SIEGEL MODULAR FORMS OF WEIGHT 13 AND THE LEECH LATTICE

GAËTAN CHENEVIER AND OLIVIER TAÏBI

ABSTRACT. For $g = 8, 12, 16$ and 24, there is a nonzero alternating g-multilinear form on the Leech lattice, unique up to a scalar, which is invariant by the orthogonal group of Leech. The harmonic Siegel theta series built from these alternating forms are Siegel modular cuspforms of weight 13 for $\mathrm{Sp}_{2g}(\mathbb{Z})$. We prove that they are nonzero eigenforms, determine one of their Fourier coefficients, and give informations about their standard L-functions. These forms are interesting since, by a recent work of the authors, they are the only nonzero Siegel modular forms of weight 13 for $\mathrm{Sp}_{2n}(\mathbb{Z})$, for any $n \geq 1$.

INTRODUCTION

As is well-known, even unimodular lattices only exist in Euclidean spaces of dimension $\equiv 0 \bmod 8$. So far, their classification up to isometry has only been achieved in dimensions 8 (the E_8 *lattice*), 16 (the lattices $\mathrm{E}_8 \oplus \mathrm{E}_8$ and E_{16}) and 24 (the *Niemeier lattices*), by works of Mordell, Witt and Niemeier respectively [CS99, Ch. 16]. An especially important Niemeier lattice is the *Leech lattice*, that we denote by Leech below. We know since Conway that, up to isometry, Leech is the unique Niemeier lattice with no *root*, *i.e.* with no element v satisfying $v.v = 2$. On the opposite, for any other even unimodular lattice L of dimension ≤ 24, then $L \otimes \mathbb{Q}$ is generated by the roots of L.

For L an integral Euclidean lattice and $g \geq 1$ an integer, we are interested in the nonzero alternating g-multilinear forms $\omega : L^g \to \mathbb{Q}$ which are invariant under the (finite) orthogonal group $\mathrm{O}(L)$ of L, *i.e.* with

$$\omega(\gamma v_1, \gamma v_2, \ldots, \gamma v_g) = \omega(v_1, v_2, \ldots, v_g)$$

for all $\gamma \in \mathrm{O}(L)$ and all $v_1, \ldots, v_g$ in L. As is easily seen, there are no such forms when $L \otimes \mathbb{Q}$ is generated by the roots of L: see Proposition 4.1. The situation is different for Leech. Indeed, recall that O(Leech) is Conway's group Co_0. A computation made in [Che20], using the character of the natural 24-dimensional representation of O(Leech) given in the $\mathbb{ATLAS}$ [CCN+85] (denoted χ_{102}) as well as the power maps there, revealed that the average characteristic polynomial of

Gaëtan Chenevier and Olivier Taïbi are supported by the C.N.R.S. and by the project ANR-14-CE25.

an element of O(Leech) is

$$\frac{1}{|\mathrm{Co}_0|}\sum_{\gamma\in\mathrm{Co}_0}\det(t-\gamma)\;=\;t^{24}+t^{16}+t^{12}+t^8+1. \tag{1}$$

Another proof of (1) can be obtained using Algorithm A given in §1.4 of [Che20]. By basic character theory of finite groups, the coefficient of t^{24-g} in the polynomial (1) is $(-1)^g$ times the dimension of the O(Leech)-invariants in $\Lambda^g\mathrm{Leech}\otimes\mathbb{Q}$, for all $g\geq 1$. It follows that for g in $\{8,12,16,24\}$, and only for those values of $g\geq 1$, there is a nonzero alternating g-multilinear form, unique up to a rational scalar,

$$\omega_g\;:\;\mathrm{Leech}^g\;\longrightarrow\;\mathbb{Q},$$

which is invariant under O(Leech). A first natural question is to exhibit concretely these ω_g. Of course, we may choose for ω_{24} the determinant taken in a $\mathbb{Z}$-basis of Leech: it is indeed O(Leech)-invariant as we know since Conway [Con69] that any element in O(Leech) has determinant 1, a non trivial fact. We will explain in §1 a simple and uniform construction of ω_8,ω_{12} and ω_{16}. It will appear that it is not an accident that the numbers $0,8,12,16$ and 24 are also the possible length of an element in the *extended binary Golay code* (see §1 for Golay codes).

The main reason why we are interested in alternating g-forms is the following classical construction of Siegel modular forms; we refer to Freitag's book [Fre83] or to van der Geer's survey [vdG08] for the general theory of Siegel modular forms. Assume L is an even unimodular lattice and $\omega : L^g\to\mathbb{Q}$ is an alternating g-form with $g\geq 1$. We may define the associated (harmonic) Siegel theta series

$$\Theta(L,\omega)\;\stackrel{\mathrm{def}}{=}\;\sum_{v\in L^g}\omega(v)\,q^{\frac{v\cdot v}{2}}. \tag{2}$$

Here $v\cdot v$ abusively denotes the Gram matrix $(v_i\cdot v_j)_{1\leq i,j\leq g}$ with $v=(v_1,\dots,v_g)$, and q^n abusively denotes the function $\tau\mapsto e^{2\,\pi\,i\,\mathrm{Tr}(n\tau)}$ for $\tau\in\mathrm{M}_g(\mathbb{C})$ in the Siegel upper-half space. As alternating g-forms on L are also *harmonic polynomials of weight* 1 on L^g, the theta series $\Theta(L,\omega)$ is a Siegel modular form of weight $1+\frac{\mathrm{rk}L}{2}$ for the full Siegel modular group $\mathrm{Sp}_{2g}(\mathbb{Z})$: see [Fre83, Kap. III §3]. Two simple observations are then in order:

(a) The modular form $\Theta(L,\omega)$ is a *cuspform*. Indeed, since $\omega(v_1,\dots,v_g)=0$ unless $v_1,\dots,v_g\in L$ are linearly independent in $L\otimes\mathbb{Q}$, the (Fourier) coefficient of $\Theta(L,\omega)$ in q^n vanishes if $\det n=0$ (which is the definition of a cuspform).

(b) We may assume that ω is $\mathrm{O}(L)$-invariant. Indeed, we easily see the equality $\Theta(L,\omega\circ\gamma^g)=\Theta(L,\omega)$ for all $\gamma\in\mathrm{O}(L)$, and thus we have $\Theta(L,\omega)=\Theta(L,\omega')$ with $\omega'=\frac{1}{|\mathrm{O}(L)|}\sum_{\gamma\in\mathrm{O}(L)}\omega\circ\gamma^g$, by linearity of $-\mapsto\Theta(L,-)$.

As a consequence of (b) and of the analysis in the second paragraph, for $\mathrm{rk}\,L\leq 24$ the only possibly nonzero $\Theta(L,\omega)$ are thus, up to a scalar, the modular forms

$$\mathrm{F}_g\;\stackrel{\mathrm{def}}{=}\;\Theta(\mathrm{Leech},\omega_g) \tag{3}$$

for $g = 8, 12, 16$ and 24. By constructions, these are cuspforms of weight $1+\frac{24}{2} = 13$ with rational Fourier coefficients. Better, F_g generates the space of all $\Theta(L, \omega)$ with L a Niemeier lattice and ω an alternating g-form on L. As this subspace of Siegel modular forms is stable under the Hecke operators by the main result of [Fre82], it follows that each F_g is actually an eigenform... provided it is nonzero ! (see §4).

Among these four forms F_g, only F_{24} seems to have been studied in the past, by Freitag, in the last section of [Fre82]. He observed that F_{24} is indeed a nonzero eigenform. Indeed, if we choose ω_{24} as above, and if $u \in \mathrm{Leech}^{24}$ is a $\mathbb{Z}$-basis of Leech with $\omega_{24}(u) = 1$, there are exactly $|\mathrm{O}(\mathrm{Leech})|$ vectors $v \in \mathrm{Leech}^{24}$ with $v \cdot v = u \cdot u$, namely the γu with γ in $\mathrm{O}(\mathrm{Leech})$. They all satisfy $\omega_{24}(v) = 1$ since any element of $\mathrm{O}(\mathrm{Leech})$ has determinant 1. It follows that the coefficient of $q^{\frac{u\cdot u}{2}}$ in F_{24} is $|\mathrm{O}(\mathrm{Leech})|$, it is thus nonzero.

Nevertheless, the following theorem was recently proved by the authors in [CT20, Cor. 1 & Prop. 5.12]:

Theorem 1. *For $g \geq 1$ the space of weight 13 Siegel modular forms for $\mathrm{Sp}_{2g}(\mathbb{Z})$ is 0, or we have $g \in \{8, 12, 16, 24\}$, it has dimension 1, and is generated by F_g.*

The proof given *loc. cit.* of the non vanishing of the forms F_g is quite indirect. Using quite sophisticated recent results from the theory of automorphic forms (Arthur's classification [Art13], recent description by Arancibia, Moeglin and Renard of certain local Arthur packets [AMR18, MR]) we observed the existence of 4 weight 13 Siegel modular eigenforms for $\mathrm{Sp}_{2g}(\mathbb{Z})$ of respective genus $g = 8, 12, 16$ and 24, and with specific standard L-function. The cases $g = 16$ and $g = 24$ are especially delicate, and use recent results of Moeglin and Renard [MR]. Using works of Böcherer [Bö89], we then checked that they must be linear combinations of Siegel theta series construction from alternating g-multilinear forms on Niemeier lattices, hence must be equal to F_g by what we explained above. Our aim here is to provide a more direct and elementary proof of the non vanishing of the 3 remaining forms F_g, by exhibiting a nonzero Fourier coefficient.

Let $F = \sum_n a_n q^n$ be a Siegel modular form for $\mathrm{Sp}_{2g}(\mathbb{Z})$ of *odd* weight, and N an even Euclidean lattice of rank g. If v and v' in N^g are $\mathbb{Z}$-bases of N, with associated Gram matrices $2n$ and $2n'$, we have $a_n = (\det \gamma)\, a_{n'}$ where γ is the unique element of $\mathrm{GL}(N)$ with $\gamma(v) = v'$. In particular, the element $\pm a_n$ (a *complex number modulo sign*) only depends on the isometry class of N, and will be denoted $a_N(F)$ and called *the N-th Fourier coefficient of F*. For instance, we have $a_{\mathrm{Leech}}(\mathrm{F}_{24}) = \pm|\mathrm{O}(\mathrm{Leech})|$. Also, we trivially have $a_N(F) = 0$ if $\mathrm{O}(N)$ has an element of determinant -1. This lead us to emphasize the following definition.

Definition. *We say that an integral lattice N is* orientable *if any element of* $\mathrm{O}(N)$ *has determinant* 1.

Four orientable rank g even lattices Q_g with g in $\{8, 12, 16, 24\}$ will play an important role below. The lattice Q_{24} is simply Leech. The lattice Q_{12} is the

unique even lattice L of rank 12 without roots with $L^\sharp/L \simeq (\mathbb{Z}/3\mathbb{Z})^6$, where $L^\sharp$ denotes the dual lattice of L (see the General Notations). It is also known as the *Coxeter-Todd lattice* [CT53] (see also [CS99, Ch. 4 §9]). The lattices Q_8 and Q_{16} are the unique even lattices L without roots, of respective rank 8 and 16, with $L^\sharp/L \simeq (\mathbb{Z}/5\mathbb{Z})^4$. The lattice Q_8 was known to Maass and is sometimes called the *icosian lattice* (see [CS88, pp.49–50] where it is denoted $Q_8(1)$). These properties, and other relevant ones for our purposes, will be reviewed in §2 and proved in §3. Some of them were already known or had been proved in a different way: see Remark 2.3. An important one is that there is a unique O(Leech)-orbit of sublattices of Leech isometric to Q_g. Our main result is the following.

Theorem 2. *For each $g \in \{8, 12, 16, 24\}$, the Q_g-Fourier coefficient of F_g is nonzero. More precisely, if we normalize ω_g as in Definition 1.5, we have*

$$a_{\mathrm{Q}_g}(\mathrm{F}_g) \;=\; \pm\, \mathrm{n}_g\, \mathrm{e}_g,$$

where n_g is the number of isometric embeddings $\mathrm{Q}_g \hookrightarrow$ Leech, and with $\mathrm{e}_8 = \mathrm{e}_{16} = 5$, $\mathrm{e}_{12} = 18$ and $\mathrm{e}_{24} = 1$.

As we will see, the quantity e_g has a conceptual explanation in terms of the extended binary Golay code and its automorphism group the Mathieu group M_{24}: see Remark 2.6. We will also prove $\mathrm{n}_g = |\mathrm{O}(\mathrm{Leech})|/\kappa_{24-g}$, with $\kappa_g = 1$ for $g < 12$, $\kappa_{12} = 3$ and $\kappa_{16} = 10$. We would like to stress that our proof of Theorem 2 does not rely on any computer calculation other than the simple summations (1) and (1.1) below. Last but not least, we discuss in the last section the standard L-functions of the eigenforms F_g: see Theorem 4.4. This last part is less elementary than the others, and relies on [Art13, AMR18, Taï19] (but not on [MR]).

We end this introduction by discussing prior works on the determination of the spaces $\mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ of Siegel modular forms of weight k for $\mathrm{Sp}_{2g}(\mathbb{Z})$, and its subspace $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ of cuspforms, for $k < 13$. For this purpose, the subspace Θ_n^g of $\mathrm{M}_n(\mathrm{Sp}_{2g}(\mathbb{Z}))$ generated by classical[1] Siegel theta series of even unimodular lattices of rank $2n$ has drawn much attention, starting with Witt's famous conjecture $\dim \Theta_8^g = 2 \Leftrightarrow g \geq 4$, proved by Igusa. The study of Θ_{12}^g has a rich history as well, that we briefly recall now (see the introduction of [CL19] for more informations). Erokhin proved $\dim \Theta_{12}^g = 24$ for $g \geq 12$ in [Ero79], and Borcherds-Freitag-Weissauer showed $\dim \Theta_{12}^{11} = 23$ in [BFW98]. Nebe and Venkov conjectured in [NV01] that the 11 integers $\dim \Theta_{12}^g$, for $g = 0, \ldots, 10$, are respectively given by

$$1, 2, 3, 4, 6, 8, 11, 14, 18, 20 \text{ and } 22,$$

and proved it for $g \neq 7, 8, 9$. Ikeda used his "lifts" [Ike01, Ike06] to determine the standard L-functions of 20 of the 24 eigenforms in Θ_{12}^{12}. The full Nebe-Venkov conjecture was finally proved by Chenevier-Lannes [CL19], as well as the determination of the 4 standard L-functions not determined by Ikeda. Moreover, these

[1]Recall that these theta series are given by Formula (2) for "$\omega = 1$".

authors show $\Theta_{12}^g = \mathrm{M}_{12}(\mathrm{Sp}_{2g}(\mathbb{Z}))$ for all $g \leq 12$, as well as $\Theta_8^g = \mathrm{M}_8(\mathrm{Sp}_{2g}(\mathbb{Z}))$ for all $g \leq 8$. Simpler proof of these results, as well as their extension to all g, were then given in [CT20], in which the vanishing of $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ is proved for $g > k$ and $k < 13$. Let us mention that dimensions and generators of $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ with $g \leq k \leq 11$, as well as standard L-functions of eigenforms, are also given in [CL19] and [CT20], completing previous works of several authors, including Ikeda, Igusa, Tsuyumine, Poor-Yuen and Duke-Imamoglu.

Acknowledgements: The authors thank an anonymous referee for bringing to their attention the references [RS98] and [GL11] (see Remark 2.3), and another referee for several remarks that led us to improve the exposition.

General notations and terminology

Let X be a set. We denote by $|X|$ the cardinality of X and by $\mathfrak{S}_X$ its symmetric group. Let k be a commutative ring. We denote by $k\,X$ the free k-module over X. The elements x of X form a natural k-basis of $k\,X$ that we will often denote by ν_x to avoid confusions. For $S \subset X$ we also set $\nu_S = \sum_{x \in S} \nu_x$.

If V and W are two k-modules, a *quadratic map* $q : V \to W$ is a map satisfying $q(\lambda v) = \lambda^2 q(v)$ for all λ in k and v in V, and such that the map $V \times V \to W$ defined by $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is k-bilinear (the *associated bilinear map*). We also use the terminology *quadratic/bilinear form* for quadratic/bilinear map in the case $W = k$.

A *quadratic space* over k is a k-module V equipped with a quadratic map (usually k-valued, but not always). Such a space has an isometry group, denoted $\mathrm{O}(V)$, defined as the subgroup of k-linear automorphisms g of V with $q \circ g = q$. If V is a quadratic space, we denote by $-V$ the quadratic space with same underlying group but opposite quadratic map. If V is furthermore a free k-module of finite rank, and with k-valued quadratic map, the determinant of the Gram matrix of its associated bilinear map in any k-basis of V will be denoted by $\det V$ (an element of k modulo multiplication by squares in $k^\times$).

A *linking quadratic space* (a qe-module in the terminology of [CL19, Ch. 2]) is a finite quadratic space over $\mathbb{Z}$ whose quadratic map is $\mathbb{Q}/\mathbb{Z}$-valued (or "linking") and with nondegenerate associated bilinear map. For p an odd integer, we denote by $\mathrm{I}_n \otimes \mathbb{Z}/p\mathbb{Z}$ the linking quadratic space $(\mathbb{Z}/p\mathbb{Z})^n$ equipped with $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$-valued quadratic map $\frac{1}{p}\sum_{i=1}^n x_i^2$. If A is a finite abelian group, the *hyperbolic* linking quadratic space over A is $\mathrm{H}(A) = A \oplus \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, with the quadratic map $(x, \varphi) \mapsto \varphi(x)$.

Let L be a lattice in the Euclidean space E, with inner product $x \cdot y$. The *dual lattice* of L is the lattice $L^\sharp = \{x \in E \mid x \cdot L \subset \mathbb{Z}\}$. Assume L is *integral*, that is $L \subset L^\sharp$. A *root* of L is an element $\alpha \in L$ with $\alpha \cdot \alpha = 2$. The roots of L form a (possibly empty) root system $\mathrm{R}(L)$ of type ADE and rank $\leq \dim E$: see the beginning of §3 for much more about roots and root systems.

