell}(\mathrm{Frob}_p)$ pour tout $p \neq \ell$.

Quelques rappels :

– Les représentations $\mathrm{r}_{i;\ell}$ et $\mathrm{r}_{j,k;\ell}$ sont respectivement de dimension 2 et 4.

– Les représentations $\mathrm{r}_{i;\ell}$ peuvent être définies sur $\mathbb{Z}_\ell$. Il est probable que les représentations $\mathrm{r}_{j,k;\ell}$ puissent l'être aussi (voir la remarque 1.4) ; nous utiliserons ci-après qu'elles peuvent être définies sur la clôture intégrale de $\mathbb{Z}_\ell$ dans une extension finie de $\mathbb{Q}_\ell$ (voir la démonstration du corollaire 1.5).

– On note $\omega_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ l'homomorphisme (la représentation ℓ-adique de dimension 1) défini par l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les racines ℓ^α-ième de l'unité, $\alpha \geq 1$.

– On a $\text{dét}\,\mathrm{r}_{i;\ell} = \omega_\ell^{i-1}$, $\text{dét}\,\mathrm{r}_{6,8;\ell} = \omega_\ell^{38}$ et $\text{dét}\,\mathrm{r}_{j,k;\ell} = \omega_\ell^{42}$ pour $(j, k) = (8, 8), (12, 6), (4, 10)$.

– On note $\bar{\mathrm{r}}_{i;\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$, $\bar{\mathrm{r}}_{j,k;\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_4(\mathbb{F}_\ell)$ et $\overline{\omega}_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ les représentations résiduelles respectivement associées aux représentations ℓ-adiques $\mathrm{r}_{i;\ell}$, $\mathrm{r}_{j,k;\ell}$ (voir le corollaire 1.5) et ω_ℓ ; $\overline{\omega}_\ell$ s'identifie à l'homomorphisme défini par l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les racines ℓ-ième de l'unité, homomorphisme que l'on notera aussi χ_ℓ.

Par la suite le nombre premier ℓ sera fixé, aussi ferons-nous disparaître, sauf dans le cas de A_ℓ, l'indice ℓ de la notation.

Revenons maintenant à la démonstration de la congruence (1).

On prend $\ell = 41$. Les égalités

$$\begin{aligned}\rho_{18} \;=\; & (\omega^{14} \oplus \omega^{13} \oplus \omega^{12} \oplus 2\,\omega^{11} \oplus \omega^{10} \oplus \omega^9 \oplus \omega^8) \oplus \\ & (\omega^7 \oplus \omega^6 \oplus \omega^5 \oplus \omega^4) \otimes \mathrm{r}_{12} \;\oplus\; (\omega^3 \oplus \omega^2) \otimes \mathrm{r}_{18} \;\oplus\; (\omega \oplus 1) \otimes \mathrm{r}_{18}\end{aligned}$$

et

$$\begin{aligned}\rho_{21} \;=\; & (\omega^{12} \oplus 2\,\omega^{11} \oplus \omega^{10}) \oplus \\ & (\omega^7 \oplus \omega^6 \oplus \omega^5 \oplus \omega^4) \otimes \mathrm{r}_{12} \;\oplus\; (\omega^3 \oplus \omega^2) \otimes \mathrm{r}_{18} \;\oplus\; (\omega \oplus 1) \otimes \mathrm{r}_{4,10}\end{aligned}$$

impliquent que l'on a dans l'anneau de Grothendieck A_{41} l'égalité

$$\overline{\rho}_{21} - \overline{\rho}_{18} \;=\; (\chi + 1)\,(\,\bar{\mathrm{r}}_{4,10} - (\bar{\mathrm{r}}_{18} + \chi^{13} + \chi^8)\,)$$

et l'équation promise

$$(\chi + 1)\,(\,\bar{\mathrm{r}}_{4,10} - (\bar{\mathrm{r}}_{18} + \chi^{13} + \chi^8)\,) \;=\; 0 \tag{4.20}$$

qui est le "pendant galoisien" de (4.7). Pour "diviser par $\chi+1$" cette équation on utilise la proposition 4.6 ci-dessous. Avant d'énoncer cette proposition, il nous faut faire quelques observations et introduire encore quelques notations.

Soit ℓ un nombre premier.

Soit ρ une représentation continue de dimension finie, à coefficients dans $\mathbb{F}_\ell$, de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, non ramifiée hors de ℓ. L'application $\rho \mapsto \dim \rho$ induit un homomorphisme d'anneaux que l'on note encore $\dim : \mathrm{A}_\ell \to \mathbb{Z}$. Le théorème de Knonecker-Weber montre que le déterminant de ρ est une puissance de χ. L'application $\rho \mapsto \text{dét}\,\rho$ induit une application $\mathrm{A}_\ell \to \mathrm{C}_\chi$, C_χ désignant le sous-groupe de $\mathrm{A}_\ell^\times$ engendré par χ, que l'on note encore dét ; puisque χ est d'ordre $\ell-1$ le groupe C_χ est canoniquement isomorphe à $\mathbb{Z}/(\ell-1)$. On vérifie que l'on a $\text{dét}(x+y) = \text{dét}(x)\,\text{dét}(y)$ et $\text{dét}(xy) = \text{dét}(x)^{\dim y}\,\text{dét}(y)^{\dim x}$ pour tous x et y dans A_ℓ.

Le groupe abélien sous-jacent à l'anneau commutatif A_ℓ est le groupe abélien libre engendré par l'ensemble, disons $\mathcal{S}$, des classes d'isomorphisme des représentations simples. Soit $H = \sum_{S\in\mathcal{S}} n_S S$, avec $n_S \in \mathbb{Z}$, un élément de A_ℓ ; on pose

$$\|H\| \;=\; \sum_{S\in\mathcal{S}} |n_S| \dim S \qquad .$$

L'application $\mathrm{A}_\ell \to \mathbb{N}$, $H \mapsto \|H\|$ est une "norme", en clair les propriétés suivantes sont satisfaites :

– $H = 0 \iff \|H\| = 0$;
– $\|n\,H\| = |n|\,\|H\|$ pour tout n dans $\mathbb{Z}$;
– $\|H_1 + H_2\| \leq \|H_1\| + \|H_2\|$ pour tous H_1 et H_2 dans A_ℓ.

Soient ρ_+ et ρ_- deux représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ à coefficients dans $\mathbb{F}_\ell$; on observera que l'on a les égalités $\|\rho_+\| = \dim \rho_+$, $\|\rho_-\| = \dim \rho_-$ et l'inégalité $\|\rho_+ - \rho_+\| \leq \dim \rho_+ + \dim \rho_-$.

Nous en arrivons enfin à l'énoncé que nous avions en vue :

Proposition 4.6. *Soit $\ell \neq 2$ un nombre premier ; soit H un élément de A_ℓ. Si l'on a $(\chi+1)\,H = 0$ alors l'entier $\|H\|$ est divisible par $\ell - 1$. Si l'on a en outre* $\det H = 1$ *alors l'entier $\|H\|$ est divisible par $2\,(\ell-1)$.*

Démonstration. L'action évidente du groupe C_χ sur le groupe abélien sous-jacent à A_ℓ, $(\chi^k, x) \mapsto \chi^k x$, préserve le sous-ensemble $\mathcal{S}$ introduit ci-dessus. Soit S un élément de $\mathcal{S}$; on note $\Omega(S)$ l'orbite de S sous l'action de C_χ, $\mathrm{m}(S)$ le cardinal de cette orbite (en clair, $\mathrm{m}(S)$ est le plus petit entier $k \geq 1$ tel que l'on a $\chi^k S = S$) et $\mathbb{Z}[\Omega(S)]$ le sous-groupe (abélien libre) du groupe abélien sous-jacent à A_ℓ qu'elle engendre. On a donc une décomposition en somme directe du groupe abélien sous-jacent à A_ℓ

$$\mathrm{A}_\ell \;=\; \bigoplus_{S\in\mathcal{S}_0} \mathbb{Z}[\Omega(S)] \qquad ,$$

$\mathcal{S}_0 \subset \mathcal{S}$ désignant un système de représentants pour l'ensemble quotient $\mathrm{C}_\chi\backslash\mathcal{S}$. Cette décomposition est compatible avec l'action de C_χ ; en particulier chaque facteur est envoyé dans lui-même par la multiplication par $\chi + 1$.

Proposition 4.7. *Soit S un élément de $\mathcal{S}$. Soient $\Omega(S)$ l'orbite de S sous l'action de C_χ et $\mathrm{m}(S)$ le cardinal de cette orbite, c'est-à-dire le plus entier $k \geq 1$ tel que l'on a $\chi^k S = S$.*

(a) *L'entier $\mathrm{m}(S)$ divise $\ell - 1$ et $\ell - 1$ divise $\mathrm{m}(S) \dim S$.*

(b) *Le noyau de l'endomorphisme du groupe abélien* $\mathbb{Z}[\Omega(S)]$ *induit par la multiplication par* $\chi+1$ *est trivial si* $\mathrm{m}(S)$ *est impair et est engendré (comme groupe abélien) par*

$$(1-\chi+\chi^2-\chi^3+\ldots-\chi^{\mathrm{m}(S)-1})\,S$$

si $\mathrm{m}(S)$ *est pair.*

Démonstration. Le seul point qui n'est pas tout à fait évident est la seconde partie de (a). Pour s'en convaincre, observer que l'on a $\chi^{\mathrm{m}(S)}S=S$ et $\text{dét}(\chi^{\mathrm{m}(S)}S)=\chi^{\mathrm{m}(S)\dim S}\,\text{dét}\,S$. □

On reprend la démonstration de la proposition 4.6. Soit $\mathcal{S}_{0,0}$ le sous-ensemble de $\mathcal{S}_0$ constitué des S avec $\mathrm{m}(S)$ pair ; la proposition ci-dessus montre que si l'on a $(\chi+1)H=0$ alors il existe des entiers relatifs n_S, S parcourant $\mathcal{S}_{0,0}$, tels que l'on a

$$H \;=\; \sum_{S\in\mathcal{S}_{0,0}} n_S\,(1-\chi+\chi^2-\chi^3+\ldots-\chi^{\mathrm{m}(S)-1})\,S \qquad . \tag{4.21}$$

Par définition même de $\|H\|$ on a

$$\|H\| \;=\; \sum_{S\in\mathcal{S}_{0,0}} |n_S|\,\mathrm{m}(S)\dim S \qquad .$$

La seconde partie du point (a) de la proposition 4.7 dit que tous les produits $\mathrm{m}(S)\dim S$ ci-dessus sont divisibles par $\ell-1$, ce qui démontre la première partie de la proposition 4.6.

Passons à la démonstration de la seconde partie de la proposition 4.6. L'égalité (4.21) implique la suivante

$$\text{dét}\,H \;=\; \chi^{-\frac{1}{2}\sum_{S\in\mathcal{S}_{0,0}} n_S\,\mathrm{m}(S)\dim S}$$

(observer que l'on a $\dim(1-\chi+\chi^2-\chi^3+\ldots-\chi^{\mathrm{m}(S)-1})=0$ et $\text{dét}(1-\chi+\chi^2-\chi^3+\ldots-\chi^{\mathrm{m}(S)-1})=\chi^{-\frac{\mathrm{m}(S)}{2}}$), si bien que l'égalité $\text{dét}\,H=1$ est équivalente à la congruence

$$\sum_{S\in\mathcal{S}_{0,0}} n_S\,\mathrm{m}(S)\dim S \;\equiv\; 0 \mod 2(\ell-1) \qquad .$$

Comme $|n_S|$ et n_S ont même parité et que tous les $\mathrm{m}(S)\dim S$ sont divisibles par $\ell-1$, les égalités $(\chi+1)H=0$ et $\text{dét}\,H=1$ entraînent bien que $\|H\|$ est divisible par $2(\ell-1)$. □□

Remarque. L'égalité $(\chi+1)H = 0$ implique $\dim H = 0$ et $(\text{dét}\, H)^2 = 1$. Cette implication est "optimale" (pour $\ell \neq 2$). Pour s'en convaincre prendre $H = H_0 := 1-\chi+\chi^2-\chi^3+\ldots-\chi^{\ell-2}$ et constater que l'on a $\text{dét}\, H_0 = \chi^{\frac{\ell-1}{2}}$. On observera également que l'on a $\|H_0\| = \ell-1$, ce qui montre que la première partie de la proposition 4.6 est optimale ; en outre, on a $(\chi+1)(2H_0) = 0$, $\text{dét}(2H_0) = 1$ et $\|2H_0\| = 2(\ell-1)$, ce qui montre la seconde partie de cette proposition est aussi optimale.

Démonstration de la congruence (1) à l'aide de 4.6.

On prend $\ell = 41$ et $H = \bar{\mathrm{r}}_{4,10} - (\bar{\mathrm{r}}_{18} + \chi^{13} + \chi^8)$. On a $\|H\| \leq 8$. Comme l'on a $(\chi+1)H = 0$ (équation (4.20)), la proposition 4.6 dit que $\|H\|$ est divisible par 40 (et même 80 si l'on observe que l'on a $\text{dét}\, H = 1$). On en déduit $\|H\| = 0$ et $H = 0$. En évaluant les représentations $\bar{\mathrm{r}}_{4,10}$ et $\bar{\mathrm{r}}_{18} \oplus \chi^{13} \oplus \chi^8$, "en la classe de conjugaison Frob_p", on obtient la congruence (1) pour $p \neq 41$. Par ailleurs la congruence (4.7) implique trivialement la congruence (1) pour $p = 41$. □□□

Démonstration de la congruence (2)

On fixe $\ell = 23$.

En prenant $m = \ell = 23$ et $\mathcal{W} = \{\mathrm{v}_{13}, \mathrm{v}_{15}\}$ dans la proposition 4.5, on obtient comme précédemment l'isomorphisme de représentations galoisiennes

$$\bar{\mathrm{r}}_{8,8} \simeq (\chi^6 \oplus 1) \otimes \bar{\mathrm{r}}_{16} \tag{4.22}$$

et la congruence

$$\tau_{8,8}(p) \equiv (p^6+1)\,\tau_{16}(p) \mod 23 \quad .$$

Pour obtenir la congruence (2) (qui raffine à la fois la congruence ci-dessus et la congruence (4.9)) on utilise le lemme ci-dessous :

Lemme 4.8. *Soient B un anneau local artinien de corps résiduel k, G un groupe, V_1, V_2, W_1 et W_2 des $B[G]$-modules que l'on suppose libres de dimension finie comme B-modules. On fait les hypothèses suivantes :*

(i) Pour $i = 1, 2$, les semi-simplifiés des $k[G]$-modules $k \otimes_B V_i$ et $k \otimes_B W_i$ sont isomorphes.

(ii) Les $k[G]$-modules $k \otimes_B V_1$ et $k \otimes_B V_2$ n'ont aucun facteur de Jordan-Hölder en commun.

(iii) Pour tout g dans G, on a $\text{dét}(t - g_{|V_1 \oplus V_2}) = \text{dét}(t - g_{|W_1 \oplus W_2})$.

Alors pour $i = 1, 2$ et pour tout g, on a $\text{dét}(t - g_{|V_i}) = \text{dét}(t - g_{|W_i})$.

Démonstration. Soient U le $B[G]$-module $V_1 \oplus V_2 \oplus W_1 \oplus W_2$ et R la B-algèbre image de $B[G]$ dans $\mathrm{End}_B(U)$. Soit J le radical de Jacobson de R. Le B-module sous-jacent à R étant de type fini, J est le plus grand idéal bilatère nilpotent de R. C'est aussi le noyau de l'homomorphisme naturel de R vers les endomorphismes du semi-simplifié de $k \otimes_B U$. En particulier, on a $\mathfrak{m}R \subset J$, $\mathfrak{m}$ désignant l'idéal maximal de B, et R/J est une k-algèbre semi-simple de dimension finie.

La théorie d'Artin-Wedderburn appliquée à R/J et l'hypothèse (ii) montrent que l'on peut trouver un idempotent f dans R/J tel que f agisse par l'identité sur le semi-simplifié de $k \otimes_B V_1$ et par 0 sur celui de $k \otimes_B V_2$. Comme J est nilpotent, cet idempotent se relève en un idempotent e dans R. Ceci assure que e agit par 0 sur V_2 (car il agit ainsi sur tous ses facteurs de Jordan-Hölder) et par l'identité sur V_1 et W_1 (pour la même raison).

L'identité classique d'Amitsur, exprimant les coefficients du polynôme caractéristique d'une somme de deux matrices comme une fonction universelle des coefficients des polynômes caractéristiques de certains monômes en ces deux matrices, montre que l'égalité de déterminants de l'hypothèse (iii) entraîne plus généralement $\text{dét}(t - r_{|V_1 \oplus V_2}) = \text{dét}(t - r_{|W_1 \oplus W_2})$ pour tout r dans R. Le théorème en résulte : soit g un élément de G ; pour $i = 1$ (resp. $i = 2$) on spécialise cette identité à $r = ge$ (resp. $r = g(1-e)$). □

Démonstration de la congruence (2) à l'aide de 4.8.

On spécialise le lemme en question.

(Rappel : Le nombre premier ℓ est fixé égal à 23, les notations $\mathrm{r}_{8,8}$, r_{16}, ω, ρ_{13}, ρ_{15} et χ qui apparaissent ci-dessous sont les abréviations de $\mathrm{r}_{8,8;23}$, $\mathrm{r}_{16;23}$, ω_{23}, $\rho_{13,23}$, $\rho_{15,23}$ et χ_{23}.)

La représentation $\mathrm{r}_{8,8}$ peut être définie sur la clôture intégrale, disons $\mathcal{D}$, de $\mathbb{Z}_{23}$ dans une extension finie de $\mathbb{Q}_{23}$. La représentation r_{16} peut être définie sur $\mathbb{Z}_{23}$ et *a fortiori* sur $\mathcal{D}$; de même la représentation ω est définie sur $\mathbb{Z}_{23}$ et *a fortiori* sur $\mathcal{D}$.

– On prend pour B l'anneau quotient $\mathcal{D}/23^2$. L'anneau B est local, son corps résiduel k est un corps fini de caractéristique 23 ; B est artinien (il est fini !).

– On prend pour G le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

– On prend pour V_1, V_2, W_1 et W_2, le B-module B^4 muni de l'action linéaire du groupe G donnée respectivement par les représentations $(\omega^6 \oplus 1) \otimes \mathrm{r}_{16}$, $\omega \otimes (\omega^6 \oplus 1) \otimes \mathrm{r}_{16}$, $\mathrm{r}_{8,8}$ et $\omega \otimes \mathrm{r}_{8,8}$.

– L'hypothèse (i) est donnée par l'isomorphisme (4.22) et l'extension des scalaires de $\mathbb{F}_{23}$ à k.

– Il n'est pas difficile de vérifier l'hypothèse (ii). La représentation (résiduelle modulo 23) $\overline{r}_{16}$ est simple [Sw72] (pour s'en convaincre *ab initio*, observer que l'on a $47 \equiv 1 \bmod 23$ et $\tau_{16}(47) \not\equiv 2 \bmod 23$) ; il en résulte, toujours d'après Kronecker-Weber, que $k \otimes_{\mathbb{F}_{23}} \overline{r}_{16}$ est encore simple. Les facteurs de Jordan-Hölder de $k \otimes_B V_1$ (resp. $k \otimes_B V_2$), sont donc $k \otimes_{\mathbb{F}_{23}} \overline{r}_{16}$ et $k \otimes_{\mathbb{F}_{23}} (\chi^6\, \overline{r}_{16})$ (resp. $k \otimes_{\mathbb{F}_{23}} (\chi\, \overline{r}_{16})$ et $k \otimes_{\mathbb{F}_{23}} (\chi^7\, \overline{r}_{16})$). On conclut en observant que le déterminant de $\overline{r}_{16}$, $\chi^6\, \overline{r}_{16}$, $\chi\, \overline{r}_{16}$ et $\chi^7\, \overline{r}_{16}$ est respectivement χ^{15}, χ^5, χ^{17} et χ^7.

- L'hypothèse (iii) est impliquée par la proposition 4.5 et le fait que l'on a $\rho_{13} = v \oplus \sigma$ et $\rho_{15} = w \oplus \sigma$, avec $v = (\omega \oplus 1) \otimes (\omega^6 \oplus 1) \otimes \mathrm{r}_{16}$, $w = (\omega \oplus 1) \otimes \mathrm{r}_{8,8}$ et σ une représentation 23-adique de dimension 16.

La conclusion du lemme dit que "les polynômes caractéristiques en Frob_p", $p \neq 23$, des représentations 23-adiques $(\omega^6 \oplus 1) \otimes \mathrm{r}_{16}$ et $\mathrm{r}_{8,8}$ sont congrus modulo 23^2. *A fortiori* "les traces en Frob_p", $p \neq 23$, sont congrues modulo 23^2, en d'autres termes la congruence (2) est satisfaite pour $p \neq 23$. Le cas $p = 23$ découle trivialement de la congruence (4.9). □□

Démonstration de la congruence (3)

On fixe $\ell = 19$.

En prenant $m = \ell = 19$ et $\mathcal{W} = \{\mathrm{v}_9, \mathrm{v}_{10}\}$ dans la proposition 4.5 et en utilisant la proposition 4.6 on obtient l'égalité

$$\overline{\mathrm{r}}_{12,6} - (\chi^4 + \chi^2)\, \overline{\mathrm{r}}_{16} + \chi^2\, \overline{\mathrm{r}}_{18} - \overline{\mathrm{r}}_{22} \;=\; 0$$

dans l'anneau de Grothendieck A_{19}, soit encore l'isomorphisme de représentations

$$\overline{\mathrm{r}}_{12,6} \oplus \chi^2\, \overline{\mathrm{r}}_{18} \;\simeq\; (\chi^4 \oplus \chi^2)\, \overline{\mathrm{r}}_{16} \oplus \overline{\mathrm{r}}_{22} \qquad . \tag{4.23}$$

Comme les représentations $\overline{\mathrm{r}}_{16}$ et $\overline{\mathrm{r}}_{22}$ sont simples (on peut s'en convaincre en observant que l'on a $\tau_{16}(5) \not\equiv \tau_{16}(43) \bmod 19$ et $\tau_{22}(5) \not\equiv \tau_{22}(43) \bmod 19$ alors que l'on a $5 \equiv 43 \bmod 19$), la représentation $\chi^2\, \overline{\mathrm{r}}_{18}$ est nécessairement isomorphe à l'une des représentations $\chi^4\, \overline{\mathrm{r}}_{16}$, $\chi^2\, \overline{\mathrm{r}}_{16}$ ou $\overline{\mathrm{r}}_{22}$. Le calcul des déterminants montre que la seule possibilité est

$$\chi^2\, \overline{\mathrm{r}}_{18} \;\simeq\; \overline{\mathrm{r}}_{22} \qquad . \tag{4.24}$$

Comme les représentations $\overline{\mathrm{r}}_{12,6}$ et $(\chi^4 \oplus \chi^2)\, \overline{\mathrm{r}}_{16}$ sont semi-simples, les isomorphismes (4.23) et (4.24) entraînent

$$\overline{\mathrm{r}}_{12,6} \;\simeq\; (\chi^4 \oplus \chi^2)\, \overline{\mathrm{r}}_{16} \qquad .$$

Cet isomorphisme implique la congruence (3) pour $p \neq 19$. On vérifie que cette congruence est aussi satisfaite pour $p = 19$ (on peut éviter d'utiliser le calcul de $\tau_{12,6}(19)$ en observant que les congruences $19^2\tau_{18}(19) \equiv \tau_{20}(19)$ et (4.10) impliquent (3) pour $p = 19$). $\square$

Démonstration des congruences (4), (5) et (6)

La démonstration de la congruence (4) est la même que celle de la congruence (3) ; elle est d'ailleurs plus rapide si l'on utilise (4.24).

Passons à (5) et (6). Evidemment on fixe $\ell = 17$.

– En utilisant le "pendant galoisien" de (4.13) et en copiant la démonstration de la congruence (3), on obtient les isomorphismes de représentations

$$\chi^2\,\bar{\mathrm{r}}_{16} \;\simeq\; \bar{\mathrm{r}}_{20} \tag{4.25}$$

et

$$\bar{\mathrm{r}}_{6,8} \;\simeq\; (\chi^6 \oplus \chi^2) \otimes \bar{\mathrm{r}}_{12} \qquad .$$

Cet isomorphisme implique la congruence (5) pour $p \neq 17$; le cas $p = 17$ peut se régler comme dans la cas de la congruence (3).

– Le pendant galoisien de (4.12) est l'équation suivante dans A_{17} :

$$(\chi+1)\,(\bar{\mathrm{r}}_{8,8} - (\chi^6+\chi^4)\bar{\mathrm{r}}_{12} + (\chi^4+\chi^2)\bar{\mathrm{r}}_{16} - (\chi^2+1)\bar{\mathrm{r}}_{20}) \;=\; 0 \qquad .$$

Cette equation et l'isomorphisme (4.25) entraînent

$$(\chi+1)\,(\bar{\mathrm{r}}_{8,8} - (\chi^6+\chi^4)\bar{\mathrm{r}}_{12}) \;=\; 0 \qquad .$$

En invoquant la proposition 4.6 on obtient l'équation

$$\bar{\mathrm{r}}_{8,8} - (\chi^6+\chi^4)\bar{\mathrm{r}}_{12} \;=\; 0 \qquad ,$$

soit encore l'isomorphisme de représentations

$$\bar{\mathrm{r}}_{8,8} \;\simeq\; (\chi^6 \oplus \chi^4) \otimes \bar{\mathrm{r}}_{12}$$

(les deux membres sont semi-simples). Cet isomorphisme implique la congruence (6) pour $p \neq 17$; le cas $p = 17$ peut se régler comme précédemment.

Remarque. Le pendant galoisien de (4.11) est l'équation suivante dans A_{17} :

$$(\chi+1)\,((\chi^4+\chi^2)\bar{\mathrm{r}}_{16} - (\chi^2+1)\bar{\mathrm{r}}_{20} + \bar{\mathrm{r}}_{22} - \chi^{17} - \chi^4) \;=\; 0 \qquad .$$

Compte tenu de (4.25), celle-ci donne l'équation

$$(\chi+1)\,(\bar{\mathrm{r}}_{22}-\chi^{17}-\chi^{4}) \;=\; 0 \qquad .$$

En invoquant à nouveau la proposition 4.6 on obtient l'équation

$$\bar{\mathrm{r}}_{22}-\chi^{17}-\chi^{4} \;=\; 0 \qquad ,$$

soit encore l'isomorphisme de représentations

$$\bar{\mathrm{r}}_{22} \;\simeq\; \chi^{17}\oplus\chi^{4} \;=\; \chi\oplus\chi^{4} \qquad .$$

L'isomorphisme $\bar{\mathrm{r}}_{22}\simeq\chi\oplus\chi^{4}$ ci-dessus est l'un des isomorphismes donnés par Swinnerton-Dyer dans [Sw72] ; nous faisons un usage systématique de ce type d'isomorphisme ci-après.

Démonstration des congruences (7), (8), (9), (11) et (13)

Le point de départ de ces démonstrations est respectivement :

– l'équation dans A_{13} qui est le pendant galoisien de la congruence (4.15) ;

– l'équation dans A_{13} qui est le pendant galoisien de la congruence (4.14) ou de la congruence (4.16) ;

– l'équation dans A_{11} qui est le pendant galoisien de la réduction modulo 11 de la congruence (4.18) (qui est une congruence modulo 11^2) ;

– l'équation dans A_{11} qui est le pendant galoisien de la réduction modulo 11 de la congruence (4.19) (qui est une congruence modulo 11^2) ;

– l'équation dans A_{7} qui est le pendant galoisien de la réduction modulo 7 de la congruence (4.17) (qui est une congruence modulo $2^5.7.13$ dont la réduction modulo 13 est la congruence (4.16) mentionnée ci-dessus).

Par la méthode que nous avons répétitivement employée ci-dessus, on exprime les $\overline{r}_{j,k}$ qui nous intéressent en fonction de certains $\overline{r}_i$ et de χ. Tous les $\overline{r}_i$ qui apparaissent peuvent à leur tour s'exprimer en fonction de χ grâce aux isomorphismes de Swinnerton-Dyer [Sw72]. Au bout du compte, on obtient des isomorphismes de la forme $\overline{r}_{j,k}\simeq\chi^{a_1}\oplus\chi^{a_2}\oplus\chi^{a_3}\oplus\chi^{a_4}$ qui conduisent aux congruences (7), (8), (9), (11) et (13).

Traitons par exemple le cas de la congruence (13).