Assume furthermore that L is even (that is $x \cdot x$ is in $2\mathbb{Z}$ for all x in L). Then we view L as a quadratic space over $\mathbb{Z}$ for the quadratic form $x \mapsto \frac{x\cdot x}{2}, L \to \mathbb{Z}$. Moreover, the finite abelian group $L^\sharp/L$ equipped with its nondegenerate $\mathbb{Q}/\mathbb{Z}$-valued quadratic map $x \mapsto \frac{x\cdot x}{2} \bmod \mathbb{Z}$ is a linking quadratic space denoted $\operatorname{res} L$ and called the *residue* of L (often also called the *discriminant group* or the *glue group*).

Contents

1. The forms ω_g

We fix a set Ω with 24 elements and identify $\mathscr{P}(\Omega)$, the set of all subsets of Ω, to the $\mathbb{Z}/2\mathbb{Z}$-vector space $(\mathbb{Z}/2\mathbb{Z})\,\Omega$, via the map $S \mapsto \nu_S$ of the General Notations. In particular, for any two subsets $S_1, S_2 \subset \Omega$ we have $S_1 + S_2 = (S_1 \cup S_2) \smallsetminus (S_1 \cap S_2)$.

We fix an *extended binary Golay code* $\mathscr{G}$ on Ω, of for short, a *Golay code*. By definition, this means that $\mathscr{G}$ a 12-dimensional linear subspace of $(\mathbb{Z}/2\mathbb{Z})\,\Omega$ such that for all $C \in \mathscr{G} \smallsetminus \{0\}$ we have $|C| \geq 8$. We refer to [Ple98, §2.4], [Ebe13, §2.8] and to [CS99] Ch. 3 §2.8 and Ch. 10 §2, for various constructions of such a code.[2] The precise choice of $\mathscr{G}$ will not matter, since Golay codes are essentially unique. Indeed, the set of Golay codes on Ω forms a single orbit under $\mathfrak{S}_\Omega$: see [Ple98, §10.2] or [Ebe13, §2.8].

As explained in any of the references above, we have $\Omega \in \mathscr{G}$ and $\mathscr{G}$ is a *doubly even code*: for all $C \in \mathscr{G}$ we have $|C| \equiv 0 \bmod 4$, and thus $|C| \equiv 0, 8, 12, 16$ or 24. An *octad* is an 8-element subset of Ω belonging to $\mathscr{G}$. Their most important properties are that they generate $\mathscr{G}$ as a vector space and that any 5 elements of Ω belong to a unique octad, *i.e.* the set of octads is a *Steiner* $S(5, 8, 24)$ *system*: see [CS99, Ch. 10, §2.1, Theorem 9]. There are in particular $\binom{24}{5}/\binom{8}{5} = 759$ octads. As Witt had previously shown that a Steiner $S(5, 8, 24)$ system is unique up to permutation [Wit37], there is thus a one-to-one correspondence between Golay codes on Ω and Steiner $S(5, 8, 24)$ system on Ω, obtained by sending $\mathscr{G}$ to is system of octades.

[2] In those references, a Golay code is often called a $[24, 12, 8]$ binary code. It is also denoted by $\mathscr{C}_{24}$ by Conway in [CS99, Ch. 10 §2], that we will use as a main reference.

We now recall how to define Leech using $\mathscr{G}$, following Conway in [CS99, Ch. 10, §3]. We view the 24-dimensional space $\mathbb{R}\,\Omega$ as an Euclidean space with orthonormal (canonical) basis the ν_i with i in Ω. For $S \subset \Omega$, recall that we set $\nu_S = \sum_{i\in S} \nu_i$. Following Conway *loc. cit.*, the Leech lattice may be defined as the subgroup of $\mathbb{R}\,\Omega$ generated by the $\frac{1}{\sqrt{8}}\ 2\nu_O$ with O an octad, and the $\frac{1}{\sqrt{8}}\ (\nu_\Omega - 4\nu_i)$ with i in Ω.

The *Mathieu group* associated to $\mathscr{G}$ is the subgroup of $\mathfrak{S}_\Omega \simeq \mathfrak{S}_{24}$ preserving $\mathscr{G}$, and is simply denoted by M_{24}. Alternatively, it is the stabilizer in $\mathfrak{S}_\Omega$ of the set of octads of $\mathscr{G}$. The original definition of M_{24} by Mathieu was given as a concrete 5-transitive subgroup of S_{24}, and the equivalence with the definition here is due to Witt: see [CS99, Ch. 10 §2.1]. The group M_{24} has $48 \cdot 24!/19! = 244823040$ elements. It acts on $\mathbb{R}\,\Omega$ (permutation representation), which realizes it as a subgroup of $\mathrm{O}(\mathrm{Leech})$. We know since Frobenius the cycle decompositions, and cardinality, of all the conjugacy classes of M_{24} acting on Ω [Fro04, p. 12-13]. Presumably Frobenius used Mathieu's original construction of M_{24}; in any case Frobenius did not give any explanation for this computation. More recently Sawabe [Saw99] gave a detailed proof of this classification using a method due to Kondo. Alternatively, nowadays such computations are straightforward for computer packages such as GAP [GAP21]. For the convenience of the reader the cycle decompositions and cardinality of all the conjugacy classes in M_{24} are gathered in Table 1 below, which gives for each cycle shape the quantity `cent` $= |\mathrm{M}_{24}|/$`card`, where `card` is the number of elements of this shape in M_{24}. We write this number in the form $n/2$ in the five cases where there are more than one conjugacy class of the given shape. In these five cases, there are exactly two conjugacy classes, each of which containing $|\mathrm{M}_{24}|/n$ elements. This table allows

shape	$1^8\,2^8$	2^{12}	$1^6\,3^6$	3^8	$2^4\,4^4$	$1^4\,2^2\,4^4$	4^6	$1^4\,5^4$	$1^2\,2^2\,3^2\,6^2$	6^4
cent	21504	7680	1080	504	384	128	96	60	24	24
shape	$1^3 7^3$	$1^2\,2\,4\,8^2$	$2^2\,10^2$	$1^2\,11^2$	$2\,4\,6\,12$	12^2	$1\,2\,7\,14$	$1\,3\,5\,15$	$3\,21$	$1\,23$
cent	42/2	16	20	11	12	12	14/2	15/2	21/2	23/2

TABLE 1. The cycle shape of the nontrivial elements of M_{24}.

us to compute the average characteristic polynomial of an element in M_{24}, and we find:

Fact 1.1. *The polynomial* $\frac{1}{|\mathrm{M}_{24}|}\sum_{\gamma\in\mathrm{M}_{24}} \det(t-\gamma)$ *is*

$$t^{24} - t^{23} - t^{17} + 2\,t^{16} - t^{15} - t^{13} + 2\,t^{12} - t^{11} - t^9 + 2\,t^8 - t^7 - t + 1.$$

In particular, the space of M_{24}-invariant alternating g-multilinear forms on $\mathbb{Q}\,\Omega$ has dimension 2 for $g = 8, 12, 16$. We will now exhibit concrete generators for the M_{24}-invariants in each $\Lambda^g\,\mathbb{Q}\,\Omega$. We start with some general preliminary remarks.

Let G be a group acting on a finite set X. A subset $S \subset X$ will be called *G-orientable* if the stabilizer G_S of S in G acts on S by even permutations. If S is G-orientable, then so is gS for all $g \in G$. An *orientation* of a G-orientable S is the choice of a numbering of its elements up to even permutations, or more formally, denoting $n = |S|$, an $\mathfrak{A}_n$-orbit of bijections $\{1, \dots, n\} \xrightarrow{\sim} S$. Consider the permutation representation of G on $\mathbb{Q}X$ and fix an integer $g \geq 1$. The dimension of the G-invariant subspace in $\Lambda^g \mathbb{Q}X$ is the number of G-orbits of G-orientable subsets of X with g elements. Indeed, fix a G-orientable subset S of X with $|S| = g$, choose an orientation $o : \{1, \dots, g\} \xrightarrow{\sim} S$, and set

$$\beta_o = o(1) \wedge o(2) \wedge \cdots \wedge o(g) \quad \text{and} \quad \sigma_o = \sum_{\gamma \text{ in } G/G_S} \gamma \, \beta_o. \tag{4}$$

Then β_o is fixed by G_S, and σ_o is a nonzero G-invariant in $\Lambda^g \mathbb{Q}X$. Both $\pm\beta_o$ and $\pm\sigma_o$ only depend on S, we denote them respectively by β_S and σ_S. We also set $\beta_\emptyset = \sigma_\emptyset = 1$.

Fact 1.2. *If a group G acts on the finite set X, and if $\mathcal{S}_g$ is a set of representatives for the G-orbits of G-orientable subsets of X with g elements, then the σ_S with S in $\mathcal{S}_g$ are a $\mathbb{Q}$-basis of the G-invariants in $\Lambda^g \mathbb{Q}X$.*

Proof. Choose, for any subset $S \subset X$ with g elements, a bijection $o_S : \{1, \dots, g\} \xrightarrow{\sim} S$, and set $\beta_{o_S} = o_S(1) \wedge o_S(2) \wedge \cdots \wedge o_S(g) \in \Lambda^g \mathbb{Q}X$ as in (4). The family $(\beta_{o_S})_S$, where S ranges over all subsets of X having g elements, is obviously a basis of $\Lambda^g \mathbb{Q}X$. Also, any $\gamma \in G$ maps β_{o_S} to $e_{\gamma,S}\beta_{o_{\gamma S}}$ for some sign $e_{\gamma,S}$. In particular, the family $(\sigma_S)_{S \in \mathcal{S}_g}$ of the statement is $\mathbb{Q}$-linearly independent. To check it is a generating family, choose an element $\lambda = \sum_S \lambda_S \beta_{o_S}$ of $\Lambda^g \mathbb{Q}X$ invariant under G, or equivalently, with $\lambda_{\gamma S} = e_{\gamma,S}\lambda_S$ for all $\gamma \in G$ and all $S \subset X$ of size g. By replacing λ with $\lambda - \sum_{S \in \mathcal{S}_g} \lambda_S \sigma_S$, we may assume $\lambda_S = 0$ for all $S \in \mathcal{S}_g$. If S is G-orientable, we have $S = \gamma S'$ for some $S' \in \mathcal{S}_g$, hence $\lambda_S = \pm\lambda_{S'} = 0$. Otherwise, we have $e_{\gamma,S} = -1$ for some $\gamma \in G_S$ by definition, hence $\lambda_S = -\lambda_S = 0$. □

The following lemma could probably be entirely deduced from Conway's results in [CS99, Ch. 10 §2]. We will rather use Facts 1.1 & 1.2 to prove it. Recall that we identify $\mathscr{P}(\Omega)$ with $(\mathbb{Z}/2\mathbb{Z})\,\Omega$.

Lemma 1.3. *Let S be a subset of Ω. Then S is M_{24}-orientable if, and only if, it is of the form $C + P$, with C in $\mathscr{G}$ and either $|P| \leq 1$, or $|P| = 2$ and $|P \cap C| = 1$.*

Proof. The elements of $\mathscr{G}$ have size $0, 8, 12, 16$ or 24. The $C + P$ with C in $\mathscr{G}$ and P a point thus have size $1, 7, 9, 11, 13, 15, 17$ or 23, and the $C + P$ with $|P| = 2$ and $|C \cap P| = 1$ have size $8, 12$ or 16. If we can show that all of those subsets are M_{24}-orientable, then Facts 1.1 and 1.2 will not only prove the lemma, but also that there is a single M_{24}-orbit of each of these 16 types of subsets (namely the aforementioned 5 types of elements of $\mathscr{G}$, and $8 + 3 = 11$ types of $C + P$.)

Fix C in $\mathscr{G}$, denote by $G_C \subset \mathrm{M}_{24}$ its stabilizer and by I_C the image of the natural morphism $G_C \to \mathfrak{S}_C$. If we have $C = 0$ or $C = \Omega$, then C is M_{24}-orientable: in [CS99, Ch. 10 §2] the group M_{24} is first defined as a subgroup of A_{24} generated by explicit elements, and Theorem 10 *loc. cit.* identifies it to the stabilizer of the Golay code. If C is an octad, Conway showed in Theorem 10 *loc. cit.* that I_C is the full alternating group of C, so that octads are M_{24}-orientable. As Ω is M_{24}-orientable, it follows that complements of octads are M_{24}-orientable as well. If C is a dodecad, *i.e.* if C has 12 elements, Conway showed that I_C is a Mathieu permutation group M_{12} over C (Theorem 15 *loc. cit.*). In [CS99, Ch. 10 §1.5] M_{12} is defined as a subgroup of A_{12}, and so dodecads are M_{24}-orientable.

Fix furthermore a subset P of Ω, assuming first $|P| \leq 3$, and consider the subset $C + P$ in $\mathscr{P}(\Omega)$. If γ in M_{24} preserves $C + P$, we have

$$C + \gamma(C) = P + \gamma(P).$$

The left-hand side is an element in $\mathscr{G}$, hence so is $P + \gamma(P)$. But this last subset has at most 6 elements, hence must be 0. It follows that the stabilizer of $C + P$ is the subgroup of G_C stabilizing P. If we assume furthermore either $|P| = 1$, or $|P| = 2$ and $|P \cap C| = 1$, we deduce that the M_{24}-orientability of C implies that of $C + P$, and we are done. □

The code $\mathscr{G}$ itself also embeds in $\mathrm{O}(\mathbb{R}\,\Omega)$ by letting the element S of $\mathscr{G}$ act on ν_i by -1 if i is in S, 1 otherwise. As shown by Conway [CS99, Ch. 10, §3, Thm. 26], this is also a subgroup of O(Leech), obviously normalized by M_{24}. The subgroup of O(Leech) generated by $\mathscr{G}$ and M_{24} is denoted by N or $2^{12}\mathrm{M}_{24}$ by Conway. It will play a role in the proof of the following proposition.

Proposition 1.4. *For all g in $\{0, 8, 12, 16, 24\}$, the line of* O(Leech)*-invariants in $\Lambda^g\mathrm{Leech} \otimes \mathbb{Q}$ is generated by σ_C, where C is any element of $\mathscr{G}$ with $|C| = g$.*

Proof. Fix $g \geq 0$ and set $V_g = \Lambda^g \mathbb{Q}\,\Omega$. We have the trivial inclusions

$$V_g^{\mathrm{O(Leech)}} \subset V_g^N \subset V_g^{\mathrm{M}_{24}},$$

the dimension of the left-hand side being given by (1), and that of the right-hand side by Fact 1.1. We will show that V_g^N is non-zero only for g in $\{0, 8, 12, 16, 24\}$, and that in theses cases V_g^N is generated by σ_C for $C \in \mathscr{G}$ with $|C| = g$ (recall from the proof of Lemma 1.3 that M_{24} acts transitively on the set of such C's). This implies the proposition.

Let S be an M_{24}-orientable subset of Ω of the form $S = C + P$ as in the statement of Lemma 1.3. If Conway's group N fixes σ_S, then the element β_S in (4) has to be fixed by the action of C. By definition, this element of $\mathscr{G}$ acts on β_S by multiplication by $(-1)^{|S\cap C|}$, so we must have $|S \cap C| \equiv 0 \bmod 2$, hence $P = 0$ or $|P| = 1$ and $P \cap C = \emptyset$. In the latter case, the element $C' = \Omega \smallsetminus C$ of $\mathscr{G}$ contains P, so it maps β_S to $-\beta_S$ and the basis σ_S of $V_g^{\mathrm{M}_{24}}$ is not fixed by N. We have proved $\dim V_g^N \leq 1$ for g in $\{0, 8, 12, 16, 24\}$, and $V_g^N = 0$ otherwise. Fix now C

in $\mathscr{G}$ and set $g = |C|$. For all C' in $\mathscr{G}$ we have $|C \cap C'| \equiv 0 \bmod 2$. This shows that N acts trivially on σ_C: we have proved $V_g^N = \mathbb{Q}\,\sigma_C$. □

The inner product Leech × Leech → $\mathbb{Z}$, $(x, y) \mapsto x \cdot y$, induces for each integer $g \geq 0$ an O(Leech)-equivariant isomorphism $\Lambda^g\text{Leech} \otimes \mathbb{Q} \xrightarrow{\sim} \text{Hom}(\Lambda^g\text{Leech}, \mathbb{Q})$. This isomorphism sends the element $v_1 \wedge v_2 \wedge \cdots \wedge v_g$, with v_i in Leech for all i, to the alternating g-multilinear form on Leech defined by $(x_1, \ldots, x_g) \mapsto \det(x_i \cdot v_j)_{1 \leq i,j \leq g}$.

Definition 1.5. *The element σ_C, where C is any element of $\mathscr{G}$ with $|C| = g$, viewed as above as an alternating g-multilinear form on* Leech*, will be denoted by ω_g. It is well defined up to a sign, nonzero, and* O(Leech)*-invariant.*

Note that by definition, we have $\omega_0 = 1$, and $\pm\omega_{24}$ is the determinant taken in the canonical basis ν_i of $\mathbb{Q}\,\Omega$, or equivalently, in a $\mathbb{Z}$-basis of Leech as the latter is unimodular.

For the sake of completeness, we end this section with the determination of the ring structure of the O(Leech)-invariants in the exterior algebra $\Lambda\,\text{Leech} \otimes \mathbb{Q}$. Denote by m_g the number of g-element subsets of $\mathscr{G}$. We have $\text{m}_0 = \text{m}_{24} = 1$, $\text{m}_8 = \text{m}_{16} = 759$ and $\text{m}_{12} = 2^{12} - 2 - 2 \cdot 759 = 2576$. Let us simply write σ_g for the element $\pm\sigma_C$ with C in $\mathscr{G}$ and $|C| = g$.

Proposition 1.6. *We have $\sigma_8 \wedge \sigma_8 = \pm 30\,\sigma_{16}$ and $\sigma_g \wedge \sigma_{24-g} = \pm\,\text{m}_g\,\sigma_{24}$ for all g in $\{0, 8, 12, 16, 24\}$.*

Proof. Fix $C \subset \Omega$ of size g, denote by C' its complement, and fix c and c' respective orientations of C and C'. The stabilizers of C and C' in M_{24} coincide, call them G. We have $\sigma_C \wedge \sigma_{C'} = \pm \sum_{\gamma,\gamma' \text{ in } \text{M}_{24}/G} \gamma(\beta_c) \wedge \gamma'(\beta_{c'})$. An element in this sum is nonzero if, and only if, we have $\gamma(C) \cap \gamma'(C') = \emptyset$, or equivalently $\gamma'(C) = \gamma(C)$, *i.e.* $\gamma = \gamma'$. We conclude the second assertion by the M_{24}-orientability of Ω and the equality $|\text{M}_{24}/G| = \text{m}_g$.

We now determine $\sigma_8 \wedge \sigma_8$. Let $\mathscr{T}$ be the set of triples (O_1, O_2, O_3) where the O_i are octads satisfying $O_1 \coprod O_2 \coprod O_3 = \Omega$ (*ordered trios*). By [CS99, Ch. 10, §2, Thm. 18], M_{24} acts transitively on $\mathscr{T}$ and we have $|\mathscr{T}| = 30\,\text{m}_8$. Fix (O_1, O_2, O_3) in $\mathscr{T}$, an orientation o_i of each O_i, and denote by S_i the stabilizer of O_i in M_{24}. As octads are M_{24}-orientable, for any $\gamma_1, \gamma_2, \gamma_3$ in M_{24} the element $t(\gamma_1, \gamma_2, \gamma_3) = \gamma_1\beta_{o_1} \wedge \gamma_2\beta_{o_2} \wedge \gamma_3\beta_{o_3}$ only depends on the γ_i modulo S_i. We have

$$\sigma_{o_1} \wedge \sigma_{o_2} \wedge \sigma_{o_3} = \sum_{\gamma_i \in \text{M}_{24}/S_i} t(\gamma_1, \gamma_2, \gamma_3). \tag{5}$$

Observe that $t(\gamma_1, \gamma_2, \gamma_3)$ is nonzero if and only if the three octads $\gamma_1(O_1)$, $\gamma_2(O_2)$ and $\gamma_3(O_3)$ are disjoint, in which case we have $t(\gamma_1, \gamma_2, \gamma_3) = \pm t(1, 1, 1) = \pm\sigma_{24}$. There are thus exactly $|\mathscr{T}|$ nonzero terms $t(\gamma_1, \gamma_2, \gamma_3)$ in the sum (5). Fix such a nonzero term. The transitivity of M_{24} on $\mathscr{T}$ shows the existence of γ in M_{24} with

$\gamma\gamma_i \in S_i$ for each i. As Ω is M_{24}-orientable, we have

$$t(\gamma_1,\gamma_2,\gamma_3) \,=\, \gamma t(\gamma_1,\gamma_2,\gamma_3) \,=\, t(\gamma\gamma_1,\gamma\gamma_2,\gamma\gamma_3) \,=\, t(1,1,1).$$

We have proved $\sigma_8 \wedge \sigma_8 \wedge \sigma_8 \,=\, \pm\,|\mathscr{T}|\,\sigma_{24}$. As $\sigma_8 \wedge \sigma_8$ must be a multiple of σ_{16}, we conclude by the identity $\sigma_8 \wedge \sigma_{16} \,=\, \pm \mathrm{m}_8\,\sigma_{24}$. □

2. Fixed point lattices of some prime order elements in M_{24}

We keep the notations of §1, and fix an element c in M_{24} of order p, with p an odd prime. We are interested in the fixed points lattice

$$Q = \{v \in \mathrm{Leech} \mid cv = v\},$$

and in its orthogonal $Q^\perp$ in Leech. Let $F \subset \Omega$ the subset of fixed points of c and $\mathscr{Z} \subset \mathscr{P}(\Omega)$ the set of supports of its p-cycles. We have $a + p\,b \,=\, 24$ with $a = |F|$, $b = |\mathscr{Z}|$, and $b \geq 1$. Those lattices are special cases of those considered in [HL90].

Lemma 2.1. *The lattices Q and $Q^\perp$ are even, without roots, of respective ranks $a+b$ and $(p-1)b$, and we have $\operatorname{res} Q \,\simeq\, \mathrm{I}_b \otimes \mathbb{Z}/p\mathbb{Z}$ and $\operatorname{res} Q^\perp \simeq -\operatorname{res} Q$.*

Proof. It is clear that Q and $Q^\perp$ are even and without roots, as so is Leech. We also have $p\,\mathrm{Leech} \,\subset Q \oplus Q^\perp$ because of the identity $1+c+c^2+\cdots+c^{p-1} \in p+(c-1)\mathbb{Z}[c]$. As Leech is unimodular and p is odd, we deduce that both $\det Q$ and $\det Q^\perp$ are odd. It is thus enough to prove both assertions about $\operatorname{res} Q$ and $\operatorname{res} Q^\perp$ after inverting 2. As Ω is the disjoint union of 3 octads, note that the 24 elements $\sqrt{2}\,\nu_i$ with $i \in \Omega$ form an orthogonal $\mathbb{Z}[\frac{1}{2}]$-basis of $\mathrm{Leech}[\frac{1}{2}]$.

On the one hand, this implies that the a elements $\sqrt{2}\,\nu_i$ with $i \in F$, and the b elements $\sqrt{2}\,\nu_Z$ with $Z \in \mathscr{Z}$, form an orthogonal $\mathbb{Z}[\frac{1}{2}]$-basis of $Q[\frac{1}{2}]$. For the quadratic form $\mathrm{q}(x) = \frac{x\cdot x}{2}$ and $S \subset \Omega$, we have $\mathrm{q}(\sqrt{2}\,\nu_S) = |S|$: we have proved the assertion about $\operatorname{res} Q$.

On the other hand, this also shows that $Q^\perp[\frac{1}{2}]$ is the submodule of $\mathrm{Leech}[\frac{1}{2}]$ consisting of the $\sum_{i\in\Omega\smallsetminus F} x_i\,\sqrt{2}\,\nu_i$ with $x_i \in \mathbb{Z}[\frac{1}{2}]$ satisfying $\sum_{i\in Z} x_i = 0$ for any Z in $\mathscr{Z}$. In other words $\frac{1}{\sqrt{2}}\,Q^\perp[\frac{1}{2}]$ is isomorphic to the root lattice A_{p-1}^b over $\mathbb{Z}[\frac{1}{2}]$. It follows that $\operatorname{res} Q^\perp[\frac{1}{2}]$ is isomorphic to $-(\mathrm{I}_b \otimes \mathbb{Z}/p\mathbb{Z})$. (See also [CL19, Prop. B.2.2 (d)] for a more conceptual proof of $\operatorname{res} Q^\perp \simeq -\operatorname{res} Q$). □

By Table 1, there are 8 conjugacy classes of elements of odd prime order in M_{24}, with respective shape 3^8, $1^6\,3^6$, $1^4\,5^4$, $1^3\,7^3$ (two classes), $1^2\,11^2$ and $1\,23$ (two classes). For our applications we are looking for cases $1^a\,p^b$ with $a+b$ in $\{8, 12, 16\}$ and Q orientable. Only the first three conjugacy classes just listed meet the first condition, and the class with shape 3^8 does not meet the second. Indeed, in this case, the description above of $Q[\frac{1}{2}]$ shows $x\cdot x \equiv 0 \bmod 3$ for all $x \in Q$. This implies that $\frac{1}{\sqrt{3}}\,Q$ is an even unimodular lattice of rank 8, necessarily isomorphic to E_8, hence non orientable. In §3, we will check that the lattice Q is actually orientable for the two remaining classes $1^6\,3^6$ and $1^4 5^4$, and has the following properties:

Proposition 2.2. *Let g be 8, 12 or 16. Up to isometry, there is a unique even lattice Q_g of rank g without roots and with residue isomorphic to $\mathrm{I}_4 \otimes \mathbb{Z}/5\mathbb{Z}$ (case $g = 8, 16$) or to $\mathrm{I}_6 \otimes \mathbb{Z}/3\mathbb{Z}$ ($g = 12$). The lattice Q_g is orientable, and there is a unique $\mathrm{O}(\text{Leech})$-orbit of sublattices of* Leech *isometric to Q_g.*

Remark 2.3. *For $g = 12$ (resp. $g = 8$) it is easy to check that the Coxeter-Todd lattice* [CT53] (*resp. the icosian lattice $Q_8(1)$ in* [CS88, Table 1 p.38]) *satisfies the assumption of Proposition 2.2. An anonymous referee pointed out to us that the construction of these two lattices as stabilizers in* Leech *of prime order elements in the Mathieu group M_{23} was already observed in* [RS98, Theorem 3 and Table I].

The same referee also remarked that the cases $g \in \{8, 16\}$ of Proposition 2.2, except for orientability of Q_g, were already proved in [GL11], *using arguments in the spirit of the ones we will give in Section 3. Moreover, note that for $g \in \{8, 12\}$ the characterization above of Q_g follows from the description of the full genus of Q_g announced in* [SV94, Theorem 4] (*unfortunately, it seems the details have not been published*). *We decided to keep our proofs however, because they are self-contained, treat all g uniformly, and pave the way for our proofs of orientability.*

Let us mention that a large part of Proposition 2.2 could also be proved using computer calculations. For example, the genus of Q_g for $g \in \{8, 12\}$ was reobtained this way in [SH98]. *Also for all g we checked the orientability of Q_g using the Plesken-Souvignier algorithm before elaborating proofs in Section 3. In fact we selected these sublattices of* Leech *for this property. We feel that the proof we give in Section 3 is more structured and illuminating than a computer calculation.*

In the remaining part of this section we explain how to deduce Theorem 2 from Proposition 2.2 (this proposition will only be used at the end, and not in the proof of the two following lemmas).

Recall that a *dodecad* is an element of $\mathscr{G}$ with 12 elements. Moreover, a subset $S \subset \Omega$ with $|S| = 4$ (resp. $|S| = 6$) is called a *tetrad* (resp. an *hexad*). Following Conway, we will also say that an hexad is *special* if it is contained in an octad, and *umbral* otherwise. The umbral hexads are obtained as follows: choose 5 points in an octad and 1 in its complement.

Lemma 2.4. (i) *A tetrad T is contained in exactly 5 octads.*

(ii) *If γ in M_{24} is an element of order 5 whose set of fixed points is a tetrad T, then the 5 octads containing T are permuted transitively by γ, and each of them intersects each orbit of γ at exactly one point.*

(iii) *An umbral hexad U is contained in exactly 18 dodecads; these 18 dodecads are permuted transitively by the stabilizer of U in M_{24}.*

(iv) *Let γ in M_{24} be an element of order 3 with 6 fixed points. The set U of fixed points of γ is an umbral hexad, and each dodecad containing U intersects each orbit of γ at exactly one point. Moreover, the stabilizer G_U of U*

in M_{24} *coincides with the normalizer of* $\langle\gamma\rangle$ *in* M_{24}*, and the natural map* $\mathrm{G}_U \to \mathfrak{S}_U$ *is surjective with kernel* $\langle\gamma\rangle$*.*

Most of these statements are certainly well-known. We will explain how to deduce them from the exposition of Conway in [CS99, Ch. 10 §2].

Proof. Proof of (i). Recall that any 5-element subset of Ω is contained in a unique octad. This shows that if T is a tetrad, its complement is the disjoint union of 5 other tetrads T_i, uniquely determined by the property that $T \cup T_i$ is an octad for each i (these six tetrads, namely T and the T_i, form a *sextet* in the sense of Conway).

Proof of (ii). The element γ permutes the five T_i above since we have $\gamma(T) = T$. Assume there is some i, some x in T_i, and k in $(\mathbb{Z}/5\mathbb{Z})^\times$, with $\gamma^k(x) \in T_i$. Then $\gamma^k(T \cup T_i)$ is the unique octad containing $T \cup \gamma^k(x)$, hence equals $T \cup T_i$, and so we have $\gamma^k(T_i) = T_i$. But this implies $|T_i| \geq 5$: a contradiction.

Proof of the first assertion of (iii). Conway shows *loc. cit.* that M_{24} acts transitively on the octads, on the dodecads, and $6+1$ transitively on an octad and its complement, hence transitively on the umbral (resp. special) hexads as well. There are thus $759 \cdot \binom{8}{6} = 21252$ special hexads in Ω, and $\binom{24}{6} - 21252 = 113344$ umbral hexads. There are also $2^{12} - 2 - 2 \cdot 759 = 2576$ dodecads. Fix a dodecad D. For any octad O, we have $|D + O| \in \{0, 8, 12, 16, 24\}$ since $D + O$ is in $\mathscr{G}$, and $|D + O| = 20 - 2|D \cap O|$, so $|D \cap O|$ is in $\{2, 4, 6\}$. Therefore the octad O containing any given 5-element subset of D has the property that $O \cap D$ is a special hexad. In other words, *any* 5*-element subset of* D *is contained in a unique special hexad included in* D. It follows that there are $\binom{12}{5}/6 = 132$ special hexads in D, hence $\binom{12}{6} - 132 = 792$ umbral hexads. By counting in two ways the pairs (U, D) with U a umbral hexad, D a dodecad, and $U \subset D$, we obtain that there are $792 \cdot 2576/113344 = 18$ dodecads containing a given umbral hexad, as asserted.

In order to prove the second assertion in (iii), we show that the pairs (U, D) as above are permuted transitively by M_{24}. Fix a dodecad D. It is enough to show that the stabilizer H of D in M_{24} permutes transitively the umbral hexads of D. But H is a Mathieu group M_{12} and is sharply 5-transitive on D by Conway. In particular, H permutes transitively the special hexads of D. Fix $S \subset D$ a special hexad and denote by S' its complement in D. The stabilizer H_S of S in H acts faithfully both on S and S', and 5-transitively on S, by the sharp 5-transitivity of H on D. The two projections of the natural morphism $H_S \to \mathfrak{S}_S \times \mathfrak{S}_{S'}$ are thus injective, and the first one is surjective: they are both bijective. (This is of course compatible with the equality $|\mathrm{M}_{12}|/132 = 720$.) By numbering S and S', we obtain two isomorphisms $H_S \xrightarrow{\sim} \mathfrak{S}_6$. We claim that they differ by an outer automorphism of $\mathfrak{S}_6$. Indeed, an element of M_{24} of order two with at least 1 fixed point on Ω has actually 8 fixed points by Table 1, which must form an octad (see the beginning of §2.2 in [CS99, Ch. 10]). The group H_S contains an element of

order 2 with 4 fixed points in S, but its 4 remaining fixed points cannot lie in D because no octad is contained in D. This proves the claim. It follows that the stabilizer in H_S of a point P of S (isomorphic to $\mathfrak{S}_5$) acts transitively on S', hence on the set of umbral hexads in D containing $S \smallsetminus P$. Together with the fact that H acts 5-transitively on D, this shows that H acts transitively on the umbral hexads in D.

Proof of (iv). If O is an octad containing U, necessarily unique, we have $\gamma(O) = O$, and so γ stabilizes the two-element set $O \smallsetminus U$ without fixed point: a contradiction. So U is an umbral hexad. For any u in U, there is a unique octad O_u containing $U \smallsetminus \{u\}$. The six O_u, and the six 3-element sets $Z_u = O_u \smallsetminus U$ are thus preserved by any element of M_{24} fixing U pointwise. In particular, the Z_u are the supports of the 3-cycles of γ. The assertion about dodecads follows as we already explained in the proof of (iii) that any octad O containing five points of a dodecad D satisfies $|O \cap D| = 6$. This also shows that the pointwise stabilizer of U in M_{24} is $\langle\gamma\rangle$: a non trivial element of M_{24} with at least 7 fixed points has shape $1^8\,2^8$ by Table 1, and as recalled above the set of its fixed points is an octad. Let now G_U be the stabilizer of U in M_{24}, and H the normalizer of $\langle\gamma\rangle$. We have $H \subset G_U$. We know that G_U has $|\mathrm{M}_{24}|/113344 = 2160$ elements. Table 1 also shows that the centralizer of γ has 1080 elements, and that its normalizer contains an element sending γ to γ^{-1}, so we have $H = G_U$. We have seen that the kernel of $G_U \to \mathfrak{S}_U$ is $\langle\gamma\rangle$, and we conclude that this morphism is surjective by the equality $2160/3 = 6!$. □

Lemma 2.5. (i) *Assume c has shape $1^4\,5^4$, so that Q and $Q^\perp$ have respective ranks 8 and 16, and fix $v \in Q^8$ and $u \in (Q^\perp)^{16}$ two $\mathbb{Z}$-bases of these respective lattices. Then we have $\omega_8(v) = \pm 5$ and $\omega_{16}(u) = \pm 5$.*

(ii) *Assume c has shape $1^6\,3^6$, so that Q has rank 12, and fix $v \in Q^{12}$ a $\mathbb{Z}$-basis of Q. Then we have $\omega_{12}(v) = \pm 18$.*

Proof. We first show $\omega_8(v) = \pm 5$ in (i) and $\omega_{12}(v) = \pm 18$ in (ii). If $v' = (v'_1, \dots, v'_g)$ is any $\mathbb{Q}$-basis of $Q \otimes \mathbb{Q}$, we have $\omega_g(v') = \det_v(v')\,\omega_g(v)$, and $|\det_v(v')|$ is the covolume of the lattice $\sum_i \mathbb{Z}v'_i$ divided by the covolume of Q (that is, by 25 or 27). Fix from now on a basis v' made of the $\sqrt{2}\,\nu_i$ with i in F, and the $\sqrt{2}\,\nu_Z$ with Z in $\mathscr{Z}$. We have $\det_v(v') = \pm 2^{g/2}$, so we need to prove that $2^{-g/2}\,\omega_g(v')$ is ± 5 in the case $g = 8$, and ± 18 in the case $g = 12$.