On fixe $\ell=7$. En prenant $m=\ell=7$ et $\mathcal{W}=\{\mathrm{v}_{10},\mathrm{v}_{11}\}$ dans la proposition 4.5 on obtient l'équation suivante dans A_7 :

$$(\chi+1)\,(\bar{\mathrm{r}}_{12,6}-(\chi^{4}+1)\,\bar{\mathrm{r}}_{18}) \;=\; 0 \qquad .$$

Puisque les représentations $\bar{\mathrm{r}}_{12,6}$ et $(\chi^4 \oplus 1) \otimes \bar{\mathrm{r}}_{18}$ ont même déterminant (à savoir χ^{42}) et que l'on a l'inégalité $\|\bar{\mathrm{r}}_{12,6} - (\chi^4+1)\bar{\mathrm{r}}_{18}\| \leq 8$, la seconde partie de la proposition 4.6 montre que l'on a en fait l'équation

$$\bar{\mathrm{r}}_{12,6} - (\chi^4+1)\bar{\mathrm{r}}_{18} \;=\; 0 \qquad ,$$

ou ce qui revient au même l'isomorphisme de représentations

$$\bar{\mathrm{r}}_{12,6} \;\simeq\; (\chi^4 \oplus 1) \otimes \bar{\mathrm{r}}_{18} \qquad .$$

Or Swinnerton-Dyer nous dit que l'on a $\bar{\mathrm{r}}_{18} \simeq \chi \oplus \chi^4$ si bien que l'on obtient au bout du compte

$$\bar{\mathrm{r}}_{12,6} \;\simeq\; \chi^5 \oplus \chi^4 \oplus \chi^2 \oplus \chi \qquad .$$

Cet isomorphisme donne la congruence (13) pour $p \neq 7$; le cas $p = 7$ peut se déduire de (4.17).

Démonstration de la congruence (10)

Elle est semblable à celle la congruence (2).

On fixe $\ell = 11$.

En prenant $m = \ell = 11$ et $\mathcal{W} = \{\mathrm{v}_{14}, \mathrm{v}_{19}\}$ dans la proposition 4.5 on obtient l'équation suivante dans A_{11} :

$$\chi(\chi+1)\,(\bar{\mathrm{r}}_{6,8} - \bar{\mathrm{r}}_{20} - \chi^{13} - \chi^6) \qquad .$$

On "divise cette équation par $\chi(\chi+1)$" en observant que χ est inversible et en utilisant la proposition 4.6 ; on obtient ainsi l'isomorphisme de représentations galoisiennes

$$\bar{\mathrm{r}}_{6,8} \;\simeq\; \bar{\mathrm{r}}_{20} \oplus \chi^{13} \oplus \chi^6$$

et la congruence

$$\tau_{6,8}(p) \;\equiv\; \tau_{20}(p) + p^{13} + p^6 \mod 11 \qquad . \tag{4.26}$$

Cette congruence se transforme en la congruence (9) en utilisant la congruence $\tau_{20}(p) \equiv p^8 + p \bmod 11$ de [Sw72].

Or nous avons vu, dans la première partie de ce paragraphe, que l'on a, pour tout nombre premier p, la congruence (4.18) suivante

$$(p+1)\,(\tau_{6,8}(p) - \tau_{20}(p) - p^{13} - p^6) \;\equiv\; 0 \mod 11^2 \qquad .$$

Pour "diviser cette congruence par $p+1$" on emploie la méthode qui nous a permis d'obtenir la congruence (2) à partir de la congruence (4.9) (à savoir la mise en oeuvre du lemme 4.8).

Remarque. On ne peut avoir de congruence de la forme

$$\tau_{6,8}(p) \;\equiv\; p^{a_1} + p^{a_2} + p^{a_3} + p^{a_4} \mod 11^2$$

pour tout nombre premier p, disons avec $p \neq 11$. En effet, compte tenu de (10), on aurait $\tau_{20}(p) \equiv p^{a_1} + p^{a_2} + p^{a_3} + p^{a_4} - p^{13} - p^6 \bmod 11^2$. Or cette congruence est en défaut pour le plus petit nombre premier p avec $p \equiv 1 \bmod 11^2$, à savoir $p = 727$: $\tau_{20}(727) \equiv 68 \not\equiv 2 \bmod 11^2$.

Remarque. Nous avons vu dans la première partie de ce paragraphe que l'on a, pour tout nombre premier p, la congruence (4.19) suivante :

$$(p+1)\,(\tau_{4,10}(p) - (p^2+1)\,\tau_{20}(p) + p^2\,\tau_{18}(p) - p^{13} - p^8) \;\equiv\; 0 \mod 11^2 \qquad .$$

Le pendant galoisien de la réduction modulo 11 de cette congruence, est l'équation suivante dans A_{11} :

$$(\chi+1)\,(\bar{\mathrm{r}}_{4,10} - (\chi^2+1)\bar{\mathrm{r}}_{20} + \chi^2\bar{\mathrm{r}}_{18} - \chi^{13} - \chi^8) \;=\; 0 \qquad .$$

En utilisant les isomorphismes $\bar{\mathrm{r}}_{20} \simeq \chi^8 \oplus \chi$ et $\bar{\mathrm{r}}_{18} \simeq \chi^6 \oplus \chi$ de [Sw72], on obtient l'équation

$$(\chi+1)\,(\bar{\mathrm{r}}_{4,10} - \chi^8 - \chi^3 - \chi - 1) \;=\; 0$$

qui après "division par $p+1$" conduit à la congruence (11). Mais cette fois le lemme 4.8 ne permet pas de "diviser par $p+1$" la congruence (4.19) car l'hypothèse concernant les facteurs de Jordan-Hölder n'est pas satisfaite. On constate cependant que la congruence

$$\tau_{4,10}(p) \;\equiv\; (p^2+1)\,\tau_{20}(p) - p^2\,\tau_{18}(p) + p^{13} + p^8 \mod 11^2$$

est vérifiée pour $p \leq 113$ (on rappelle que l'on a déterminé les $\tau_{j,k}(p)$ pour $p \leq 113$) ; on observera que ceci n'est vraiment une information que pour les nombres premiers $p \leq 113$ avec $p+1 \equiv 0 \bmod 11$, à savoir 43 et 109 !

Démonstration des congruences (12) et (14)

Les démonstrations de ces trois congruences sont toutes du même type (c'est pourquoi nous les avons mises dans le même chapeau). Démontrons par exemple que l'on a, pour tout nombre premier p, la congruence

$$p\,\tau_{6,8}(p) \;\equiv\; \tau_{8,8}(p) \mod 7 \qquad . \tag{4.27}$$

On fixe $\ell = 7$.

En prenant $m = \ell = 7$ et $\mathcal{W} = \{\mathrm{v}_{15}, \mathrm{v}_{19}\}$ dans la proposition 4.5 on obtient l'équation suivante dans A_7 :

$$\begin{aligned}(4.28)\qquad & (\chi+1)\bar{\mathrm{r}}_{8,8} - \chi(\chi+1)\bar{\mathrm{r}}_{6,8} \\ & + (\chi^5+\chi^2)\bar{\mathrm{r}}_{16} - (\chi^5+1)\bar{\mathrm{r}}_{12} - \mathrm{Sym}^2\,\bar{\mathrm{r}}_{12} + \chi^5 + 2\chi^2 \;=\; 0 \qquad .\end{aligned}$$

Or on constate que les isomorphismes $\bar{\mathrm{r}}_{16} \simeq \chi^2+\chi$ et $\bar{\mathrm{r}}_{12} \simeq \chi^4+\chi$ de [Sw72] entraînent

$$(\chi^5+\chi^2)\bar{\mathrm{r}}_{16} - (\chi^5+1)\bar{\mathrm{r}}_{12} - \mathrm{Sym}^2\,\bar{\mathrm{r}}_{12} + \chi^5 + 2\chi^2 \;=\; 0$$

si bien que l'équation (4.28) se simplifie en la suivante :

$$(4.29)\qquad (\chi+1)\bar{\mathrm{r}}_{8,8} - \chi(\chi+1)\bar{\mathrm{r}}_{6,8} \;=\; 0 \qquad .$$

Posons $H = \bar{\mathrm{r}}_{8,8} - \chi\bar{\mathrm{r}}_{6,8}$; l'équation ci-dessus dit que l'on a $(\chi+1)\,H = 0$ et on constate que l'on a $\mathrm{dét}\,H = 1$. On peut donc appliquer la seconde partie de la proposition 4.6 : $\|H\|$ est divisible par 12. Comme l'on a *a priori* $\|H\| \leq 8$, on en déduit l'égalité $H = 0$, l'isomorphisme de représentations

$$(4.30)\qquad \chi\,\bar{\mathrm{r}}_{6,8} \;\simeq\; \bar{\mathrm{r}}_{8,8}$$

et la congruence (4.27) pour $p \neq 7$. Le cas $p = 7$ est laissé au lecteur.

Démonstration des congruences (15), (16), (17) et (18)

A nouveau, les démonstrations de ces congruences sont toutes du même type. Nous donnons quelques détails sur la démonstration des congruences (16) et nous bornons à indiquer les modifications essentielles à apporter à celle-ci pour avoir les démonstrations de (15), (17) et (18).

On fixe $\ell = 5$.

On considère le sous-ensemble $\mathcal{W} := \{\mathrm{v}_{10}, \mathrm{v}_{17}, \mathrm{v}_{19}, \mathrm{v}_{21}\}$ de $\mathcal{V}$; on vérifie que $\mathcal{W}$ est 5-lié minimal. On en déduit, toujours grâce à la proposition 4.5, que les quatre représentations $\overline{\rho}_{10}$, $\overline{\rho}_{17}$, $\overline{\rho}_{19}$ et $\overline{\rho}_{21}$ sont deux à deux isomorphes. L'isomorphisme $\overline{\rho}_{10} \simeq \overline{\rho}_{17}$ donne l'équation suivante dans A_5 :

$$\begin{aligned}(4.31)\qquad (\chi+1)\bar{\mathrm{r}}_{12,6} \;=\; & (\chi^3+\chi^2+\chi+1)\bar{\mathrm{r}}_{20} - (\chi^3+\chi^2)\bar{\mathrm{r}}_{18} \\ & + (\chi^3+\chi^2+\chi+1)\bar{\mathrm{r}}_{12} - 2\chi^3 - \chi^2 - 1 \qquad .\end{aligned}$$

Compte tenu de [Sw72], cette équation devient

$$(1+\chi)\bar{\mathrm{r}}_{12,6} \;=\; 2(1+\chi+\chi^2+\chi^3) \qquad . \tag{4.32}$$

Cette équation montre que la représentation (semi-simple) $(1\oplus\chi)\otimes\bar{\mathrm{r}}_{12,6}$ est somme directe de puissance de χ ; il en résulte qu'il en est de même pour $\bar{\mathrm{r}}_{12,6}$. On en déduit que l'on a dans A_5 une équation de la forme

$$\bar{\mathrm{r}}_{12,6} \;=\; a_0 + a_1\chi + a_2\chi^2 + a_3\chi^3 \tag{4.33}$$

avec a_k, $k=0,1,2,3$, des entiers vérifiant $a_k \geq 0$ et $a_0+a_1+a_2+a_3=1$. L'équation 4.32 peut être réécrite de la façon suivante :

$$(1+\chi)(\bar{\mathrm{r}}_{12,6} - (1+\chi+\chi^2+\chi^3)) \;=\; 0 \qquad ;$$

cette réécriture et le point (b) de la proposition 4.7 (prendre $S=\chi$) montrent qu'il existe un entier relatif n tel que l'on a

$$\bar{\mathrm{r}}_{12,6} \;=\; 1+\chi+\chi^2+\chi^3+n(1-\chi+\chi^2-\chi^3) \qquad .$$

Les inégalités $a_k \geq 0$ montrent que l'on a $|n| \leq 1$. Le calcul du déterminant des deux membres montre que l'on a $n \equiv 0 \bmod 2$. On a donc $n=0$ et un isomorphisme de représentations

$$\bar{\mathrm{r}}_{12,6} \;\simeq\; 1\oplus\chi\oplus\chi^2\oplus\chi^3 \qquad .$$

Cet isomorphisme implique la congruence $\tau_{12,6}(p) \equiv 1+p+p^2+p^3 \bmod 5$, ou ce qui revient au même $\tau_{12,6}(p) \equiv p^4+p^3+p^2+p \bmod 5$, pour $p \neq 5$. Le cas $p=5$ est laissé au lecteur.

Les isomorphismes $\overline{\rho}_{19} \simeq \overline{\rho}_{17}$ et $\overline{\rho}_{21} \simeq \overline{\rho}_{17}$ conduisent pareillement aux congruences $\tau_{6,8}(p) \equiv p^4+p^3+p^2+p \bmod 5$ et $\tau_{4,10}(p) \equiv p^4+p^3+p^2+p \bmod 5$. (On observera que l'isomorphisme $\overline{\rho}_{19} \simeq \overline{\rho}_{17}$ conduit naturellement à l'isomorphisme $\chi\bar{\mathrm{r}}_{6,8} \simeq 1\oplus\chi\oplus\chi^2\oplus\chi^3$ mais que l'on a $\chi^{-1}(1\oplus\chi\oplus\chi^2\oplus\chi^3) \cong 1\oplus\chi\oplus\chi^2\oplus\chi^3$.)

La congruence (15) s'obtient quant à elle en prenant par exemple $\mathcal{W} = \{\mathrm{v}_3, \mathrm{v}_{15}\}$.

Passons enfin aux congruences (17) et (18). On peut les démontrer en prenant $\ell = 2,3$, $m=6$ et $\mathcal{W} = \{\mathrm{v}_6,\mathrm{v}_{10}\},\{\mathrm{v}_6,\mathrm{v}_{15}\},\{\mathrm{v}_6,\mathrm{v}_{19}\},\{\mathrm{v}_6,\mathrm{v}_{21}\}$ dans la proposition 4.5.

On rappelle que quand le nombre premier ℓ est 2 ou 3 les isomorphismes de [Sw72] qui nous concernent prennent une forme particulièrement simple : $\bar{\mathrm{r}}_i \simeq 1\oplus 1$ pour $\ell=2$ et $\bar{\mathrm{r}}_i \simeq 1\oplus\chi$ pour $\ell=3$.

Pour $\ell = 2$, on obtient par les méthodes précédentes

$$\bar{\mathrm{r}}_{j,k} \simeq 1 \oplus 1 \oplus 1 \oplus 1 \quad . \tag{4.34}$$

Pour $\ell = 3$, on trouve que les représentations $\bar{\mathrm{r}}_{j,k}$ sont chacune isomorphe à l'une des trois représentations suivantes, $1 \oplus 1 \oplus 1 \oplus 1$, $1 \oplus 1 \oplus \chi \oplus \chi$ ou $\chi \oplus \chi \oplus \chi \oplus \chi$. On lève l'ambiguité en utilisant le fait que la représentation duale $\bar{\mathrm{r}}^*_{j,k}$ est isomorphe à la représentation $\chi \bar{\mathrm{r}}_{j,k}$ (voir le début de la remarque 1.6) :

$$\bar{\mathrm{r}}_{j,k} \simeq 1 \oplus 1 \oplus \chi \oplus \chi \quad . \tag{4.35}$$

Sur la décomposition en irréductibles des $\bar{\mathrm{r}}_{j,k;\ell}$

Comme nous venons de le voir, les congruences (12) et (14) du théorème 4.4 sont conséquences d'isomorphismes entre certaines représentations de la forme $\bar{\mathrm{r}}_{j,k;\ell}$ ou $\chi \otimes \bar{\mathrm{r}}_{j,k;\ell}$. Chacune des autres congruences de ce théorème, à l'exception de (2) et (10), est la manifestation d'une propriété de réductibilité d'une représentation $\bar{\mathrm{r}}_{j,k;\ell}$. La proposition 4.9 ci-dessous, sans doute bien connue, décrit de façon exhaustive les différentes possibilités pour une réduction d'une représentation de ce type ; elle explique en partie la structure des congruences que nous avons dégagées.

Soit ℓ un nombre premier. Soit κ un entier, on note $\mathrm{R}_{\kappa,\ell}$ l'ensemble (fini) des classes d'isomorphisme de représentations irréductibles $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ de la forme $\overline{\rho}_{\pi,\iota}$, où $\pi \in \Pi_{\mathrm{cusp}}(\mathrm{PGL}_2)$ est la représentation automorphe engendrée par un élément de $\mathrm{S}_\kappa(\mathrm{SL}_2(\mathbb{Z}))$ propre pour les opérateurs de Hecke. On rappelle que l'on note $\nu : \mathrm{GSp}_{2g} \to \mathbb{G}_{\mathrm{m}}$ l'homomorphisme "facteur de similitude" (voir §II.1). Enfin, si S est une $\overline{\mathbb{F}}_\ell$-représentation irréductible de dimension finie de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, on note $\mathrm{m}(S)$ le plus petit entier $m \geq 1$ tel que l'on a $\chi^m \otimes S \simeq S$ (on rappelle que l'on a posé $\chi = \overline{\omega_\ell}$) ; cette notation est en accord avec celle que l'on a introduite dans la proposition 4.7.

Proposition 4.9. *Soient ℓ un nombre premier impair et*

$$r : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_4(\overline{\mathbb{F}}_\ell)$$

une représentation semi-simple, continue, et non ramifiée hors de ℓ. Notons w l'élément de $\mathbb{Z}/(\ell-1)$ tel que l'on a $\nu \circ r = \chi^w$, et supposons $w \equiv 1 \bmod 2$.

Alors on est dans un, et un seul, des cas suivants :

(i) il existe a et b dans $\mathbb{Z}/(\ell-1)$ tels que l'on a $r \simeq \chi^a \oplus \chi^b \oplus \chi^{w-a} \oplus \chi^{w-b}$;

(ii) il existe $\kappa \leq \ell+1$, une représentation ρ dans $\mathrm{R}_{\kappa;\ell}$ et a, b dans $\mathbb{Z}/(\ell-1)$ avec $2a+\kappa-1 \equiv w \bmod \mathrm{m}(\rho)$, tels que l'on a $r \simeq (\chi^a \otimes \rho) \oplus \chi^b \oplus \chi^{w-b}$;

(iii)$_1$ il existe $\kappa \leq \ell+1$, une représentation ρ dans $\mathrm{R}_{\kappa,\ell}$ et a dans $\mathbb{Z}/(\ell-1)$ avec $2a+\kappa-1 \not\equiv w \bmod \mathrm{m}(\rho)$, tels que l'on a $r \simeq (\chi^a \oplus \chi^{w-a-\kappa+1}) \otimes \rho$;

(iii)$_2$ il existe une $\overline{\mathbb{F}}_\ell$-représentation ρ, irréductible de dimension 2, de déterminant $\det \rho = \chi^a$ avec $a \in 2\mathbb{Z}$ et $a \not\equiv w \bmod \mathrm{m}(\rho)$, telle que l'on a $r \simeq (1 \oplus \chi^{w-a}) \otimes \rho$;

(iv) pour $i = 1, 2$, il existe $\kappa_i \leq \ell+1$, une représentation ρ_i dans $\mathrm{R}_{\kappa_i;\ell}$ et a_i dans $\mathbb{Z}/(\ell-1)$ avec $2a_i+\kappa_i-1 \equiv w \bmod \mathrm{m}(\rho_i)$, tels que l'on a $r \simeq (\chi^{a_1} \otimes \rho_1) \oplus (\chi^{a_2} \otimes \rho_2)$;

(v) r est irréductible.

Démonstration. Soit V est une $\overline{\mathbb{F}}_\ell$-représentation de dimension finie de $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; on note $\mathrm{i}(V)$ la représentation $V^* \otimes \chi^w$. Il est clair que l'on $V \cong \mathrm{i}(\mathrm{i}(V))$, et que l'application $V \mapsto \mathrm{i}(V)$ définit une auto-équivalence, exacte et contravariante, de la catégorie des $\overline{\mathbb{F}}_\ell$-représentations de dimension finie de G. En particulier, l'ensemble fini $\mathrm{J}(r)$ des facteurs de Jordan-Hölder de la représentation r est stable par l'involution i.

Observons que les éléments de $\mathrm{J}(r)$ sont de dimension 1 ou 2. En effet, supposons $r \simeq V \oplus W$ avec V irréductible de dimension 3 (et W de dimension 1). La forme bilinéaire alternée non dégénérée dont est muni, par définition, le $\overline{\mathbb{F}}_\ell$-espace vectoriel sous-jacent à r, fournit un isomorphisme G-équivariant naturel $r \to \mathrm{i}(r)$ qui induit un isomorphisme $V \to \mathrm{i}(V)$. Il en résulte en particulier que la restriction à V de la forme bilinéaire alternée évoquée ci-dessus est non dégénérée ; ce qui est absurde car la dimension de V est impaire.

Comme nous l'avons déjà dit, le théorème de Kronecker-Weber assure que les seuls homomorphismes $G \to \overline{\mathbb{F}}_\ell^\times$, supposés continus et non ramifiés hors de ℓ, sont les puissances de χ. Comme les entiers ℓ et w sont impairs, on a $\mathrm{i}(\chi^a) = \chi^{w-a} \neq \chi^a$ pour tout a dans $\mathbb{Z}$, de sorte qu'aucune représentation de dimension 1 de G n'est "fixée" par i. En particulier, r est somme de 4 caractères si, et seulement si, nous sommes dans le cas (i) de l'énoncé.

Soit V une $\overline{\mathbb{F}}_\ell$-représentation irréductible de dimension 2 de G supposée continue et non ramifiée hors de ℓ. Rappelons que l'on dit que V est *impaire* si la classe de conjugaison de G constituée des conjugaisons complexes admet les valeurs propres 1 et -1 dans la représentation V. Il revient au même de

dire que $\det V = \chi^s$ avec $s \equiv 1 \bmod 2$. Si V est impaire, la conjecture de Serre "en niveau 1", démontrée par Khare [Kha06], assure qu'il existe a dans $\mathbb{Z}/(\ell-1)$, un entier $\kappa \leq \ell+1$ et une représentation ρ dans $\mathrm{R}_{\kappa;\ell}$, tels que l'on a $V \simeq \chi^a \otimes \rho$. L'égalité $\det \rho = \chi^{\kappa-1}$ montre de plus que l'on a $V \simeq \mathrm{i}(V)$ si et seulement si l'on a $2a+\kappa-1 \equiv w \bmod \mathrm{m}(\rho)$.

Supposons qu'il existe V dans $\mathrm{J}(r)$ de dimension 2 avec $\mathrm{i}(V) \not\simeq V$. Dans ce cas, on a $r \simeq V \oplus \mathrm{i}(V)$ et $\mathrm{i}(V) \simeq V \otimes \chi^w (\det V)^{-1}$. On est donc dans le cas $(\mathrm{iii})_1$ si V est impaire, et dans le cas $(\mathrm{iii})_2$ sinon. On observera que V est impaire si et seulement si $\mathrm{i}(V)$ l'est, de sorte que les cas $(\mathrm{iii})_1$ et $(\mathrm{iii})_2$ s'excluent mutuellement.

On peut donc supposer que toute représentation V de $\mathrm{J}(r)$ est soit de dimension 1, soit de dimension 2 avec $\mathrm{i}(V) \simeq V$. Notons que dans ce dernier cas, V est automatiquement impaire (car $w \equiv 1 \bmod 2$). D'après le théorème de Khare, V est donc de la forme $\chi^a \otimes \rho$ avec $\rho \in \mathrm{R}_{\kappa;\ell}$ et $\kappa \leq \ell+1$, et de plus $2a+\kappa-1 \equiv w \bmod \mathrm{m}(\rho)$. On est donc dans les cas (ii) et (iv), selon respectivement que $\mathrm{J}(r)$ contient une représentation de dimension 1 ou deux représentations de dimension 2. Dans le cas restant, r est irréductible. $\square$

Ce résultat et la table C.3 permettent en retour de démontrer l'inexistence de certaines congruences. Donnons quelques exemples pour terminer.

Proposition[⋆] **4.10.** *La représentation $\bar{\mathrm{r}}_{j,k;\ell}$ est irréductible (sur $\overline{\mathbb{F}}_\ell$) dans chacun des cas suivants :*

- $(j,k) = (6,8)$ *et* $\ell = 7, 13, 19$ *;*
- $(j,k) = (8,8)$ *et* $\ell = 7, 11, 19$ *;*
- $(j,k) = (12,6)$ *et* $\ell = 11, 17$ *;*
- $(j,k) = (4,10)$ *et* $\ell = 7, 13, 17$.

De plus, on a dans chacun de ces cas $\mathrm{m}(\bar{\mathrm{r}}_{j,k;\ell}) = \ell-1$*, sauf pour* $(j,k) = (6,8)$ *et* $\ell = 13$*, auquel cas on a simplement* $\mathrm{m}(\bar{\mathrm{r}}_{6,8;13}) \equiv 0 \bmod 6$.

Démonstration. La représentation $\bar{\mathrm{r}}_{j,k;\ell}$, vue sur $\overline{\mathbb{F}}_\ell$, satisfait les hypothèses de la proposition 4.9 (avec $w = j+2k-3$), d'après la remarque 1.6. Appliquant cette proposition, il s'agit donc d'exclure pour chacun des triplets (j,k,ℓ) de l'énoncé ci-dessus, la possibilité d'une décomposition de la forme (i) à (iv). La table C.3 est suffisamment fournie pour qu'il y ait plusieurs manières de procéder. Donnons quelques recettes simples :

Critère 1. *Si* $\bar{\mathrm{r}}_{j,k;\ell}$ *est dans l'un des cas (i), (ii),* $(iii)_1$ *et (iv), et si* p *est un nombre premier avec* $p \equiv 1 \bmod \ell$*, on a respectivement :*

– $\tau_{j,k}(p) \equiv 4 \bmod \ell$ *dans le cas (i) ;*

– $\tau_{j,k}(p) \equiv \tau_\kappa(p) + 2 \bmod \ell$ *dans le cas (ii) ;*

– $\tau_{j,k}(p) \equiv 2\tau_\kappa(p) \bmod \ell$ *dans le cas* $(iii)_1$ *;*

– *et* $\tau_{j,k}(p) \equiv \tau_{\kappa_1}(p) + \tau_{\kappa_2}(p) \bmod \ell$ *dans le cas (iv).*

Critère 2. *Si* $\bar{\mathrm{r}}_{j,k;\ell}$ *est dans le cas* $(iii)_2$*, alors* $\tau_{j,k}(p) \equiv 0 \bmod \ell$ *pour tout nombre premier* p *avec* $p \equiv -1 \bmod \ell$*.*

– Supposons d'abord $\ell = 7$. On a $\mathrm{S}_\kappa(\mathrm{SL}_2(\mathbb{Z})) = 0$ pour tout $\kappa \leq \ell + 1$, puis $\mathrm{R}_{\kappa,7} = \emptyset$ pour $\kappa \leq 8$. Il suffit donc d'éliminer les cas (i) et $(\mathrm{iii})_2$. On a $29 \equiv 1 \bmod 7$ et l'on tire de la table C.3 les congruences

$$\tau_{6,8}(29) \equiv \tau_{4,10}(29) \equiv \tau_{8,8}(29) \equiv 0 \bmod 7 \qquad ,$$

ce qui élimine le cas (i) par le critère 1. On élimine de même le cas $(\mathrm{iii})_2$ à l'aide du critère 2 : on a $13 \equiv -1 \bmod 7$, $\tau_{6,8}(13) \equiv 6 \bmod 7$ et $\tau_{4,10}(13) \equiv \tau_{8,8}(13) \equiv 1 \bmod 7$.

– Supposons $\ell = 11$. On élimine les cas (i) et $(\mathrm{iii})_2$ comme précédemment, en observant que l'on a $23 \equiv 1 \bmod 11$ et $\tau_{8,8}(23) \equiv \tau_{12,6}(23) \equiv 0 \bmod 11$, puis $43 \equiv -1 \bmod 11$ et $\tau_{8,8}(43) \equiv \tau_{12,6}(43) \equiv 6 \bmod 11$. L'unique entier $\kappa \leq \ell+1$ tel que $\mathrm{S}_\kappa(\mathrm{SL}_2(\mathbb{Z})) \neq 0$ est $\kappa = 12$, et l'on a $\tau_{12}(23) \equiv -1 \bmod 11$. On conclut à l'irréductibilité de $\bar{\mathrm{r}}_{j,k;11}$ pour $(j,k) = (8,8)$ et $(12,6)$ en observant $\tau_{j,k}(23) \not\equiv 1, -2 \bmod 11$ (critère 1).

– Le cas $\ell = 13$ est similaire car $\mathrm{S}_{14}(\mathrm{SL}_2(\mathbb{Z})) = 0$. Le critère 1 s'applique car $53 \equiv 1 \bmod 13$, $\tau_{12}(53) \equiv -3 \bmod 13$ et $\tau_{6,8}(53) \equiv \tau_{4,10}(53) \equiv 3 \bmod 13$. Le critère 2 s'applique aussi car $103 \equiv -1 \bmod 13$, $\tau_{6,8}(103) \equiv 11 \bmod 13$ et $\tau_{4,10}(103) \equiv 5 \bmod 13$.