By Definition 1.5, $\omega_g(v')$ is a sum of terms of the form $\det(v'_i \cdot x_j)_{1\le i,j\le g}$ where $\{x_1, \dots, x_g\}$ runs over all the possible elements C of $\mathscr{G}$ of size g, numbered in an M_{24}-equivariant way. For such a determinant to be nonzero, each linear form $v \mapsto v \cdot x_i$ has to be nonzero on Q: the subset C has thus to contain all the elements of F, and a point in each Z in $\mathscr{Z}$. In other words, such a C has to meet each of the g orbits of c in exactly one point. Denote by $\mathscr{C}(c)$ the set of elements of $\mathscr{G}$ of

size g with this property. For all $C = \{x_1, \dots, x_g\}$ in $\mathscr{C}(c)$ we have

$$\det (v'_i \cdot x_j)_{1 \le i,j \le g} \;=\; \pm\, 2^{g/2}. \tag{6}$$

By Lemma 2.4 (ii) and (iv), the set $\mathscr{C}(c)$ consists of 5 octads (resp. 18 dodecads) if c has shape $1^4\,5^4$ (resp. $1^6\,3^6$), and the normalizer G of $\langle c\rangle$ in M_{24} permutes $\mathscr{C}(c)$ transitively. If we fix $C = \{x_1, \dots, x_g\}$ in $\mathscr{C}(c)$, we may thus find a $|\mathscr{C}(c)|$-element subset $\Gamma \subset G$ with

$$\omega_g(v') = \pm \sum_{\gamma \in \Gamma} \det\, (v'_i \cdot\, \gamma\, x_j)_{1 \le i,j \le g}.$$

We claim that the $|\Gamma|$ determinants above are equal. This will show $\omega_g(v') = \pm|\mathscr{S}(c)|2^{g/2}$ by (6). For any $\gamma \in G$ we have

$$\det (v'_i \cdot \gamma x_j)_{1 \le i,j \le g} \;=\; \det (\gamma^{-1} v'_i \cdot x_j)_{1 \le i,j \le g} \;=\; \det \gamma_{|Q}^{-1}\; \det (v'_i \cdot x_j)_{1 \le i,j \le g}.$$

As Q is orientable by Lemma 2.1 and Proposition 2.2, we have $\det \gamma_{|Q} = 1$, and we are done. We may actually avoid the use of these lemma and proposition as follows. If c has shape $1^4\,5^4$, we may choose $\Gamma = \langle c\rangle$ by Lemma 2.4 (ii), and we clearly have $\gamma_{|Q} = \mathrm{id}$. If c has shape $1^6\,3^6$, the proof of Lemma 2.4 (iv) defines a natural G-equivariant bijection $u \mapsto Z_u$ between U and $\mathscr{Z}$. For any $\gamma \in G$ we have thus $\det \gamma_{|Q} = \epsilon^2 = 1$, where ϵ is the signature of the image of γ in $\mathfrak{S}_U$.

We now prove $\omega_{16}(u) = \pm 5$ in (i). Observe first that for any oriented octad (O, o), there is a sign ϵ such that for all $u'_1, \dots, u'_{16}$ in $\mathbb{Q}\,\Omega$ we have

$$\omega_{16}(u'_1, \dots, u'_{16}) \;=\; \epsilon\, \omega_{24}(\sigma_o \wedge u'_1 \wedge u'_2 \wedge \cdots \wedge u'_{16}). \tag{7}$$

Indeed, the alternating 16-form on the right is O(Leech)-invariant, as both σ_o and ω_{24} are, so it is proportional to ω_{16}. But if $\{u'_1, \dots, u'_{16}\}$ is a 16-element subset of $\mathscr{G}$, both sides are equal to ± 1, and we are done.

Choose a basis u' of $Q^\perp \otimes \mathbb{Q}$ made of 16 elements of the form $\sqrt{2}\,(\nu_i - \nu_{c(i)})$ with i in $\Omega \smallsetminus F = \bigsqcup_{Z \in \mathscr{Z}} Z$ (i.e. choose 4 elements i in each $Z \in \mathscr{Z}$). Comparing covolumes as in the first case of the proof, we have to show $\omega_{16}(u') = \pm 5 \cdot 2^8$. Apply Formula (7) to $u' = (u'_1, \dots, u'_{16})$. If $\gamma(O)$ is an octad such that $\gamma(\beta_O) \wedge u'_1 \wedge u'_2 \wedge \cdots \wedge u'_{16}$ is nonzero, that octad meets at most once each Z in $\mathscr{Z}$. We have $|\mathscr{Z}| = |F| = 4$ and $|O| = 8$, so $\gamma(O)$ must meet each Z of $\mathscr{Z}$ in one point and contain F. By Lemma 2.4 (i) and (ii), there are 5 such octads, permuted transitively by c. We may choose O to be one of them. We then have

$$\omega_{16}(u'_1, \dots, u'_{16}) \;=\; \epsilon \sum_{k \text{ in } \mathbb{Z}/5\mathbb{Z}} \omega_{24}(c^k \beta_o \wedge u'_1 \wedge u'_2 \wedge \cdots \wedge u'_{16}).$$

Now c preserves $Q^\perp$ and has determinant 1 on it (being of order 5), so we have $u'_1 \wedge \cdots \wedge u'_{16} = c^k(u'_1 \wedge \cdots \wedge u'_{16})$ and the sum above is 5 times $\omega_{24}(\beta_o \wedge u'_1 \wedge u'_2 \wedge \cdots \wedge u'_{16})$ by c-invariance of ω_{24}. An easy computation shows that we have $\omega_{24}(\beta_o \wedge u'_1 \wedge u'_2 \wedge \cdots \wedge u'_{16}) = \pm\, 2^8$. □

We are now able to prove Theorem 2, assuming Proposition 2.2.

Proof. (Proposition 2.2 implies Theorem 2) Let $\mathscr{L}_g$ be the set of sublattices of Leech isometric to Q_g. This set is nonempty by Lemma 2.1 and we fix one of its elements, that we denote Q_g. By Proposition 2.2, O(Leech) acts transitively on $\mathscr{L}_g$, so we may find an n_g-element subset $\Gamma \subset \mathrm{O}(\text{Leech})$ with $\mathscr{L}_g = \Gamma \cdot Q_g$.

Fix a $\mathbb{Z}$-basis $u_1, \dots, u_g$ of Q_g, and denote by $2n = (u_i.u_j)_{1\leq i,j\leq g}$ its Gram matrix. The n-th Fourier coefficient of F_g is by definition

$$\sum_{\substack{(v_1,\dots,v_g)\in \mathrm{Leech}^g \\ \text{with } (v_i\cdot v_j)_{1\leq i,j\leq g}=2n}} \omega_g(v_1,\dots,v_g).$$

The index set in this sum has exactly $\mathrm{n}_g|\mathrm{O}(Q_g)|$ elements, namely the g-tuples $(\gamma\gamma' u_1, \dots, \gamma\gamma' u_g)$ with $\gamma \in \Gamma$ and $\gamma' \in \mathrm{O}(Q_g)$. The O(Leech)-invariance of ω_g, the trivial equality $\omega_g(\gamma' u_1, \dots, \gamma' u_g) = (\det \gamma')\, \omega_g(u_1, \dots, u_g)$ for γ' in $\mathrm{O}(Q_g)$, and the property $\det \gamma' = 1$ (as Q_g is orientable), imply that the n-th Fourier coefficient of F_g is $\mathrm{n}_g|\mathrm{O}(Q_g)|\omega_g(u_1, \dots, u_g)$. We conclude by Lemma 2.5. □

Remark 2.6. Define e_g as in the statement of Theorem 2 and write $\operatorname{res} \mathrm{Q}_g \simeq (\mathbb{Z}/p_g\mathbb{Z})^{r_g}$. It follows from Lemmas 2.4 & 2.5 that e_g coincides with the number of g-element subsets of $\mathscr{G}$ containing the fixed point set of a given element of M_{24} of shape $1^{24-p_g r_g}\, p_g^{r_g}$.

3. Properties of the lattices Q_g

The aim of this section is to prove Proposition 2.2. We make first some preliminary remarks about root lattices and their sublattices.

Let R be a root system in the Euclidean space V. We will follow Bourbaki's definitions and notations in [Bou68, Ch. VI] and assume furthermore that R is *of type* ADE, *i.e.* that we have $\alpha \cdot \alpha = 2$ for all α in R. As suggested by this terminology, each irreducible component of R is then of type $\mathbf{A}_l$ ($l \geq 1$), $\mathbf{D}_l$ ($l \geq 3$) or $\mathbf{E}_l$ ($l = 6, 7, 8$), and R is identified to its dual root system, with $\alpha^\vee = \alpha$ for all roots α. As a typical example, if L is an integral Euclidean lattice then the set $\mathrm{R}(L) = \{\alpha \in L \mid \alpha.\alpha = 2\}$ of *roots* of L is such a root system in the Euclidean space it generates. We denote by $\mathrm{Q}(R)$ the even lattice of V generated by R and by $\mathrm{P}(R)$ the dual lattice $\mathrm{Q}(R)^\sharp$, so that we have

$$\operatorname{res} \mathrm{Q}(R) \;=\; \mathrm{P}(R)/\mathrm{Q}(R).$$

It is well known that the trivial inclusion $R \subset \mathrm{R}(\mathrm{Q}(R))$ is an equality.

We will simply denote by A_l, D_l and E_l for $\mathrm{Q}(R)$ when R is $\mathbf{A}_l$, $\mathbf{D}_l$ or $\mathbf{E}_l$ respectively. The *Weyl group* of R will be denoted by $\mathrm{W}(R)$, and the orthogonal group of $\mathrm{Q}(R)$ by $\mathrm{A}(R)$. The group $\mathrm{W}(R)$ is the subgroup of $\mathrm{A}(R)$ generated by the orthogonal symmetries $\mathrm{s}_\alpha(x) = x - (\alpha \cdot x)\alpha$ with $\alpha \in R$, hence acts trivially on $\operatorname{res} \mathrm{Q}(R)$. It permutes simply transitively the positive root systems R_+ of R. Fix such an R_+, and denote by $\{\alpha_i \mid i \in I\}$ its simple roots. The α_i form a $\mathbb{Z}$-basis

of $\mathrm{Q}(R)$, whose dual basis ϖ_i (the *fundamental weights*) is thus a $\mathbb{Z}$-basis of $\mathrm{P}(R)$. The *Weyl vector* ρ associated to R_+ is the half-sum of elements of R_+, it satisfies $\rho = \sum_{i\in I} \varpi_i$.

Assume now R is irreducible of rank $\dim V = |I| = l$; we will always identify the set I with $\{1, \dots, l\}$ as in Bourbaki. The *highest positive root* is the unique element $\widetilde{\alpha}$ in R_+ satisfying $\alpha \cdot \varpi_i \leq \widetilde{\alpha} \cdot \varpi_i$ for all i in I and α in R. There are unique integers $n_i > 0$ for $i = 1, \dots, l$ with $\widetilde{\alpha} = \sum_{i=1}^{l} n_i \alpha_i$. Let $\mathrm{h}(R)$ be the Coxeter number of R [Bou68, Ch. VI §1.11], for $h = \mathrm{h}(R)$ we have

$$(8)\quad |R| = l\,h, \qquad n_1 + n_2 + \ldots + n_l = h - 1 \qquad \text{and} \qquad \rho \cdot \rho = \frac{l}{12}\, h\,(h+1).$$

Indeed, the first equality is [Bou68, Ch. V §6 Thm. 1] and the second is [Bou68, Ch. VI §1 Prop. 31] (see also [Kos59, Theorem 8.4]). The last equality may be checked case by case using the ADE classification (as is mentioned *e.g.* in [Ebe13, Lemma 1.17]). We will give in the appendix a proof of this equality which does not use the classification.

Recall $\mathrm{h}(\mathbf{A}_l) = l+1$, $\mathrm{h}(\mathbf{D}_l) = 2l-2$, $\mathrm{h}(\mathbf{E}_6) = 12$, $\mathrm{h}(\mathbf{E}_7) = 18$ and $\mathrm{h}(\mathbf{E}_8) = 30$. Following Borel-de Siebenthal and Dynkin, the sublattice

$$\mathrm{BS}_i(R) = \{x \in \mathrm{Q}(R) \,|\, x \cdot \varpi_i \equiv 0 \bmod n_i\}$$

is the root lattice $\mathrm{Q}(R_i)$ where R_i is the root system of V having as a set of simple roots $-\widetilde{\alpha}$ and the α_j with $j \neq i$ [Bou68, Ch. VI, §4, Exercise 4]. The Dynkin diagram of R_i is thus obtained by removing α_i from the extended Dynkin diagram of R. We clearly have $\mathrm{W}(R_i) \subset \mathrm{W}(R)$. The fundamental weights of R_i with respect to the simple roots above are $-\frac{1}{n_i}\varpi_i$ and the $\varpi_j - \frac{n_j}{n_i}\varpi_i$ for $j \neq i$; in particular, the corresponding Weyl vector of R_i is $\rho - \frac{h}{n_i}\varpi_i$.

Observe that for any integer $p \geq 1$, we have an $\mathrm{A}(R)$-equivariant isomorphism

$$\begin{aligned} \mathrm{P}(R) \otimes \mathbb{Z}/p\mathbb{Z} &\xrightarrow{\sim} \mathrm{Hom}(\mathrm{Q}(R), \mathbb{Z}/p\mathbb{Z}) \\ \xi &\longmapsto (x \mapsto \xi \cdot x \bmod p). \end{aligned}$$

Assertion (ii) and (iii) below are Propositions 3.4.1.2 and 3.2.4.8 in [CL19] (see also [Kos59]).

Lemma 3.1. *Let R be an irreducible root system, $h = \mathrm{h}(R)$, and $p \geq 1$ an integer.*

(i) *Each $\mathrm{W}(R)$-orbit in $\mathrm{P}(R)/p\,\mathrm{Q}(R)$ admits a unique representative of the form $\sum_i m_i\varpi_i$ with $m_i \geq 0$ for all i and $\sum_i m_i n_i \leq p$.*

(ii) *The kernel of any linear form $\mathrm{Q}(R) \to \mathbb{Z}/p\mathbb{Z}$ with $p < h$ contains some element of R.*

(iii) *There is a unique $\mathrm{W}(R)$-orbit of linear forms $\mathrm{Q}(R) \to \mathbb{Z}/h\mathbb{Z}$ whose kernel does not contain any root, namely the orbit of the form $x \mapsto \rho \cdot x \bmod h$.*

Proof. The set Π of $v \in V$ with $v \cdot \alpha_i \geq 0$ for all i, and with $v \cdot \widetilde{\alpha} \leq 1$, is a fundamental domain for the affine Weyl group $\mathrm{W}_{\mathrm{aff}}(R) = \mathrm{Q}(R) \rtimes \mathrm{W}(R)$ acting on V [Bou68, Ch. VI §2]. For any ξ in $\mathrm{P}(R)$, the $\mathrm{W}_{\mathrm{aff}}(R)$-orbit of $\frac{1}{p}\xi$ meets thus Π in a unique element: this proves (i). Any linear form $\varphi : \mathrm{Q}(R) \to \mathbb{Z}/p\mathbb{Z}$ may be written $\varphi(x) = \xi \cdot x \bmod p$ for some $\xi \in \mathrm{P}(R)/p\,\mathrm{Q}(R)$. Replacing φ by $w(\varphi)$ for some $w \in \mathrm{W}(R)$ we may assume ξ has the form $\sum_i m_i \varpi_i$ with the m_i as in (i). If the kernel of φ contain neither the α_i nor $\widetilde{\alpha}$, we must have $m_i > 0$ for all i and $\sum_i m_i n_i < p$, and thus $h - 1 = \sum_i n_i \leq \sum_i m_i n_i < p$. This proves (ii). In the case $p = h$ this inequality implies $m_i = 1$ for each i, hence $\xi = \sum_i \varpi_i = \rho$. For any positive root α in R we have $0 < \alpha \cdot \rho \leq \widetilde{\alpha} \cdot \rho = h - 1$. As we have $R = \mathrm{R}(\mathrm{Q}(R))$, this shows (iii). □

A root system R is called *equi-Coxeter* if its irreducible components all have the same Coxeter number, called the Coxeter number of R, and denoted by $\mathrm{h}(R)$.

Corollary 3.2. *Let R be an equi-Coxeter root system of rank l and Coxeter number h. Then assertion (iii) of Lemma 3.1 holds and there is a unique $\mathrm{W}(R)$-orbit of sublattices $L \subset \mathrm{Q}(R)$ with no root and $\mathrm{Q}(R)/L \simeq \mathbb{Z}/h\mathbb{Z}$. These lattices are of the form $\{x \in \mathrm{Q}(R) \mid x \cdot \rho \equiv 0 \bmod h\}$ for a Weyl vector ρ for R. Assuming furthermore $\rho \in \mathrm{Q(R)}$, h odd and $l(h+1) \equiv 0 \bmod 12$, they satisfy $\operatorname{res} L \simeq \mathrm{H}(\mathbb{Z}/h\mathbb{Z}) \oplus \operatorname{res} \mathrm{Q}(R)$.*

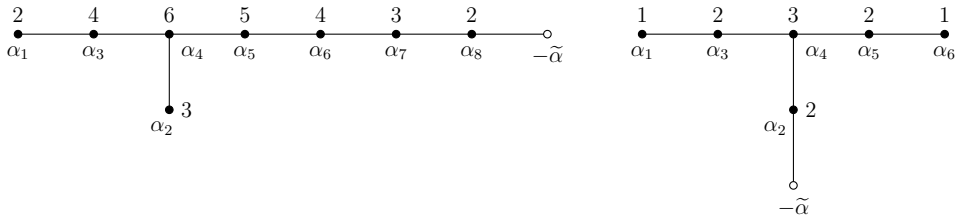
Proof. The first assertion is a trivial consequence of (iii) of Lemma 3.1 and of $\rho \cdot \alpha = 1$ for a simple root α of R. The identity $\rho \cdot \rho = l\,h(h+1)/12$ stated in (8) shows that ρ is a nonzero isotropic vector in $\mathrm{Q}(R) \otimes \mathbb{Z}/h\mathbb{Z}$, so the last assertion follows from the general Lemma 3.16 below. □

We have $\operatorname{res} \mathrm{A}_n \simeq \mathbb{Z}/(n+1)\mathbb{Z}$ with $\mathrm{q}(\overline{1}) \equiv \frac{n}{2(n+1)} \bmod \mathbb{Z}$, $\operatorname{res} \mathrm{E}_6 \simeq -\operatorname{res} \mathrm{A}_2$, $\operatorname{res} \mathrm{E}_8 = 0$. As -1 is a square modulo 5, Corollary (3.2) implies:

Corollary-Definition 3.3. *Let R be either $2\,\mathbf{A}_4$ or $3\,\mathbf{A}_2$, and set $p = \mathrm{h}(R)$ (either 5 or 3) and $g = \operatorname{rank} R$ (either 8 or 6). Define Q_g as the sublattice of $\mathrm{Q}(R)$ whose elements x satisfy $x \cdot \rho \equiv 0 \bmod p$, for a fixed Weyl vector ρ in $\mathrm{Q}(R)$. Then Q_g is an even lattice, without roots, satisfying $\operatorname{res} \mathrm{Q}_g \simeq \operatorname{res} \mathrm{E}_g \oplus \mathrm{H}(\mathbb{Z}/p\mathbb{Z})^2$.*

Proposition 3.4. *Assume either $p = 5$ and E is the root lattice E_8, or $p = 3$ and E is the root lattice E_6. Up to isometry, there is a unique triple of even lattices (A, B, C) with $A \subset B \subset C$, both inclusions of index p, $C \simeq E$ and $\mathrm{R}(A) = \emptyset$.*

Proof. Set $R = \mathrm{R}(E)$, so that we have $E = \mathrm{Q}(R)$. We have to show that there is a unique $\mathrm{W}(R)$-orbit of index p subgroups $B \subset E$ such that B possesses an index p subgroup without roots, and that for such a B there is a unique $\mathrm{O}(B) \cap \mathrm{O}(E)$-orbit of index p subgroups of B without roots. We claim (provocatively) that both properties follow at once from Lemma 3.1 and an inspection of the extended Dynkin diagrams of $\mathbf{E}_8$ and $\mathbf{E}_6$ drawn below:



(Each simple root α_i is labelled with the integer n_i.) Indeed, assume for instance $R \simeq \mathbf{E}_8$ and $p = 5 = n_5$. Note that the irreducible root systems with Coxeter number ≤ 5 are the $\mathbf{A}_l$ with $1 \leq l \leq 4$, so by assertion (ii) of the lemma, the irreducible components of $\mathrm{R}(B)$ must have this form. On the other hand, assertion (i) asserts that for a suitable choice of a positive system of R the lattice B is the kernel of $x \mapsto \xi \cdot x \bmod 5$ with $\xi = \sum_i m_i \varpi_i$ and $\sum_i m_i n_i \leq 5$. Consider the set

$$J = \{\ j \mid m_j \neq 0\}.$$

We must have $|J| \leq 2$ (note $n_i \geq 2$ for all i) and $\alpha_j \in \mathrm{R}(B)$ for $j \notin J$. An inspection of the Dynkin diagram of $\mathbf{E}_8$ shows that in the case $|J| = 2$, we have $J \subset \{1, 2, 7, 8\}$ and $\{2, 7\} \not\subset J$, and $\mathrm{R}(B)$ contains an irreducible root system of rank 5: a contradiction. So we have $|J| = 1$ and $J \neq \{4\}$. But this clearly implies $J = \{5\}$ and $\xi = \omega_5$ by another inspection of this diagram. So B is the Borel-de Siebenthal lattice $\mathrm{BS}_5(R) = \mathrm{Q}(R_5)$, and is isomorphic to the root lattice $\mathrm{A}_4 \oplus \mathrm{A}_4$. Note that we have $\mathrm{h}(\mathrm{A}_4) = 5 = p$. By the last assertion of Lemma 3.1 applied to R_5, there is a unique $\mathrm{W}(R_5)$-orbit of index 5 sublattices of $\mathrm{Q}(R_5)$ without root. As we have $\mathrm{W}(R_5) \subset \mathrm{W}(R)$, this concludes the proof in the case $R \simeq \mathbf{E}_8$. The case $R \simeq \mathbf{E}_6$ is entirely similar. □

Proposition 3.5. *Let (g, p, m) be either $(8, 5, 4)$ or $(6, 3, 5)$. Up to isometry, Q_g is the unique even lattice of rank g without roots satisfying $\mathrm{Q}_g^\sharp/\mathrm{Q}_g \simeq (\mathbb{Z}/p\mathbb{Z})^m$.*

Moreover, $\mathrm{O}(\mathrm{Q}_g)$ permutes transitively the totally isotropic planes (resp. lines, resp. flags) of $\operatorname{res}\mathrm{Q}_g$. The inverse image in $\mathrm{Q}_g^\sharp$ of such an isotropic plane (resp. line) is isometric to E_g (resp. to $\mathrm{A}_4 \oplus \mathrm{A}_4$ for $g = 8$, to $\mathrm{A}_2 \oplus \mathrm{A}_2 \oplus \mathrm{A}_2$ for $g = 6$).

In the statement above, by a *totally isotropic flag* of $\operatorname{res}\mathrm{Q}_g$ we mean a pair (D, P) with D a line and P a totally isotropic plane containing D.

Proof. Let A be an even lattice of rank g with $A^\sharp/A \simeq (\mathbb{Z}/p\mathbb{Z})^m$. As p is an odd prime, the isomorphism class of an m-dimensional linking quadratic space V over $\mathbb{Z}/p\mathbb{Z}$ is determined by its determinant, or equivalently, by its Gauss sum $\gamma(V) = |V|^{-1/2} \sum_{v \in V} e^{2\pi i\, \mathrm{q}(v)}$. But the Milgram formula [MH73, Appendix 4] asserts $\gamma(\operatorname{res} A) = e^{\frac{2\pi i g}{8}} = \gamma(\operatorname{res}\mathrm{Q}_g)$. This proves $\operatorname{res} A \simeq \operatorname{res}\mathrm{Q}_g$.

The even lattices L containing A with index p^i are in natural bijection with the totally isotropic subspaces of dimension i over $\mathbb{Z}/p\mathbb{Z}$ inside $\operatorname{res} A$, via the map $L \mapsto L/A$. We have already proved $\operatorname{res} A \simeq \mathrm{H}(\mathbb{Z}/p\mathbb{Z})^2 \oplus \operatorname{res}\mathrm{E}_g$. By Witt's theorem, any isotropic line (or plane) is thus part of a totally isotropic flag of $\operatorname{res} A$.

By Proposition 3.4, it only remains to show that any even lattice L containing A with $\dim_{\mathbb{Z}/p\mathbb{Z}} L/A = 2$ is isometric to E_g. But such an L has determinant 1 in the case $g = 8$, and determinant 3 otherwise. As is well known, this shows $L \simeq \mathrm{E}_8$ in the first case, and $L \simeq \mathrm{E}_6$ in the second (use e.g. that such a lattice must be the orthogonal of an A_2 embedded in E_8). □

This proposition implies in particular that the fixed point lattice Q considered in Lemma 2.1, in the case of an element c with shape $1^4 5^4$, is isometric to Q_8.

Proposition 3.6. *For $g = 6, 8$, the natural morphism $\mathrm{O}(\mathrm{Q}_g) \to \mathrm{O}(\operatorname{res} \mathrm{Q}_g)$ is an isomorphism.*

Proof. Set $A = \mathrm{Q}_g$. Fix an isotropic line D in the quadratic space $\operatorname{res} A$ over $\mathbb{F}_p$ (with $p = 3$ for $g = 6$, $p = 5$ otherwise). We have a canonical filtration $0 \subset D \subset D^\perp \subset \operatorname{res} A$, and a nondegenerate quadratic space $V = D^\perp/D$ over $\mathbb{F}_p$. The stabilizer P of D in $\mathrm{O}(\operatorname{res} A)$ is in a natural (splittable) exact sequence

$$1 \longrightarrow U \longrightarrow P \longrightarrow \mathrm{GL}(D) \times \mathrm{O}(V) \longrightarrow 1 \tag{9}$$

(P is a "parabolic subgroup" with "unipotent radical" U). We have an isomorphism $\beta : U \xrightarrow{\sim} \mathrm{Hom}((\operatorname{res} A)/D^\perp, V)$ characterized by

$$g(x) \equiv x + \beta(g)(x) \mod D$$

for all $g \in U$ and $x \in \operatorname{res} A$. (By duality U is also naturally isomorphic to $\mathrm{Hom}(V, D)$, but we will not need this point of view.) Denote by B the even lattice defined as the inverse image of D in $A^\sharp$. We have natural isomorphisms $V \simeq \operatorname{res} B$ and $B/A \simeq D$ (see Lemma 3.16 (i)). The stabilizer S of D in $\mathrm{O}(A)$ is $\mathrm{O}(A) \cap \mathrm{O}(B)$. By Proposition 3.5, we are left to check that the natural map $S \to P$ is an isomorphism. We first study $\mathrm{O}(A) \cap \mathrm{O}(B)$. Set $k = g/(p-1)$. By the same proposition, we may also assume that we have

$$B = \mathrm{A}_{p-1}^k \quad \text{and} \quad A = \{ (a_i)_{1 \le i \le k} \in B \mid \sum_{i=1}^{k} \rho' \cdot a_i \equiv 0 \bmod p \},$$

where ρ' is some Weyl vector in A_{p-1} (e.g. the vector $((p-1)/2, ..., -(p-1)/2)$). Let $R = k\,\mathbf{A}_{p-1}$ be the root system of B. For general reasons, the subgroup $\mathrm{G}(R)$ of $\mathrm{A}(R)$ fixing the Weyl vector $\rho = (\rho', \ldots, \rho')$ of R is naturally isomorphic to $\{\pm 1\}^k \rtimes \mathfrak{S}_k$ (automorphisms of the Dynkin diagram of R), and we have $\mathrm{O}(B) = \mathrm{A}(R) = \mathrm{W}(R) \rtimes \mathrm{G}(R)$. This proves

$$\mathrm{O}(B) \simeq {\mathfrak{S}_p}^k \rtimes (\{\pm 1\}^k \rtimes \mathfrak{S}_k).$$

We trivially have $\mathrm{G}(R) \subset \mathrm{O}(A)$, hence we only have to determine $\mathrm{W}(R) \cap \mathrm{O}(A)$. By definition of A, this is the subgroup of $\mathrm{W}(R)$ preserving $\mathbb{Z}\rho + p\mathrm{P}(R)$. As ρ is in $\mathrm{Q}(R)$ and $p\mathrm{P}(R) \subset \mathrm{Q}(R)$, $\mathrm{W}(R) \cap \mathrm{O}(A)$ is also the subgroup of $\mathrm{W}(R)$ preserving the subspace of the quadratic space $\mathrm{Q}(R) \otimes \mathbb{F}_p$ generated by ρ and the kernel $p\mathrm{P}(R)/p\mathrm{Q}(R)$ of the symmetric bilinear form. But the kernel of the symmetric

bilinear form on $\mathrm{A}_{p-1}\otimes\mathbb{F}_p$ is generated by the image e of the vector $(1-p,1,\dots,1)$, and is fixed by $\mathfrak{S}_p$. So $\mathrm{W}(R)\cap\mathrm{O}(A)$ is the subgroup of $(\sigma_1,\dots,\sigma_k)$ in $\mathfrak{S}_p^k$ such that there is λ in $\mathbb{F}_p^\times$ such that for all $j=1,\dots,k$ there is b_j in $\mathbb{F}_p$ with

$$\sigma_j(\rho') \equiv \lambda\,\rho' + b_j\,e \bmod p\mathrm{A}_{p-1}. \tag{10}$$

To go further it will be convenient to identify A_{p-1} with the subgroup of $(x_i)_{i\in\mathbb{F}_p}$ in $\mathbb{Z}^{\mathbb{F}_p}$ satisfying $\sum_i x_i = 0$ in such a way that we have $\rho'_i = i$ for all i in $\mathbb{F}_p$. If we do so, $\mathrm{W}(R)\cap\mathrm{O}(A)$ becomes the subgroup of $(\sigma_1,\dots,\sigma_k)$ in $\mathfrak{S}_{\mathbb{F}_p}^k$ such that there is λ in $\mathbb{F}_p^\times$ and $b_1,\dots,b_k$ in $\mathbb{F}_p$ with $\sigma_j^{-1}(i) = \lambda i + b_j$ for all i in $\mathbb{F}_p$ and all $j=1,\dots,k$ ("k affine transformations with common slope"). We have shown $\mathrm{W}(R)\cap\mathrm{O}(A) = {\mathbb{F}_p}^k \rtimes \mathbb{F}_p^\times$ and

$$\mathrm{O}(A)\cap\mathrm{O}(B) = {\mathbb{F}_p}^k \rtimes (\mathbb{F}_p^\times \times (\{\pm1\}^k \rtimes \mathfrak{S}_k)). \tag{11}$$

It remains to identify the action of this group on $\operatorname{res} A$. The reduction modulo A of the natural inclusions $A\subset B\subset B^\sharp\subset A^\sharp$, is $0\subset D\subset D^\perp\subset \operatorname{res} A$ by definition, and we have set $V=\operatorname{res} B$. Note that $\operatorname{res} A$ is generated by $D^\perp$ and the image of the vector $p^{-1}\rho$, and that $W(R)$ acts trivially on V. Dividing Formula (10) by p gives the action of $\mathrm{W}(R)\cap\mathrm{O}(A)$ on $(\operatorname{res} A)/D$:

- λ is an element of $\mathrm{GL}((\operatorname{res} A)/D^\perp)$, which is naturally isomorphic to $\mathrm{GL}(D)$ by duality, and
- for $\lambda=1$, i.e. when considering an element of $\mathrm{W}(R)\cap\mathrm{O}(A)$ mapping to U, the family $(b_j)_{1\le j\le k}$ is the matrix of an element of $\mathrm{Hom}((\operatorname{res} A)/D^\perp, V)$ in the bases $p^{-1}\rho$ of $(\operatorname{res} A)/D^\perp$ and $((p^{-1}e,0,\dots,0),\dots,(0,\dots,0,p^{-1}e))$ of V.

The natural map $\mathrm{O}(A)\to\mathrm{O}(\operatorname{res} A)$ thus identifies $\mathrm{W}(R)\cap\mathrm{O}(A)$ with the inverse image of $\mathrm{GL}(D)\times 1$ in P. In order to conclude that $\mathrm{O}(A)\cap\mathrm{O}(B)\to P$ is an isomorphism, we are left to check that the natural map

$$\{\pm1\}^k \rtimes \mathfrak{S}_k \to \mathrm{O}(\operatorname{res} \mathrm{A}_{p-1}^k) = \mathrm{O}(\mathrm{I}_k\otimes\mathbb{F}_p)$$

is an isomorphism. Injectivity is clear (for any $p>2$ and $k>0$). Surjectivity is particular to the two cases at hand: for $(p,k)=(3,3)$ or $(5,2)$, the only elements of norm 1 in $\mathrm{I}_k\otimes\mathbb{F}_p$ are the standard basis elements and their opposites. □

Proposition 3.7. *The lattice* Q_8 *is orientable, whereas* Q_6 *is not.*

Proof. Set again $A=\mathrm{Q}_g$ and $p=3$ (case $g=6$) or $p=5$ (case $g=8$). We will view the linking quadratic space $\operatorname{res} A$ over $\mathbb{Z}/p\mathbb{Z}$ as traditional quadratic space over $\mathbb{Z}/p\mathbb{Z}$ by multiplying its quadratic map by p (making it $\mathbb{Z}/p\mathbb{Z}$-valued instead of $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$-valued). This quadratic space is nondegenerate and isotropic (it has dimension >2) so by a classical theorem of Eichler [Die71, Ch. II §8.I] the determinant and spinor norm maps induce an isomorphism

$$\mathrm{O}(\operatorname{res} A)^{\mathrm{ab}} \simeq \{\pm1\}\times(\mathbb{F}_p^\times\otimes\mathbb{Z}/2\mathbb{Z}). \tag{12}$$

We will give two elements γ, γ' of $\mathrm{O}(A)$ inducing orthogonal reflections of $\operatorname{res} A$ and with distinct spinor norms. The previous proposition and (12) will then imply that γ and γ' generate $\mathrm{O}(A)^{\mathrm{ab}}$.

Set $k = g/(p-1)$. By definition, A is the index p subgroup of the root lattice $B = \mathrm{A}_{p-1}^k$ defined by $x \cdot \rho \equiv 0 \bmod p$, where $\rho = (\rho', \dots, \rho')$ is a fixed Weyl vector in B. As already seen in the proof of Proposition 3.6 the subgroup G of $\mathrm{O}(B)$ fixing ρ is a subgroup of $\mathrm{O}(A)$ naturally isomorphic to $\{\pm 1\}^k \rtimes \mathfrak{S}_k$. The subgroup $1 \rtimes \mathfrak{S}_k \subset G$ is the obvious one, but the element $(-1, 1, \dots, 1) \rtimes 1$ acts on B as $(x_1, \dots, x_k) \mapsto (-\sigma x_1, x_2, \dots, x_k)$, where σ in $\mathfrak{S}_p$ is the unique element sending ρ' to $-\rho'$. We take γ, γ' in G with $\gamma = (-1, 1, \dots, 1) \rtimes \mathrm{id}$ and $\gamma' = (1, \dots, 1) \rtimes \tau$, where τ is a transposition in $\mathfrak{S}_k$. Then γ and γ' act trivially on $A^\sharp / B^\sharp = \langle\, p^{-1}\rho \,\rangle$ and induce orthogonal reflections of $\operatorname{res} B$ and $\operatorname{res} A$, with spinor norm $\frac{1}{2}\det(\operatorname{res} \mathrm{A}_{p-1})$ for γ and $2 \cdot \frac{1}{2}\det(\operatorname{res} \mathrm{A}_{p-1})$ for γ'. We actually have $\frac{1}{2}\det(\operatorname{res} \mathrm{A}_{p-1}) \equiv \frac{p-1}{2}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, but what only matters for this proof is that these spinor norms are distinct, as 2 is not a square in $(\mathbb{Z}/p\mathbb{Z})^\times$ for $p = 3, 5$.

We have $\det \gamma_{|A} = (-1)^{(p-1)/2}$ and $\det \gamma'_{|A} = (-1)^{p-1} = 1$: this shows that det is trivial on O(A) for $p = 5$ but not for $p = 3$. □

For $g = 6, 8$, we have seen that there is a unique $\mathrm{O}(\mathrm{Q}_g)$-orbit of overlattices $E \supset \mathrm{Q}_g$ isomorphic to E_g. We now define Q_{2g} by a doubling process.

Definition 3.8. *Set $(g, p) = (6, 3)$ or $(8, 5)$ and fix an embedding $\mathrm{Q}_g \subset \mathrm{E}_g$ arbitrarily. Define Q_{2g} as the sublattice of $\mathrm{E}_g \oplus \mathrm{E}_g$ consisting of elements (x, y) satisfying $x + y \in \mathrm{Q}_g$. Then Q_{2g} is an even lattice, without roots, satisfying $\operatorname{res} \mathrm{Q}_{2g} \simeq \mathrm{H}(\mathbb{Z}/p\mathbb{Z})^2 \oplus \operatorname{res} \mathrm{E}_g^2$.*

Let us check the last assertion in the definition above. Note that a root in $\mathrm{E}_g \oplus \mathrm{E}_g$ must belong either to $\mathrm{E}_g \oplus 0$ or to $0 \oplus \mathrm{E}_g$, so the fact that Q_g has no root implies that Q_{2g} has no root either. The assertion on the residue of Q_{2g} follows from $(\mathrm{E}_g \oplus \mathrm{E}_g)/\mathrm{Q}_{2g} \simeq (\mathbb{Z}/p\mathbb{Z})^2$, the fact that $\operatorname{res} \mathrm{Q}_{2g}$ is a subquotient of the $\mathbb{Z}/p\mathbb{Z}$-vectorspace $\operatorname{res} \mathrm{Q}_g \oplus \operatorname{res} \mathrm{Q}_g$, and Lemma 3.16. The following statements are analogues of Propositions 3.4 and 3.5 (although their proofs are slightly different).