– Dans le cas $\ell = 17$, on conclut encore par les critères 1 et 2 grâce aux congruences suivantes : $103 \equiv 1 \bmod 17$, $\tau_{12}(103) \equiv 2 \bmod 17$, $\tau_{16}(103) \equiv 6 \bmod 17$, $\tau_{18}(103) \equiv 8 \bmod 17$, $\tau_{4,10}(103) \equiv \tau_{12,6}(103) \equiv 1 \bmod 17$, et $67 \equiv -1 \bmod 17$, $\tau_{4,10}(67) \equiv 8 \bmod 67$ et $\tau_{12,6}(67) \equiv 12 \bmod 67$.

– Dans le cas $\ell = 19$, le plus petit nombre premier $\equiv 1 \bmod 19$ est $191 > 113$, qui est en dehors de la table C.3. En revanche, le critère 2 élimine encore le cas $(\mathrm{iii})_2$ car on a $37 \equiv -1 \bmod 19$, $\tau_{6,8}(37) \equiv 4 \bmod 19$ et $\tau_{8,8}(37) \equiv 8 \bmod 19$. Dégageons un autre critère. Celui-ci est basé sur l'observation suivante : pour

$\ell \leq 19$, si $\bar{\mathrm{r}}_{j,k;\ell}$ n'est pas dans le cas $(\mathrm{iii})_2$, alors tous ses facteurs de Jordan-Hölder sont définis sur $\mathbb{F}_\ell$. Cela résulte en effet de la proposition 4.9 et du fait que $\dim \mathrm{S}_\kappa(\mathrm{SL}_2(\mathbb{Z})) \leq 1$ pour $\kappa \leq \ell + 1 \leq 20$.

Critère 3. *Supposons que l'on a $\ell \leq 19$ et que $\bar{\mathrm{r}}_{j,k;\ell}$ n'est pas dans le cas $(\mathrm{iii})_2$. Supposons de plus qu'il existe un nombre premier $p \neq \ell$ tel que le polynôme $\mathrm{P}_p(t) := \mathrm{dét}(t - \mathrm{r}_{j,k;\ell}(\mathrm{Frob}_p))$ de $\mathbb{Z}[t]$ soit irréductible modulo ℓ. Alors la représentation $\bar{\mathrm{r}}_{j,k;\ell}$ est irréductible.*

Comme nous avons déterminé les $\tau_{j,k}(p)$ pour $p \leq 113$ (table C.3) et les $\tau_{j,k}(p^2)$ pour $p \leq 29$ (table C.4), la formule (1.3) montre que nous disposons des polynômes $\mathrm{P}_p(t)$ pour $p \leq 29$; dans le cas $\ell = 19$, le critère ci-dessus est vérifié, pour $(j,k) = (6,8)$ et $p = 3$, pour $(j,k) = (8,8)$ et $p = 13$.

Il ne reste plus qu'à justifier la dernière assertion de la proposition 4.10 portant sur les $\mathrm{m}(\bar{\mathrm{r}}_{j,k;\ell})$. On utilise l'observation suivante : soit $p \neq \ell$ un nombre premier avec $\tau_{j,k}(p) \not\equiv 0 \bmod \ell$, alors $\mathrm{m}(\bar{\mathrm{r}}_{j,k;\ell})$ est divisible par l'ordre de p dans $(\mathbb{Z}/\ell)^\times$.

Par exemple, le nombre premier 3 engendre $(\mathbb{Z}/7)^\times$ et on vérifie les congruences $3\tau_{6,8}(3) \equiv \tau_{4,10}(3) \equiv \tau_{8,8}(3) \equiv 4 \bmod 7$. Ceci montre $\mathrm{m}(\bar{r}_{6,8;7}) = \mathrm{m}(\bar{r}_{8,8;7}) = \mathrm{m}(\bar{\mathrm{r}}_{4,10;7}) = 6$. Les autres cas sont similaires. Pour $\ell = 13$, on utilise que le nombre premier 2 engendre $(\mathbb{Z}/\ell)^\times$, et la congruence $\tau_{4,10}(2) \equiv 10 \bmod 13$, de sorte que l'on a $\mathrm{m}(\bar{r}_{4,10;13}) = 12$. En revanche, on a $\tau_{6,8}(2) \equiv 0 \bmod 13$. On montre $\mathrm{m}(\bar{\mathrm{r}}_{6,8;13}) \equiv 0 \bmod 6$ à l'aide de la congruence $\tau_{6,8}(17) \equiv 7 \bmod 13$. □

Il est évident que les méthodes *ad hoc* employées ci-dessus sont assez grossières, et qu'il est possible d'étudier les décompositions éventuelles des représentations $\bar{\mathrm{r}}_{j,k;\ell}$ pour des caractéristiques $\ell > 19$. Nous reportons cette étude, ainsi que la question plus intéressante de déterminer les images des $\bar{\mathrm{r}}_{j,k;\ell}$, à un travail ultérieur. Pour nous autocongratuler, observons que les triplets $(j,k;\ell)$ intervenant dans l'énoncé de la proposition 4.10 sont exactement ceux n'intervenant pas dans l'énoncé du théorème 4.4, lorsque l'on a $\ell \leq 19$.

Remarque 4.11. Supposons que $\bar{\mathrm{r}}_{j,k;\ell}$ est irréductible sur $\overline{\mathbb{F}}_\ell$ (et donc, en particulier, que l'on a $\ell > 5$). Les assertions suivantes sont équivalentes :

(i) pour tout premier p non carré modulo ℓ, on a $\tau_{j,k}(p) \equiv 0 \bmod \ell$;

(ii) $\mathrm{m}(\bar{\mathrm{r}}_{j,k;\ell})$ divise $\frac{\ell-1}{2}$;

(iii) $\bar{r}_{j,k;\ell}$ est induite d'une représentation irréductible de dimension 2, à coefficients dans $\mathbb{F}_{\ell^2}$, du groupe de Galois absolu de $\mathbb{Q}(\sqrt{\ell^*})$ avec $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$.

Dans le cas $(j,k) = (6,8)$ et $\ell = 13$, une inspection de la table C.3 montre que la congruence de l'assertion (i) vaut pour tout premier $p \leq 113$. Il est tentant de conjecturer qu'elle est toujours satisfaite, autrement dit que l'on a $\mathrm{m}(\overline{r}_{6,8;13}) = 6$.

A. Le réseau de Barnes-Wall et les séries thêta de Siegel des réseaux unimodulaires pairs de dimension 16

(d'après Martin Kneser [Kn67])

Le réseau en question est un remarquable réseau de dimension 16 découvert par Barnes et Wall en 1959 [BW59]. Il apparaît à de nombreuses reprises dans [CS99] où il est noté Λ_{16} ou BW_{16} (Conway et Sloane mentionnent malicieusement qu'il a été redécouvert par beaucoup d'auteurs). Barnes et Wall définissent en fait dans [BW59] une suite de réseaux $(\Lambda_{2^n})_{n\in\mathbb{N}-\{0\}}$, Λ_{2^n} étant de dimension 2^n ; les trois premiers réseaux de cette suite sont respectivement isomorphes à I_2, D_4 et E_8. Pour une présentation simple et élégante des réseaux de Barnes-Wall nous conseillons [NRS01] et [NRS02], on pourra également consulter [BE73] ; le réseau U qui apparaît dans la référence [Kn67] est un avatar de Λ_{16}. La définition de Λ_{16} que nous donnons ci-après suffira à notre bonheur.

Soit I un lagrangien du q-espace vectoriel $\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8$ (on a donc $\mathrm{q}(I) = 0$ et $\dim_{\mathbb{F}_2} I = 4$) . On note Λ_{16} le sous-module de $\mathrm{E}_8 \oplus \mathrm{E}_8$ constitué des couples (x_1, x_2) d'éléments de E_8 dont les réductions modulo 2, disons $\bar{x}_1$ et $\bar{x}_2$, vérifient $\bar{x}_1 + \bar{x}_2 \in I$; Λ_{16} peut donc être vu comme un réseau entier (au sens quadratique) dans $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathrm{E}_8 \oplus \mathrm{E}_8)$.

Proposition A.1. *Le réseau Λ_{16} vérifie les propriétés suivantes :*
(a) *On a $\mathrm{q}(x) \geq 2$ (ou encore $x.x \geq 4$) pour tout x dans $\Lambda_{16} - \{0\}$.*
(b) *On a $\xi.\xi \in \mathbb{Z}$ pour tout ξ dans le réseau dual $\Lambda_{16}^\sharp$ et $\Lambda_{16}^\sharp$ muni de la forme quadratique $\xi \mapsto \xi.\xi$ est isomorphe (comme $\widetilde{\mathrm{q}}$-module) à Λ_{16}.*
(c) *Le module sous-jacent au* qe-*module* $\operatorname{rés}\Lambda_{16}$ *est annulé par* 2 *et le* qe-*module* $\operatorname{rés}\Lambda_{16}$ *est isomorphe, via le plongement canonique de $\mathbb{F}_2$ dans $\mathbb{Q}/\mathbb{Z}$, au $\mathbb{F}_2$-q-espace vectoriel hyperbolique* $\mathrm{H}(I)$.

Démonstration de (a). Soit $x = (x_1, x_2)$ un élément de $\Lambda_{16} - \{0\}$. Si x_1 et x_2 sont non nuls alors on a $\mathrm{q}(x) = \mathrm{q}(x_1) + \mathrm{q}(x_2) \geq 1 + 1$. Si x_i est nul alors x_{3-i} appartient à I (et est non nul) et $\mathrm{q}(x_{3-i})$ est pair.

Démonstration de (b). On constate que le réseau $\Lambda_{16}^\sharp$ est le sous-module de $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathrm{E}_8 \oplus \mathrm{E}_8)$ constitué des éléments $\xi = (\xi_1, \xi_2)$ tels que $(\xi_1 + \xi_2, \xi_1 - \xi_2)$ appartient à Λ_{16}. Or on a l'identité $\mathrm{q}(\xi_1 + \xi_2) + \mathrm{q}(\xi_1 - \xi_2) = 2(\mathrm{q}(\xi_1) + \mathrm{q}(\xi_2))$.

Démonstration de (c). Soit ΔI le sous-espace vectoriel de $\mathbb{F}_2 \otimes_{\mathbb{Z}} (\mathrm{E}_8 \oplus \mathrm{E}_8) = (\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8) \oplus (\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathrm{E}_8)$ image diagonale de I ; on observe que Λ_{16} est le sous-module de $\mathrm{E}_8 \oplus \mathrm{E}_8$ image réciproque de $(\Delta I)^\perp$ par l'homomorphisme $\mathrm{E}_8 \oplus \mathrm{E}_8 \to \mathbb{F}_2 \otimes_{\mathbb{Z}} (\mathrm{E}_8 \oplus \mathrm{E}_8)$. Cette observation faite, la propriété (c) est une manifestation du phénomène général décrit ci-dessous.

Soit L un q-module sur $\mathbb{Z}$. Soient p un nombre premier et J un sous-espace vectoriel de $\mathbb{F}_p \otimes_{\mathbb{Z}} L$ avec $\mathrm{q}(J) = 0$; soit M le sous-module de L constitué des éléments dont la réduction modulo p est orthogonale à J. Alors le groupe abélien $\operatorname{rés} M$ est annulé par p et le qe-module $\operatorname{rés} M$ est isomorphe, *via* le plongement canonique de $\mathbb{F}_p$ dans $\mathbb{Q}/\mathbb{Z}$, au $\mathbb{F}_p$-q-espace vectoriel hyperbolique $\mathrm{H}(J)$ ($\cong \mathrm{H}(J^*) \cong \mathrm{H}(L/M)$). □

Corollaire A.2. *On a $\xi.\xi \geq 2$ pour tout ξ dans $\Lambda_{16}^\sharp - \{0\}$.*

On explique maintenant comment déduire des propriétés du réseau Λ_{16}, en suivant la stratégie de Kneser, l'égalité des séries thêta

$$\vartheta^{(g)}_{\mathrm{E}_8 \oplus \mathrm{E}_8} = \vartheta^{(g)}_{\mathrm{E}_{16}}$$

pour $g \leq 3$ (résultat dû à Witt pour $g \leq 2$ [Wit41].

Cette égalité peut être reformulée en termes de représentations de formes quadratiques entières par $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16}. Précisons la terminologie. Soient L un réseau unimodulaire pair et G un $\mathbb{Z}$-module libre de dimension finie muni d'une forme quadratique à valeurs entières (compte tenu de ce qui va suivre, on peut supposer que ces valeurs sont positives ou nulles) ; une *représentation* de G par L est un homomorphisme $f : G \to L$ avec $\mathrm{q}(f(x)) = \mathrm{q}(x)$ pour tout x dans G. On note $\mathrm{Rep}(G, L)$ l'ensemble des représentations de G par L ; il est clair que cet ensemble est fini. Voici la reformulation promise :

Théorème A.3. *Soit G un $\mathbb{Z}$-module libre de dimension finie muni d'une forme quadratique à valeurs entières. S l'on a $\dim G \leq 3$ alors les ensembles $\mathrm{Rep}(G, \mathrm{E}_8 \oplus \mathrm{E}_8)$ et $\mathrm{Rep}(G, \mathrm{E}_{16})$ ont même cardinal.*

Démonstration. Le point-clé est l'observation ci-après.

Soit $\gamma : \Lambda_{16}^\sharp \to \operatorname{rés} \Lambda_{16}$ l'homomorphisme de passage au quotient. On note $\mathcal{I}$ l'ensemble (fini) des lagrangiens de $\operatorname{rés} \Lambda_{16}$ et $\mathcal{L}$ l'ensemble des réseaux unimodulaires pairs contenant Λ_{16} (et contenus dans $\Lambda_{16}^\sharp$) ; on rappelle que l'application $\mathcal{I} \to \mathcal{L}$, $I \mapsto \gamma^{-1}(I)$ est une bijection (compatible avec les relations d'inclusion).

Soit J un sous-module de $\operatorname{rés}\Lambda_{16}$ avec $\mathrm{q}(J) = 0$ et $\dim_{\mathbb{F}_2} J = 3$. Soit M le réseau $\gamma^{-1}(J)$; on a $\operatorname{rés} M \cong J^{\perp}/J \simeq \mathrm{H}(\mathbb{Z}/2)$ (voir II.1.1). Soit B le réseau image réciproque, par l'homomorphisme $M^{\sharp} \to \operatorname{rés} M$, de la "droite" non isotrope (non isotrope au sens quadratique mais isotrope au sens bilinéaire) ; B est un réseau unimodulaire impair (voir la discussion "2-voisins, le point de vue de Borcherds" qui suit III.1.8). Comme B est contenu dans $\Lambda_{16}^{\sharp}$, le corollaire A.2 implique que l'on a $x.x \geq 2$ pour tout x dans $B - \{0\}$. Le scholie III.3.3.2 montre enfin que B est isomorphe à Bor_{16} (définition III.3.3.2) et que les deux réseaux unimodulaires pairs, images réciproques des deux "droites" isotropes de $\operatorname{rés} M$, sont non isomorphes (on observera incidemment que ce scholie montre aussi que la classe d'isomorphisme de M est indépendante du choix de J).

L'observation ci-dessus conduit au lemme ci-dessous. On appelle encore représentation de G par $\Lambda_{16}^{\sharp}$ un homomorphisme $f : G \to \Lambda_{16}^{\sharp}$ avec $\mathrm{q}(f(x)) = \mathrm{q}(x)$ pour tout x dans G.

Lemme A.4. *Soit f une représentation de G par $\Lambda_{16}^{\sharp}$ avec $\dim G \leq 3$. Soit $\mathcal{L}(f)$ le sous-ensemble de $\mathcal{L}$ constitué des réseaux L contenant $f(G)$; soient $\mathcal{L}_1(f)$ et $\mathcal{L}_2(f)$ les sous-ensembles de $\mathcal{L}(f)$ constitués des réseaux L respectivement isomorphes à $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16}. Alors $\mathcal{L}_1(f)$ et $\mathcal{L}_2(f)$ ont même cardinal.*

Démonstration. On note $\mathcal{I}(f)$, $\mathcal{I}_1(f)$ et $\mathcal{I}_2(f)$ les sous-ensembles de $\mathcal{I}$ images des sous-ensembles $\mathcal{L}(f)$, $\mathcal{L}_1(f)$ et $\mathcal{L}_2(f)$ de $\mathcal{L}$ par la bijection inverse de la bijection $I \mapsto \gamma^{-1}(I)$. On note $\mathcal{J}$ l'ensemble des J considérés plus haut et $\mathcal{J}(f)$ le sous-ensemble de $\mathcal{J}$ constitué des J avec $J \supset (\gamma \circ f)(G)$. On note $\mathcal{K}(f)$ (resp. $\mathcal{K}_1(f)$, resp. $\mathcal{K}_2(f)$) le sous-ensemble de $\mathcal{I}(f) \times \mathcal{J}(f)$ (resp. $\mathcal{I}_1(f) \times \mathcal{J}(f)$, resp. $\mathcal{I}_2(f) \times \mathcal{J}(f)$) constitué des couples (I, J) avec $I \supset J$. On note enfin $\pi_{\mathcal{J}} : \mathcal{K}(f) \to \mathcal{J}(f)$ et $\pi_{\mathcal{I}} : \mathcal{K}(f) \to \mathcal{I}(f)$ les applications $(I, J) \mapsto J$ et $(I, J) \mapsto I$. Il est clair que $\pi_{\mathcal{J}}$ est surjective et que ses fibres ont toutes 2 éléments. Pareillement $\pi_{\mathcal{I}}$ est surjective et ses fibres ont toutes $2^{(4-\delta(f))} - 1$ éléments, $\delta(f) \leq 3$ désignant la dimension du $\mathbb{F}_2$-espace vectoriel $(\gamma \circ f)(G)$. Compte tenu de ce qui précède, les applications $\mathcal{K}_1(f) \to \mathcal{J}(f)$ et $\mathcal{K}_2(f) \to \mathcal{J}(f)$, induites par $\pi_{\mathcal{J}}$, sont toujours surjectives. Comme l'on a $|\mathcal{K}_1(f)| + |\mathcal{K}_2(f)| = |\mathcal{K}(f)| = 2|\mathcal{J}(f)|$ (la notation $|-|$ désigne ici le cardinal d'un ensemble fini), on voit que l'on a $|\mathcal{K}_1(f)| = |\mathcal{J}(f)|$ et $|\mathcal{K}_2(f)| = |\mathcal{J}(f)|$. Par définition on a $\mathcal{K}_1(f) = \pi_I^{-1}(\mathcal{I}_1(f))$ et $\mathcal{K}_2(f) = \pi_I^{-1}(\mathcal{I}_2(f))$, d'où l'égalité $|\mathcal{I}_1(f)| = |\mathcal{I}_2(f)|$. $\square$

Fin de la démonstration du théorème. On note $\mathcal{L}_1$ et $\mathcal{L}_2$ les sous-ensembles de $\mathcal{L}$ constitués des réseaux respectivement isomorphes à $\mathrm{E}_8 \oplus \mathrm{E}_8$ et E_{16} ; on observe que l'on a $\mathcal{L}_1 = \mathcal{L}_1(0)$, $\mathcal{L}_2 = \mathcal{L}_2(0)$ (0 désignant l'unique représentation

de 0 par $\Lambda_{16}^{\sharp}$) et donc $|\mathcal{L}_1| = |\mathcal{L}_2|$. On note encore $\mathrm{Rep}(G, \Lambda_{16}^{\sharp})$ l'ensemble (fini) des représentations de G par $\Lambda_{16}^{\sharp}$, on pose $\mathrm{r}_1(G) = |\mathrm{Rep}(G, \mathrm{E}_8 \oplus \mathrm{E}_8)|$, $\mathrm{r}_2(G) = |\mathrm{Rep}(G, \mathrm{E}_{16})|$ et l'on considère les sous-ensembles de $\mathcal{L}_i \times \mathrm{Rep}(G, \Lambda_{16}^{\sharp})$, disons $\mathcal{R}_i(G)$ $(i = 1, 2)$, constitués des couples (L, f) avec $L \supset f(G)$. En projetant sur chacun des deux facteurs du produit $\mathcal{L}_i \times \mathrm{Rep}(G, \Lambda_{16}^{\sharp})$, on constate que l'on a

$$|\mathcal{R}_i(G)| = |\mathcal{L}_i|\, \mathrm{r}_i(G) \qquad \text{et} \qquad |\mathcal{R}_i(G)| = \sum_{f \in \mathrm{Rep}(G, \Lambda_{16}^{\sharp})} |\mathcal{L}_i(f)| \qquad .$$

Le lemme A.4 implique bien l'égalité $\mathrm{r}_1(G) = \mathrm{r}_2(G)$. □□

B. Formes quadratiques et voisins en dimension impaire

On présente dans cet appendice le pendant , “en dimension impaire”, d'une partie de la théorie que nous avons développée, “en dimension paire”, dans les chapitres II et III.

1. Généralités concernant les formes quadratiques sur un module projectif de rang constant impair

Soit A un anneau commutatif unitaire. Au chapitre II, nous avons défini un q-module sur A comme un A-module projectif de type fini L muni d'une forme quadratique $\mathrm{q} : L \to A$ telle que la forme bilinéaire symétrique associée est non dégénéré. Si 2 est non inversible dans A et si L est de rang constant, alors cette non dégénéréscence force ce rang à être pair (considérer un homomorphisme de A dans un corps k de caractéristique 2 et observer que la forme bilinéaire symétrique associée à la forme quadratique dont $k \otimes_A L$ est muni, est alternée). Si L est de rang constant impair il est classique de dire que q est non dégénérée si la dégénérescence de la forme bilinéaire symétrique associée est “minimale”. Nous précisons cette définion ci-après. Notre présentation met en avant la notion de demi-déterminant (voir par exemple [Knu88]) ; pour une présentation plus sophistiquée voir [SGA7, Exposé XII].

Soit $k \geq 1$ un entier ; on note respectivement

$$\psi_L^k : \Lambda^k L \to \Lambda^{k-1} L \otimes L \qquad , \qquad \phi_L^k : \Lambda^{k-1} L \otimes L \to \Lambda^k L$$

les homomorphismes “coproduit” et “produit” induits par la structure d'algèbre de Hopf de l'algèbre extérieure ΛL (les produits tensoriels et l'algèbre extérieure sont sur A).

Lemme 1.1. *Soit L un A-module muni d'une forme quadratique $q : L \to A$; soit $b : L \times L \to A$ la forme bilinéaire symétrique associée. La forme bilinéaire symétrique associée à la forme quadratique $(\Lambda^{k-1} b \otimes q) \circ \psi_L$ est $k \Lambda^k b$.*

Démonstration. Elle résulte de ce que l'homomorphisme composé $\phi_L^k \circ \psi_L^k$ est k-fois l'identité de $\Lambda^k L$. $\square$

Soit β une forme bilinéaire symétrique, on note $\mathrm{qd}(\beta)$ la forme quadratique $x \mapsto \beta(x,x)$; on observe que la forme bilinéaire qui lui est associée est 2β.

La démonstration des énoncés 1.2, 1.3 et 1.4 ci-après est immédiate.

Proposition-Définition 1.2 (puissances extérieures impaires d'une forme quadratique)**.** *Soient L un A-module muni d'une forme quadratique q et k un entier impair. On pose*

$$\Lambda^k q = (\Lambda^{k-1} b \otimes q) \circ \psi_L^k - \frac{k-1}{2}\,\mathrm{qd}\,(\Lambda^k b) \qquad ,$$

b désignant la forme bilinéaire symétrique associée à q ($\Lambda^k q$ est donc une forme quadratique sur $\Lambda^k L$).

La forme bilinéaire symétrique associée à $\Lambda^k q$ est $\Lambda^k b$. On appelle $\Lambda^k q$ la k-ième puissance extérieure *de q.*

Proposition 1.3. *Soit L un A-module projectif de type fini. Soit $\mathcal{B}(L)$ (resp. $\mathcal{Q}(L)$) le A-module constitué des formes bilinéaires symétriques $L \times L \to A$ (resp. des formes quadratiques $L \to A$). Si L est de rang 1 alors l'homomorphisme de A-modules* $\mathrm{qd} : \mathcal{B}(L) \to \mathcal{Q}(L)$ *est un isomorphisme.*

Proposition-Définition 1.4. *Soit L un A-module projectif de type fini de rang constant impair, disons n, muni d'une forme quadratique q ; on note b la forme bilinéaire symétrique associée à q. Les deux formes bilinéaires symétriques $\Lambda^n b$ et $\mathrm{qd}^{-1}(\Lambda^n q)$, dont le A-module $\Lambda^n L$, projectif de rang 1, est muni, sont reliées par l'égalité*

$$\Lambda^n b \;=\; 2\,\mathrm{qd}^{-1}(\Lambda^n q) \qquad .$$

La forme bilinéaire symétrique $\mathrm{qd}^{-1}(\Lambda^n q)$ (ou le A-module projectif $\Lambda^n L$ muni de cette forme) s'appelle le demi-déterminant *de q (on rappelle que la forme bilinéaire symétrique $\Lambda^n b$ s'appelle le déterminant de b, voir II.1). Le demi-déterminant de q est noté $\frac{1}{2}$-$\mathrm{dét}\, q$ ou $\frac{1}{2}$-$\mathrm{dét}\, L$.*

(La terminologie et la notation sont évidemment justifiées par le fait que l'on a $\mathrm{dét}\, L = 2\,(\frac{1}{2}\text{-}\,\mathrm{dét}\, L)$!).

Exemple. Soit a un élément de A. On rappelle que l'on note $\langle a \rangle$ le A-module A muni de la forme bilinéaire symétrique $(x,y) \mapsto axy$; on note donc $\mathrm{qd}(\langle a \rangle)$ le A-module A muni de la forme quadratique $x \mapsto ax^2$. Nous avons tout fait pour que le demi-déterminant de $\mathrm{qd}(\langle a \rangle)$ soit $\langle a \rangle$.

Proposition 1.5. *Soient P et L deux A-modules projectifs de type fini, respectivement de rang constant pair et impair, munis de forme quadratique. On a un isomorphisme canonique de A-modules projectifs de rang* 1 *munis de forme bilinéaire symétrique*

$$\tfrac{1}{2}\text{-}\operatorname{dét}(P \oplus L) \;\cong\; \operatorname{dét} P \otimes \tfrac{1}{2}\text{-}\operatorname{dét} L \qquad .$$

Démonstration. Soient respectivement q_P, b_P, q_L, b_L les formes quadratiques et bilinéaires dont P et L sont munis ; soit m le rang de P et n celui de L. Il faut montrer que l'on a $\Lambda^{m+n}(q_P \oplus q_L) = \Lambda^m b_P \otimes \Lambda^n q_L$. En utilisant la naturalité des puissances extérieures des formes bilinéaires (resp. puissances extérieures impaires des formes quadratiques) on se ramène au "cas universel". Dans ce cas l'anneau A est un anneau de polynômes, à coefficients dans $\mathbb{Z}$, en $\frac{m(m+1)}{2} + \frac{n(n+1)}{2}$ indéterminées, et 2 n'est pas diviseur de 0 ; or on sait que l'on a $\operatorname{dét}(P \oplus L) \cong \operatorname{dét} P \otimes \operatorname{dét} L$. □

Définition 1.6. *Soit L un A-module projectif de type fini de rang constant impair muni d'une forme quadratique q. Nous dirons que q est* minimalement dégénérée *si la forme bilinéaire symétrique $\frac{1}{2}\text{-}\operatorname{dét} q$ est non dégénérée. Pour faire court un A-module projectif de type fini de rang constant impair muni d'une forme quadratique minimalement dégénérée, sera appelé un* q-i-module *sur A.*

Exemple-Remarque. Soient A un anneau, P un q-module sur A de rang constant pair et u un élément de $A^\times$. La proposition 1.5 montre que la somme orthogonale $P \oplus \operatorname{qd}(\langle u \rangle)$ est un q-i-module sur A. La proposition 1.2 de [SGA7, Exposé XII] dit que, localement pour la topologie étale, tout q-i-module est de ce type avec en outre P hyperbolique.

Groupes classiques (suite)

Soit L un q-i-module sur A, disons de rang n ; comme au chapitre II, un endomorphisme α du A-module sous-jacent à L est dit *orthogonal* s'il préserve la forme quadratique. La naturalité des puissances extérieures des formes quadratiques montre que $\Lambda^n\alpha$ est un endomorphisme orthogonal du b-module $\frac{1}{2}\text{-}\operatorname{dét} L$ et donc que les endomorphismes $\Lambda^n\alpha$ et α sont des automorphismes. Les endomorphismes orthogonaux forment un groupe pour la composition que l'on appelle le *groupe orthogonal* de L et que l'on note $\mathrm{O}(L)$. Le foncteur $R \mapsto \mathrm{O}(R \otimes_A L)$, défini sur la catégorie des A-algèbres commutatives et à valeurs dans la catégorie des groupes, est un A-schéma en groupes que l'on note O_L. Compte tenu de ce l'on a vu plus haut, l'homomorphisme composé

$\mathrm{O}_L \to \mathrm{GL}_L \overset{\text{dét}}{\to} \mathbb{G}_{\mathrm{m}}$, induit un homomorphisme dét : $\mathrm{O}_L \to \mu_2$ (observer que $\mathrm{O}_{\frac{1}{2}\text{-dét}\,L}$ s'identifie à μ_2). On note SO_L le noyau de ce dernier homomorphisme.

Si L est de rang 1, alors le groupe O_L s'identifie encore μ_2, si bien que l'on ne peut espérer que O_L soit lisse sur A, en toute généralité. C'est cependant le cas pour SO_L :

Proposition 1.7. *Pour tout* q-i-*module L sur un anneau A, le A-schéma en groupes SO_L est lisse sur A.*

Démonstration. Puisque la propriété que l'on veut vérifier est locale pour la topologie étale, on peut supposer, d'après la proposition 1.2 de [SGA7, Exposé XII] déjà citée plus haut, que l'on a $L = \mathrm{H}(A^n) \oplus \mathrm{qd}(\langle u \rangle)$ avec u dans $A^\times$. Comme les deux q-modules $\mathrm{H}(A^n)$ et $\langle u \rangle \otimes \mathrm{H}(A^n)$ sont isomorphes on peut supposer en outre $u = 1$ et donc au bout du compte $A = \mathbb{Z}$ et $L = \mathrm{H}(\mathbb{Z}^n) \oplus \mathrm{A}_1$; le groupe SO_L est alors le groupe que l'on a noté $\mathrm{SO}_{n+1,n}$ en VIII.1. Le fait que $\mathrm{SO}_{n+1,n}$ est lisse sur $\mathbb{Z}$ est bien connu. Nous montrons ci-après que cette propriété peut être vue comme une conséquence de II.1.5 ; cette démonstration (très indirecte !) est dans l'esprit du paragraphe 2.

On pose $P = \mathrm{H}(\mathbb{Z}^n) \oplus \mathrm{H}(\mathbb{Z})$. On note (e_1, e_2) la base canonique facteur $\mathrm{H}(\mathbb{Z})$ et on pose $e = e_1 + e_2$ et $f = e_1 - e_2$; on a donc $\mathrm{q}(e) = 1$, $\mathrm{q}(f) = -1$ et $e.f = 0$. On constate que L s'identifie (avec sa forme quadratique) à l'orthogonal de f.

Soit $\mathcal{C}$ la quadrique affine d'équation $\mathrm{q} = -1$; on observe que ce $\mathbb{Z}$-schéma est lisse sur $\mathbb{Z}$. On note $\mathrm{O}_{P,f}$ le sous-groupe du groupe O_P (qui est lisse sur $\mathbb{Z}$ d'après II.1.5), stabilisateur de f, pour l'action évidente de O_P sur $\mathcal{C}$; le "calcul différentiel" montre que le groupe $\mathrm{O}_{P,f}$ est lisse sur $\mathbb{Z}$. L'égalité $L = f^\perp$ fournit un homomorphisme de schémas en groupes, disons $\omega : \mathrm{O}_{P,f} \to \mathrm{O}_L$. Les énoncés 1.8 et 1.9 ci-après concernent cet homomorphisme ; le second implique 1.7. La démonstration du premier est laissée au lecteur.

Proposition 1.8 *Le diagramme*

$$\begin{array}{ccc} \mathrm{O}_{P,f} & \xrightarrow{\omega} & \mathrm{O}_L \\ {\scriptstyle \widetilde{\text{dét}}}\downarrow & & {\scriptstyle \text{dét}}\downarrow \\ \mathbb{Z}/2 & \longrightarrow & \mu_2 \end{array}$$

dans lequel la flèche notée $\widetilde{\text{dét}}$ *est la restriction de l'homomorphisme* $\widetilde{\text{dét}} : \mathrm{O}_P \to \mathbb{Z}/2$, *est commutatif.*

On note $\mathrm{SO}_{P,f}$ le noyau de l'homomorphisme $\widetilde{\text{dét}} : \mathrm{O}_{P,f} \to \mathbb{Z}/2$. La proposition ci-dessus montre que l'homomorphisme ω induit un homomorphisme, disons ω_{S}, de $\mathrm{SO}_{P,f}$ dans SO_L.

Proposition 1.9. *L'homomorphisme de $\mathbb{Z}$-schémas en groupes*

$$\omega_{\mathrm{S}} : \mathrm{SO}_{P,f} \longrightarrow \mathrm{SO}_L$$

est un isomorphisme.

Démonstration. Soit A un anneau commutatif unitaire.

On se convainc tout d'abord l'injectivité de l'homomorphisme $\mathrm{SO}_{P,f}(A) \to \mathrm{SO}_L(A)$. Pour cela on contemple le diagramme commutatif de $\mathbb{Z}$-schémas en groupes

$$\begin{tikzcd}
\mathrm{O}_{\mathrm{H}(\mathbb{Z}),f} \arrow[r] \arrow[d, "\omega"'] & \mathrm{O}_{P,f} \arrow[r, "\widetilde{\text{dét}}"] \arrow[d, "\omega"'] & \mathbb{Z}/2 \arrow[d] \\
\mathrm{O}_{\mathrm{A}_1} \arrow[r] & \mathrm{O}_L \arrow[r, "\text{dét}"] & \mu_2
\end{tikzcd}$$

dans lequel les deux flèches horizontales de gauche sont les inclusions évidentes. Comme un élément de $\mathrm{O}_P(A)$ dont la restriction à $A \otimes_{\mathbb{Z}} \mathrm{H}(\mathbb{Z}^n)$ est l'identité s'identifie à un élément de $\mathrm{O}_{\mathrm{H}(\mathbb{Z})}(A)$, cette contemplation montre que les noyaux des $\mathrm{O}_{P,f}(A) \to \mathrm{O}_L(A)$ et $\mathrm{O}_{\mathrm{H}(\mathbb{Z}),f}(A) \to \mathrm{O}_{\mathrm{A}_1}(A)$ coïncident ; on conclut en observant que la composée des deux flèches horizontales du haut est un isomorphisme.

On se convainc ensuite de ce que l'homomorphisme $\mathrm{SO}_{P,f}(A) \to \mathrm{SO}_L(A)$ est surjectif. Soit α un élément de $\mathrm{O}_L(A)$. On écrit $A \otimes_{\mathbb{Z}} L = \mathrm{H}(A^n) \oplus Ae$ et on pose $M = \alpha(\mathrm{H}(A^n))$. Soit $M^\perp$ l'orthogonal dans P de M vu comme un sous-module de $A \otimes_{\mathbb{Z}} P$; $M^\perp$ possède les propriétés suivantes :

– $M^\perp$ est un A-module projectif de rang 2,

– la restriction à $M^\perp$ de la forme quadratique de $A \otimes_{\mathbb{Z}} P$ est non-dégénérée,

– le q-module $A \otimes_{\mathbb{Z}} P$ est isomorphe à la somme orthogonale $M \oplus M^\perp$,

– le discriminant $\Delta(M^\perp)$ est trivial (voir [SGA7, Exposé XII, 1.11]),

– $\alpha(e)$ et f appartiennent à $M^\perp$.

La proposition suivante, dont la démonstration est laissée au lecteur, montre que le q-module $M^\perp$ est isomorphe à $\mathrm{H}(A)$ (observer que l'on a $\mathrm{q}(\alpha(e)) = 1$) :

Proposition 1.10. *Soit N un* q*-module sur A de rang* 2*. Les propriétés suivantes sont équivalentes :*
(i) N est isomorphe au q*-module hyperbolique* $\mathrm{H}(A)$ *;*
(ii) le discriminant $\Delta(M)$ est trivial et il existe e dans M avec $\mathrm{q}(e) = 1$.

Soit γ un automorphisme du q-module $A \otimes_{\mathbb{Z}} P = \mathrm{H}(A^n) \oplus \mathrm{H}(A)$ induit par l'isomorphisme $\alpha : \mathrm{H}(A^n) \to M$, un isomorphisme $\beta : \mathrm{H}(A) \to M^\perp$ et l'isomorphisme $M \oplus M^\perp \to P$. Comme le groupe orthogonal $\mathrm{O}_{\mathrm{H}(\mathbb{Z})}(A)$ agit transitivement sur l'ensemble des x avec $\mathrm{q}(x) = 1$, on peut supposer $\beta(f) = f$ et donc $\gamma \in \mathrm{O}_{P,f}(A)$; comme l'homomomorphisme $\widetilde{\text{dét}} : \mathrm{O}_{\mathrm{H}(\mathbb{Z}),f} \to \mathbb{Z}/2$ est un isomorphisme on peut supposer en outre $\gamma \in \mathrm{SO}_{P,f}(A)$. Par construction $\alpha^{-1} \circ \omega_{\mathrm{S}}(\gamma)$ est alors un élément de $\mathrm{SO}_L(A)$ qui est l'identité sur $\mathrm{H}(A^n)$; or un tel élément est l'identité. □

Remarque. L'homomorphisme $\mathrm{O}_{\mathrm{H}(\mathbb{Z}),f} \to \mathrm{O}_{P,f}$ s'identifie à un homomorphisme $\mathbb{Z}/2 \to \mathrm{O}_{P,f}$ qui est une section "centrale" de l'homomorphisme $\widetilde{\text{dét}} : \mathrm{O}_{P,f} \to \mathbb{Z}/2$; il en résulte que le groupe $\mathrm{O}_{P,f}$ est canoniquement isomorphe au produit $\mathrm{SO}_{P,f} \times \mathbb{Z}/2$. Pareillement le groupe O_L est canoniquement isomorphe au produit $\mathrm{SO}_L \times \mu_2$ et l'homomorphisme $\omega : \mathrm{O}_{P,f} \to \mathrm{O}_L$ s'identifie au produit de l'isomorphisme ω_S et de l'homomorphisme canonique $\mathbb{Z}/2 \to \mu_2$.

Nous achevons ce paragraphe en dégageant l'énoncé suivant dont le lecteur n'aura pas de mal à décoder les notations :

Scholie 1.11. *Soit A un anneau comutatif unitaire. Soit P un* q*-module sur A, de rang constant pair, muni d'un élément e avec* $\mathrm{q}(e) \in A^\times$ *; soit L l'orthogonal de e dans P. Alors :*

– *L est un* qi*-module sur A,*

– *le A-groupe SO_L s'identifie au A-groupe $\mathrm{SO}_{P,e}$,*

– *les A-groupes $\mathrm{O}_{P,e}$ et O_L s'identifient respectivement au produits $\mathrm{SO}_L \times \mathbb{Z}/2$ et $\mathrm{SO}_L \times \mu_2$,*

– *l'homomorphisme canonique $\mathrm{O}_{P,e} \to \mathrm{O}_L$ s'identifie à l'homomorphisme induit par l'homomorphisme $\mathbb{Z}/2 \to \mu_2$.*

2. Sur les q-i-modules sur $\mathbb{Z}$

Un q-i-module sur $\mathbb{Z}$ n'est rien d'autre qu'un $\mathbb{Z}$-module libre L, de dimension finie impaire, muni d'une forme bilinéaire symétrique paire (c'est-à-dire telle que l'on a $x.x$ pair pour tout x dans L) avec $|\text{dét}\, L| = 2$. En fait, le point (a) de la proposition ci-dessous montre que les propriétés de la forme bilinéaire entraînent celle de la dimension.

Proposition 2.1 (classification des $\mathbb{Z}$-q-i-modules)**.**

(a) *Soit L un $\mathbb{Z}$-module libre de dimension finie, muni d'une forme bilinéaire symétrique paire, avec $|\text{dét}\, L| = 2$. Alors il existe un élément ϵ de $\{\pm 1\}$, uniquement déterminé en fonction de L, tel que la signature de L vérifie la congruence $\tau(L) \equiv \epsilon \pmod 8$ (si bien que la dimension de L est impaire).*

(b) *Soit P un $\mathbb{Z}$-module libre de dimension finie, muni d'une forme bilinéaire symétrique paire, avec $|\text{dét}\, P| = 1$, et d'un élément e avec $|e.e| = 2$. Soit L l'orthogonal de e, muni de la forme bilinéaire symétrique paire restriction de celle de P. Alors est L est un $\mathbb{Z}$-module libre de dimension finie (P/L étant libre de dimension 1) avec* $\text{dét}\, L = (e.e)\, \text{dét}\, P$.

(c) *Soit (n, ϵ) un élément de $\mathbb{N} \times \{\pm 1\}$ avec n impair ; soit $\mathrm{QI}_{n,\epsilon}$ l'ensemble des classes d'isomorphisme de $\mathbb{Z}$-q-i-modules L, avec $\dim L = n$ et $\tau(L) \equiv \epsilon \pmod 8$. Soit (n, ϵ) un élément de $\mathbb{N} \times \{\pm 1\}$ avec n pair ; soit $\mathrm{QR}_{n,\epsilon}$ l'ensemble des classes d'isomorphisme de $\mathbb{Z}$-q-modules munis d'un élément e avec $e.e = 2\epsilon$. Alors l'application*

$$(P, e) \;\mapsto\; e^\perp$$

induit une bijection de $\mathrm{QR}_{n,\epsilon}$ sur $\mathrm{QI}_{n-1,-\epsilon}$.

Démonstration du point (a) de 2.1. On considère L comme un $\widetilde{\mathrm{q}}$-module. Le groupe sous-jacent à son résidu $\text{rés}\, L$ s'identifie à $\mathbb{Z}/2$ et sa forme quadratique d'enlacement vérifie $\mathrm{q}(\bar{1}) = \frac{\epsilon}{4}$ avec $\epsilon = \pm 1$. On est donc amené à introduire la somme orthogonale de $\widetilde{\mathrm{q}}$-modules $L \oplus \langle -\epsilon \rangle \otimes \mathrm{A}_1$ ($\mathrm{A}_1 = \mathrm{Q}(\mathbf{A}_1)$ n'est rien

d'autre que le $\mathbb{Z}$-module $\mathbb{Z}$ muni de la forme quadratique $x \mapsto x^2$) dont le résidu s'identifie à la somme orthogonale de qe-modules $\operatorname{rés} L \oplus \langle -1 \rangle \otimes \operatorname{rés} L$. Ce qe-module possède un unique lagrangien à savoir la diagonale ; on note P le q-module qui correspond à ce lagrangien *via* II.1.1. La signature de P étant divisible par 8, on a bien la congruence $\tau(L) \equiv \epsilon \pmod 8$.

Démonstration du point (b) de 2.1. Elle résulte par exemple du point (c) de l'énoncé suivant dont il sera commode de disposer dans ce mémoire. La vérification de cet énoncé est laissée au lecteur.

Proposition 2.2. *Soit A un anneau de Dedekind. Soient L un* q*-module sur A, M un sous-module et $M^\perp$ son orthogonal.*

On suppose que M est facteur direct dans L (autrement dit que le quotient L/M est sans torsion, on observera que $M^\perp$ est facteur direct dans L pour tout M).

Alors :

(a) *On a $(M^\perp)^\perp = M$.*

On suppose en outre que la restriction à M de la forme bilinéaire de L est non singulière, en clair que l'homomorphisme induit $M \to \operatorname{Hom}_A(M, A)$ est injectif ; M est donc un $\widetilde{\mathrm{q}}$*-module sur A.*

Alors :

(b) *La restriction à $M^\perp$ de cette forme bilinéaire est aussi non singulière.*

(c) *L'homomorphisme de A-modules canonique $M \oplus M^\perp \to L$ est injectif et l'on a une suite exacte de A-modules*

$$0 \longrightarrow M \oplus M^\perp \longrightarrow L \longrightarrow \operatorname{rés} M \longrightarrow 0 \qquad ,$$

dans laquelle l'homomorphisme $L \to \operatorname{rés} M$ est le composé de l'isomorphisme $L \to \operatorname{Hom}_A(L, A)$ induit par la forme bilinéaire de L, et des homomorphismes canoniques $\operatorname{Hom}_A(L, A) \to \operatorname{Hom}_A(M, A)$, $\operatorname{Hom}_A(M, A) \to \operatorname{rés} M$.

(d) *Les isomorphismes de A-modules, $\operatorname{rés} M \cong L/(M \oplus M^\perp)$ et $\operatorname{rés} M^\perp \cong L/(M \oplus M^\perp)$ (observer que M et $M^\perp$ jouent des rôles symétriques), induisent un isomorphisme de A-modules $\varphi : \operatorname{rés} M \to \operatorname{rés} M^\perp$ tel que l'on a $\mathrm{q}(\varphi(\xi)) = -\mathrm{q}(\xi)$ pour tout ξ dans $\operatorname{rés} M$. En d'autres termes on a un isomorphisme canonique de A-*qe*-modules*

$$\operatorname{rés} M^\perp \cong \langle -1 \rangle \otimes \operatorname{rés} M \qquad .$$

(e) *Le* q*-module L correspond via II.1.1 et l'isomorphisme de* qe*-modules $\operatorname{rés}(M \oplus M^\perp) \cong \operatorname{rés} M \oplus \operatorname{rés} M^\perp$ au lagrangien de $\operatorname{rés} M \oplus \operatorname{rés} M^\perp$ qu'est le graphe de φ.*

Remarques

– Il existe une “version bilinéaire” de la proposition 2.2 dans laquelle les q-modules (resp. $\widetilde{\mathrm{q}}$-modules, resp. qe-modules) sont remplacés par des b-modules (resp. $\widetilde{\mathrm{b}}$-modules, resp. e-modules).

– Il existe aussi, dans un cas particulier, une “version bilinéaire-quadratique" de la proposition 2.2. Précisons un peu. Soit L un b-module impair sur $\mathbb{Z}$; soit u un vecteur de Wu de L que l'on suppose indivisible et non isotrope. Par construction, l'orthogonal $u^{\perp}$ de u dans L est un $\widetilde{\mathrm{b}}$-module pair, en d'autres termes un $\widetilde{\mathrm{q}}$-module. La proposition 2.2 dit que $\operatorname{rés} u^{\perp}$, en tant que e-module, est isomorphe à $\mathbb{Z}/u.u$ muni de la forme d'enlacement défini par $\bar{1}.\bar{1} = -\frac{1}{u.u}$. On vérifie que la forme quadratique d'enlacement est quant à elle définie par

$$\mathrm{q}(\bar{1}) \;=\; \frac{1}{2}\,(1 - \frac{1}{u.u}) \qquad .$$

Démonstration du point (c) de 2.1. On note $\omega_{n,\epsilon} : \mathrm{QR}_{n,\epsilon} \to \mathrm{QI}_{n-1,-\epsilon}$ l'application induite par l'application $(P, e) \mapsto e^{\perp}$. Soit (n, ϵ) un élément de $\mathbb{N} \times \{\pm 1\}$ avec n impair ; le q-module P qui apparaît dans la démonstration du point (a) de 2.1 est par construction muni d'un élément e avec $e.e = -2\epsilon$. L'unicité du lagrangien invoquée dans cette construction montre que l'application $L \mapsto (P, e)$ induit une application $\mathrm{QI}_{n,\epsilon} \to \mathrm{QR}_{n+1,-\epsilon}$ que l'on note $\pi_{n,\epsilon}$. On constate que les deux applications $\omega_{n,\epsilon}$ et $\pi_{n-1,-\epsilon}$ sont inverses l'une de l'autre. □

Scholie 2.3 *Soit L un* q-i-*modules sur $\mathbb{Z}$; soit ϵ l'élément de $\{\pm 1\}$ défini par $\tau(L) \equiv \epsilon \pmod 8$. Alors le* qe *module* $\operatorname{rés} L$ *est isomorphe à $\mathbb{Z}/2$ muni de la forme quadratique d'enlacement définie par* $\mathrm{q}(\bar{1}) = \frac{\epsilon}{4}$.

La proposition 2.1 et le scholie II.2.1 conduisent également au scholie suivant :

Scholie 2.4. *Soient L_1 et L_2 deux* q-i-*modules sur $\mathbb{Z}$. Les deux conditions suivantes sont équivalentes :*
(i) les deux b-*espaces vectoriels sur $\mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} L_1$ et $\mathbb{Q} \otimes_{\mathbb{Z}} L_2$, sont isomorphes ;*
(ii) les deux b-*espaces vectoriels sur $\mathbb{R}$, $\mathbb{R} \otimes_{\mathbb{Z}} L_1$ et $\mathbb{R} \otimes_{\mathbb{Z}} L_2$, sont isomorphes.*

Genre d'un q-i-module sur $\mathbb{Z}$

La méthode de démonstration de la proposition 2.1 fournit l'énoncé suivant (l'intertitre fait référence au point (b)) :

Proposition 2.5. *Soit L un* q-i-*module sur $\mathbb{Z}$ de dimension $2n+1$ et de déterminant 2ϵ avec $\epsilon = \pm 1$; soit p un nombre premier.*

(a) *Le* q-i-*espace vectoriel $\mathbb{F}_p \otimes_{\mathbb{Z}} L$ est isomorphe à $\mathrm{H}(\mathbb{F}_p^n) \oplus \langle (-1)^n \epsilon \rangle \otimes \mathrm{A}_1$.*

(b) *Le* q-i-*module $\mathbb{Z}_p \otimes_{\mathbb{Z}} L$ est isomorphe à $\mathrm{H}(\mathbb{Z}_p^n) \oplus \langle (-1)^n \epsilon \rangle \otimes \mathrm{A}_1$.*

Remarques. Pour $p \neq 2$, un q-i-espace vectoriel sur $\mathbb{F}_p$ (resp. un q-i-module sur $\mathbb{Z}_p$) n'est rien d'autre qu'un b-espace vectoriel (resp. b-module) de dimension impaire. Soient A un anneau (commutatif unitaire) et u un élément de $A^\times$, alors on a $\langle u \rangle \otimes \mathrm{H}(A^n) \cong \mathrm{H}(A^n)$; on peut donc remplacer dans l'énoncé 2.4 $\mathrm{H}(\mathbb{F}_p^n) \oplus \langle (-1)^n \epsilon \rangle \otimes \mathrm{A}_1$ par $\langle (-1)^n \epsilon \rangle \otimes (\mathrm{H}(\mathbb{F}_p^n) \oplus \mathrm{A}_1)$ et $\mathrm{H}(\mathbb{Z}_p^n) \oplus \langle (-1)^n \epsilon \rangle \otimes \mathrm{A}_1$ par $\langle (-1)^n \epsilon \rangle \otimes (\mathrm{H}(\mathbb{Z}_p^n) \oplus \mathrm{A}_1)$.

Le cas défini positif

Soit L un q-i-module sur $\mathbb{Z}$ avec $\mathbb{R} \otimes_{\mathbb{Z}} L$ défini positif. Compte tenu de ce que nous avons vu plus haut, un tel L n'est rien d'autre qu'un réseau (entier) pair de déterminant 2. Nous abandonnons ci-après la terminologie "q-i-module sur $\mathbb{Z}$ défini positif" (qui est loin d'être classique !) pour la terminologie "réseau pair de déterminant 2".

Soit L un réseau pair de déterminant 2 ; le point (a) de 2.1 montre que l'on a la congruence $\dim L \equiv \pm 1 \pmod 8$.

On étudie d'abord le cas $\dim L \equiv -1 \pmod 8$. Le point (c) de la proposition 2.1 se spécialise de la façon suivante :

Proposition 2.6. *Soit $n > 0$ un entier avec $n \equiv -1 \pmod 8$; soit X_n l'ensemble des classes d'isomorphisme de réseaux pairs L, avec $\dim L = n$ et $\operatorname{dét} L = 2$. Soit $n > 0$ un entier avec $n \equiv 0 \pmod 8$ pair ; soit $\mathrm{X}_n^{\mathrm{A}_1}$ l'ensemble des classes d'isomorphisme de réseaux unimodulaires pairs P de dimension n munis d'un élément e avec $e.e = 2$ (en d'autres termes d'une racine). Alors l'application*

$$(P; e) \mapsto e^\perp$$

induit une bijection de $\mathrm{X}_n^{\mathrm{A}_1}$ sur X_{n-1}.

(La justification de la notation $\mathrm{X}_n^{\mathrm{A}_1}$ est la suivante : la donnée d'une racine de P est équivalente à celle d'une représentation de A_1 par P. Elle est le pendant de la notation $\mathrm{X}_n^{\mathrm{E}_7}$ qui sera introduite plus bas.)

Exemples

Détermination de X_7. Comme X_8 n'a qu'un élément, à savoir la classe de E_8, et que le groupe Weyl de $\mathbf{E}_8$ (qui coïncide avec le groupe orthogonal de E_8) agit transitivement sur l'ensemble des racines, l'ensemble X_7 n'a qu'un élément, à savoir la classe de l'orthogonal d'une racine dans E_8. Cet orthogonal est noté E_7, notation en accord avec celle que nous avons adoptée au chapitre II : $\mathrm{E}_7 = \mathrm{Q}(\mathbf{E}_7)$.

Détermination de X_{15}. Comme le groupe de Weyl de $\mathbf{D}_{16}$ (qui coïncide avec le groupe orthogonal de E_{16}) agit transitivement sur l'ensemble des racines et qu'il en est de même pour le groupe orthogonal de $\mathrm{E}_8 \oplus \mathrm{E}_8$, l'ensemble X_{15} a deux éléments :

- la classe de l'orthogonal d'une racine dans E_{16}, disons E_{15} ;
- la classe de $\mathrm{E}_7 \oplus \mathrm{E}_8$.

Détermination de X_{23}

Compte tenu de la proposition 2.6 et du théorème II.3.17, cette détermination est conséquence de l'observation suivante :

Soit L un réseau unimodulaire pair de dimension 24 avec racines. Soient e_1 et e_2 deux racines de L ; soit R_i, $i = 1, 2$, la composante irréductible du système de racines $\mathrm{R}(L)$ à laquelle appartient e_i. Alors les deux conditions suivantes sont équivalentes :

(i) Les deux systèmes de racines R_1 et R_2 sont isomorphes.

(ii) Il existe un élément α du groupe orthogonal $\mathrm{O}(L)$ tel que l'on a $\alpha(e_1) = e_2$.

L'implication (ii)⇒(i) est évidente. L'implication (i)⇒(ii) se vérifie par inspection. Nous détaillons un peu cette vérification ci-après.

On considère la décomposition en composantes irréductibles du système de racines $\mathrm{R}(L)$:

$$\mathrm{R}(L) \simeq \coprod_{R \in \mathcal{R}} \mathrm{m}(R)\, R \qquad ,$$

$\mathcal{R}$ désignant, ci-dessus, l'ensemble des classes d'isomorphisme de système de racines irréductibles de type ADE, $\mathrm{m} : \mathcal{R} \to \mathbb{N}$ une application à support fini et $\mathrm{m}(R)\, R$ la réunion disjointe de $\mathrm{m}(R)$ copies de R. On rappelle que l'on note $\mathrm{A}(\mathrm{R}(L))$ le groupe orthogonal du réseau $\mathrm{Q}(\mathrm{R}(L))$ et que le groupe de Weyl $\mathrm{W}(\mathrm{R}(L))$ est un sous-groupe distingué de $\mathrm{A}(\mathrm{R}(L))$. On rappelle également que l'on note $\mathrm{G}(\mathrm{R}(L))$ le groupe quotient $\mathrm{A}(\mathrm{R}(L))/\mathrm{W}(\mathrm{R}(L))$ et que l'on a un isomorphisme de groupes (canonique en un sens manifeste) :

$$\mathrm{G}(\mathrm{R}(L)) \cong \prod_{R \in \mathcal{R}} \left(\mathrm{G}(R)^{\mathrm{m}(R)} \rtimes \mathfrak{S}_{\mathrm{m}(R)} \right) = \left(\prod_{R \in \mathcal{R}} \mathrm{G}(R)^{\mathrm{m}(R)} \right) \rtimes \left(\prod_{R \in \mathcal{R}} \mathfrak{S}_{\mathrm{m}(R)} \right)$$

($\mathfrak{S}_{\mathrm{m}(R)}$ désignant le groupe symétrique d'ordre $\mathrm{m}(R)$ qui opère de façon évidente sur le groupe $\mathrm{G}(R)^{\mathrm{m}(R)}$). On paraphrase enfin le point (b) du scholie II.3.15 : le groupe orthogonal $\mathrm{O}(L)$ est le sous-groupe de $\mathrm{A}(\mathrm{R}(L))$ image inverse par l'homomorphisme $\mathrm{A}(\mathrm{R}(L)) \to \mathrm{G}(\mathrm{R}(L))$ du sous-groupe qui stabilise le lagrangien $L/\mathrm{Q}(\mathrm{R}(L))$ du qe-module $\operatorname{rés}\mathrm{Q}(\mathrm{R}(L))$. Dans [Ero82], V. A. Erokhin explicite au cas par cas ce stabilisateur, qu'il note $\mathrm{H}(L)$, pour les 23 classes d'isomorphisme de réseaux unimodulaires pairs de dimension 24 avec racines. Il est clair que l'on a une suite exacte de groupes canonique

$$1 \to \mathrm{H}_1(L) \to \mathrm{H}(L) \to \mathrm{H}_2(L) \to 1 \qquad ,$$

$\mathrm{H}_1(L)$ s'identifiant à un sous-groupe du produit $\prod_{R\in\mathcal{R}} \mathrm{G}(R)^{\mathrm{m}(R)}$ et $\mathrm{H}_2(L)$ à un sous-groupe du produit $\prod_{R\in\mathcal{R}} \mathfrak{S}_{\mathrm{m}(R)}$, à savoir l'image de la restriction à $\mathrm{H}(L)$ de l'homomorphisme canonique $\mathrm{G}(\mathrm{R}(L)) \to \prod_{R\in\mathcal{R}} \mathfrak{S}_{\mathrm{m}(R)}$ (bien que cela ne soit pas explicitement précisé, les groupes $\mathrm{H}_1(L)$ et $\mathrm{H}_2(L)$ sont les groupes G_1 et G_2 dont les cardinaux apparaissent dans les colonnes 5 et 6 de [CS99, Ch. 16, Table 16.1]).