Proposition 3.9. *Set $(g, p) = (6, 3)$ or $(8, 5)$ and $E = \mathrm{E}_g$. Up to the action of $\mathrm{O}(E) \times \mathrm{O}(E)$ there is a unique sublattice A of index p^2 in $E \oplus E$ without roots. For such an A, the natural map $\mathrm{O}(A) \cap (\mathrm{O}(E) \times \mathrm{O}(E)) \to \mathrm{GL}((E \oplus E)/A)$ is surjective.*

Proof. Fix A as in the statement. The sublattice $A \cap (E \oplus 0)$ of $E \oplus 0$ has index dividing p^2 and has no root, so by Proposition 3.4 it has index p^2 and there is γ in $\mathrm{O}(E)$ with $(\gamma \times 1)(A \cap (E \oplus 0)) = \mathrm{Q}_g \oplus 0$. Arguing similarly with $A \cap (0 \oplus E)$, we obtain the existence of h in $\mathrm{O}(E) \times \mathrm{O}(E)$ such that $h(A)$ contains $\mathrm{Q}_g \oplus \mathrm{Q}_g$. Set $A' = h(A)$.

Denote by P the totally isotropic plane E/Q_g of $\operatorname{res}\mathrm{Q}_g$, and by I the plane $A'/(\mathrm{Q}_g \oplus \mathrm{Q}_g)$ inside $P \oplus P$. We have seen that the two natural projections $I \to P$ are injective, hence bijective. There is thus an element φ in $\mathrm{GL}(P)$ with $I = \{(x, \varphi(x)), x \in P\}$. Set $S = \mathrm{O}(E) \cap \mathrm{O}(\mathrm{Q}_g)$. By Proposition 3.6, the natural morphism $S \to \mathrm{GL}(P)$ is surjective. By multiplying h by a suitable element in $1 \times \mathrm{O}(E)$ we may thus assume that we have $\varphi = -\mathrm{id}_P$, that is, $A' = \mathrm{Q}_{2g}$. We have proved the first assertion. For the second, observe that S embeds diagonally in $\mathrm{O}(E) \times \mathrm{O}(E)$, and as such, it preserves Q_{2g} and acts on the totally isotropic plane $P' = (E \oplus E)/\mathrm{Q}_{2g}$ of $\operatorname{res}\mathrm{Q}_{2g}$. Moreover, the natural map

$$E/\mathrm{Q}_g \to (E \oplus E)/\mathrm{Q}_{2g}, \;\; x \mapsto (x, 0) \bmod \mathrm{Q}_{2g},$$

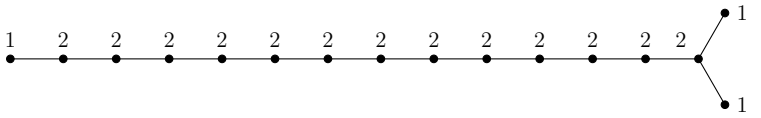
defines an S-equivariant isomorphism $P \to P'$. The surjectivity of $S \to \mathrm{GL}(P)$ thus implies that of $S \to \mathrm{GL}(P')$. □

Proposition 3.10. *Let (g, p, m) be either $(8, 5, 4)$ or $(6, 3, 6)$. Up to isometry, Q_{2g} is the unique even lattice of rank $2g$ without roots satisfying $\mathrm{Q}_{2g}^\sharp/\mathrm{Q}_{2g} \simeq (\mathbb{Z}/p\mathbb{Z})^m$.*

Moreover, $\mathrm{O}(\mathrm{Q}_{2g})$ permutes transitively the totally isotropic planes (resp. lines, resp. flags) of $\operatorname{res}\mathrm{Q}_{2g}$. The inverse image in $\mathrm{Q}_{2g}^\sharp$ of such an isotropic plane (resp. line) is isometric to $\mathrm{E}_g \oplus \mathrm{E}_g$ (resp. to an even lattice with root system $m\mathbf{A}_{p-1}$).

Proof. Let A be an even lattice of rank $2g$ with $A^\sharp/A \simeq (\mathbb{Z}/p\mathbb{Z})^m$. The Milgram formula applied to A and Q_{2g} shows $\operatorname{res} A \simeq \operatorname{res}\mathrm{Q}_{2g}$ (see the proof of Corollary 3.5). The even lattices L containing A with index p^i are in natural bijection with the totally isotropic subspaces of dimension i over $\mathbb{Z}/p\mathbb{Z}$ inside $\operatorname{res} A$, via the map $L \mapsto L/A$. As we have $\operatorname{res} A \simeq \mathrm{H}(\mathbb{Z}/p\mathbb{Z})^2 \oplus \operatorname{res}\mathrm{E}_g^2$, the maximal isotropic subspaces of $\operatorname{res} A$ have dimension 2 over $\mathbb{Z}/p\mathbb{Z}$. Fix such a plane in $\operatorname{res} A$ and denote by F its inverse image in $A^\sharp$. We have $\operatorname{res} F \simeq \operatorname{res}\mathrm{E}_g^2$, so F is an even lattice with same rank and residue as $\mathrm{E}_g \oplus \mathrm{E}_g$.

Assume first $g = 8$. Then F is unimodular. We know since Witt [Wit41] (see also [Kne57]) that F is either isometric to $\mathrm{E}_8 \oplus \mathrm{E}_8$, or to a certain lattice E_{16} with root system $\mathbf{D}_{16}$ and $\mathrm{E}_{16}/\mathrm{D}_{16} = \mathbb{Z}/2\mathbb{Z}$. Assuming furthermore that A has no root, we claim that F cannot be isometric to E_{16}. Indeed, using the method explained in the proof of Proposition 3.4, Lemma 3.1 (i) and an inspection of the Dynkin diagram of $\mathbf{D}_{16}$ (including the n_i's):



we see that an index 5 subgroup of D_{16} always contains an irreducible root system isomorphic to $\mathbf{A}_5$. But $\mathbf{A}_5$ has Coxeter number 6, so A_5 has no index 5 subgroup without roots by Lemma 3.1 (ii), so D_{16} has no index 25 subgroup without roots. If L is an index 25 subgroup of E_{16} then $L \cap \mathrm{D}_{16}$ is a subgroup of D_{16} of index

dividing 25 (in fact, equal to 25) and so its root system is not empty. This proves the claim.

Assume now $g = 6$. We have $\operatorname{res} F \simeq -\operatorname{res} \mathrm{A}_2^2$. This is well-known to imply that F is isometric to $\mathrm{E}_6 \oplus \mathrm{E}_6$, $\mathrm{E}_8 \oplus \mathrm{A}_2 \oplus \mathrm{A}_2$ or to a certain lattice E_{12} having root system $\mathbf{D}_{10}$. (One way to prove this is to start by observing that such a lattice is the orthogonal of some $\mathrm{A}_2 \oplus \mathrm{A}_2$ embedded in an even unimodular lattice, hence in $\mathrm{E}_8 \oplus \mathrm{E}_8$ or in E_{16}.) An inspection of the Dynkin diagrams of $\mathbf{E}_8$ and $\mathbf{D}_{10}$ shows that an index 3 subgroup of E_8 or D_{10} always contains an irreducible root system isomorphic to $\mathbf{A}_3$, whose Coxeter number is > 3. Assuming A has no root, this implies $F \simeq \mathrm{E}_6 \oplus \mathrm{E}_6$ by Lemma 3.1 (ii).

We have just shown that in both cases, assuming A has no roots, the inverse image in $A^\sharp$ of a totally isotropic plane of $\operatorname{res} A$ is isometric to $\mathrm{E}_g \oplus \mathrm{E}_g$. By Proposition 3.9, there is a unique isometry class of pairs (A, F) with $F \simeq \mathrm{E}_g \oplus \mathrm{E}_g$, A of index p^2 in F, and $\mathrm{R}(A) = \emptyset$. This shows $A \simeq \mathrm{Q}_{2g}$ as well as the transitivity of $\mathrm{O}(\mathrm{Q}_{2g})$ on the totally isotropic planes in $\operatorname{res} \mathrm{Q}_{2g}$. Moreover, the same proposition also asserts that the stabilizer in $\mathrm{O}(\mathrm{Q}_{2g})$ of an isotropic plane P in $\operatorname{res} \mathrm{Q}_{2g}$ surjects naturally onto $\mathrm{GL}(P)$. This shows the transitivity of $\mathrm{O}(\mathrm{Q}_{2g})$ on the isotropic lines (resp. flags) in $\operatorname{res} \mathrm{Q}_{2g}$.

Fix an even lattice $B \subset \mathrm{E}_g$ containing Q_g with index p. We known from Proposition 3.4 that such a B exists and is a root lattice with root system $\frac{g}{p-1}\mathbf{A}_{p-1}$. The sublattice $C \subset \mathrm{E}_g \oplus \mathrm{E}_g$ whose elements (x, y) satisfy $x + y \in B$ contains Q_{2g}, and defines an isotropic line C/Q_{2g} in $\operatorname{res} \mathrm{Q}_{2g}$. Its root system $\mathrm{R}(C)$ is isomorphic to $2\frac{g}{p-1}\mathbf{A}_{p-1}$. This concludes the proof of the proposition. □

Proposition 3.11. *For $g = 6, 8$, the natural morphism $\mathrm{O}(\mathrm{Q}_{2g}) \to \mathrm{O}(\operatorname{res} \mathrm{Q}_{2g})$ is surjective, with kernel isomorphic to $\mathbb{Z}/3\mathbb{Z}$ for $g = 6$, $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ for $g = 8$.*

Proof. Set $E = \mathrm{E}_g$, $Q = \mathrm{Q}_g$ and consider the group $S = \mathrm{O}(E) \cap \mathrm{O}(Q)$. The inclusions $Q \subset E \subset E^\sharp \subset Q^\sharp$ define a composition series $U_1 \lhd U_2 \lhd U_3 \lhd S$, where:

- U_3 is the kernel of the natural morphism $\beta : S \to \mathrm{GL}(E/Q)$,
- U_2 is the kernel of the natural morphism $\beta_3 : U_3 \to \mathrm{O}(\operatorname{res} E)$,
- U_1 is the kernel of the natural morphism $\beta_2 : U_2 \to \mathrm{Hom}(E^\sharp/E, E/Q)$ given by $g(x) = x + \beta_2(g)(\overline{x})$ for all g in U_2 and all x in $E^\sharp$ with image $\overline{x}$ in $E^\sharp/E$.

Moreover, if $\mathrm{Hom}(Q^\sharp/E^\sharp, E/Q)^{\mathrm{antisym}}$ denotes the group of antisymmetric group homomorphisms $Q^\sharp/E^\sharp \to E/Q$, with E/Q identified with $\mathrm{Hom}(Q^\sharp/E^\sharp, \mathbb{Q}/\mathbb{Z})$ using the symmetric bilinear form of $Q \otimes \mathbb{Q}$, we have a natural morphism:

- $\beta_1 : U_1 \to \mathrm{Hom}(Q^\sharp/E^\sharp, E/Q)$, given by $g(x) = x + \beta_1(g)(\overline{x})$ for all g in U_1 and all x in $Q^\sharp/Q$ with image $\overline{x}$ in $Q^\sharp/E^\sharp$.

Last but not least, since the natural map $\mathrm{O}(Q) \to \mathrm{O}(\operatorname{res} Q)$ is an isomorphism by Proposition 3.6, the morphisms β, β_3, β_2 above are surjective, and β_1 is an

isomorphism. Let p denote the prime such that we have $E/Q \simeq (\mathbb{Z}/p\mathbb{Z})^2$, we have proved in particular $U_1 \simeq \mathbb{Z}/p\mathbb{Z}$.

Set now $F = E \oplus E$, $A = \mathrm{Q}_{2g}$ and consider the group $T = \mathrm{O}(F) \cap \mathrm{O}(A)$. On the one hand, we have $\mathrm{O}(F) = \mathrm{O}(E)^2 \rtimes \mathfrak{S}_2$. As $\mathfrak{S}_2$ clearly stabilizes A, this shows

$$T = G \rtimes \mathfrak{S}_2 \quad \text{with} \quad G = \{(g_1, g_2) \in S \times S \,|\, \beta(g_1) = \beta(g_2)\}\,.$$

On the other hand, T is also the stabilizer in $\mathrm{O}(A)$ of the subspace F/A of $\operatorname{res} A$. By Proposition 3.10 we are left to prove that the natural morphism $\nu : T \to \overline{T}$, where $\overline{T}$ is the stabilizer of F/A in $\mathrm{O}(\mathrm{res}A)$, is a surjection whose kernel is as in the statement.

To the inclusions $A \subset F \subset F^\sharp \subset A^\sharp$ is associated as above a composition series $V_1 \lhd V_2 \lhd V_3 \lhd \overline{T}$, whose successive quotients $\overline{T}/V_3$, V_3/V_2, V_2/V_1 and V_1 are naturally identified with the groups $\mathrm{GL}(F/A)$, $\mathrm{O}(\operatorname{res} F)$, $\mathrm{Hom}(F^\sharp/F, F/A)$ and $\mathrm{Hom}(A^\sharp/F^\sharp, F/A)^{\mathrm{antisym}}$. The following observations below will prove $\nu(U_i \times U_i \rtimes \mathfrak{S}_2) = V_i$ for $i = 1, 2, 3$, $\nu(T) = \overline{T}$ and identify $\ker \nu$.

Action of $\mathfrak{S}_2$. By definition of A the group $\mathfrak{S}_2$ acts trivially on F/A, hence on $A^\sharp/F^\sharp$ as well. Moreover, it swaps the two factors of $\operatorname{res} F = \operatorname{res} E \oplus \operatorname{res} E$. Recall that this linking quadratic space is 0 for $g = 8$, isomorphic to $\mathrm{H}(\mathbb{Z}/3\mathbb{Z})$ for $g = 6$. As V_2 is a p-group and p is odd it follows that $\mathfrak{S}_2$ acts trivially on $\operatorname{res} A$ for $g = 8$.

Action of G *on* F/A. As $\mathfrak{S}_2$ acts trivially on F/A, Proposition 3.9 implies that ν induces an isomorphism $T/((U_3 \times U_3) \rtimes \mathfrak{S}_2) \simeq \overline{T}/V_3$.

Restriction of ν *to* $(U_3 \times U_3) \rtimes \mathfrak{S}_2$. For $g = (g_1, g_2)$ in $U_3 \times U_3$ and (x_1, x_2) in $F^\sharp = E^\sharp \oplus E^\sharp$, we have $g(x_1, x_2) \equiv (g_1(x_1), g_2(x_2)) \bmod F$. So ν induces an isomorphism between $U_3/U_2 \times U_3/U_2$ and the subgroup $\mathrm{O}(\operatorname{res} E) \times \mathrm{O}(\operatorname{res} E)$ of $\mathrm{O}(\operatorname{res} E \oplus \operatorname{res} E)$. This subgroup has index 2 for $g = 6$ (and 1 for $g = 8$) but recall that in this case $\mathfrak{S}_2$ swaps the two factors of $\operatorname{res} E \oplus \operatorname{res} E$.

Restriction of ν *to* $U_2 \times U_2$. The map $\iota : E/Q \to F/A, x \mapsto (x, 0)$, is an isomorphism. For $g = (g_1, g_2)$ in $U_2 \times U_2$ and (x_1, x_2) in $F^\sharp = E^\sharp \oplus E^\sharp$ we thus have the following equalities in F/A :

$$g(x_1, x_2) - (x_1, x_2) = (\beta_2(g_1)(x_1), \beta_2(g_2)(x_2)) = \iota(\beta_2(g_1)(x_1) + \beta_2(g_2)(x_2)).$$

This shows that ν induces an isomorphism $U_2/U_1 \times U_2/U_1 \xrightarrow{\sim} V_2/V_1$.

Restriction of ν *to* $U_1 \times U_1$. We have $A^\sharp = \{(y_1, y_2) \in Q^\sharp \oplus Q^\sharp \,|\, y_1 \equiv y_2 \bmod E^\sharp\}$. For $g = (g_1, g_2)$ in $U_1 \times U_1$ and $(x_1 + y, x_2 + y)$ in $A^\sharp$ with x_i in $E^\sharp$ and y in $Q^\sharp$, we have the following equality in F/A (with ι defined as above):

$$g(x_1+y, x_2+y) - (x_1+y, x_2+y) = (\beta_1(g_1)(y), \beta_1(g_2)(y)) = \iota(\beta_1(g_1)(y) + \beta_1(g_2)(y)).$$

This shows $\nu(U_1 \times U_1) = V_1$ and

$$\ker \nu_{|U_1 \times U_1} = \{(g_1, g_2) \in U_1 \times U_1 \,|\, \beta_1(g_1) + \beta_1(g_2) = 0\} \simeq \mathbb{Z}/p\mathbb{Z}. \tag{13}$$

All in all, we have shown $\nu(T) = \overline{T}$, and if $K \simeq \mathbb{Z}/p\mathbb{Z}$ denotes the group in (13), $\ker \nu = K \rtimes \mathfrak{S}_2$ for $g = 8$, and $\ker \nu = K$ for $g = 6$. □

Proposition 3.12. *The lattice* Q_{12} *is orientable.*

Proof. As the kernel of $\mathrm{O}(\mathrm{Q}_{12}) \to \mathrm{O}(\operatorname{res}\mathrm{Q}_{12})$ has odd cardinality (namely 3) by Proposition 3.11, it is contained in $\mathrm{SO}(\mathrm{Q}_{12})$. Arguing as in the proof of Proposition 3.7, we are left to find two elements g, g' in $\mathrm{O}(\mathrm{Q}_{12})$ with determinant 1 and whose images in $\mathrm{O}(\operatorname{res}\mathrm{Q}_{12})$ are reflections with distinct spinor norms. In the following arguments, it will be convenient to view linking quadratic spaces over $\mathbb{Z}/3\mathbb{Z}$ as traditional quadratic spaces over $\mathbb{Z}/3\mathbb{Z}$ by multiplying their quadratic map by 3 (which becomes then $\mathbb{Z}/3\mathbb{Z}$-valued instead of $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$-valued), so that it makes sense to talk about their determinant.