L'implication (i)$\Rightarrow$(ii) qui nous occupe résulte du fait que pour tout R dans $\mathcal{R}$ l'image de $\mathrm{H}_2(L)$ dans $\mathfrak{S}_{\mathrm{m}(R)}$ est un sous-groupe transitif, ce que l'on vérifie en parcourant l'inventaire de [Ero82] (évidemment les seuls R à considérer sont ceux pour lesquels on a $\mathrm{m}(R) \geq 2$!). Explicitons, à titre d'exemple, ces sous-groupes transitifs, pour les 5 premiers systèmes de racines de l'inventaire en question :

1) $\mathrm{R}(L) = 24\mathbf{A}_1$

L'image de $\mathrm{H}_2(L)$ dans $\mathfrak{S}_{24}$ est le groupe de Mathieu M_{24}.

2) $\mathrm{R}(L) = 12\mathbf{A}_2$

L'image de $\mathrm{H}_2(L)$ dans $\mathfrak{S}_{12}$ est le groupe de Mathieu M_{12}.

3) $\mathrm{R}(L) = 8\mathbf{A}_3$

Il existe une bijection de l'ensemble $\{1, 2, \ldots, 8\}$ sur l'ensemble sous-jacent à $\mathbb{F}_2^3$, vu comme un espace affine de dimension 3 sur $\mathbb{F}_2$, qui induit un isomorphisme de $\mathrm{H}_2(L)$ sur le sous-groupe des transformations affines.

4) $\mathrm{R}(L) = 6\mathbf{A}_4$

Il existe une bijection de l'ensemble $\{1, 2, \ldots, 6\}$ sur l'ensemble sous-jacent à $\mathbf{P}^1(\mathbb{F}_5)$ qui induit un isomorphisme de $\mathrm{H}_2(L)$ sur le sous-groupe des transformations projectives. (Attention : la liste de générateurs donnée dans [Ero82] pour $\mathrm{H}(L)$ est incomplète.)

Plus précisément, la suite exacte $1 \to \mathrm{H}_1(L) \to \mathrm{H}(L) \to \mathrm{H}_2(L) \to 1$ est dans ce cas isomorphe à la suite exacte $1 \to \mathbb{F}_5^\times/\{\pm 1\} \to \mathrm{GL}_2(\mathbb{F}_5)/\{\pm\mathrm{Id}\} \to \mathrm{PGL}_2(\mathbb{F}_5) \to 1$.

5) $\mathrm{R}(L) = 4\mathbf{A}_6$

L'image de $\mathrm{H}_2(L)$ dans $\mathfrak{S}_4$ est le sous-groupe alterné $\mathfrak{A}_4$.

On constate donc au bout du compte que l'ensemble X_{23} s'identifie au sous-ensemble du produit $\mathrm{X}_{24} \times \mathcal{R}$ constitué des couples (x, r) tels que r est la classe d'isomorphisme d'une composante irréductible du système de racines $\mathrm{R}(x)$ (l'abus de notation est véniel). Le cardinal de X_{23} s'obtient en contemplant la deuxième colonne de [CS99, Ch. 16, Table 16.1] (Table I.1 de notre mémoire) :

$$|\mathrm{X}_{23}| \;=\; 32 \;=\; {\scriptstyle 1+2+1+1+1+2+2+2+1+1+3+1+2+1+1+2+1+2+1+1+1+1+1+0}$$

(ce cardinal est évidemment à comparer au nombre des représentations de la table C.7).

On étudie maintenant le cas $\dim L \equiv 1 \pmod 8$.

Proposition 2.7. *Soit $n > 0$ un entier avec $n \equiv 1 \pmod 8$; soit X_n l'ensemble des classes d'isomorphisme de réseaux pairs L, avec $\dim L = n$ et $\operatorname{dét} L = 2$. Soit $n > 0$ un entier avec $n \equiv 0 \pmod 8$ pair ; soit $\mathrm{X}_n^{\mathrm{E}_7}$ l'ensemble des classes d'isomorphisme de réseaux unimodulaires pairs P de dimension n munis d'un homomorphisme $f : \mathrm{E}_7 \to P$ avec $\mathrm{q}(f(x)) = \mathrm{q}(x)$ pour tout x dans E_7 (en d'autres termes d'une représentation de E_7 par P).*

Alors l'application

$$(P; f) \;\mapsto\; (f(\mathrm{E}_7))^{\perp}$$

induit une bijection de $\mathrm{X}_n^{\mathrm{E}_7}$ sur X_{n-7}.

Démonstration. C'est une variante de la démonstration du point (c) de 2.1. On considère cette fois la somme orthogonale $L \oplus \mathrm{E}_7$. D'après le scholie 2.3, le résidu de ce que $\widetilde{\mathrm{q}}$-module est encore isomorphe à $\operatorname{rés} L \oplus \langle -1 \rangle \otimes \operatorname{rés} L$. On achève *mutatis mutandis.* □

Notation-remarque. Soient G et L deux réseaux entiers ; on rappelle qu'une représentation de G par L est un homomorphisme de $\mathbb{Z}$-modules $f : G \to L$ avec $f(x).f(y) = x.y$ pour tous x et y dans G et que l'ensemble (fini) de ces f est noté $\mathrm{Rep}(G, L)$. On note $\overline{\mathrm{Rep}}(G, L)$ le quotient $\mathrm{Rep}(G, L)/\mathrm{O}(G)$ de l'action à droite du groupe orthogonal $\mathrm{O}(G)$ sur $\mathrm{Rep}(G, L)$ (action qui est libre) ; $\overline{\mathrm{Rep}}(G, L)$ peut être vu comme l'ensemble des sous-modules de L isomorphes, comme réseaux entiers, à G.

Exemples

Détermination de X_{17}. On constate par inspection que les seuls systèmes de racines irréductibles de type ADE qui contiennent $\mathbf{E}_7$ sont $\mathbf{E}_7$ et $\mathbf{E}_8$

(utiliser par exemple [Bou81b, Ch. VI, §1, Proposition 24]). On en déduit, toujours par inspection, que les seuls systèmes de racines apparaissant dans la classification de Niemeier qui contiennent $\mathbf{E}_7$ sont $\mathbf{R}_2 = \mathbf{D}_{16} \coprod \mathbf{E}_8$, $\mathbf{R}_3 = \mathbf{E}_8 \coprod \mathbf{E}_8 \coprod \mathbf{E}_8$, $\mathbf{R}_6 = \mathbf{A}_{17} \coprod \mathbf{E}_7$ et $\mathbf{R}_7 = \mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{E}_7$. Soit P_i, $i \in \{2, 3, 6, 7\}$, le réseau unimodulaire pair avec $\mathrm{R}(\mathrm{P}_i) \approx \mathbf{R}_i$; on vérifie que le groupe orthogonal $\mathrm{O}(\mathrm{P}_i)$ agit transitivement sur l'ensemble $\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{P}_i)$ dans les quatre cas. La vérification est immédiate dans les trois premiers ; pour le quatrième on utilise l'observation faite à la fin de la cinquième illustration que nous avons donnée au chapitre II de la proposition 3.9. La proposition 2.7 montre donc que l'ensemble X_{17} a 4 éléments. Précisons lourdement. On choisit un sous-réseau de P_i isomorphe à E_7 et on note L_i l'orthogonal de ce sous-réseau ; on a $\mathrm{X}_{17} = \{[\mathrm{L}_2], [\mathrm{L}_3], [\mathrm{L}_6], [\mathrm{L}_7]\}$ (la notation $[L]$ désignant la classe d'isomorphisme d'un réseau pair L de dimension 17 et de déterminant 2).

Il n'est pas difficile de donner une définition *ab initio* des réseaux L_i :

– $\mathrm{L}_2 = \mathrm{E}_{16} \oplus \mathrm{A}_1$;

– $\mathrm{L}_3 = \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{A}_1$;

– $\mathrm{L}_6 = \mathrm{A}_{17}^+$ (le qe-module $\mathrm{rés}\,\mathrm{A}_{17}$ est isomorphe à $\mathbb{Z}/18$ avec $\mathrm{q}(\bar{k}) = \frac{17k^2}{36}$, A_{17}^+ est le réseau pair correspondant *via* le point (b) de II.1.1 au sous-module engendré par $\bar{6}$) ;

– $\mathrm{L}_7 = (\mathrm{D}_{10} \oplus \mathrm{E}_7)^+$ (le qe-module $\mathrm{rés}(\mathrm{D}_{10} \oplus \mathrm{E}_7)$ contient deux sous-modules non triviaux isotropes, $(\mathrm{D}_{10} \oplus \mathrm{E}_7)^+$ est le réseau pair correspondant *via* le point (b) de II.1.1 à l'un ou l'autre de ces deux sous-modules).

Détermination de X_9. La proposition 2.7 montre que X_9 a un seul élément à savoir la classe du réseau $\mathrm{E}_8 \oplus \mathrm{A}_1$.

Sur la détermination de X_{25}. L'isomorphisme $\mathrm{X}_{25} \cong \mathrm{X}_{32}^{\mathrm{E}_7}$ de la proposition 2.7 n'est pas très utile pour déterminer X_{25} car X_{32} n'a pas encore été déterminé. Par contre le point (c) de la proposition 2.1 peut être mis en oeuvre. Le point en question dit que X_{25} est en bijection avec l'ensemble des classes d'isomorphisme des couples $(P; e)$, P désignant un q-module sur $\mathbb{Z}$ de dimension 26 et de signature 24 et e un élément de P avec $e.e = -2$. Or tous les P de ce type sont isomorphes d'après le théorème II.2.7. On peut choisir comme représentant de cette classe d'isomorphisme le q-module $\mathrm{II}_{25,1}$ (notation de [CS99][Bor84]) qui peut être vu comme le réseau du q-espace vectoriel $\mathbb{Q}^{26}$ muni de la forme quadratique $\frac{1}{2}(\sum_{i=1}^{25} x_i^2 - x_{26}^2)$, engendré par le sous-module de $\mathbb{Z}^{26}$ constitué des $(x_1, x_2, \ldots, x_{26})$ avec $\sum_{i=1}^{26} x_i$ pair et le vecteur $\frac{1}{2}(1, 1, \ldots, 1)$. Soit Y l'ensemble des éléments e de $\mathrm{II}_{25,1}$ avec $e.e = -2$; Borcherds décrit dans [Bor84] un algorithme pour déterminer l'ensemble $\mathrm{O}(\mathrm{II}_{25,1}) \backslash \mathrm{Y}$ qui d'après ce qui précède est en bijection avec X_{25} ($|\mathrm{X}_{25}| = 121$).

3. Théorie des p-voisins pour les q-i-modules sur $\mathbb{Z}$

Voici le pendant (au moins pour l'anneau de Dedekind $\mathbb{Z}$) du point (a) de la proposition III.1.1.

Proposition 3.1. *Soit V un* q*-espace vectoriel sur $\mathbb{Q}$; soient L_1 et L_2 deux réseaux entiers (au sens quadratique) de V d'indice 2 dans leurs duaux (les réseaux L_1 et L_2 sont donc en particulier deux* q-i*-modules et $L_1 \cap L_2$ un* $\widetilde{\mathrm{q}}$*-module sur $\mathbb{Z}$).*

On pose $I_1 = L_1/(L_1 \cap L_2)$, $I_2 = L_2/(L_1 \cap L_2)$ et $R = (L_1^\sharp \cap L_2^\sharp)/(L_1 \cap L_2)$.

(a) *On a $L_1 \cap L_2^\sharp = L_1 \cap L_2$ et $L_2 \cap L_1^\sharp = L_1 \cap L_2$.*

(b) *Les deux homomorphismes canoniques $R \to L_i^\sharp/L_i$, $i = 1, 2$, sont des isomorphismes.*

(c) *Les trois inclusions, de L_1, L_2 et $L_1^\sharp \cap L_2^\sharp$, dans $(L_1 \cap L_2)^\sharp$ induisent un isomorphisme canonique de groupes abéliens*

$$I_1 \oplus I_2 \oplus R \cong \text{rés}(L_1 \cap L_2)$$

(qui permet d'identifier la source et le but).

(d) *L'accouplement $I_1 \times I_2 \to \mathbb{Q}/\mathbb{Z}$ induit par la forme d'enlacement de* $\text{rés}(L_1 \cap L_2)$ *est non dégénéré. Pour cette forme les deux sous-modules $I_1 \oplus I_2$ et R sont orthogonaux et canoniquement isomorphes, comme* qe*-modules, respectivement à* $\mathrm{H}(I_1)$ *et* $\text{rés}\, L_1$*, si bien que le* qe*-module* $\text{rés}(L_1 \cap L_2)$ *est canoniquement isomorphe à la somme orthogonale* $\mathrm{H}(I_1) \oplus \text{rés}\, L_1$.

Démonstration. On vérifie le point (a) et l'isomorphisme de qe-modules $R \cong \text{rés}\, L_1$; la vérification du reste de l'énoncé est laissée au lecteur.

– Soit $\mathcal{L}(V)$ l'ensemble des réseaux entiers de V ordonné par inclusion ; on observe qu'un réseau entier de V qui est d'indice 2 dans son dual est un élément maximal de $\mathcal{L}(V)$ (en fait, tous les éléments maximaux sont de ce type). Le point (a) résulte de cette observation. On considère le réseau $(L_1 \cap L_2^\sharp) + L_2$. Ce réseau appartient à $\mathcal{L}(V)$ et contient L_2 ; on a donc l'égalité $(L_1 \cap L_2^\sharp) + L_2 = L_2$ qui implique $L_1 \cap L_2^\sharp = L_1 \cap L_2$.

– Le sous-module L_1 de $(L_1 \cap L_2)^\sharp$ correspond *via* le point (b) de la proposition II.1.1 au sous-module isotrope I_1 de $\text{rés}(L_1 \cap L_2)$. Le point (c) de cette même proposition montre que l'on a $\text{rés}\, L_1 \cong I_1^\perp/I_1$. Or $I_1^\perp/I_1$ s'identifie comme qe-module à R. □

La vérification de l'énoncé ci-dessous est immédiate.

Proposition-Définition 3.2. *Soit V un* q*-espace vectoriel sur $\mathbb{Q}$; soient L_1 et L_2 deux réseaux entiers (au sens quadratique) de V d'indice 2 dans leurs duaux.*

Soit p un nombre premier ; les conditions suivantes sont équivalentes :
(i) $L_1 \cap L_2$ est d'indice p dans L_1 ;
(ii) $L_1 \cap L_2$ est d'indice p dans L_2.

*Si ces conditions sont vérifiées alors on dit que L_1 et L_2 sont p-*voisins *(ou que L_2 est un p-*voisin *de L_1). Dans ce cas $L_1/(L_1 \cap L_2)$ et $L_2/(L_1 \cap L_2)$ sont les seuls sous-modules isotropes non triviaux de* $\mathrm{rés}(L_1 \cap L_2)$.

On fixe maintenant un q-i-module L sur $\mathbb{Z}$ et on analyse l'ensemble des p-voisins de L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$; dans ce contexte, un p-voisin de L est un réseau entier L' dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$ avec L' d'indice 2 dans $L'^{\sharp}$ et $L \cap L'$ d'indice p dans L. L'analyse en question se déroule comme au chapitre III :

On pose $M = L \cap L'$. D'après ce qui précède :

– Le réseau pL' est contenu dans M.

– L'image de l'homomorphisme composé $pL' \subset M \subset L \to L/pL$ est une droite isotrope, disons c, de L/pL muni de sa structure de q-i-espace vectoriel sur $\mathbb{Z}/p$.

– Le réseau M est l'image inverse par l'homomorphisme $L \to L/pL$ de $c^{\perp}$, $c^{\perp}$ désignant le sous-espace vectoriel de L/pL orthogonal de la droite c.

– Le réseau L' est l'image inverse par l'homomorphisme $M^{\sharp} \to \mathrm{rés}\, M$ de l'unique sous-module non trivial, isotrope pour la forme quadratique d'enlacement, distinct de L/M.

Réciproquement :

Proposition 3.3. *Soit c une droite isotrope de L/pL ; soit M le sous-module de L image inverse par l'homomorphisme $L \to L/pL$ de $c^{\perp}$. Alors :*

(a) *Le* qe*-module* $\mathrm{rés}\, M$ *est isomorphe à* $\mathrm{H}(\mathbb{Z}/p) \oplus \mathrm{rés}\, L$.

(b) *L'image inverse par l'homomorphisme $M^{\sharp} \to \mathrm{rés}\, M$ de l'unique sous-module non trivial, isotrope pour la forme quadratique d'enlacement, distinct de L/M, est un p-voisin L' de L avec $L \cap L' = M$.*

Démonstration du point (a). Elle est très semblable à celle de III.1.4 :

Soit u un élément de L dont la classe modulo p engendre la droite c ; puisque cette droite est isotrope on a $\mathrm{q}(u) \equiv 0 \bmod p$. Soit b la forme bilinéaire symétrique associée à la forme quadratique de L/pL. Si p est différent de 2 alors b est non dégénérée si bien qu'il existe un élément v de L avec

$u.v \equiv 1 \bmod p$. C'est encore le cas pour $p = 2$. Pour s'en convaincre il suffit de montrer que la classe modulo 2 de u n'appartient pas à $\ker b$. Comme L est un q-i-module sur $\mathbb{Z}$, $L/2L$ est naturellement un q-i-espace vectoriel sur $\mathbb{Z}/2$; le point (a) de 2.5 montre que $\ker b$ est de dimension 1 et que la restriction de la forme quadratique à $\ker b$ est non triviale (en fait, il s'agit là d'un phénomène général pour les q-i-espaces vectoriels sur un corps de caractéristique 2, voir par exemple la remarque qui suit 1.6).

On constate que v et $\frac{u}{p}$ appartiennent à $M^\sharp$; on pose $w = \frac{u}{p} - \frac{\mathrm{q}(u)}{p} v$. On observe que l'on a dans $\mathbb{Q}/\mathbb{Z}$ les égalités $\mathrm{q}(v) = 0$, $\mathrm{q}(w) = 0$ et $v.w = \frac{1}{p}$. Soit H le sous-module de $\operatorname{rés} M$ engendré par les classes de v et w (ou celles de v et $\frac{u}{p}$) ; l'observation précédente montre que la restriction de la forme d'enlacement à H est non dégénérée, que H est un $\mathbb{Z}/p$-espace vectoriel de dimension 2 dont une base est constituée des classes de v et w, que H est isomorphe comme qe-module à $\mathrm{H}(\mathbb{Z}/p)$ et enfin que le qe-module $\operatorname{rés} M$ est isomorphe à la somme orthogonale $H \oplus H^\perp$. Soit I le sous-module L/M de $\operatorname{rés} M$ (le sous-module engendré par v) ; I est isotrope et le qe-module $I^\perp/I$ s'identifie à $H^\perp$. Le point (c) de la proposition II.1.1 montre donc que $H^\perp$ s'identifie à $\operatorname{rés} L$. □

On constate au bout du compte que l'énoncé III.1.5 concernant les q-modules sur $\mathbb{Z}$ reste valable, mot pour mot, pour les q-i-modules sur $\mathbb{Z}$; l'énoncé ci-dessous fait seulement intervenir les p-voisins, p pemier, le lecteur n'aura aucun mal à vérifier qu'il s'étend aux d-voisins pour tout $d \geq 1$. Précisons. Soit L un q-i-module sur $\mathbb{Z}$. On note C_L la quadrique projective ; C_L est encore lisse sur $\mathbb{Z}$ (c'est d'ailleurs le critère élégant que choisit Deligne dans [SGA7, Exposé XII] pour caractériser les formes quadratiques qu'il qualifie de non dégénérées). Soit c un point de $\mathrm{C}_L(\mathbb{Z}/p)$; on note $\mathrm{vois}_p(L; c)$ le réseau L' de $\mathbb{Q} \otimes_{\mathbb{Z}} L$ associé à c par le procédé décrit dans le point (b) de 3.3 et $\mathrm{Vois}_p(L)$ l'ensemble des p-voisins de L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L$.

Proposition 3.4. *L'application*

$$\mathrm{C}_L(\mathbb{Z}/p) \to \mathrm{Vois}_p(L) \qquad , \qquad c \mapsto \mathrm{vois}_p(L; c)$$

est une bijection.

4. Théorie des p-voisins pour les réseaux pairs de déterminant 2

Soit E l'un des deux réseaux pairs de déterminant 2, A_1 ou E_7 ; dans la suite de ce paragraphe, sauf mention expresse du contraire, E est fixé.

Soit $n > 0$ un entier avec $n \equiv -\dim \mathrm{E} \pmod 8$.

On note U_n le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$ muni de la forme quadratique

$$(x_1, x_2, \ldots, x_n) \;\mapsto\; \frac{1}{2}\sum_{i=1}^{n-1} x_i^2 \,+\, x_n^2 \qquad .$$

On pose $\mathrm{V}_n = \mathrm{U}_n \oplus (\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{E})$ (V_n est isomorphe, comme q-espace vectoriel, à $\mathbb{Q}^{n+\dim \mathrm{E}}$ muni de la forme quadratique $(x_1, x_2, \ldots, x_{n+\dim \mathrm{E}}) \mapsto \frac{1}{2}\sum_i x_i^2$).

Soit $\mathcal{X}(\mathrm{U}_n))$ (resp. $\mathcal{X}(\mathrm{V}_n)$) l'ensemble des réseaux pairs de déterminant 2 de U_n (resp. des réseaux unimodulaires pairs de V_n). On a donc $\mathrm{X}_n = \mathrm{O}(\mathrm{U}_n)\backslash\mathcal{X}(\mathrm{U}_n) = \mathrm{SO}(\mathrm{U}_n)\backslash\mathcal{X}(\mathrm{U}_n)$ (resp. $\mathrm{X}_{n+\dim E} = \mathrm{O}(\mathrm{V}_n)\backslash\mathcal{X}(\mathrm{V}_n)$). Soient $\mathcal{X}(\mathrm{V}_n; \mathrm{E})$ le sous-ensemble de $\mathcal{X}(\mathrm{V}_n)$ constitué des P contenant E et $\mathrm{O}(\mathrm{V}_n; \mathrm{E})$ le sous-groupe de $\mathrm{O}(\mathrm{V}_n)$ constitué des éléments qui sont l'identité sur E. Avec ces notations, on peut paraphraser les propositions 2.6 et 2.7 de la façon suivante :

Proposition 4.1. *L'application*

$$\mathcal{X}(\mathrm{V}_n; \mathrm{E}) \to \mathcal{X}(\mathrm{U}_n) \qquad , \qquad P \mapsto P \cap \mathrm{U}_n$$

est une bijection équivariante relativement à l'isomorphisme de groupes

$$\mathrm{O}(\mathrm{V}_n; \mathrm{E}) \overset{\cong}{\to} \mathrm{O}(\mathrm{U}_n) \qquad .$$

La spécialisation au cas défini positif du paragraphe 3 conduit quant à elle à l'énoncé suivant :

Proposition 4.2. *Soient P_1 et P_2 deux réseaux unimodulaires pairs de V_n contenant* E *; soient respectivement, L_1 et L_2 les deux résaux pairs de déterminant 2 de U_n, $P_1 \cap \mathrm{U}_n$ et $P_2 \cap \mathrm{U}_n$. Soit p un nombre premier, les deux conditions suivantes sont équivalentes :*
(i) P_1 et P_2 sont p-voisins ;
(ii) L_1 et L_2 sont p-voisins.

Démonstration de (i)⇒(ii). Par définition même, l'homomorphisme canonique $L_i/(L_1 \cap L_2) \to P_i/(P_1 \cap P_2)$, $i = 1, 2$, est injectif. D'après 3.2 on a l'alternative suivante : $L_1 \cap L_2$ d'indice p dans L_1 et L_2 ou $L_1 = L_2$. Or l'application $P \mapsto P \cap \mathrm{U}_n$ est injective. □

Démonstration de (ii)⇒(i). On considère le réseau N de V_n suivant :

$$N \;:=\; (L_1 \oplus \mathrm{E}) \cap (L_2 \oplus \mathrm{E}) \;=\; (L_1 \cap L_2) \oplus \mathrm{E} \qquad .$$

D'après le point (d) de 3.1 et le point (d) de 2.2, le qe-module $\text{rés}\, N$ est canoniquement isomorphe à la somme orthogonale

$$\mathrm{H}(L_1/(L_1 \cap L_2)) \ \oplus \ \langle -1 \rangle \otimes \text{rés}\,\mathrm{E} \ \oplus \ \text{rés}\,\mathrm{E}$$

et l'on vérifie que $P_1 \cap P_2$ est le sous-module de $N^\sharp$ correspondant *via* le point (b) de la proposition II.1.1 à la "diagonale" du facteur $\langle -1 \rangle \otimes \text{rés}\,\mathrm{E} \oplus \text{rés}\,\mathrm{E}$. Le point (c) de cette même proposition montre que l'on a $\text{rés}(P_1 \cap P_2) \cong \mathrm{H}(L_1/(L_1 \cap L_2))$. On conclut à l'aide du point (a) de III.1.1. $\square$

Soit comme ci-dessus $n > 0$ un entier avec $n \equiv -\dim \mathrm{E} \pmod 8$; soit p un nombre premier. Les opérateurs de Hecke $\mathrm{T}_p : \mathbb{Z}[\mathrm{X}_n] \to \mathbb{Z}[\mathrm{X}_n]$ sont définis comme dans le cas $n \equiv 0 \pmod 8$:

$$\mathrm{T}_p[L] \ := \sum_{L' \in \mathrm{Vois}_p(L)} [L'] \qquad ,$$

pour tout réseau pair L de déterminant 2 et de dimension n. Soient L et L' deux réseaux pairs de déterminant 2 et de dimension n, l'entier $\mathrm{N}_p(L, L')$ est défini pareillement comme la $[L']$-coordonnée de $\mathrm{T}_p[L]$.

Le point (a) de 2.5 montre que toutes les quadriques $\mathrm{C}_L(\mathbb{Z}/p)$ ont le même cardinal, disons encore $\mathrm{c}_n(p)$; on a cette fois

$$\mathrm{c}_n(p) = \sum_{m=0}^{n-2} p^m \qquad .$$

L'énoncé III.2.2 reste valable, mot pour mot :

Proposition 4.3. *Soit p un nombre premier. On a*

$$\sum_{y \in \mathrm{X}_n} \mathrm{N}_p(x, y) \ = \ \mathrm{c}_n(p)$$

pour tout x dans X_n.

On dégage ci-après l'analogue de la proposition III.1.10.

– On note $\mathrm{B}_n(p)$ l'ensemble des classes d'isomorphisme des $\widetilde{\mathrm{q}}$-modules M sur $\mathbb{Z}$, avec $\dim M = n$, $\mathbb{R} \otimes_{\mathbb{Z}} M > 0$ et $\text{rés}\, M \simeq \mathrm{H}(\mathbb{Z}/p) \oplus \langle -1 \rangle \otimes \text{rés}\,\mathrm{E}$; on observera que tout automorphisme du qe-module $\mathrm{H}(\mathbb{Z}/p) \oplus \langle -1 \rangle \otimes \text{rés}\,\mathrm{E}$ est l'identité sur le facteur $\langle -1 \rangle \otimes \text{rés}\,\mathrm{E}$ si bien que le qe-module est muni canoniquement d'un facteur direct $\langle -1 \rangle \otimes \text{rés}\,\mathrm{E}$.

– On note $\widetilde{\mathrm{B}}_n(p)$ l'ensemble des classes d'isomorphisme de couples $(M;\omega)$ avec M comme précédemment et ω une bijection de l'ensemble des sous-modules isotropes non-trivaux de $\operatorname{rés} M$ sur l'ensemble $\{1,2\}$. Par définition $\widetilde{\mathrm{B}}_n(p)$ est muni d'une action à gauche du groupe symétrique $\mathfrak{S}_2$ et l'ensemble quotient $\mathfrak{S}_2\backslash\widetilde{\mathrm{B}}_n(p)$ s'identifie à $\mathrm{B}_n(p)$.

– Soit $(M;\omega)$ comme ci-dessus, on note $\mathrm{d}_i(M;\omega)$, $i=1,2$, l'image réciproque par la surjection $M^\sharp \to \operatorname{rés} M$ de $\omega^{-1}(i)$; $\mathrm{d}_1(M;\omega)$ et $\mathrm{d}_2(M;\omega)$ sont deux réseaux pairs de déterminant 2 (de dimension n), p-voisins dans $\mathbb{Q}\otimes_{\mathbb{Z}} M$. En passant aux classes d'isomorphisme on obtient deux applications que l'on note encore d_1 et d_2 de $\widetilde{\mathrm{B}}_n(p)$ dans X_n.

Nous pouvons énoncer :

Proposition 4.4. *Soit p un nombre premier ; soient x_1 et x_2 deux éléments de X_n. On a :*

$$\mathrm{N}_p(x_1,x_2) \;=\; \sum_{\beta\,\in\,\mathrm{d}_1^{-1}(x_1)\cap\mathrm{d}_2^{-1}(x_2)} \frac{|\mathrm{O}(x_1)|}{|\mathrm{O}(\beta)|}$$

(avec $|\mathrm{O}(\beta)| = |\mathrm{Aut}(M;\omega)|$, $(M;\omega)$ représentant β).

On reformule maintenant, au moins dans un cas particulier, l'énoncé ci-dessus en faisant intervenir les réseaux unimodulaires pairs associés aux réseaux pairs de déterminant 2.

Soit L un réseau pair de déterminant 2, de dimension n. On pose comme précédemment $P=(L\oplus\mathrm{E})^+$. Par construction, P est canoniquement muni d'une représentation $\mathrm{i}:\mathrm{E}\to P$. On note $\rho(L)$ (resp. $\bar\rho(L)$) le cardinal de l'orbite de i (resp. i(E)) sous l'action du groupe $\mathrm{O}(P)$. Comme nous l'avons déjà dit (au moins dans le cas $\mathrm{E}=\mathrm{E}_7$) on a $\rho(L)=\bar\rho(L)|\mathrm{O}(\mathrm{E})|$. On dispose donc de deux fonctions, ρ et $\bar\rho$, de X_n dans $\mathbb{N}-\{0\}$ (en fait il sera plus commode de travailler avec ρ dans le cas $\mathrm{E}=\mathrm{A}_1$ et avec $\bar\rho$ dans le cas $\mathrm{E}=\mathrm{E}_7$).

Soit M un $\widetilde{\mathrm{q}}$-module M sur $\mathbb{Z}$, avec $\dim M=n$, $\mathbb{R}\otimes_{\mathbb{Z}} M>0$ et $\operatorname{rés} M\simeq \mathrm{H}(\mathbb{Z}/p)\oplus\langle -1\rangle\otimes\operatorname{rés}\mathrm{E}$. On pose $R=(M\oplus\mathrm{E})^+$. Décodons. Il résulte de l'observation faite plus haut que le qe-module $\operatorname{rés}(M\oplus\mathrm{E})$ est muni canoniquement d'un facteur direct $\langle -1\rangle\otimes\operatorname{rés}\mathrm{E}\oplus\operatorname{rés}\mathrm{E}$; R est le réseau correspondant *via* le point (b) de la proposition II.1.1 à la "diagonale" de facteur direct et le point (c) de cette même proposition montre que l'on a $\operatorname{rés} R\simeq\mathrm{H}(\mathbb{Z}/p)$. A nouveau R est canoniquement muni d'une représentation $\mathrm{i}:\mathrm{E}\to R$ et l'on note encore $\rho(M)$ (resp. $\bar\rho(M)$) le cardinal de l'orbite de i (resp. i(E)) sous l'action du groupe $\mathrm{O}(R)$. On dispose donc aussi de deux fonctions, ρ et $\bar\rho$, de $\mathrm{B}_n(p)$ dans $\mathbb{N}-\{0\}$ avec $\rho(-)=\bar\rho(-)|\mathrm{O}(\mathrm{E})|$.

Ce qui précède montre que l'on dispose d'applications naturelles de X_n (resp. $\mathrm{B}_n(p)$) dans $\mathrm{X}_{n+\dim \mathrm{E}}$ (resp. $\mathrm{B}_{n+\dim \mathrm{E}}(p)$) ; ces applications sont notées π.

Soit enfin $\mathrm{B}_n^0(p)$ le sous-ensemble de $\mathrm{B}_n(p)$ constitué des classes d'isomorphisme des M comme ci-dessus, tels que les deux réseaux pairs de déterminant 2, L_1 et L_2, associés à M, sont non isomorphes. On note e l'application de $\mathrm{B}_n^0(p)$ dans l'ensemble des paires d'éléments de X_n, qui envoie $[M]$ sur la paire $\{[L_1],[L_2]\}$.

Proposition 4.5. *Soient x_1 et x_2 deux éléments distincts de X_n. On a :*

$$\mathrm{N}_p(x_1,x_2) = \sum_{b\,\in\,\mathrm{e}^{-1}(\{x_1,x_2\})} \frac{|\mathrm{O}(\pi(x_1))|}{|\mathrm{O}(\pi(b))|}\,\frac{\rho(b)}{\rho(x_1)} = \sum_{b\,\in\,\mathrm{e}^{-1}(\{x_1,x_2\})} \frac{|\mathrm{O}(\pi(x_1))|}{|\mathrm{O}(\pi(b))|}\,\frac{\bar\rho(b)}{\bar\rho(x_1)}\ .$$

Démonstration. On vérifie que l'hypothèse $x_1 \neq x_2$ permet de transformer l'énoncé 4.4 en l'énoncé 4.5. On représente l'élément β de $\widetilde{\mathrm{B}}_n(p)$ qui apparaît en 4.4 par un couple $(M;\omega)$; on pose $L_1 = \mathrm{d}_1(M;\omega)$, $P_1 = (L_1 \oplus \mathrm{E})^+$ et $R = (M \oplus \mathrm{E})^+$. On a :

$$\frac{|\mathrm{O}(L_1)|}{|\mathrm{O}(M;\omega)|} = [\mathrm{O}(M) : \mathrm{O}(M;\omega)]\,\frac{|\mathrm{O}(L_1)|}{|\mathrm{O}(M)|} = [\mathrm{O}(M) : \mathrm{O}(M;\omega)]\,\frac{|\mathrm{O}(P_1)|}{|\mathrm{O}(R)|}\,\frac{\rho(M)}{\rho(L_1)}\,.$$

Or l'hypothèse $x_1 \neq x_2$ implique $\mathrm{O}(M;\omega) = \mathrm{O}(M)$; en effet, dans le cas contraire il existe un élément de $\mathrm{O}(M)$ qui échange les deux sous-modules istropes non triviaux de $\operatorname{rés}\mathrm{M}$ et l'on a $x_1 = x_2$. □

2-voisins, le point de vue de Borcherds (suite)

Les propositions 2.6 et 2.7 disent que l'application $\pi : \mathrm{X}_n \to \mathrm{X}_{n+\dim \mathrm{E}}$ considérée ci-dessus est la composée d'une bijection $\mathrm{X}_n \cong \mathrm{X}^{\mathrm{E}}_{n+\dim \mathrm{E}}$ et d'une "application d'oubli" $\mathrm{X}^{\mathrm{E}}_{n+\dim \mathrm{E}} \to \mathrm{X}_{n+\dim \mathrm{E}}$. Pareillement, l'application $\pi : \mathrm{B}_n(p) \to \mathrm{B}_{n+\dim \mathrm{E}}(p)$ est la composée d'une bijection $\mathrm{B}_n(p) \cong \mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(p)$ et d'une application d'oubli $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(p) \to \mathrm{B}_{n+\dim \mathrm{E}}(p)$; la définition de l'ensemble $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(p)$ est sans surprise : $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(p)$ est l'ensemble des classes d'isomorphisme des couples $(R;f)$, R et f désignant respectivement un réseau pair avec $\operatorname{rés} R \simeq \mathrm{H}(\mathbb{Z}/p)$ et une représentation de E dans R.

On a vu au chapitre III (en suivant Borcherds) que l'ensemble $\mathrm{B}_{n+\dim \mathrm{E}}(2)$ s'identifie à l'ensemble, que nous avons noté $\mathrm{B}_{n+\dim \mathrm{E}}$, des classes d'isomorphisme des réseaux unimodulaires impairs de dimension $n + \dim \mathrm{E}$. Pareillement, l'ensemble $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(2)$ s'identifie à l'ensemble des classes d'isomorphisme des réseaux unimodulaires impairs de dimension $n + \dim \mathrm{E}$ munis

d'une représentation de E, ensemble que nous noterons $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}$. On dispose aussi d'une identification à la Borcherds $\mathrm{B}_n(2) \cong \mathrm{B}_n$, B_n désignant l'ensemble des réseaux impairs de déterminant 2 : à un réseau pair M avec $\operatorname{rés} M \simeq \mathrm{H}(\mathbb{Z}/2) \oplus \langle -1 \rangle \otimes \operatorname{rés} \mathrm{E}$ on associe le réseau correspondant *via* II.1.1 (version bilinéaire) à l'unique sous-module non trivial de $\operatorname{rés} M$ qui est isotrope au sens bilinéaire mais non quadratique.

Soit $(Q; f)$ un réseau unimodulaire impair de dimension $n+\dim \mathrm{E}$ muni d'une représentation $f : \mathrm{E} \to Q$. Le lecteur vérifiera que la correspondance $Q \mapsto M$ peut être décrite des deux façons suivantes :

– On considère le sous-module R d'indice 2 de Q constitué des x avec $x.x$ pair. On observe que l'on a $f(\mathrm{E}) \subset R$; M est l'orthogonal de $f(\mathrm{E})$ dans R.

– On considère l'orthogonal de $f(\mathrm{E})$ dans Q, disons Λ. On observe que Λ est impair (si ce n'était le cas, on aurait $R = \Lambda \oplus f(\mathrm{E})$, égalité interdite parce que le résidu bilinéaire du second membre n'est pas hyperbolique) ; M est le sous-module de Λ constitué des x avec $x.x$ pair.

Enfin l'application $\rho : \mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}} \to \mathbb{N} - \{0\}$ (resp $\bar{\rho} : \mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}} \to \mathbb{N} - \{0\}$) induite par l'identification $\mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}(2) \cong \mathrm{B}^{\mathrm{E}}_{n+\dim \mathrm{E}}$ associe à la classe du couple $(Q; f)$ le cardinal de l'orbite de f (resp. f(L)) sous l'action du groupe $\mathrm{O}(Q)$.

On a observé au chapitre III, avec Nebe et Venkov, que si un réseau unimodulaire impair L, de dimension divisible par 8, représente 1, alors les deux réseaux unimodulaires pairs 2-voisins de L sont isomorphes (Corollaire III.1.16). Nous terminons ce paragraphe en dégageant l'énoncé technique ci-dessous que l'on peut voir comme le pendant, dans le contexte présent, de cette observation.

Proposition 4.6. *Soit $n > 0$ un entier avec $n \equiv -\dim \mathrm{E} \pmod 8$. Soient L_1 et L_2 deux réseaux pairs de déterminant 2 dans un* q*-espace vectoriel U de dimension n ; on pose $V = U \oplus (\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{E})$. On suppose que L_1 et L_2 sont 2-voisins dans U et non isomorphes. On note P_i, $i = 1, 2$, le réseau unimodulaire pair dans V, contenant* E*, associé à L_i ; on note Q le réseau unimodulaire impair dans V, contenant* E*, dont les 2-voisins pairs sont P_1 et P_2.*

(a) *Dans le cas $\mathrm{E} = \mathrm{E}_7$ le réseau Q ne représente pas 1.*

(b) *Dans le cas $\mathrm{E} = \mathrm{A}_1$ on a l'alternative suivante :*

(b.1) *Le réseau Q ne représente pas 1.*

(b.2) *Les réseaux P_1 et P_2 sont isomorphes et il existe un isomorphisme de réseaux $\phi : Q \cong \mathrm{I}_2 \oplus Q'$ avec I_2 contenant $\phi(\mathrm{A}_1)$ et Q' ne représentant pas 1.*

Démonstration. On note Q^1 le sous-module de Q engendré par les éléments x avec $x.x = 1$ et Q' son orthogonal ; on a donc une décomposition en somme orthogonale $Q = Q^1 \oplus Q'$, le réseau Q^1 est isomorphe à I_m (avec $m = \dim_{\mathbb{Z}} Q^1$) et l'ensemble $\mathrm{R}(Q)$ des racines de Q est isomorphe à la réunion disjointe $\mathrm{R}(\mathrm{I}_m) \coprod \mathrm{R}(Q') = \mathrm{R}(\mathrm{D}_m) \coprod \mathrm{R}(Q')$.

Cas $\mathrm{E} = \mathrm{E}_7$. D'après ce qui précède E_7 est contenu dans Q' ce qui force $m = 0$. En effet, s'il existe e dans Q avec $e.e = 1$ alors la symétrie orthogonale s_e est l'identité sur E_7 et échange P_1 et P_2 (voir III.1.16), si bien que L_1 et L_2 sont isomorphes. □

Cas $\mathrm{E} = \mathrm{A}_1$ et $m \neq 0$. Les réseaux P_1 et P_2 sont isomorphes d'après III.1.16. Soit α une racine de A_1, disons "la" racine positive. On a nécessairement $\alpha \in \mathrm{Q}^1$ ou $\alpha \in \mathrm{Q}'$. Le même argument que précédemment interdit $\alpha \in \mathrm{Q}'$. On a donc $\alpha \in \mathrm{Q}^1$ ce qui entraîne $m \geq 2$. On a d'autre part $m < 3$. En effet, si l'on a $m \geq 3$, alors il existe un élément e dans Q^1 avec $e.e = 1$ et $e.\alpha = 0$ et l'on a encore $\mathrm{s}_e(\alpha) = \alpha$ et $\mathrm{s}_e(P_1) = P_2$. □

5. Exemples

5.1. Détermination de T_2 pour $n = 17$

La matrice de l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{17}] \to \mathbb{Z}[\mathrm{X}_{17}]$, dans la base $(\mathrm{E}_{16} \oplus \mathrm{A}_1, \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{A}_1, \mathrm{A}_{17}^+, (\mathrm{D}_{10} \oplus \mathrm{E}_7)^+)$ est la suivante (on la note encore T_2) :

$$\mathrm{T}_2 = \begin{bmatrix} 20265 & 18225 & 153 & 63 \\ 12870 & 14910 & 0 & 90 \\ 16384 & 0 & 21624 & 18432 \\ 16016 & 32400 & 43758 & 46950 \end{bmatrix} .$$

On explique ci-dessous comment la théorie du paragraphe 4 conduit à cette égalité. On reprend les notations introduites à la fin du paragraphe 2.

Soient i et j deux éléments de l'ensemble $\{2, 3, 6, 7\}$ avec $i \neq j$. La table de Borcherds [CS99, Chap. 17] fournit la liste des classes d'isomorphisme des réseaux unimodulaires impairs de dimension 24 dont les 2-voisins unimodulaires pairs sont isomorphes à P_i et P_j :

– Cette liste est vide pour $\{i, j\} = \{3, 6\}$.

– Cette liste contient un seul élément, disons $[\mathrm{Bor}_{i,j}]$, pour $\{i, j\} \neq \{3, 6\}$.

La table de Borcherds montre aussi que dans le cas $\{i, j\} \neq \{3, 6\}$ le groupe orthogonal $\mathrm{O}(\mathrm{Bor}_{i,j})$ agit transitivement sur l'ensemble $\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{Bor}_{i,j})$.

On rappelle que le groupe $\mathrm{O}(\mathrm{P}_i)$ agit transitivement sur l'ensemble $\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{P}_i)$ pour $i = 2, 3, 6, 7$.

La proposition III.3.3.1 donne

$$\mathrm{N}_2(\mathrm{P}_i, \mathrm{P}_j) \;=\; 0 \;\text{ pour }\; \{i, j\} = \{3, 6\} \qquad ,$$

$$\mathrm{N}_2(\mathrm{P}_i, \mathrm{P}_j) \;=\; \frac{|\mathrm{O}(\mathrm{P}_i)|}{|\mathrm{O}(\mathrm{Bor}_{i,j})|} \;\text{ pour }\; \{i, j\} \neq \{3, 6\} \qquad .$$

La proposition 4.5 et la discussion qui suit cette proposition donnent donc

$$\mathrm{N}_2(\mathrm{L}_i, \mathrm{L}_j) \;=\; 0 \;\text{ pour }\; \{i, j\} = \{3, 6\} \qquad ,$$

$$\mathrm{N}_2(\mathrm{L}_i, \mathrm{L}_j) \;=\; \frac{|\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{Bor}_{i,j})|}{|\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{P}_i)|}\, \mathrm{N}_2(\mathrm{P}_i, \mathrm{P}_j) \;\text{ pour }\; \{i, j\} \neq \{3, 6\} \qquad .$$

Considérons par exemple le cas $\{i, j\} = \{7, 2\}$. La table de Borcherds mentionnée ci-dessus montre que l'on a dans ce cas $|\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{Bor}_{7,2})| = 1$; en effet, Borcherds nous dit que l'ensemble des racines de $\mathrm{Bor}_{7,2}$ (qui a le numéro 150 dans sa table) est isomorphe à $\mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{D}_6 \coprod \mathbf{A}_1$. On a d'autre part $|\overline{\mathrm{Rep}}(\mathrm{E}_7, \mathrm{P}_7)| = 2$ puisque l'ensemble des racines de P_7 est isomorphe à $\mathbf{D}_{10} \coprod \mathbf{E}_7 \coprod \mathbf{E}_7$. On en déduit

$$\mathrm{N}_2(\mathrm{L}_7, \mathrm{L}_2) \;=\; \frac{1}{2}\, \mathrm{N}_2(\mathrm{P}_7, \mathrm{P}_2) \;=\; 63 \qquad .$$

Remarque. Le lecteur observera que l'on a $\mathrm{N}_2(\mathrm{E}_{16} \oplus \mathrm{A}_1, \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{A}_1) = \mathrm{N}_2(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)$ et $\mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{A}_1, \mathrm{E}_{16} \oplus \mathrm{A}_1) = \mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16})$... et n'aura pas de mal à trouver une explication à ce phénomène.

Comme dans le cas $n = 24$, on constate que les valeurs propres de l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{17}] \to \mathbb{Z}[\mathrm{X}_{17}]$ sont entières et simples. Du coup, si l'on admet la conjecture VIII.1.2, le point (ii) du théorème IX.7.2 détermine les opérateurs de Hecke $\mathrm{T}_p : \mathbb{Z}[\mathrm{X}_{17}] \to \mathbb{Z}[\mathrm{X}_{17}]$ pour tout nombre premier p. On obtient par exemple la formule suivante :

$$\frac{7}{286}\, \mathrm{N}_p(\mathrm{E}_{16} \oplus \mathrm{A}_1, \mathrm{E}_8 \oplus \mathrm{E}_8 \oplus \mathrm{A}_1) \;=$$
$$(5p^4 + 7p^3 + 7p^2 + 7p + 5)\, \frac{p^{11} - \tau(p) + 1}{691} - 26\, \frac{p^{15} - \tau_{16}(p) + 1}{3617} \qquad ,$$

$\tau_{16}(p)$ désignant ci-dessus le p-ième coefficient de Fourier de la forme modulaire (pour $\mathrm{SL}_2(\mathbb{Z})$) parabolique normalisée de poids 16.

5.2. Détermination de T_2 pour $n = 15$

Le point (b) de la proposition 4.6 et les mêmes arguments que précédemment (en plus simple) donnent

$$\frac{\mathrm{N}_2(\mathrm{E}_{15}, \mathrm{E}_7 \oplus \mathrm{E}_8)}{\mathrm{N}_2(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)} = \frac{|\mathrm{R}(\mathrm{Bor}_{16})|}{|\mathrm{R}(\mathrm{E}_{16})|} \quad , \quad \frac{\mathrm{N}_2(\mathrm{E}_7 \oplus \mathrm{E}_8, \mathrm{E}_{15})}{\mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16})} = \frac{|\mathrm{R}(\mathrm{Bor}_{16})|}{|\mathrm{R}(\mathrm{E}_8 \oplus \mathrm{E}_8))|} \quad ,$$

Bor_{16} étant le réseau unimodulaire impair de dimension 16, introduit en III.3.3.2, qui "fait le pont" entre E_{16} et $\mathrm{E}_8 \oplus \mathrm{E}_8$. Comme l'on a $\mathrm{R}(\mathrm{Bor}_{16}) = \mathbf{D}_8 \coprod \mathbf{D}_8$ (Scholie III.3.3.2), on trouve

$$(*) \qquad \frac{\mathrm{N}_2(\mathrm{E}_{15}, \mathrm{E}_7 \oplus \mathrm{E}_8)}{\mathrm{N}_2(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)} = \frac{7}{15} \quad , \quad \frac{\mathrm{N}_2(\mathrm{E}_7 \oplus \mathrm{E}_8, \mathrm{E}_{15})}{\mathrm{N}_2(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16})} = \frac{7}{15} \quad .$$

On en déduit la matrice de l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{15}] \to \mathbb{Z}[\mathrm{X}_{15}]$ dans la base $(\mathrm{E}_{15}, \mathrm{E}_7 \oplus \mathrm{E}_8)$ (matrice que l'on note encore T_2) :

$$\mathrm{T}_2 = \begin{bmatrix} 10377 & 8505 \\ 6006 & 7878 \end{bmatrix} \quad .$$

Comme précédemment, si l'on admet la conjecture VIII.1.2, le point (i) du théorème IX.7.2 montre que les égalités (*) ci-dessus se généralisent pour tout nombre premier p :

$$\frac{\mathrm{N}_p(\mathrm{E}_{15}, \mathrm{E}_7 \oplus \mathrm{E}_8)}{\mathrm{N}_p(\mathrm{E}_{16}, \mathrm{E}_8 \oplus \mathrm{E}_8)} = \frac{p^3 - 1}{p^4 - 1} \quad , \quad \frac{\mathrm{N}_p(\mathrm{E}_7 \oplus \mathrm{E}_8, \mathrm{E}_{15})}{\mathrm{N}_p(\mathrm{E}_8 \oplus \mathrm{E}_8, \mathrm{E}_{16})} = \frac{p^3 - 1}{p^4 - 1} \quad .$$

5.3. Sur le problème de la détermination de T_2 pour $n = 23$

On constate que l'application $\pi : \mathrm{X}_{15} \to \mathrm{X}_{16}$ est injective ; ceci implique que l'alternative (b.2) de 4.6 n'a pas lieu pour $n = 15$ (cet argument a été en fait utilisé ci-dessus pour déterminer T_2 pour $n = 15$). Par contre l'application $\pi : \mathrm{X}_{23} \to \mathrm{X}_{24}$ n'est pas injective et nous allons voir que l'alternative (b.2) de 4.6 a bien lieu pour $n = 23$.

Explicitons par exemple $\pi^{-1}([\mathrm{E}_{16} \oplus \mathrm{E}_8])$. Le quotient $\mathrm{O}(\mathrm{E}_{16} \oplus \mathrm{E}_8) \backslash \mathrm{R}(\mathrm{E}_{16} \oplus \mathrm{E}_8)$ s'identifie à la réunion disjointe $\mathrm{O}(\mathrm{E}_{16}) \backslash \mathrm{R}(\mathrm{E}_{16}) \coprod \mathrm{O}(\mathrm{E}_8) \backslash \mathrm{R}(\mathrm{E}_8)$ (et est donc un ensemble à deux éléments) ; on en déduit, grâce à la proposition 2.6, $\pi^{-1}([\mathrm{E}_{16} \oplus \mathrm{E}_8]) = \{[\mathrm{E}_{15} \oplus \mathrm{E}_8], [\mathrm{E}_{16} \oplus \mathrm{E}_7]\}$.

On montre ci-après que les deux éléments $[\mathrm{E}_{15} \oplus \mathrm{E}_8]$ et $[\mathrm{E}_{16} \oplus \mathrm{E}_7]$ de X_{23} sont 2-voisins et que l'ensemble $\mathrm{e}^{-1}(\{[\mathrm{E}_{15} \oplus \mathrm{E}_8], [\mathrm{E}_{16} \oplus \mathrm{E}_7]\})$ (notation de 4.5), vu

comme un sous-ensemble de $\mathrm{B}_{24}^{\mathrm{A}_1}$ (notation introduite dans la discussion du paragraphe 4 intitulée "2-voisins, le point de vue de Borcherds (suite)"), est le singleton $\{[(\mathrm{I}_2 \oplus \Lambda; \iota)]\}$, Λ désignant le réseau unimodulaire de dimension 22 correspondant au lagrangien évident du e-module $\mathrm{rés}(\mathrm{E}_{15} \oplus \mathrm{E}_7)$ (Λ pourrait être aussi noté $(\mathrm{E}_{15} \oplus \mathrm{E}_7)^+$) et $\iota : \mathrm{A}_1 \to \mathrm{I}_2 \oplus \Lambda$ désignant la représentation induite par la représentation canonique $\mathrm{A}_1 \to \mathrm{I}_2$.

On pose $S = \mathrm{A}_1 \oplus \mathrm{A}_1 \oplus \mathrm{E}_{15} \oplus \mathrm{E}_7$; on note σ l'élément évident de $\mathrm{O}(S)$ qui échange les deux facteurs A_1. On note ϖ_i le générateur du résidu du i-ème facteur de S. Le qe-module $\mathrm{rés}\, S$ est donc un $\mathbb{Z}/2$-espace vectoriel de dimension 4, de base $\{\varpi_1, \varpi_2, \varpi_3, \varpi_4\}$, la forme quadratique d'enlacement étant définie par $\mathrm{q}(\varpi_i) = \frac{1}{4}$ pour $i = 1, 2$, $\mathrm{q}(\varpi_i) = -\frac{1}{4}$ pour $i = 3, 4$ et $\varpi_i.\varpi_j = 0$ pour $i \neq j$; la structure de qe-module de Venkov est quant à elle déterminée par par $\mathrm{qm}(\varpi_i) = \frac{1}{4}$ pour $i = 1, 2$ et $\mathrm{qm}(\varpi_i) = \frac{3}{4}$ pour $i = 3, 4$. Le qe-module $\mathrm{rés}\, S$ possède deux lagrangiens :

– le sous-espace, disons J_1, engendré par $\varpi_1 + \varpi_3$ et $\varpi_2 + \varpi_4$,

– le sous-espace, disons J_2, engendré par $\varpi_1 + \varpi_4$ et $\varpi_2 + \varpi_3$.

On observera que ces deux lagrangiens sont les graphes des deux isomorphismes de qe-modules de $\mathrm{rés}(\mathrm{A}_1 \oplus \mathrm{A}_1)$ sur $\langle -1 \rangle \otimes \mathrm{rés}(\mathrm{E}_{15} \oplus \mathrm{E}_7)$ et qu'il sont échangés par σ.

On note P_k, $k = 1, 2$, le réseau unimodulaire pair avec $S \subset P_k \subset S^\sharp$ et $P_k/S = J_k$. Il est clair que P_1 et P_2 sont tous deux isomorphes à $\mathrm{E}_{16} \oplus \mathrm{E}_8$ et qu'il sont échangés par $\mathbb{Q} \otimes_{\mathbb{Z}} \sigma$.

On pose $K = J_1 \cap J_2$; K est le sous-espace de dimension 1 de $\mathrm{rés}\, S$ engendré par $\varpi_1 + \varpi_2 + \varpi_3 + \varpi_4$. On note R le réseau pair avec $S \subset R \subset S^\sharp$ et $R/S = K$; il est clair que l'on a $R = P_1 \cap P_2$. On identifie le qe-module $\mathrm{rés}\, R$ à $K^\perp/K$ (Proposition II.1.1) ; on observe que $\mathrm{rés}\, R$ est engendré par les classes de $\varpi_1 + \varpi_3$ et $\varpi_1 + \varpi_4$, cette observation permet de se convaincre de ce que $\mathrm{rés}\, R$ est isomorphe à $\mathrm{H}(\mathbb{Z}/2)$. On constate donc que P_1 et P_2 sont 2-voisins, disons dans $\mathbb{Q} \otimes_{\mathbb{Z}} S$.

Soit L_k, $k = 1, 2$, l'orthogonal dans P_k du premier facteur A_1 de S. On constate que l'on a $L_1 \simeq \mathrm{E}_{15} \oplus \mathrm{E}_8$ et $L_2 \simeq \mathrm{E}_{16} \oplus \mathrm{E}_7$. La proposition 4.2 montre bien que L_1 et L_2 sont 2-voisins (disons dans l'orthogonal, dans $\mathbb{Q} \otimes_{\mathbb{Z}} S$, du premier facteur A_1 de S).