Consider first the non-trivial element g of the group $\mathfrak{S}_2$ naturally acting on $\mathrm{E}_6 \oplus \mathrm{E}_6$. Then g acts trivially on $(\mathrm{E}_6 \oplus \mathrm{E}_6)/\mathrm{Q}_{12}$, and in the obvious way on $\operatorname{res}\mathrm{E}_6 \oplus \operatorname{res}\mathrm{E}_6$. It acts thus as a reflection with spinor norm $2 \cdot \frac{1}{2}\det(\operatorname{res}\mathrm{E}_6)$ in $(\mathbb{Z}/3\mathbb{Z})^\times$ (the squares of $(\mathbb{Z}/3\mathbb{Z})^\times$ are $\{1\}$). Moreover, we have $\det g = (-1)^6 = 1$.

Let s be an order two element of $\mathrm{O}(\mathrm{Q}_6) \cap \mathrm{O}(\mathrm{E}_6)$ acting trivially on $\mathrm{E}_6/\mathrm{Q}_6$ and by -1 on $\operatorname{res}\mathrm{E}_6$. Such an s exists by Proposition 3.6. By construction, it is a reflection in $\mathrm{O}(\operatorname{res}\mathrm{Q}_6)$ with spinor norm $\frac{1}{2}\det(\operatorname{res}\mathrm{E}_6) = \det(\operatorname{res}\mathrm{A}_2)$ in $(\mathbb{Z}/3\mathbb{Z})^\times$. So s is conjugate in $\mathrm{O}(\mathrm{Q}_6)$ to the element denoted γ' in the proof of Proposition 3.7, and we have thus $\det s = \det\gamma' = 1$ as was shown *loc. cit.* Consider now the order 2 element $g' = (s, 1)$ in $\mathrm{O}(\mathrm{E}_6) \times \mathrm{O}(\mathrm{E}_6)$. As s preserves Q_6 ands acts trivially on $\mathrm{E}_6/\mathrm{Q}_6$, the element g' preserves Q_{12} and has a trivial image in $\mathrm{GL}((\mathrm{E}_6 \oplus \mathrm{E}_6)/\mathrm{Q}_{12})$. It acts as $\operatorname{diag}(-1, 1)$ in $\operatorname{res}\mathrm{E}_6 \oplus \operatorname{res}\mathrm{E}_6$. It acts thus on $\operatorname{res}\mathrm{Q}_{12}$ as a reflection with spinor norm $\frac{1}{2}\det(\operatorname{res}\mathrm{E}_6)$. This spinor norm is not the same as that of g as 2 is not a square in $(\mathbb{Z}/3\mathbb{Z})^\times$. The orientabiliy of Q_{12} follows then from the equalities $\det g' = \det s \times 1 = 1$. □

We finally set $\mathrm{Q}_0 = 0$ and $\mathrm{Q}_{24} = \text{Leech}$. We denote by n_g the number of isometric embeddings $\mathrm{Q}_g \to \text{Leech}$, and by K_g the kernel of the morphism $\mathrm{O}(\mathrm{Q}_g) \to \mathrm{O}(\operatorname{res}\mathrm{Q}_g)$. By Propositions 3.6 and 3.11 we have $|\mathrm{K}_g| = 1$ for $g < 12$, $|\mathrm{K}_{12}| = 3$, $|\mathrm{K}_{16}| = 10$, and of course $\mathrm{K}_{24} = \mathrm{O}(\text{Leech})$.

Proposition 3.13. *For* g *in* $\{0, 8, 12, 16, 24\}$ *there is a unique* $\mathrm{O}(\text{Leech})$*-orbit of sublattices* Q *of* Leech *with* $Q \simeq \mathrm{Q}_g$*, and we have* $\mathrm{n}_g\,|\mathrm{K}_{24-g}| = |\mathrm{O}(\text{Leech})|$.

Proof. Let Q be a sublattice of Leech isomorphic to Q_g. By [CL19, Prop. B.2.2 (d)], the lattice $Q^\perp$ satisfies $\operatorname{res} Q^\perp \simeq -\operatorname{res} Q$. By Propositions 3.5 and 3.10, we have $Q^\perp \simeq \mathrm{Q}_{g'}$ with $g' = 24 - g$. Moreover, the stabilizer of Q in O(Leech) trivially coincides with that of $Q^\perp$. To prove uniqueness we are thus left to show that there is a unique $\mathrm{O}(\mathrm{Q}_g) \times \mathrm{O}(\mathrm{Q}_{g'})$-orbit of overlattices $L \supset \mathrm{Q}_g \oplus \mathrm{Q}_{g'}$ with $L \simeq \text{Leech}$. Note that the existence of such an L follows from Lemma 2.1.

Consider now an arbitrary maximal isotropic subspace I in $\operatorname{res}\mathrm{Q}_g \oplus \operatorname{res}\mathrm{Q}_{g'}$ (which is a hyperbolic linking quadratic space over $\mathbb{F}_p$ with $p = 5$ or 3). Let L be the inverse image of I in $\mathrm{Q}_g^\sharp \oplus \mathrm{Q}_{g'}^\sharp$, an even unimodular lattice. We assume furthermore

that it has no root. Then $L \cap (\mathrm{Q}_g^\sharp \oplus 0)$ is an even lattice without root containing $\mathrm{Q}_g \oplus 0$. By Propositions 3.5 and 3.10 it must be $\mathrm{Q}_g \oplus 0$, and similarly we have $L \cap (0 \oplus \mathrm{Q}_{g'}^\sharp) = 0 \oplus \mathrm{Q}_{g'}$. It follows that both projections $I \to \operatorname{res} \mathrm{Q}_g$ and $I \to \operatorname{res} \mathrm{Q}_{g'}$ are injective, hence isomorphisms. So there is an isometry $\varphi : \operatorname{res} \mathrm{Q}_g \xrightarrow{\sim} -\operatorname{res} \mathrm{Q}_{g'}$ such that we have $I = I_\varphi$, with $I_\varphi = \{(x, \varphi(x)), x \in \operatorname{res} \mathrm{Q}_g\}$. By Propositions 3.6 and 3.11, the map $\mathrm{O}(\mathrm{Q}_{g'}) \to \mathrm{O}(\operatorname{res} \mathrm{Q}_{g'})$ is surjective. This shows that $1 \times \mathrm{O}(\mathrm{Q}_{g'})$ permutes transitively the I_φ, and that the stabilizer in this group of any I_φ is the kernel of $\mathrm{O}(\mathrm{Q}_{g'}) \to \mathrm{O}(\operatorname{res} \mathrm{Q}_{g'})$, and we are done. □

We have also proved above the following:

Corollary 3.14. *Fix g in $\{0, 8, 12, 16, 24\}$ and an isometric embedding of $\mathrm{Q}_g \oplus \mathrm{Q}_{g'}$ in* Leech*, with $g' = 24 - g$. The stabilizer S of Q_g in* O(Leech) *is* $\mathrm{O}(\text{Leech}) \cap (\mathrm{O}(\mathrm{Q}_g) \times \mathrm{O}(\mathrm{Q}_{g'}))$ *and the natural map $S \to \mathrm{O}(\mathrm{Q}_g)$ is surjective with kernel $1 \times \mathrm{K}_{g'}$.*

Proposition 3.15. *The lattice Q_{16} is orientable.*

Proof. Fix an isometric embedding of $\mathrm{Q}_8 \oplus \mathrm{Q}_{16}$ in Leech. By Corollary 3.14, for any γ in $\mathrm{O}(\mathrm{Q}_{16})$ there is γ' in $\mathrm{O}(\mathrm{Q}_8)$ such that $\gamma \oplus \gamma'$ is in O(Leech). As any element of O(Leech) has determinant 1 we have $\det \gamma \det \gamma' = 1$. But we have $\det \gamma' = 1$ as Q_8 is orientable, hence $\det \gamma = 1$. □

We have used several times the following simple lemma.

Lemma 3.16. *Let L be an even lattice, and $q : \operatorname{res} L \to \mathbb{Q}/\mathbb{Z}$ the associated linking quadratic map (see the General Notations).*

(i) *The map $M \mapsto M/L$ defines a bijection between the set of even lattices M in $L \otimes \mathbb{Q}$ containing L and the set of totally isotropic subgroups $I \subset \operatorname{res} L$ (that is, with $q(I) = 0$). In this bijection, we have $\operatorname{res} M \simeq I^\perp / I$. If furthermore I is a direct summand of the abelian group $\operatorname{res} L$, and if $|I|$ is odd, then we have a (noncanonical) isomorphism $\operatorname{res} L \simeq \mathrm{H}(I) \oplus \operatorname{res} M$.*

(ii) *Let h be an odd integer ≥ 1 and $x \in L$ with $x \cdot x \equiv 0 \bmod h$. Assume that the natural map $L \to \mathbb{Z}/h\mathbb{Z}, y \mapsto y \cdot x \bmod h$ is surjective, and denote by M its kernel. Then M is an even lattice with $L/M \simeq \mathbb{Z}/h\mathbb{Z}$ and $\operatorname{res} M \simeq \operatorname{res} L \oplus \mathrm{H}(\mathbb{Z}/h\mathbb{Z})$.*

Proof. The first two assertions in (i) are obvious [CL19, Prop. 2.1.1]. For the last assertion of (i) choose first a subgroup J of $I^\perp$ with $I^\perp = J \oplus I$. Then J is nondegenerate in $\operatorname{res} L$, I is a totally isotropic direct summand of $V := J^\perp$, and we have an exact sequence $0 \to I \to V \to \mathrm{Hom}(I, \mathbb{Q}/\mathbb{Z}) \to 0$. We now argue as in the proof of Proposition 2.1.2 of [CL19] (beware however that the statement *loc. cit.* does not hold for linking quadratic spaces of even cardinality). Choose a supplement I' of I in V, *i.e.* $V = I \oplus I'$. As V is nondegenerate, any bilinear form on I' is of the form $(x, y) \mapsto x \cdot \varphi(y)$ for some morphism $\varphi : I' \to I$. We

apply this to the form $(x,y) \mapsto \frac{1}{2}x \cdot y$, which is well defined as $|V|$ is odd. Then the subgroup $\{x - \varphi(x), x \in I'\}$ is a totally isotropic supplement of I in V. This implies $V \simeq \mathrm{H}(I)$ (see Proposition-Definition 2.1.3 *loc. cit.*).

For assertion (ii), consider the natural map $M^\sharp \to \mathbb{Z}/h\mathbb{Z}, y \mapsto y \cdot x \bmod h$. This is well defined as we have $x \in M$ by assumption, and its restriction to L induces an isomorphism $L/M \xrightarrow{\sim} \mathbb{Z}/h\mathbb{Z}$. So L/M is a direct summand of $\operatorname{res} M$ and we conclude the proof by (i). □

4. Standard L-functions of the eigenforms F_g

In this section, we show that the Siegel modular forms F_g defined in (3) are eigenforms and give an expression for their standard L-functions.

Proposition 4.1. *Let L be an integral lattice whose roots generate $L \otimes \mathbb{R}$. For any $g \geq 1$, there is no nonzero, $\mathrm{O}(L)$-invariant, alternating g-form on L.*

Proof. Let $\omega : L^g \to \mathbb{R}$ be such a form. It is enough to show $\omega(x_1, \ldots, x_g) = 0$ for any $x_1, \ldots, x_g$ in L, with x_i roots of L. Fix such x_i and let s be the reflection associated to the root x_1. We have $s \in \mathrm{O}(L)$ as L is integral, $s(x_1) = -x_1$ and $s(x_i) \in x_i + \mathbb{Z}\, x_1$ for all i, hence the following equalities

$$\omega(x_1, x_2, \ldots, x_g) = \omega(s(x_1), s(x_2), \ldots, s(x_g)) = -\omega(x_1, x_2, \ldots, x_g) = 0.$$

□

Fix an integer $n \equiv 0 \bmod 8$ and consider the set $\mathscr{L}_n$ of even unimodular lattices in the standard Euclidean space $V = \mathbb{R}^n$. For all $g \geq 1$ we denote by Alt_n^g the quotient of the free $\mathbb{R}$-vector space with generators the (L, ω), with L in $\mathscr{L}_n$ and ω an alternating g-form on V, by the relations

$$(\gamma^{-1}(L), \omega \circ \gamma) = (L, \omega) \quad \text{and} \quad (L, \lambda\,\omega + \omega') \,=\, \lambda\,(L, \omega) \,+\, (L, \omega'),$$

for all L in $\mathscr{L}_n$, all γ in $\mathrm{O}(V)$, all alternating g-forms ω, ω' on V and all λ in $\mathbb{R}$. As usual $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ denotes the space of (scalar-valued) Siegel cusp forms of genus g, weight k and level one. It follows readily from these definitions that the Siegel theta series construction $(L, \omega) \mapsto \Theta(L, \omega) = \sum_{\underline{v} \in L^g} \omega(\underline{v}) q^{\frac{\underline{v} \cdot \underline{v}}{2}}$ factors through an $\mathbb{R}$-linear map

$$\Theta : \mathrm{Alt}_n^g \longrightarrow \mathrm{S}_{n/2+1}(\mathrm{Sp}_{2g}(\mathbb{Z})). \tag{14}$$

If $L_1, \ldots, L_h$ denote representatives for the isometry classes of even unimodular lattices in V, we also have an $\mathbb{R}$-linear isomorphism

$$\mathrm{Alt}_n^g \simeq \bigoplus_{i=1}^{h} (\Lambda^g V^*)^{\mathrm{O}(L_i)}. \tag{15}$$

The classification of even unimodular lattices in rank ≤ 24 (or simply, Venkov's argument in [CS99, Ch. 18, §2, Prop. 1]) shows that appart from Leech these

lattices are generated over $\mathbb{Q}$ by their roots. Proposition 4.1 and Formula (15) thus show that Alt_n^g vanishes for $n < 24$, and together with (1), imply:

Proposition 4.2. Alt_{24}^g *has dimension* 1 *for* g *in* $\{8, 12, 16, 24\}$, 0 *otherwise.*

Let us denote by O_n the orthogonal group scheme of a fixed even unimodular lattice of rank n, *e.g.* of $\mathrm{D}_n + \mathbb{Z}\,e$ with $e = \frac{1}{2}(1, \dots, 1)$. For any finite dimensional representation U of $\mathrm{O}(V)$, the space[3] $\mathrm{M}_U(\mathrm{O}_n)$ of $\mathrm{O}(V)$-equivariant functions $\mathscr{L}_n \to U$, is the space of level 1 automorphic forms of O_n with coefficients in U [CL19, §4.4.4]. As such it is equipped with an action of the (commutative) Hecke ring $\mathrm{H}(\mathrm{O}_n)$ of O_n [CL19, §4.2.5 & §4.2.6]. For all $g \geq 1$ we have a perfect pairing

$$\begin{aligned} \mathrm{M}_{\Lambda^g V}(\mathrm{O}_n) \times \mathrm{Alt}_n^g &\longrightarrow \mathbb{C} \\ (f, (L, \omega)) &\longmapsto \omega(f(L)) \end{aligned}$$

identifying Alt_n^g with the dual of $\mathrm{M}_{\Lambda^g V}(\mathrm{O}_n)$. In particular Alt_n^g also carries an $\mathrm{H}(\mathrm{O}_n)$-action. As an example, for any prime p the Kneser p-neighbor operator is the endomorphism of Alt_n^g sending (L, ω) to the sum of (L', ω) over the L' in $\mathscr{L}_n$ with $L \cap L'$ of covolume p. The so-called *Eichler commutations relations* imply that the map Θ in (14) sends an $\mathrm{H}(\mathrm{O}_n)$-eigenvector on the left-hand side either to 0 or to a Siegel eigenform on the right-hand side (i.e. an $\mathrm{H}(\mathrm{Sp}_{2g})$-eigenvector): see [Fre82], as well as [Ral82] for an interpretation in terms of Satake parameters.

For $g = 8, 12, 16, 24$, the space Alt_{24}^g has dimension 1, so it is generated by an $\mathrm{H}(\mathrm{O}_{24})$-eigenvector. Our main theorem asserts that the image of Alt_{24}^g under Θ is generated by F_g and is nonzero. We have proved:

Corollary 4.3. *For* $g = 8, 12, 16, 24$, *the Siegel modular form* F_g *is an eigenform.*

We now discuss the standard L-functions of the eigenforms F_g, or more precisely, their collections of Satake parameters. We need some preliminary remarks and notations mostly borrowed from [CL19, §6.4].

For any integer $n \geq 1$ we denote by $\mathscr{X}_n$ the set of sequences $c = (c_\infty, c_2, \dots, c_p, \dots)$, where c_∞ is a semisimple conjugacy class in $\mathrm{M}_n(\mathbb{C})$ and the c_p are semisimple conjugacy classes in $\mathrm{GL}_n(\mathbb{C})$ indexed by the primes p. The direct sum and tensor product induce componentwise two natural operations $\mathscr{X}_m \times \mathscr{X}_n \to \mathscr{X}_{m+n}$ and $\mathscr{X}_m \times \mathscr{X}_n \to \mathscr{X}_{mn}$, denoted respectively $(c, c') \mapsto c \oplus c'$ and $(c, c') \mapsto c\,c'$. An important role will be played by the element $[n]$ of $\mathscr{X}_n$ such that $[n]_p$ (resp. $[n]_\infty$) has the eigenvalues $p^{\frac{n-1}{2} - i}$ (resp. $\frac{n-1}{2} - i$) for $i = 0, \dots, n-1$. In particular, for any $c \in \mathscr{X}_m$ and any integer $n \geq 1$, we have a well-defined element $c[n] \in \mathscr{X}_{mn}$, namely the element cc' with $c' = [n]$.