Soit J_3 le sous-espace vectoriel de $\mathrm{rés}\, S$ engendré par $\varpi_1 + \varpi_2$ et $\varpi_3 + \varpi_4$; J_3 est un "lagrangien au sens bilinéaire" de $\mathrm{rés}\, S$. Le e-module $\mathrm{rés}(\mathrm{A}_1 \oplus \mathrm{A}_1)$ (resp. $\mathrm{rés}(\mathrm{E}_{15} \oplus \mathrm{E}_7)$) possède un unique lagrangien, disons J_4 (resp. J_5) ; J_3 est la somme orthogonale de J_4 et J_5. Le réseau unimodulaire associé au couple $(\mathrm{A}_1 \oplus \mathrm{A}_1; J_4)$ est isomorphe à I_2. Comme on l'a dit plus haut, on note Λ le

réseau unimodulaire de dimension 22 associé au couple $(\mathrm{E}_{15}\oplus\mathrm{E}_7; J_5)$; Λ est le premier réseau de la table de Conway et Sloane [CS99, Chap. 16, Table 16.7, dim = 22]. On se convainc de ce que Λ ne représente pas 1 en invoquant la structure de qe-module de Venkov de rés$(\mathrm{E}_{15} \oplus \mathrm{E}_7)$. Le réseau unimodulaire associé au couple $(S; J_3)$ est donc isomorphe à $\mathrm{I}_2 \oplus \Lambda$. On constate que l'on a $K \subset J_3$; il en résulte que le lagrangien au sens bilinéaire de rés R est J_3/K et que le réseau unimodulaire impair dont les 2-voisins pairs sont P_1 et P_2 coïncide avec le réseau unimodulaire associé au couple $(S; J_3)$.

On se convainc enfin de l'égalité dans $\mathrm{B}_{24}^{\mathrm{A}_1}$

$$\mathrm{e}^{-1}(\{[\mathrm{E}_{15} \oplus \mathrm{E}_8], [\mathrm{E}_{16} \oplus \mathrm{E}_7]\}) \;=\; \{[(\mathrm{I}_2 \oplus \Lambda; \iota)]\}$$

en contemplant la première colonne de la table de Conway et Sloane évoquée ci-dessus.

Compte tenu de cette égalité, on peut déterminer $\mathrm{N}_2(\mathrm{E}_{15} \oplus \mathrm{E}_8, \mathrm{E}_{16} \oplus \mathrm{E}_7)$ à l'aide par exemple de 4.4 :

$$\mathrm{N}_2(\mathrm{E}_{15} \oplus \mathrm{E}_8, \mathrm{E}_{16} \oplus \mathrm{E}_7) \;=\; \frac{|\mathrm{O}(\mathrm{E}_{15} \oplus \mathrm{E}_8)|}{|\mathrm{O}(\mathrm{A}_1 \oplus \mathrm{E}_{15} \oplus \mathrm{E}_7)|} \;=\; \frac{|\mathrm{O}(\mathrm{E}_8)|}{|\mathrm{O}(\mathrm{A}_1 \oplus \mathrm{E}_7)|} \;=\; 120\ .$$

Pour terminer ce sous-paragraphe, reprenons pour $n = 23$ l'observation faite par Nebe et Venkov pour $n = 24$: comme la somme $\sum_{y\in \mathrm{X}_{23}} \mathrm{N}_2(x, y)$ est connue pour tout x (Proposition 4.3), il suffit pour déterminer l'opérateur de Hecke $\mathrm{T}_2 : \mathbb{Z}[\mathrm{X}_{23}] \to \mathbb{Z}[\mathrm{X}_{23}]$ de calculer $\mathrm{N}_2(x, y)$ pour $x \neq y$. Cette observation et le point (b) de 4.6 (et l'exemple précédent) amènent à se poser la question suivante :

Peut-on déterminer T_2 pour $n = 23$, à la Nebe-Venkov, en contemplant simplement la table de Borcherds [CS99, Chap. 17] et de celle de Conway et Sloane [CS99, Chap. 16, Table 16.7, dim = 22] ?

C. Tables

g	$\psi(\pi, \mathrm{St})$	g	$\psi(\pi, \mathrm{St})$
		7	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4] \oplus \Delta_{11}[2]$
1	$\mathrm{Sym}^2\Delta_{11}$	7	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{15}[6]$
2	$\Delta_{21}[2] \oplus [1]$	8	$\Delta_{15}[8] \oplus [1]$
3	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2]$	8	$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1]$
4	$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus [1]$	8	$\Delta_{19}[4] \oplus \Delta_{11}[4] \oplus [1]$
4	$\Delta_{19}[4] \oplus [1]$	8	$\Delta_{21,9}[2] \oplus \Delta_{15}[4] \oplus [1]$
5	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2]$	9	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{11}[6]$
5	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4]$	9	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2]$
6	$\Delta_{17}[6] \oplus [1]$	10	$\Delta_{21}[2] \oplus \Delta_{11}[8] \oplus [1]$
6	$\Delta_{21}[2] \oplus \Delta_{15}[4] \oplus [1]$	10	$\Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1]$
6	$\Delta_{21,13}[2] \oplus \Delta_{17}[2] \oplus [1]$	11	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10]$
7	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2]$	12	$\Delta_{11}[12] \oplus [1]$

TABLE C.1 – Paramètres standards $\psi(\pi, \mathrm{St})$ des représentations π dans $\Pi_{\mathrm{cusp}}(\mathrm{Sp}_{2g})$ engendrées par une forme de Siegel de poids 12 pour $\mathrm{Sp}_{2g}(\mathbb{Z})$, en genre $g \leq 12$.

Gram \ (j,k)	$(0,10)$	$(6,8)$	$(0,12)$	$(8,8)$	$(12,6)$	$(4,10)$
$\begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}$	1	$Y^2X^2(X-Y)^2$	1	$Y^2X^2(X-Y)^2(X^2-YX+Y^2)$	$Y^4X^4(X-Y)^4$	$(X^2-YX+Y^2)^2$
$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	-2	$-2\,Y^2X^2(X^2+Y^2)$	10	$-2\,Y^2X^2(X^4-5\,Y^2X^2+Y^4)$	$-2\,Y^4X^4(X-Y)^2(X+Y)^2$	$-2\,(X^4-9\,Y^2X^2+Y^4)$
$\begin{bmatrix} 2 & -1 \\ -1 & 4 \end{bmatrix}$	-16	$-8\,Y^2(X-2\,Y)(X+Y)$ $\times(2\,X^2-2\,YX+Y^2)$	-88	$-8\,Y^2(2\,X^6-6\,YX^5+14\,Y^2X^4$ $-18\,Y^3X^3+14\,Y^4X^2-6\,Y^5X+3\,Y^6)$	$-16\,Y^4X^2(X-2\,Y)(X-Y)^2$ $\times(X+Y)(X^2-YX+Y^2)$	$-8(2X^4-4\,YX^3+21\,Y^2X^2$ $-19\,Y^3X-14\,Y^4)$
$\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$	36	$12\,Y^2(X^2+Y^2)(3\,X^2-2\,Y^2)$	-132	$12\,Y^2(X^2-3\,Y^2)(3\,X^4-5\,Y^2X^2-Y^4)$	$12\,Y^4X^2(3\,X^6-10\,Y^2X^4$ $+3\,Y^4X^2-4\,Y^4)$	$36\,(X^4-7\,Y^2X^2-\,7Y^4)$
$\begin{bmatrix} 2 & -1 \\ -1 & 6 \end{bmatrix}$	99	$3\,Y^2(33\,X^4-66\,YX^3$ $-91\,Y^2X^2+124\,Y^3X-44\,Y^4)$	1275	$3\,Y^2(33\,X^6-99\,YX^5$ $+410\,Y^2X^4-655\,Y^3X^3$ $+343\,Y^4X^2-32\,Y^5X-132\,Y^6)$	$3\,Y^4(33\,X^8-132\,YX^7+142\,Y^2X^6$ $+36\,Y^3X^5-207\,Y^4X^4+200\,Y^5X^3$ $+88\,Y^6\,X^2-160\,Y^7X+80\,Y^8)$	$99\,(X^4-2\,YX^3+23\,Y^2X^2$ $-22\,Y^3X-7\,Y^4)$
$\begin{bmatrix} 4 & -2 \\ -2 & 4 \end{bmatrix}$	240	0	2784	$1344\,Y^2X^2(X-Y)^2(X^2-YX+Y^2)$	$-240\,Y^4X^4(X-Y)^4$	$-1680\,(X^2-YX+Y^2)^2$
$\begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}$	-272	$-16\,Y^2\,(X-Y)(X+Y)$ $\times(17\,X^2+13\,Y^2)$	736	$-16\,Y^2(X-Y)(X+Y)$ $\times(17\,X^4-62\,Y^2X^2+39\,Y^4)$	$-16\,Y^4(X-Y)(X+Y)$ $\times(17\,X^6-63\,Y^2X^4-6\,Y^4X^2-20\,Y^6)$	$-16\,(17\,X^4-96\,Y^2X^2-144\,Y^4)$

TABLE C.2 – Coefficients de Fourier en $\frac{1}{2}$Gram d'un générateur bien choisi de $\mathrm{S}_{j,k}$

p	$\tau_{6,8}(p)$	$\tau_{8,8}(p)$	$\tau_{12,6}(p)$	$\tau_{4,10}(p)$
2	0	1344	−240	−1680
3	−27000	−6408	68040	55080
5	2843100	−30774900	14765100	−7338900
7	−107822000	451366384	−334972400	609422800
11	3760397784	13030789224	3580209624	25358200824
13	9952079500	−328006712228	91151149180	−263384451140
17	243132070500	5520456217764	−11025016477020	−2146704955740
19	595569231400	−28220918878760	−22060913325080	43021727413960
23	−6848349930000	79689608755152	195863810691120	−233610984201360
29	53451678149100	−1105748270340	−1743496339579620	−545371828324260
31	234734887975744	1851264166857664	1979302106496064	830680103136064
37	448712646713500	22115741387845324	−3685951226317460	11555498201265580
41	−1267141915544076	−29442241674311916	106065086529460884	−56208480716702316
43	−1828093644641000	308109789751260712	74859021001125400	160336767963955000
47	−6797312934516000	43932618784857504	156108802652634720	−116311331328502560
53	30226618925077500	−1178253142902441108	−1224706812408694260	−1944489787072554420
59	−51143734375273800	−3366234739477561080	6289866383536712760	1843701997761637080
61	7626516406720684	−8962102322409921476	4857626575164933724	2376385974282228124
67	−12252758021387000	14381861853876396664	10336923176891703880	487223803841627560
71	−225641741059730736	40475791736823448944	−39237199980379430256	18272191888645387344
73	486083162996216500	−11604559187113183148	9078939377243940820	26899631446378070740
79	1424574980940205600	14996327278915320160	71873557961577515680	−80184572998399700960
83	−1351980902639367000	−15450289322179219216 8	94316650925918995560	157078549808482338120
89	−1127953215815294700	−49999331367987019020	115915137334350529140	22873692749841743220
97	−2710671093611565500	765838865005585444804	894968190691418183620	−219326787347594393660
101	14595359522423307804	−1274759541025862678196	75745749887557044204	867394381514415093804
103	18796572299556586000	1130145111856472690992	229164380766640031440	−657903326636255684720
107	−23385476046562641000	542230976527798722984	−3571178446181577738600	−3958679731685155400
109	36219247764172458700	−884687494456719863780	−2024515635534667135940	30287010492785677180
113	−53733316769620465500	705599831303150185572	−4230007868022803115420	1657202008073896578660

TABLE C.3 – Quelques valeurs propres d'opérateurs de Hecke en genre 2 : l'entier $\tau_{j,k}(p)$, pour p premier et $p \leq 113$.

p	$\tau_{6,8}(p^2)$	$\tau_{8,8}(p^2)$
2	409600	348160
3	333371700	748312020
5	-15923680827500	-395299890927500
7	-253514141409500	-155544419215478300
11	-75764187476725473836	19641545832571328136244
13	-4843967045593944889100	-5961842806869417583052 60
17	1011614857159203797593 00	-2084242598429354457907386 20
19	2430966330762186234484084	-1388004707990982166729991276
23	-1298893998107549887939199 00	-3643516974292143143619092 0540
29	-7216762572241226809807993676	-1863607020307668639314099774 7116
p	$\tau_{12,6}(p^2)$	$\tau_{4,10}(p^2)$
2	4276480	-700160
3	-8215290540	1854007380
5	722477627072500	-904546757727500
7	-1126868422025500700	-391120313742441500
11	-2263452414601610414156	-18738678558496864257356
13	-2999411517177710946591 80	3234946006659478223878 60
17	-9426080311525420228324 1660	7047769318442322713783 4820
19	-4755145650371033833075 81676	-1048771276144665792567133676
23	-5058684922279650577532 70620	-9329951542417743934687945 0460
29	-1109715507227649460845966 4937516	-2847689414234249875206600521516

TABLE C.4 – Quelques valeurs propres d'opérateurs de Hecke en genre 2 : l'entier $\tau_{j,k}(p^2)$, pour p premier et $p \leq 29$.

i	ψ_i	λ_i	g_i
1	$[23] \oplus [1]$	8390655	0
2	$\mathrm{Sym}^2\Delta_{11} \oplus [21]$	4192830	1
3	$\Delta_{21}[2] \oplus [1] \oplus [19]$	2098332	2
4	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus [17]$	1049832	3
5	$\Delta_{19}[4] \oplus [1] \oplus [15]$	533160	4
6	$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus [1] \oplus [15]$	519120	4
7	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus [13]$	268560	5
8	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4] \oplus [13]$	244800	5
9	$\Delta_{21}[2] \oplus \Delta_{15}[4] \oplus [1] \oplus [11]$	145152	6
10	$\Delta_{21,13}[2] \oplus \Delta_{17}[2] \oplus [1] \oplus [11]$	126000	6
11	$\Delta_{17}[6] \oplus [1] \oplus [11]$	99792	6
12	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{15}[6] \oplus [9]$	91152	7
14	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [9]$	69552	7
16	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{17}[4] \oplus \Delta_{11}[2] \oplus [9]$	45792	7
13	$\Delta_{15}[8] \oplus [1] \oplus [7]$	89640	8
15	$\Delta_{21,9}[2] \oplus \Delta_{15}[4] \oplus [1] \oplus [7]$	51552	8
17	$\Delta_{19}[4] \oplus \Delta_{11}[4] \oplus [1] \oplus [7]$	35640	8
18	$\Delta_{21}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [7]$	21600	8
19	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19,7}[2] \oplus \Delta_{15}[2] \oplus \Delta_{11}[2] \oplus [5]$	17280	9
20	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{19}[2] \oplus \Delta_{11}[6] \oplus [5]$	5040	9
21	$\Delta_{21,5}[2] \oplus \Delta_{17}[2] \oplus \Delta_{11}[4] \oplus [1] \oplus [3]$	-7920	10
22	$\Delta_{21}[2] \oplus \Delta_{11}[8] \oplus [1] \oplus [3]$	-16128	10
23	$\mathrm{Sym}^2\Delta_{11} \oplus \Delta_{11}[10] \oplus [1]$	-48528	11
24	$\Delta_{11}[12]$	-98280	12

TABLE C.5 – Paramètres standards $\psi(\pi, \mathrm{St})$ des 24 représentations π dans $\Pi_{\mathrm{disc}}(\mathrm{O}_{24})$ telles que π_∞ est triviale, rangées par degré croissant.

$(m_1, \ldots, m_8)$	$\dim V_\lambda^\Gamma$	$(m_1, \ldots, m_8)$	$\dim V_\lambda^\Gamma$	$(m_1, \ldots, m_8)$	$\dim V_\lambda^\Gamma$
$(0,0,0,0,0,0,0,0)$	1	$(4,4,0,0,0,0,0,0)$	1	$(4,4,4,4,2,2,0,0)$	1
$(2,2,0,0,0,0,0,0)$	1	$(4,4,2,2,0,0,0,0)$	1	$(4,4,4,4,2,2,2,2)$	1
$(2,2,2,2,0,0,0,0)$	1	$(4,4,2,2,2,2,0,0)$	1	$(4,4,4,4,4,0,0,0)$	1
$(2,2,2,2,2,2,0,0)$	1	$(4,4,2,2,2,2,2,2)$	1	$(4,4,4,4,4,2,2,0)$	1
$(2,2,2,2,2,2,2,2)$	1	$(4,4,4,0,0,0,0,0)$	1	$(4,4,4,4,4,4,0,0)$	1
$(4,0,0,0,0,0,0,0)$	1	$(4,4,4,2,2,0,0,0)$	1	$(4,4,4,4,4,4,2,2)$	1
$(4,2,2,0,0,0,0,0)$	1	$(4,4,4,2,2,2,2,0)$	1	$(4,4,4,4,4,4,4,0)$	1
$(4,2,2,2,2,0,0,0)$	1	$(4,4,4,4,0,0,0,0)$	2	$(4,4,4,4,4,4,4,4)$	2
$(4,2,2,2,2,2,2,0)$	1				

TABLE C.6 – Les 8-uples d'entiers $(m_1, \ldots, m_8)$, vérifiant $4 \geq m_1 \geq m_2 \geq \cdots \geq m_8 \geq 0$, tels que $V_\lambda^\Gamma \neq 0$, où V_λ est la représentation irréductible de $\mathrm{SO}(\mathbb{R}^{16})$ de plus haut poids $\lambda = \sum_{i=1}^{8} m_i \varepsilon_i$ et $\Gamma = \mathrm{SO}(\mathrm{E}_8 \oplus \mathrm{E}_8)$.

$[22]$	$\Delta_{11}[11]$
$\Delta_{15}[7] \oplus [8]$	$\Delta_{17}[5] \oplus [12]$
$\Delta_{19}[3] \oplus [16]$	$\Delta_{21} \oplus [20]$
$\Delta_{17}[5] \oplus \Delta_{11} \oplus [10]$	$\Delta_{19}[3] \oplus \Delta_{11}[5] \oplus [6]$
$\Delta_{19}[3] \oplus \Delta_{15} \oplus [14]$	$\Delta_{21} \oplus \Delta_{11}[9] \oplus [2]$
$\Delta_{21} \oplus \Delta_{15}[5] \oplus [10]$	$\Delta_{21} \oplus \Delta_{17}[3] \oplus [14]$
$\Delta_{21} \oplus \Delta_{19} \oplus [18]$	$\Delta_{21,9} \oplus \Delta_{15}[5] \oplus [8]$
$\Delta_{21,13} \oplus \Delta_{17}[3] \oplus [12]$	$\Delta_{19}[3] \oplus \Delta_{15} \oplus \Delta_{11}[3] \oplus [8]$
$\Delta_{21} \oplus \Delta_{17}[3] \oplus \Delta_{11}[3] \oplus [8]$	$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{11}[7] \oplus [4]$
$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{15}[3] \oplus [12]$	$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{17} \oplus [16]$
$\Delta_{21,13} \oplus \Delta_{17}[3] \oplus \Delta_{11} \oplus [10]$	$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{15}[3] \oplus \Delta_{11} \oplus [10]$
$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{11}[5] \oplus [6]$	$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{15} \oplus [14]$
$\Delta_{21,5} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{11}[5] \oplus [4]$	$\Delta_{21,9} \oplus \Delta_{19} \oplus \Delta_{15}[3] \oplus \Delta_{11} \oplus [8]$
$\Delta_{21,9} \oplus \Delta_{19,7} \oplus \Delta_{15}[3] \oplus \Delta_{11} \oplus [6]$	$\Delta_{21,13} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{15} \oplus [12]$
$\Delta_{21} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{15} \oplus \Delta_{11}[3] \oplus [8]$	$\Delta_{21} \oplus \Delta_{19,7} \oplus \Delta_{17} \oplus \Delta_{15} \oplus \Delta_{11}[3] \oplus [6]$
$\Delta_{21,5} \oplus \Delta_{19,7} \oplus \Delta_{17} \oplus \Delta_{15} \oplus \Delta_{11}[3] \oplus [4]$	$\Delta_{21,13} \oplus \Delta_{19} \oplus \Delta_{17} \oplus \Delta_{15} \oplus \Delta_{11} \oplus [10]$.

TABLE C.7 – Paramètres standards des 32 représentations π dans $\Pi_{\mathrm{cusp}}(\mathrm{SO}_{23})$ telles que $\pi_\infty = 1$, admettant la conjecture VIII.4.25.

D. Bibliographie

[Ada11] J. Adams, *Discrete series and characters of the component group*, dans [GRFA11, Ch. 4.2].

[ABV92] J. Adams, D. Barbasch & D. Vogan, *The Langlands classification and irreducible characters for real reductive groups*, Progress in Math. 104, Birkhaüser, Boston-Basel-Berlin (1992).

[AJ87] J. Adams & J. Johnson, *Endoscopic groups and packets of non-tempered representations*, Compositio Math. 64, 271–309 (1987).

[And74] A. N. Andrianov, *Euler products corresponding to Siegel modular forms of genus* 2, Uspekhi Mat. Naut 29, 43–110 (1974).

[And87] A. N. Andrianov, *Quadratic forms and Hecke operators*, Springer Verlag Grundlehren der math. Wiss. 286 (1987).

[AK79] A. N. Andrianov & V. L. Kalinin, *On the analytic properties of standard zeta functions of Siegel modular forms*, Math. USSR, Sb. 35, 1–17 (1979).

[Ara83] T. Arakawa, *Vector valued Siegel modular forms of degree two and the associated Andrianov* L*-function*, Manuscripta Math. 44, 155–185 (1983).

[Art89] J. Arthur, *Unipotent automorphic representations : conjectures*, dans *Orbites unipotentes et représentations II : groupes p-adiques et réels*, Astérisque 171–172, 13–71 (1989).

[Art99] J. Arthur, *On the transfer of distributions : weighted orbital integrals*, Duke Math. J. 99, 209–283 (1999).

[Art02] J. Arthur, *A note on the automorphic Langlands group*, Canad. Math. Bull. 45, 466–482 (2002).

[Art04] J. Arthur, *Automorphic representations of* GSp(4), dans *Contributions to automorphic forms, geometry, and number theory*, 65/81, Johns Hopkins Univ. Press, Baltimore (2004).

[Art13] J. Arthur, *The endoscopic classification of representations : orthogonal and symplectic groups*, Colloquium Publ. 61, Amer. Math. Soc. (2013).

[AS01] M. Asgari & R. Schmidt, *Siegel modular forms and representations*, Manuscripta Math. 104, 173–200 (2001).

[ABS64] M.F. Atiyah, R. Bott & A. Shapiro, *Clifford modules*, Topology 3 (suppl. 1), 3–38 (1964).

[BL08] J. Barge & J. Lannes, *Suites de Sturm, indice de Maslov et périodicité de Bott*, Progress in Math. 267, Birkhäuser Verlag, Basel (2008).

[BLLV74] J. Barge, J. Lannes, F. Latour & P. Vogel, Λ-*sphères*, Ann. Sci. Éc. Norm. Sup. 7, 463–505 (1974).

[Bar47] V. Bargmann, *Irreducible unitary representations of the Lorentz group*, Annals of Math. 48, 568–640 (1947).

[BW59] E. S. Barnes & G. E. Wall, *Some extreme forms defined in terms of abelian groups*, J. Austral. Math. Soc. 1, 47–63 (1959).

[BC11] J. Bellaïche & G. Chenevier, *The sign of Galois representations attached to automorphic forms for unitary groups*, Compositio Math. 147, 1337–1352 (2011).

[BFG14] J. Bergström, C. Faber & G. van der Geer, *Siegel modular forms of degree three and the cohomology of local systems*, Selecta Math. 20, 83–124 (2014).

[BS59] F. van der Blij & T. A. Springer, *The arithmetic of octaves and the groups* G_2, Proc. Kon. Ak. Amsterdam 62 (= Ind. Math. 21), 406–418 (1959).

[BS60] F. van der Blij & T. A. Springer, *Octaves and triality*, Nieuw Archief voor Wiskunde 8, 158–169 (1960).

[Boc83] S. Böcherer, *Über die Fourier-Jacobi-Entwicklung Siegelscher Eisensteinreihen*, Math. Z. 183, 21–46 (1983).

[Boc85] S. Böcherer, *Über die Fourier-Jacobi-Entwicklung Siegelscher Eisensteinreihen II*, Math. Z. 189, 81–110 (1985).

[Boc89] S. Böcherer, *Siegel modular forms and theta series*, Amer. Math. Soc. , Proc. Symp. in Pure Math. 49, Bowdoin 1987, 3–17 (1989).

[Boc85] S. Böcherer, *Über die Funktionalgleichung automorpher* L-*Funktionen zur Siegelschen Modulgruppe*, J. Reine Angew. Math. 362, 146–168 (1985).

[Boc90] S. Böcherer, *Über den kern der thetaliftung*, Abh. Math. Sem. Univ. Hamburg 60, 209–223 (1990).

[Bor84] R. Borcherds, *The Leech lattice and other lattices*, Ph. D. dissertation, University of Cambridge (1984).

[Bor85] R. Borcherds, *The Leech lattice*, Proc. R. Soc. Lond. A 398, 365–376 (1985).

[BFW98] R. Borcherds, E. Freitag & R. Weissauer, *A Siegel cusp form of degree 12 and weight 12*, J. reine angew. Math 494, 141–153 (1998).

[Bor63] A. Borel, *Some finiteness theorems for adeles groups over number fields*, Publ. Math. de l'I.H.É.S. 16, 101–126 (1963).

[Bor77] A. Borel, *Automorphic L-functions*, dans [Cor77] vol. II, 27–61 (1977).

[Bor91] A. Borel, *Linear algebraic groups, 2nd ed.*, Graduate Texts in Math. 126, Springer Verlag (1991).

[Bor97] A. Borel, *Automorphic forms on* $\mathrm{SL}_2(\mathbb{R})$, Cambridge Tracts in Math. 130, Cambridge Univ. Press (1997).

[BJ79] A. Borel & H. Jacquet, *Automorphic forms and automorphic representation*, dans [Cor77] vol. II, 189–203 (1979).

[Bor14] M. Borovoi, *Galois cohomology of reductive algebraic groups over the field of real numbers*, prépublication disponible à l'adresse http://arxiv.org/abs/1401.5913.

[Bou81a] N. Bourbaki, *Éléments de mathématique, Algèbre, Chapitre 9*, Masson, Paris (1981).

[Bou81b] N. Bourbaki, *Éléments de mathématique, Groupes et algèbres de Lie, Chapitres 4, 5 et 6*, Masson, Paris (1981).

[BK00] S. Breulmann & M. Kuss, *On a conjecture of Duke-Imamoğlu*, Proceedings of the Amer. Math. Soc. 128, 1595–1604 (2000).

[BE73] M. Broué & M. Enguehard, *Une famille infinie de formes quadratiques entières ; leurs groupes d'automorphismes*, Ann. Sci. Éc. Norm. Sup. 6, 17–51 (1973).

[Buz] K. Buzzard, *Notes on Siegel modular forms*, http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/siegel_modular_forms_notes.pdf.

[BG10] K. Buzzard & T. Gee, *The conjectural connections between automorphic representations and Galois representations*, à paraître aux Proceedings of the London Math. Soc., Durham Symposium 2011.

[CG13] F. Calegari & T. Gee, *Irreducibility of automorphic Galois representations of* $\mathrm{GL}(n)$*, n at most 5*, Annales de l'Institut Fourier 63, 1881–1912 (2013).

[Ca12] A. Caraiani, *Local-global compatibility and the action of monodromy on nearby cycles*, Duke Math. J. 161, 2311–2413 (2012).

[Car72] R. W. Carter, *Conjugacy classes in the Weyl group*, Compositio Math. 25, 1–59 (1972).

[Car79] P. Cartier, *Representations of p-adic groups : a survey*, dans [Cor77] vol. I, 111–157 (1979).

[ChaL10] P.-H. Chaudouard & G. Laumon, *Le lemme fondamental pondéré. I. Constructions géométriques*, Compositio Math. 146, 1416–1506 (2010).

[ChaL12] P.-H. Chaudouard & G. Laumon, *Le lemme fondamental pondéré. II. Énoncés cohomologiques*, Annals of Math. 176, 1647–1781 (2012).

[Che13] G. Chenevier, *Représentations galoisiennes automorphes et conséquences arithmétiques des conjectures de Langlands et Arthur*, mémoire d'habilitation à diriger des recherches, université Paris XI (2013).

[CH13] G. Chenevier & M. Harris, *Construction of automorphic Galois representations II*, Cambridge Math. J. 1, 53–73 (2013).

[CL11] G. Chenevier & J. Lannes, *Kneser neighbours and orthogonal Galois representations in dimensions* 16 *and* 24, Algebraic Number Theory, Oberwolfach Report 31 (2011).

[CL PARI] G. Chenevier & J. Lannes, feuille de calculs disponible à l'adresse http://gaetan.chenevier.perso.math.cnrs.fr/articles/CL_Programmes.txt.

[CR12] G. Chenevier & D. Renard, *Level one algebraic cusp form of classical groups of small rank*, Mem. Amer. Math. Soc. 1121, 128 p. (2015).

[Ch97] C. Chevalley, *The algebraic theory of spinors and Clifford algebras*, oeuvres complètes vol. 2, Springer-Verlag, Berlin (1997), 1re éd. 1954.

[CF90] C. L. Chai & G. Faltings, *Degeneration of abelian varieties*, Ergebnisse der Math. und ihrer Grenzgebiete 22, Springer-Verlag, avec un appendice de D. Mumford (1990).

[CvdG14] F. Cléry & G. van der Geer, *Constructing vector-valued Siegel modular forms from scalar valued Siegel mofular forms*, prépublication disponible sur arXiv http://arxiv.org/pdf/1409.7176v2.pdf (2014).

[Clo90] L. Clozel, *Motifs et formes automorphes : applications du principe de fonctorialité*, dans *Automorphic forms, Shimura varieties, and L-functions, Vol. I* (Ann Arbor, MI, 1988), Perspectives in Math. 10, Academic Press, Boston, MA (1990).

[Clo13] L. Clozel, *Purity Reigns Supreme*, I.M.R.N. 2013, 328–346 (2013).

[CHL11] L. Clozel, M. Harris & J.-P. Labesse, *Construction of automorphic Galois representations I*, dans *Stabilization of the Trace Formula, Shimura Varieties, and Arithmetic Applications*, édité par L. Clozel, M. Harris, J.-P. Labesse et B.-C. Ngô, International Press (2011).

[Cog04] J. Cogdell, *Lectures on* L*-functions, converse theorems, and functoriality for* GL_n, dans *Lectures on automorphic* L*-functions*, Fields Institute Monographs, A.M.S. (2004).

[Con11] B. Conrad, *Reductive group schemes*, notes de l'école d'été SGA3 (Luminy, 2011), notes disponibles à l'adresse http://math.stanford.edu/~conrad/papers/.

[CoFa99] J. B. Conrey & D. W. Farmer, *Hecke operators and the non-vanishing of L-functions*, dans *Topics in number theory* (University Park, PA, 1997), Math. Appl. 467, Kluwer Acad. Publ., Dordrecht, 143–150 (1999).

[Co69a] J. Conway, *A group of order 8,315,553,613,086,720,000*, Bull. London Math. Soc. 1, 79–88 (1969).

[Co69b] J. H. Conway, *A characterisation of Leech's lattice*, Inventiones Math. 7, 137–142 (1969).

[CS82] J .H. Conway & N. J. A. Sloane, *Twenty-three constructions for the Leech lattice*, Proc. Roy. Soc. London 381, 275–283 (1982).

[CS99] J .H. Conway & N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der Math. Wissenschaften 290, Springer-Verlag, New York (1999).

[Cor77] *Automorphic forms, representations and L-functions, Part I & II*, Proc. Symp. in Pure Math. XXXIII, Oregon State Univ., Corvallis, Ore., Providence, R.I., Amer. Math. Soc. (1977).

[Cox46] H. M. S Coxeter, *Integral Cayley Numbers*, Duke Math. J. 13, 567–578 (1946).

[Del71] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki, exposé no. 355, 139–172 (1968/1960).

[DG70] M. Demazur & P. Gabriel, *Groupes algébriques, Tome 1*, Masson (1970).

[Di55] J. Dieudonné, *Pseudo-discriminant and Dickson invariant*, Pacific. J. Math. 5, 907–910 (1955).

[Di73] J. Dieudonné, *Sur les groupes classiques*, Hermann (1997), 1re éd. 1973.

[Dix74] J. Dixmier, *Algèbres enveloppantes*, Gauthier-Villars Éd. (1974).

[DI98] W. Duke & Ö. Imamoğlu, *Siegel modular forms of small weight*, Math. Ann. 310, 73–82 (1998).

[Eic52] M. Eichler, *Quadratische formen und orthogonal gruppen*, Grundlehren der Math. Wissenschaften, Springer Verlag (1952).

[EZ85] M. Eichler & D. Zagier, *The theory of Jacobi forms*, Progr. Math. 55, Birkhauser Boston (1985).

[Ero79] V. Erokhin, *Theta series of even unimodular 24-dimensional lattices* (in Russian), Zap. Naučn. Sem. Leningrad Otdel. Mat. Inst. Steklov. (LOMI) 86 (1979), 82–93. ; traduction anglaise dans J. Soviet Math. 17, 1999–2008 (1981).

[Ero82] V. A. Erokhin, *Groups of automorphisms of 24-dimensional even unimodular lattices.* (in Russian), Zap. Naučn. Sem. Leningrad Otdel. Mat. Inst. Steklov. (LOMI) 116 (1982), 68–73, 162.

[Fab13] C. Faber, *Modular forms and the cohomology of moduli spaces*, dans *Automorphic forms and automorphic* L*-functions*, Surikaisekikenkyusho Kokyuroku 1826, 129–137 (2013).

[FvdG04] C. Faber & G. van der Geer, *Sur la cohomologie des systèmes locaux sur les espaces de modules des courbes de genre 2 et des surfaces abéliennes, I et II*, C. R. Acad. Sci. Paris, Sér. I 338, 381–384 (2004).

[Fer96] S. Fermigier, *Annulation de la cohomologie cuspidale de sous-groupes de congruence de* $\mathrm{GL}_n(\mathbb{Z})$, Math. Ann. 306, 247–256 (1996).

[FP85] U. Fincke & M. Pohst, *Improved methods for calculating vectors of short lenght in a lattice, including a complexity analysis*, Math. of Computation 44, 463–471 (1985).

[Fre80] E. Freitag, *Thetareihen mit harmonischen Koeffizienten zur Siegelschen Modulgruppe*, Math. Ann. 254, 27–50 (1980).

[Fre82] E. Freitag, *Die Wirkung von Heckeoperatoren auf Thetareihen mit harmonischen Koeffizienten*, Math. Ann. 258, 419–440 (1982).

[Fre83] E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren der Math. Wissenschaften 254, Springer Verlag (1983).

[vdG08] G. van der Geer, *Siegel modular forms and their applications*, dans *The 1–2–3 of modular forms*, édité par J. H. Bruinier, G. van der Geer, G. Harder et D. Zagier, Universitext, Springer Verlag, Berlin, 181–245 (2008).

[GJ78] S. Gelbart & H. Jacquet, *A relation between automorphic representations of* GL(2) *and* GL(3), Ann. Sci. Éc. Norm. Sup. 11, 1–73 (1978).

[GSha01] S. Gelbart & F. Shahidi, *Boundedness of automorphic L-functions in vertical strips*, Journal of the A. M. S. 14, 79–107 (2001).

[GGPS66] I. M. Gel'fand, M. I. Graev & I. I. Pyatetskii-Shapiro, *Representation theory and automorphic functions*, Academic Press (1990), 1re éd. 1968.

[GRS11] D. Ginzburg, S. Rallis & D. Soudry, *The descent map from automorphic representations of* $\mathrm{GL}(n)$ *to classical groups*, World Sci. Publishing (2011).

[Gol14] W. Goldring, *Galois representations associated to holomorphic limits of discrete series I : unitary groups*, Compositio Math. 150, 191-228 (2014).

[GW98] R. Goodman & N. Wallach, *Representations and invariants of the classical groups*, Cambridge Univ. Press (1998).

[Gro96] B. Gross, *Reductive groups over* $\mathbb{Z}$, Inventiones Math. 124, 263–279 (1996).

[Gro98] B. Gross, *On the Satake isomorphism*, dans *Galois representations in arithmetic algebraic geometry*, A. Scholl & R. Taylor Ed., Cambridge Univ. Press (1998).

[Gro99] B. Gross, *Algebraic modular forms*, Israel J. Math. 113, 61–93 (1999).

[Gro00] B. Gross, *On minuscule representations and the principal* SL_2, Electronic J. of Repr. Theory 4, 225–244 (2000).

[GRFA11] *Stabilization of the Trace Formula, Shimura Varieties, and Arithmetic Applications*, édité par L. Clozel, M. Harris, J.-P. Labesse et B.-C. Ngô, International Press (2011).

[Har08] G. Harder, *A congruence between a Siegel and an elliptic modular form*, dans *The 1–2–3 of modular forms*, édité par J.H. Bruinier, G. van der Geer, G. Harder et D. Zagier, Universitext, Springer Verlag, Berlin, 247–260 (2008).

[HC68] Harish-Chandra, *Automorphic forms on semisimple Lie groups*, Lecture Notes in Math. 62, Springer Verlag (1968).

[Hu72] J. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Math. 9, Springer Verlag (1972).

[Hu75] J. Humphreys, *Linear algebraic groups*, Graduate Texts in Math. 21, Springer Verlag (1975).

[Hu90] J. Humphreys, *Reflection groups and Coxeter groups*, Cambridge Studies in Adv. Math. 29, Cambridge University Press (1990).

[Igu62] J. Igusa, *On Siegel modular forms of genus two*, Amer. J. of Math. 84, 175–200 (1962).

[Igu67] J. Igusa, *Modular forms and projective invariants*, Amer. J. of Math. 89, 817–855 (1967).

[Igu81] J. Igusa, *Schottky's invariant and quadratic forms*, E. B. Christoffel (Aachen/Monschau, 1979), Birkhäuser, Basel-Boston Mass., 352–362 (1981).

[JS76] H. Jacquet & J. Shalika, *A non-vanishing theorem for zeta-functions of* GL_n, Inventiones Math. 38, 1–16 (1976).

[JS81a] H. Jacquet & J. Shalika, *On Euler products and the classification of automorphic representations I*, Amer. J. of Math. 103, 499–558 (1981).

[JS81b] H. Jacquet & J. Shalika, *On Euler products and the classification of automorphic representations II*, Amer. J. of Math. 103, 777–815 (1981).

[Ike01] T. Ikeda, *On the lifting of elliptic cusp forms to Siegel cusp forms of degree 2n*, Ann. of Math. 154, 641–681 (2001).

[Ike06] T. Ikeda, *Pullback of the lifting of elliptic cusp forms and Miyawaki's conjecture*, Duke Math. J. 131, 469–497 (2006).

[Ike13] T. Ikeda, *On the lifting of automorphic representations from* $\mathrm{PGL}_2(\mathbb{A})$ *to* $\mathrm{Sp}_{2n}(\mathbb{A})$ *or* $\widetilde{\mathrm{Sp}_{2n+1}}(\mathbb{A})$ *over a totally real field*, prépublication disponible à l'adresse https://www.math.kyoto-u.ac.jp/~ikeda/.

[Jan03] J. Jantzen, *Representations of algebraic groups*, Math. Survey and Monographs 107, A.M.S. (2003), deuxième éd. 2007.

[Kal13] T. Kaletha, *Rigid inner forms of real and p-adic groups*, prépublication disponible à l'adresse http://arxiv.org/abs/1304.3292.

[kv78] M. Kashiwara & M. Vergne, *On the Segal-Shale-Weil representations and harmonic polynomials*, Inventiones Math. 44, 1-47 (1978).

[Kha06] C. Khare, *Serre's modularity conjecture : the level one case*, Duke math. journal 134, 557–589 (2006).

[Kin03] O. King, *A mass formula for unimodular lattices with no roots*, Mathematics of Computation 72 (242), 839–863 (2003).

[Kna86] A. W. Knapp, *Representation theory of semisimple groups*, Princeton Univ. Press (1986).

[Kna94] A. Knapp, *Local Langlands correspondence : the archimedean case*, dans *Motives* vol. II, Proc. Symp. in Pure Math. 55, Amer. Math. Soc., Providence, RI, 393–410 (1994).

[KZ77] A. Knapp & G. Zuckerman, *Normalizing factors, tempered representations and L-groups*, dans [Cor77] vol. I, 93–105 (1977).

[Kn57] M. Kneser, *Klassenzahlen definiter quadratischer formen*, Archiv der Math. 8, 241–250 (1957).

[Kn66] M. Kneser, *Strong approximation, algebraic groups and discontinuous subgroups*, Proc. Symp. in Pure Math. 9, Amer. Math. Soc., Boulder, 187–196 (1966).

[Kn67] M. Kneser, *Lineare relationen zwischen darstellungsanzahlen quadratischer formen*, Math. Ann. 168, 31–39 (1967).

[Knu88] M.-A. Knus, *Quadratic forms, Clifford algebras and spinors*, Sem. de Mat. 1, Campinas (1988).

[KPS94] M.-A. Knus, R. Parimala & R. Sridharan, *On compositions and triality*, J. reine angew. Math. 457, 45–70 (1994).

[KV89] H. Koch & B. Venkov, *Über ganzzahlige unimodulare euklidische Gitter*, J. reine angew. Math. 398, 144-168 (1989)

[Kos59] B. Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. of Math. 81, 973–1032 (1959).

[Kot84] R. Kottwitz, *Stable trace formula : cuspidal tempered terms*, Duke Math. J. 51, 611-650 (1984).

[Kot90] R. Kottwitz, *Shimura varieties and λ-adic representations*, dans *Automorphic forms, Shimura varieties, and L-functions* vol. I, Perspectives in Math. 10, Ann Arbor (1998), 161-209 (1990).

[KS65] M. Kuga & G. Shimura, *On the zêta function of a fibre variety whose fibres are abelian varieties*, Annals of Math. 82, 478–539 (1965).

[Kur78] N. Kurokawa, *Examples of eigenvalues of Hecke operators on Siegel cusp forms of degree two*, Inventiones Math. 49, 149-165 (1978).

[LL79] J.-P. Labesse & R. Langlands, *L-indistinguishability for* SL(2), Canadian J. of Math. 31, 726-785 (1979).

[LW13] J.-P. Labesse & J.-L. Waldspurger, *La formule des traces tordue d'après le Friday Morning Seminar*, C. R. M. Monograph Series 31 (2013).

[Lan67] R. Langlands, *Letter to André Weil*, disponible à l'adresse http://www.sunsite.ubc.ca/DigitalMathArchive/Langlands/functoriality.html (1967).

[Lan70] R. Langlands, *Problems in the theory of automorphic forms*, Lecture Notes in Math. 170, Springer Verlag (1970).

[Lan71] R. Langlands, *Euler products*, Yale Math. Monographs 1, Yale University Press (1971).

[Lan73a] R. Langlands, *A little bit of number theory*, lettre à A. Weil, disponible à l'adresse http://www.sunsite.ubc.ca/DigitalMathArchive/Langlands/functoriality.html (1973).

[Lan73b] R. Langlands, *The classification of representations of real reductive groups*, Amer. Math. Soc. Math. Surveys and Monographs 31 (1973).

[Lan76] R. Langlands, *On the functional equation satisfied by Eisenstein series*, Lecture Notes in Math. 544, Springer Verlag (1976).

[Lan78] R. Langlands, *L-functions and automorphic representations*, actes du congrès international des mathématiciens, Helsinki (1978).

[Lan79] R. Langlands, *Automorphic representations, Shimura varieties, and motives (Ein Märchen)*, dans [Cor77] vol. II, 205–246 (1979).

[Lan97] R. Langlands, *Where stands functoriality today ?*, Proc. Symp. in Pure Math. 61, Edinbugh, Amer. Math. Soc. (1997).

[LS87] R. Langlands & D. Shelstad, *On the definition of transfer factors*, Math. Ann. 278, 219-271 (1987).

[Lus83] G. Lusztig, *Singularities, character formulas, and a q-analog of weight multiplicities*, Astérisque 101, Soc. Math. France, 208–227 (1983).

[MAA51] H. Maass, *Die Primzahlen in des Theorie des Siegelschen Modulfunktionen*, Math. Ann. 124, 87–122 (1951).

[MEG] T. Mégarbané, à venir.

[MES86] J.-F. Mestre, *Formules explicites et minorations de conducteurs des variétés algébriques*, Compositio Math. 58, 209–232 (1986).

[MEZ11] P. Mezo, *Character identities in the twisted endoscopy of real reductive groups*, Mem. Amer. Math. Soc. 222 (2013).

[MEZ13] P. Mezo, *Tempered spectral transfer in the twisted endoscopy of real groups*, prépublication disponible à l'adresse http://people.math.carleton.ca/~mezo/ (2013).

[MIL02] S. Miller, *The highest-lowest zero and other applications of positivity*, Duke Math. J. 112, 83-116 (2002).

[MH73] J. Milnor & D. Husemoller, *Symmetric bilinear forms*, Ergebnisse der Math. und ihrer Grenzgebiete 73, Springer Verlag (1973).

[MIY92] I. Miyawaki, *Numerical examples of Siegel cusp forms of degree 3 and their zeta-functions*, Mem. of the Faculty of Sci., Kyushu University Ser. A 46, 307–339 (1992).

[MIZ91] S.-I. Mizumoto, *Poles and residues of standard L-functions attached to Siegel modular forms*, Math. Ann. 289, 589–612 (1991).

[MW89] C. Moeglin & J.-L. Waldspurger, *Le spectre résiduel de* $\mathrm{GL}(n)$, Ann. Sci. Éc. Norm. Sup. 22, 605–674 (1989).

[MW14] C. Moeglin & J.-L. Waldspurger, *Stabilisation de la formule des traces tordue VI & X*, prépublication disponible à l'adresse http://webusers.imj-prg.fr/~jean-loup.waldspurger/ (2014).

[MOT91] *Motives*, U. Jannsen, S. Kleiman & J.-P. Serre Ed., Proc. Symp. in Pure Math. 55, Amer. Math. Soc. (1991).

[NRS01] G. Nebe, E. M. Rains & N. J. A. Sloane, *The invariants of the Clifford groups*, Des. Codes Cryptogr. 24, 99–121 (2001).

[NRS02] G. Nebe, E. M. Rains & N. J. A. Sloane, *A simple construction for the Barnes-Wall lattices*, dans *Forney Festschrift* (2002).

[NV01] G. Nebe & B. Venkov, *On Siegel modular forms of weight 12*, J. reine angew. Math. 351, 49–60 (2001).

[NGÔ10] B. C. Ngô, *Le lemme fondamental pour les algèbres de Lie*, Publ. Math. I.H.É.S. 111, 1–169 (2009).

[NI73] H.-V. Niemeier, *Definite quadratische Formen der Dimension* 24 *und Diskriminante* 1, J. Number Theory 5, 142–178 (1973).

[O'M73] O. T. O'Meara, *Introduction to quadratic forms*, Classics in Math. 117, Sringer Verlag (1973).

[PARI/GP] The PARI Group, PARI/GP version `2.5.0`, Bordeaux, 2014, http://pari.math.u-bordeaux.fr/.

[PSR87] I. Piatetski-Shapiro & S. Rallis, *L-functions for the classical groups*, Lecture Notes in Math. 1254, Springer Verlag, 1–52 (1987).

[PR94] V. Platonov & A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics 139 (1994).

[PL68] V. Pless, *On the uniqueness of the Golay codes*, J. Combinatorial Theory 5, 215–228 (1968).

[PLS74] V. Pless & N. J. A. Sloane, *Binary self-dual codes of length* 24, Bull. Amer. Math. Soc. 80, 1173–1178 (1974).

[POI76A] G. Poitou, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou, Théorie des nombres, tome 18, n. 1 exp. 6, 1–17 (1976).

[POI76B] G. Poitou, *Minorations de discriminants (d'après A. M. Odlyzko)*, Séminaire Bourbaki no. 479 1975/1976.

[PY96] C. Poor & D. S. Yuen, *Dimensions of spaces of Siegel modular forms of low weight in degree four*, Bull. Austral. Math. Soc. 54 no. 2, 309–315 (1996).

[PY07] C. Poor & D. S. Yuen, *Computations of spaces of Siegel modular cusp forms*, J. Math. Soc. Japan 59, 185-222 (2007).

[RAL79] S. Rallis, *The Eichler commutation relation and the continuous spectrum of the Weil representation*, dans *Non-Commutative Harmonic Analysis*, Lecture Notes in Math. 728, Springer Verlag, 211-244 (1979).

[RAL82] S. Rallis, *Langlands' functoriality and the Weil representation*, Amer. J. Math. 104, 469–515 (1982).

[RAM09] D. Ramakrishnan, *An exercise concerning the selfdual cuspforms on* GL(3), prépublication disponible à l'adresse http://www.math.caltech.edu/~dinakar/papers/exercise-Selfdual-GL(3).pdf (2009).

[RRST] M. Raum, N. C. Ryan, N.-P. Skoruppa, G. Tornarìa, *Explicit computations of Siegel modular forms of degree two*, prépublication disponible à l'adresse http://arxiv.org/abs/1205.6255.

[RS74] H. Resnikoff & R. Saldaña, *Some properties of Fourier coefficients of Eisenstein series of degree* 2, J. reine angew. Math. 265, 90–109 (1974).

[RUD87] W. Rudin, *Real and complex analysis*, McGraw-Hill international ed. , 3e édition (1987).

[RuS96] Z. Rudnick & P. Sarnak, *Zeros of principal* L*-functions and random matrix theory*, Duke Math. J. 81, 251–494 (1996).

[Sat63] I. Satake, *Theory of spherical functions on reductive algebraic groups over p-adic fields*, Publ. Math. I.H.É.S. 18, 5–69 (1963).

[SP99] R. Schulze-Pillot, *Siegel modular forms having the same L-functions*, J. Math. Sci. Univ. Tokyo 6, 217-227 (1999).

[SCA53] *Variétés analytiques complexes et fonctions automorphes*, séminaire H. Cartan, tome 6, Éc. Norm. Sup. Paris (1953/54).

[SCA57] *Fonctions automorphes*, séminaire H. Cartan, tome 10, Éc. Norm. Sup. Paris (1957/58).

[Ser64] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. 5, Springer Verlag (1964), 5e éd. (1994).

[Ser70] J.-P. Serre, *Cours d'arithmétique*, P.U.F., Paris (1970).

[SGA3] M. Demazur & A. Grothendieck, *Schémas en groupes*, SGA 3, Tome III, *Structure des schémas en groupes réductifs*, Séminaire de Géométrie Algébrique du Bois Marie 1962-1964, Documents mathématiques 8, Soc. Math. France (2011).

[SGA7] P. Deligne & N. Katz, *Groupes de monodromie en géométrie algébrique*, SGA7, Tome II, Séminaire de géométrie algébrique du Bois Marie 1967-69, Lecture Notes in Math. 340, Springer Verlag (1973).

[Sha10] F. Shahidi, *Eisenstein series and automorphic L-functions*, Colloquium Publ. 58, Amer. Math. Soc. (2010).

[She79] D. Shelstad, *Orbital integrals and a family of groups attached to a real reductive group*, Ann. Sci. Éc. Norm. Sup. 12, 1–31 (1979).

[She82] D. Shelstad, *L-indistinguishability for real groups*, Math. Ann. 259, 385–430 (1982).

[She08a] D. Shelstad, *Tempered endoscopy for real groups III : inversion of transfer and L-packet structure*, Representation Theory 12, 369-402 (2008).

[She08b] D. Shelstad, *Examples in endoscopy for real groups*, notes d'exposé de la conférence *Stable trace formula*, Banff (2008). Disponibles à l'adresse http://andromeda.rutgers.edu/~shelstad/.

[She11] D. Shelstad, *Some results on endoscopic transfer*, notes d'exposé de la conférence *L-packets*, Banff (2011). Disponibles à l'adresse http://andromeda.rutgers.edu/~shelstad/.

[She12a] D. Shelstad, *On geometric transfer in real twisted endoscopy*, Annals of Math. 176, 1919–1985 (2012).

[SHE12b] D. Shelstad, *On the structure of endoscopic transfer factors*, prépublication disponible à l'adresse http://andromeda.rutgers.edu/~shelstad/.

[SHE14] D. Shelstad, *On spectral transfer factors in real twisted endoscopy*, prépublication disponible à l'adresse http://andromeda.rutgers.edu/~shelstad/.

[SHI63] G. Shimura, *On the modular correspondences of* $\mathrm{Sp}(n, \mathbb{Z})$ *and their congruence relation*, Proceedings of the Nat. Academy of Sci. 49, 824–828 (1963).

[SHI71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press (1971).

[SHIN11] S.-W. Shin, *Galois representations arising from some compact Shimura varieties*, Annals of Math. 173, 1645–1741 (2011).

[SPO94] J. L. Spouge, *Computation of the Gamma, Digamma, and Trigamma functions*, SIAM. J. Numer. Anal. 31, 931–944 (1994).

[SPR81] T. Springer, *Linear algebraic groups*, Progress in Math. 9, Birkhäuser (1981), seconde éd. (1998).

[SPR79] T. Springer, *Reductive groups*, dans [COR77] vol. I, 3–27 (1979).

[ST98] J. R. Stembridge, *The partial order of dominant weights*, Adv. in Math. 136, 340–364 (1998).

[SW72] H.P.F. Swinnerton-Dyer, *On* ℓ*-adic representations and congruences for coefficients of modular forms*, dans *Modular fonctions in one variable III*, International Summer School on Modular fonctions, Antwerp (1972).

[TAI14] O. Taïbi, *Dimensions of spaces of level one automorphic forms for split classical groups using the trace formula*, prépublication disponible sur arXiv http://arxiv.org/abs/1406.4247 (2014).

[TAT79] J. Tate, *Number theoretic background*, dans [COR77] vol. II, 3–26 (1979).

[TAY91] R. Taylor, *Siegel modular forms of low weight*, Duke Math. J. 63, 281–332 (1991).

[TIT79] J. Tits, *Reductive groups over local fields*, dans [COR77] vol. I, 29–69 (1979).

[TSU83] T. Tsushima, *An explicit dimension formula for the spaces of generalized automorphic forms with respect to* $\mathrm{Sp}(2, \mathbb{Z})$, Proc. Japan Acad. 59 (1983).

[TSUY86] S. Tsuyumine, *Siegel modular forms of degree* 3, American Journal of Mathematics 108, 755–862 (1986).

[VEN80] B. Venkov, *On the classification of integral even unimodular* 24*-dimensional quadratic forms*, Chapitre 18 de [CS99].

[Vog81] D. Vogan, *Representations of real reductive Lie groups*, Progress in Math. 15 (1981).

[Vog84] D. Vogan, *On the unitarizability of certain series of representations*, Annals of Math. 120, 141-187 (1984).

[VZ84] D. Vogan & G. Zuckerman, *Unitary representations with non-zero cohomology*, Composito Math. 53, 51–90 (1984).

[Wal79] J.-L. Waldspurger, *Engendrement par des séries thêta de certains espaces de formes modulaires*, Inventiones Math. 50, 135–168 (1979).

[Wal06] J.-L. Waldspurger, *Endoscopie et changement de caractéristique*, J. Inst. Math. Jussieu 5, 423-525 (2006).

[Wal14] J. L-. Waldspurger, *Stabilisation de la formule des traces tordues I, II, III, IV, V, VII, VIII, IX*, prépublications disponibles à l'adresse http://webusers.imj-prg.fr/~jean-loup.waldspurger/ (2014).

[Wall84] N. Wallach, *On the constant term of a square integrable automorphic form*, Operator algebras and group representations, Vol. II (Neptun, 1980), 227-237, Monogr. Stud. Math. 18, Pitman, Boston, MA (1984).

[Wall88] N. Wallach, *Real reductive groups I*, Academic Press, Pure and applied math. 132 (1988).

[Walli06] L. Walling, *Action of Hecke operators on Siegel theta series I*, Int. J. Number Theory 2, 169–186 (2006).

[Wei40] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, 2e éd., Hermann (1940).

[Weis05] R. Weissauer, *Four dimensional Galois representations*, dans *Formes automorphes (II), le cas du groupe* GSp(4), édité par H. Carayol, M. Harris, J. Tilouine & Marie-France Vignéras, Astérisque 302, Soc. Math. France (2005).

[Wit41] E. Witt, *Eine Identität zwischen Modulformen zweiten Grades*, Abh. Math. Sem. Hansischen Univ. 14, 323–337 (1941).

[Wu50] W. Wu, *Classes caractéristiques et i-carrés d'une variété*, *C. R. Acad. Sci.*, 508–511 (1950).

[Yo86] H. Yoshida, *The action of Hecke operators on theta series*, Algebraic and Topological Theories (Kinosaki, 1984), 197–238, Kinokuniya, Tokyo (1986).

[Za80] D. Zagier, *Sur la conjecture de Saito-Kurokawa (d'après H. Maass)*, Séminaire de Théorie des Nombres, Paris 1979-1980 (Sém. Delange-Pisot-Poitou), Progr. in Math. 12, Birkhäuser-Verlag, Boston-Basel-Stuttgart 372-394 (1980).