Any Siegel eigenform F for $\mathrm{Sp}_{2g}(\mathbb{Z})$ has an associated collection of Satake parameters, semisimple conjugacy classes in $\mathrm{SO}_{2g+1}(\mathbb{C})$ indexed by the primes, as well as an infinitesimal character (as defined by Harish-Chandra), which may be

[3]We have a similar definition with O replaced by SO that we will also use below.

viewed as a semisimple conjugacy class in the Lie algebra of $\mathrm{SO}_{2g+1}(\mathbb{C})$. So F gives rise to an element in $\mathscr{X}_{2g+1}$ using the natural (or "standard") representation $\mathrm{SO}_{2g+1}(\mathbb{C}) \to \mathrm{GL}_{2g+1}(\mathbb{C})$. This element is called the *standard parameter* of F. Similarly, any $\mathrm{H}(\mathrm{O}_n)$-eigenvector in $\mathrm{M}_U(\mathrm{O}_n)$ or $\mathrm{M}_U(\mathrm{SO}_n)$ gives rise to an element of $\mathscr{X}_n$: see e.g. [CL19, Sch. 6.2.4 & Def. 6.4.9].

For $g = 8, 12, 16, 24$ we denote by ψ_g the standard parameter of the eigenform F_g, and by ψ'_g that of a generator of $\mathrm{M}_{\Lambda^g V}(\mathrm{O}_{24}) = (\mathrm{Alt}^g_{24})^*$. By definition, ψ_g is in $\mathscr{X}_{2g+1}$ and ψ'_g is in $\mathscr{X}_{24}$. Using Theorem 2, Rallis's aforementioned generalization and reinterpretation of the Eichler commutation relations asserts

$$\psi'_8 = \psi_8 \oplus [7] \quad \text{and} \quad \psi_g = \psi'_g \oplus [2g-23] \ \text{ for } \ g \geq 12. \tag{16}$$

In the spirit of standard conjectures by Langlands and Arthur (see. [CL19, §6.4.4]), we will express those ψ_g and ψ'_g in terms of Satake parameters of certain cuspidal automorphic eigenforms for $\mathrm{GL}_m(\mathbb{Z})$. The four following forms will play a role:

– For $w = 11, 17$, we denote by $\Delta_w \in \mathscr{X}_2$ the collection of the Satake parameters, and of the infinitesimal character, of the classical modular normalized eigenform of weight $w+1$ for $\mathrm{PGL}_2(\mathbb{Z})$. For example, the p-th component of Δ_{11} has determinant 1 and trace $\tau(p)/p^{11/2}$, where τ is the classical Ramanujan function, defined by

$$\sum_{n\geq 1} \tau(n) q^n = q \prod_{n \geq 1} (1-q^n)^{24}.$$

The eigenvalues of $(\Delta_w)_\infty$ are $\pm\frac{w}{2}$.

– For $(w, v) = (19, 7)$ and $(21, 13)$, and following [CL19, §9.1.3], there is a unique (up to scalar) cuspidal eigenform for $\mathrm{PGL}_4(\mathbb{Z})$ whose infinitesimal character has the eigenvalues $\pm w/2, \pm v/2$: we denote by $\Delta_{w,v} \in \mathscr{X}_4$ the collection of its Satake parameters, and of this infinitesimal character. As explained *loc. cit.*, they are also the spinor parameters of generators of the 1-dimensional space of Siegel modular forms for $\mathrm{Sp}_4(\mathbb{Z})$ with coefficients in the representations $\mathrm{Sym}^6 \otimes \det^8$ and $\mathrm{Sym}^{12} \otimes \det^6$ of $\mathrm{GL}_2(\mathbb{C})$ respectively. See [CL19, Tables C3 & C.4] and [BCFvdG17] for more information on these Satake parameters.

Theorem 4.4. *The parameters ψ_g and ψ'_g are given by the following table:*

g	8	12	16	24
ψ_g	$\Delta_{21,13}[4] \oplus [1]$	$\Delta_{19,7}[6] \oplus [1]$	$\Delta_{17}[8] \oplus [9] \oplus [7] \oplus [1]$	$\Delta_{11}[12] \oplus [25]$
ψ'_g	$\Delta_{21,13}[4] \oplus [7] \oplus [1]$	$\Delta_{19,7}[6]$	$\Delta_{17}[8] \oplus [7] \oplus [1]$	$\Delta_{11}[12]$

Proof. By Proposition 7.5.1 of [CL19], relying on [Ike01] and [Wei86] or [Bö89], we have $\psi'_{24} = \Delta_{11}[12]$, and thus $\psi_{24} = \Delta_{11}[12] \oplus [25]$ by (16). The remaining parameters are harder to determine, and at the moment we only know how to do it using Arthur's results [Art13] together with [AMR18, Taï19].

The irreducible representation $\Lambda^{12} V$ of $\mathrm{O}(V)$ is the sum of two irreducible non-isomorphic representations $A^{\pm}$ of $\mathrm{SO}(V)$. As a consequence, the two spaces $\mathrm{M}_{A^{\pm}}(\mathrm{SO}_{24})$ have dimension 1 and are isomorphic to $\mathrm{M}_{\Lambda^{12} V}(\mathrm{O}_{24})$ as $\mathrm{H}(\mathrm{O}_{24})$-modules (see [CL19, §4.4.4]). The eigenvalues of $s = (\Delta_{19,7}[6])_\infty$ are $\pm i$ with $i = 1, \dots, 12$, so s is the image in $\mathrm{M}_{24}(\mathbb{C})$ of the infinitesimal character of $A^{\pm}$. By Arthur's multiplicity formula for SO_{24}, discussed in [CL19, Thm. 8.5.8] and which applies by [AMR18, Taï19], there is an $\mathrm{H}(\mathrm{O}_{24})$-eigenvector in $\mathrm{M}_{A^{\pm}}(\mathrm{SO}_{24})$ with standard parameter $\Delta_{19,7}[6]$: this parameter must be ψ'_{12} because we have $\dim \mathrm{M}_{A^{\pm}}(\mathrm{SO}_{24}) = 1$.

The two non-isomorphic representations $\Lambda^8 V$ and $\Lambda^{16} V$ of $\mathrm{O}(V)$ have isomorphic and irreducible restriction B to $\mathrm{SO}(V)$. As a consequence, the space

$$\mathrm{M}_B(\mathrm{SO}_{24}) \simeq \mathrm{M}_{\Lambda^8 V}(\mathrm{O}_{24}) \oplus \mathrm{M}_{\Lambda^{16} V}(\mathrm{O}_{24}) \tag{17}$$

has dimension 2 (see [CL19, §4.4.4]). Assume $\psi \in \mathscr{X}_{24}$ is either $\Delta_{21,13}[4] \oplus [7] \oplus [1]$ or $\Delta_{17}[8] \oplus [7] \oplus [1]$. The eigenvalues of ψ_∞ are the $\pm i$ with $0 \leq i \leq 12$ and $i \neq 4$, so ψ_∞ is the image in $\mathrm{M}_{24}(\mathbb{C})$ of the infinitesimal character of B. An inspection of Arthur's multiplicity formula for SO_{24} [CL19, Thm. 8.5.8] shows that there is an $\mathrm{H}(\mathrm{O}_{24})$-eigenvector in $\mathrm{M}_B(\mathrm{SO}_{24})$ with standard parameter ψ. These two parameters are distinct and the isomorphism (17) is $\mathrm{H}(\mathrm{O}_{24})$-equivariant by [CL19, §4.4.4], it thus only remains to explain which of the two eigenvectors above belongs to $\mathrm{M}_{\Lambda^8 V}(\mathrm{O}_{24})$. But Arthur's multiplicity formula for Sp_{16} (or Ikeda's results) shows that there is no cuspidal Siegel eigenform for $\mathrm{Sp}_{16}(\mathbb{Z})$ with standard parameter $\Delta_{17}[8] \oplus [1]$, as explained in [CL19, Example 8.5.3]. This proves $\psi'_8 = \Delta_{21,13}[4] \oplus [7] \oplus [1]$ by (16), hence $\psi'_{16} = \Delta_{17}[8] \oplus [7] \oplus [1]$, and the whole table follows from (16) again. □

Appendix A. The norm of the Weyl vector of an ADE root system

The following proposition was promised in Section 3, to which we refer for the notations and definitions concerning root systems.

Proposition A.1. *Let R be an irreducible root system of type* ADE*, rank l, Coxeter number h and Weyl vector ρ, in the Euclidean space V, so that we have $\alpha.\alpha = 2$ for all $\alpha \in R$. Then we have $\rho \cdot \rho = \frac{l}{12} h(h+1)$.*

Proof. Recall that the *height* of the positive root $\alpha \in R_+$ is $\mathrm{ht}(\alpha) = \rho \cdot \alpha$. We thus have $2\,\rho \cdot \rho = \sum_{\alpha \in R_+} \mathrm{ht}(\alpha)$. By Bourbaki's theory of the canonical bilinear form [Bou68, Ch. VI §1.12] we obtain that for any $v \in V$ we have

$$v \cdot v = h^{-1} \sum_{\alpha \in R_+} (\alpha \cdot v)^2.$$

Applying this to $v = \rho$ we obtain a second expression

$$\rho \cdot \rho = h^{-1} \sum_{\alpha \in R_+} \mathrm{ht}(\alpha)^2.$$

Let $m_1 \leq \cdots \leq m_l$ be the exponents of R [Bou68, Ch. V §6 Déf. 2]. Kostant showed that these exponents can also be obtained by considering the adjoint representation of a principal three-dimensional subalgebra of the Lie algebra corresponding to R [Kos59, Thms. 6.7 and 8.6]. This implies that for any map $f : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ we have the identity $\sum_{\alpha \in R_+} f(\mathrm{ht}(\alpha)) = \sum_{j=1}^{l} F(m_j)$ with $F(m) = \sum_{u=1}^{m} f(u)$ (see [CL19, p. 82]). The two relations involving $\rho \cdot \rho$ above can be written in terms of the exponents as follows.

$$\sum_{j=1}^{l} \binom{m_j+1}{2} = \sum_{\alpha \in R_+} \mathrm{ht}(\alpha) = 2\,\rho \cdot \rho$$

$$\sum_{j=1}^{l} \binom{m_j+2}{3} = \sum_{\alpha \in R_+} \binom{\mathrm{ht}(\alpha)+1}{2} = \sum_{\alpha \in R_+} \frac{\mathrm{ht}(\alpha)^2}{2} + \frac{\mathrm{ht}(\alpha)}{2} = \left(\frac{h}{2}+1\right) \rho \cdot \rho$$

The exponents satisfy $m_j + m_{l+1-j} = h$ [Bou68, Ch. V §6.2], and so we have

$$\sum_{j=1}^{l} \binom{h-m_j+2}{3} = \sum_{j=1}^{l} \binom{m_j+2}{3}. \tag{18}$$

As a special case of Vandermonde's convolution we have for any $m \in \mathbb{Z}$

$$\sum_{k=0}^{3} \binom{-m}{k} \binom{h+2}{3-k} = \binom{h-m+2}{3}.$$

Using the relation $\binom{m+k-1}{k} = (-1)^k \binom{-m}{k}$ this can be written

$$\binom{m+2}{3} - \binom{h-m+2}{3} = 2\binom{m+2}{3} - (h+2)\binom{m+1}{2} + \binom{h+2}{2} m - \binom{h+2}{3}.$$

Plugging this relation into (18) we obtain

$$\begin{aligned} 0 &= 2\sum_{j=1}^{l} \binom{m_j+2}{3} - (h+2)\sum_{j=1}^{l} \binom{m_j+1}{2} + \binom{h+2}{2} \sum_{j=1}^{l} m_j - l\binom{h+2}{3} \\ &= (h+2)\rho \cdot \rho - (2h+4)\rho \cdot \rho + \binom{h+2}{2} \frac{lh}{2} - l\binom{h+2}{3} \\ &= (-h-2)\rho \cdot \rho + l\left(\binom{h+2}{2}\frac{h}{2} - \binom{h+2}{3}\right) \end{aligned}$$

and the formula for $\rho \cdot \rho$ follows. □

References

[AMR18] Nicolás Arancibia, Colette Moeglin, and David Renard, *Paquets d'Arthur des groupes classiques et unitaires*, Ann. Fac. Sci. Toulouse **27** (2018), 1023–1105.

[Art13] James Arthur, *The Endoscopic Classification of Representations: Orthogonal and Symplectic groups*, American Mathematical Society Colloquium Publications, vol. 61, American Mathematical Society, 2013.

[BCFvdG17] Jonas Bergström, Fabien Cléry, Carel Faber, and Gerard van der Geer, *Siegel modular forms of degree two and three*, 2017, Retrieved March 2019.

[BFW98] Richard E. Borcherds, Eberhard Freitag, and Rainer Weissauer, *A Siegel cusp form of degree 12 and weight 12*, J. Reine Angew. Math. **494** (1998), 141–153, Dedicated to Martin Kneser on the occasion of his 70th birthday.

[Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.

[Bö89] Siegfried Böcherer, *Siegel modular forms and theta series*, Theta functions—Bowdoin 1987, Part 2 (Brunswick, ME, 1987), Proc. Sympos. Pure Math., vol. 49, Amer. Math. Soc., Providence, RI, 1989, pp. 3–17.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[Che20] Gaëtan Chenevier, *The characteristic masses of Niemeier lattices*, Journal Th. Nombres de Bordeaux **32** (2020), 545–583.

[CL19] Gaëtan Chenevier and Jean Lannes, *Automorphic forms and even unimodular lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 69, Springer Verlag, 2019.

[Con69] J. H. Conway, *A group of order* $8,315,553,613,086,720,000$, Bull. London Math. Soc. **1** (1969), 79–88.

[CS88] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices. II. Subgroups of* $\mathrm{GL}(n, \mathbf{Z})$, Proc. Roy. Soc. London Ser. A **419** (1988), no. 1856, 29–68.

[CS99] ———, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[CT53] H. S. M. Coxeter and J. A. Todd, *An extreme duodenary form*, Canadian Journal of Mathematics **5** (1953), 384–392.

[CT20] Gaëtan Chenevier and Olivier Taïbi, *Discrete series multiplicities for classical groups over* $\mathbb{Z}$ *and level* 1 *algebraic cusp forms*, Publ. Math. I. H.É.S. **131** (2020), 261–323.

[Die71] Jean A. Dieudonné, *La géométrie des groupes classiques*, Springer-Verlag, 1971, Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5.

[Ebe13] Wolfgang Ebeling, *Lattices and codes*, third ed., Advanced Lectures in Mathematics, Springer Spektrum, Wiesbaden, 2013, A course partially based on lectures by Friedrich Hirzebruch.

[Ero79] V. A. Erokhin, *Theta series of even unimodular* 24*-dimensional lattices*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **86** (1979), 82–93, 190, Algebraic numbers and finite groups.

[Fre83] E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren der Mathematischen Wissenschaften, vol. 254, Springer-Verlag, Berlin, 1983.

[Fre82] ———, *Die Wirkung von Heckeoperatoren auf Thetareihen mit harmonischen Koeffizienten*, Math. Ann. **258** (1981/82), no. 4, 419–440.

[Fro04] G. Frobenius, *Über die charaktere der mehrfach transitiven gruppen*, Preussische Akademie der Wissenschaften Berlin: Sitzungsberichte der Preußischen Akademie der Wissenschaften zu Berlin, Reichsdr., 1904.

[GAP21] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[GL11] Robert L. Griess, Jr. and Ching Hung Lam, *A moonshine path for* $5A$ *and associated lattices of ranks 8 and 16*, J. Algebra **331** (2011), 338–361.

[HL90] Koichiro Harada and M.-L. Lang, *On some sublattices of the Leech lattice*, Hokkaido Math. J. **19** (1990), no. 3, 435–446.

[Ike01] Tamotsu Ikeda, *On the lifting of elliptic cusp forms to Siegel cusp forms of degree* $2n$, Ann. of Math. (2) **154** (2001), no. 3, 641–681.

[Ike06] ———, *Pullback of the lifting of elliptic cusp forms and Miyawaki's conjecture*, Duke Math. J. **131** (2006), no. 3, 469–497.

[Kne57] Martin Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250.

[Kos59] Bertram Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. Math. **81** (1959), 973–1032.

[MH73] John Milnor and Dale Husemoller, *Symmetric bilinear forms*, Springer-Verlag, New York-Heidelberg, 1973, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[MR] Colette Moeglin and David Renard, *Sur les paquets d'arthur de* $\mathrm{Sp}(2n, \mathbb{R})$ *contenant des modules unitaires de plus haut poids, scalaires*, `https://arxiv.org/abs/1802.04611`, version 4, to appear in Nagoya Math. Journal.

[NV01] Gabriele Nebe and Boris Venkov, *On Siegel modular forms of weight 12*, J. Reine Angew. Math. **531** (2001), 49–60.

[Ple98] Vera Pless, *Introduction to the theory of error-correcting codes*, third ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication.

[Ral82] Stephen Rallis, *Langlands' functoriality and the Weil representation*, Amer. J. Math. **104** (1982), no. 3, 469–515.

[RS98] E. M. Rains and N. J. A. Sloane, *The shadow theory of modular and unimodular lattices*, J. Number Theory **73** (1998), no. 2, 359–389.

[Saw99] Masato Sawabe, *A combinatorial approach to the conjugacy classes of the Mathieu simple groups,* M_{24}*,* M_{23}*,* M_{22}, Journal of the Mathematical Society of Japan **51** (1999), no. 3, 661 – 678.

[SH98] Rudolf Scharlau and Boris Hemkemeier, *Classification of integral lattices with large class number*, Math. Comp. **67** (1998), no. 222, 737–749.

[SV94] Rudolf Scharlau and Boris B. Venkov, *The genus of the Barnes-Wall lattice*, Comment. Math. Helv. **69** (1994), no. 2, 322–333.

[Taï19] Olivier Taïbi, *Arthur's multiplicity formula for certain inner forms of special orthogonal and symplectic groups*, Journal of the European Mathematical Society **21** (2019), 839–871.

[vdG08] Gerard van der Geer, *Siegel modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 181–245.

[Wei86] Rainer Weissauer, *Stabile Modulformen und Eisensteinreihen*, Lecture Notes in Mathematics, vol. 1219, Springer-Verlag, Berlin, 1986.

[Wit37] Ernst Witt, *über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg **12** (1937), no. 1, 265–275.

[Wit41] ———, *Eine Identität zwischen Modulformen zweiten Grades*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 323–337.

(Gaëtan Chenevier) CNRS, Laboratoire de Mathématiques d'Orsay, Université Paris-Saclay

(Olivier Taïbi) CNRS, École Normale Supérieure de Lyon