Commun. Math. Phys. 164, 87–104 (1994)

Communications in Mathematical Physics

An Orbifold Theory of Genus Zero Associated to the Sporadic Group M_{24}

Chongying Dong[1], **Geoffrey Mason**[2]
Department of Mathematics, University of California, Santa Cruz, CA 95064, USA

Received: 15 July 1993

Abstract: Let V_{Γ_l} be the self-dual (or holomorphic) bosonic conformal field theory associated with the spin lattice Γ_l of rank l divisible by 24. In earlier work of the authors we showed how it is possible to establish the existence and uniqueness of irreducible g-twisted sectors for V_{Γ_l}, for certain automorphisms g of V_{Γ_l}, and to establish the modular invariance of the space of partition functions $Z(g, h, \tau)$ corresponding to commuting pairs g, h of elements in certain groups G of automorphisms of V_{Γ_l}. In the present work we show that if we take $l=24$ and G the sporadic simple group M_{24}, then the corresponding orbifold has the *genus zero property*. That is, each $Z(g, h, \tau)$ is either identically zero or a *hauptmodul*, i.e., it generates the field of functions on the subgroup of $SL_2(\mathbb{R})$ which fixes $Z(g, h, \tau)$, which then necessarily has genus zero.

1. Introduction

The most famous example of a holomorphic (or self-dual) conformal field theory (CFT) is undoubtedly the *Moonshine module* whose automorphism group is the Monster M ([B1, FLM]). In their equally famous paper [CN], Conway and Norton laid out an impressive set of data related to their conjecture that for each $m \in M$, the graded trace of m on $V^\natural$ (sometimes called the *Thompson series* of m, and denoted $T_m(\tau)$) is a particular kind of modular function called a *hauptmodul*. That is, the subgroup of $SL_2(\mathbb{R})$ which leaves $T_m(\tau)$ invariant is a discrete group Γ_m commensurable with $SL_2(\mathbb{Z})$ and such that the compactified orbit space $X_m = \Gamma_m \backslash \mathfrak{h}^*$ for the usual action on the upper half-plane $\mathfrak{h}$ is topologically a sphere. Furthermore, the field of meromorphic functions on X_m is precisely $\mathbb{C}(T_m)$; that is, each such function is a rational function of T_m. These conjectures have

[1] Supported by NSA grant MDA904-92-H-3099, by a Regent's Junior Faculty Fellowship of the University of California, and by faculty research funds granted by the University of California, Santa Cruz.
[2] Supported by NSF grant DMS-9122030.

been established by Borcherds [B2], but even before this Norton introduced his notion of generalized Moonshine (see the appendix to [M1]) involving pairs of commuting elements in M and suggested that there was an extension of the Conway–Norton conjectures to this more general situation, except that the Thompson series corresponding to a commuting pair may now be either constant or a hauptmodul. We refer to this general situation as the *genus zero property*.

Subsequently it was realized in [DGH] and elsewhere, that generalized Moonshine was intimately related to the theory of so-called *orbifolds* (see below), and indeed recently Tuite [Tu] has given heuristic (but compelling) arguments that the generalized CN-conjectures are consequences of natural conjectures concerning the structure of the Monster orbifold based on $V^\natural$. However it seems likely that it will be some time before these conjectures are put on a rigorous mathematical footing.

In this paper we will give a completely rigorous account of a CFT V_{Γ_l} of central charge 24 which admits the Mathieu group M_{24} as automorphisms and is such that the corresponding orbifold has the genus zero property for commuting pairs as discussed above. Conway–Norton made precise conjectures [CN] concerning the nature of the fixing group of the corresponding hauptmodul, and we shall verify their assertions for the M_{24} orbifold. Thus one can in every way think of the Mathieu orbifold as a toy version of the Monster orbifold in which all of the relevant conjectures are theorems.

An important point is that our arguments are almost always general in nature and do not involve examination of individual Fourier expansions. Essentially, the genus zero property is shown to be a consequence solely of group-theoretic properties of M_{24} itself.

The results of the present paper were announced awhile ago [M2], but at that time it was not realized that there was a CFT underlying the theory. This was subsequently established in [DM].

The paper is arranged as follows: in Sect. 2 we give some background from [DM] concerning the bosonic orbifolds. We also cover here some results from [M2] about modular-invariance which are crucial in later sections. In Sect. 3 we state the main theorems A, B and C, together with a table of useful data concerning the individual modular functions that arise. Proofs are given in Sects. 4–6, and includes verification of all of the CN-conjectures that are relevant to the present situation. Most of the proofs are based on the theory of modular forms.

2. Background

A *vertex operator algebra* (VOA) is a $\mathbb{Z}$-graded vector space $V=\coprod_{n\in\mathbb{Z}} V_n$ such that $\dim V_n<\infty$ and $V_n=0$ if n is sufficiently small, and such that there is a linear map

$$V\to(\mathrm{End}\ V)[[z,z^{-1}]]\ ,$$
$$v\mapsto Y(v,z)=\sum_{n\in\mathbb{Z}} v_n z^{-n-1}\ (v_n\in\mathrm{End}\ V)\ . \tag{2.1}$$

A number of axioms are also required, most of which we shall pass over here, referring the reader to [FLM or DM], for example. We do, however, mention the *Virasoro axiom*, which posits the existence of $\omega\in V_2$ such that $\omega_{n+1}=L(n)$, that is

$$Y(\omega,z)=\sum_{n\in\mathbb{Z}} L(n)z^{-n-2}\ , \tag{2.2}$$

and is such that the operators $L(n)$ generate a representation of the Virasoro algebra of central charge c. That is, we have

$$[L(m), L(n)] = (m-n)L(m+n) + \frac{1}{12}(m^3 - m)\delta_{m+n,0}c ,$$

$$L(0)v = nv = (\mathrm{wt}\, v)v \quad \text{for} \quad v \in V_n \tag{2.3}$$

for $m, n \in \mathbb{Z}$. We denote the vertex operator algebra just defined by $(V, Y, \mathbf{1}, \omega)$ (or briefly, by V) where $\mathbf{1} \in V_0$ is the vacuum vector.

An *automorphism* of $(V, Y, \mathbf{1}, \omega)$ is an invertible linear transformation g on V which preserves $\mathbf{1}$ and ω and satisfies

$$gY(v, z)g^{-1} = Y(gv, z) . \tag{2.4}$$

If g is an automorphism of V of finite order N, a *g-twisted module* for V is a $\mathbb{Q}$-graded vector space $M = \coprod_{n \in \mathbb{Q}} M_n$ such that $\dim M_n < \infty$ and $M_n = 0$ for n is sufficiently small, and such that there is a linear map

$$V \to (\mathrm{End}\, M)[[z^{1/N}, z^{-1/N}]] ,$$

$$v \mapsto Y_g(v, z) = \sum_{n \in \frac{1}{N}\mathbb{Z}} v_n z^{-n-1} \quad (v_n \in \mathrm{End}\, M) . \tag{2.5}$$

Axioms analogous to those for $(V, Y, \mathbf{1}, \omega)$ are imposed in this situation. We denote this module by (M, Y_g).

If $g = 1$ we call (M, Y_1) a *V-module*. Moreover (M, Y_g) is called *irreducible* in case no nonzero proper subspace of M is invariant by all v_n for $v \in V$ and $n \in \mathbb{Q}$. The VOA V is called *holomorphic* (or self-dual) in case V is the *unique* irreducible V-module (up to isomorphism).

Our main example of a holomorphic VOA is constructed as follows (see [DM]). Let $(\cdot, \cdot)$ be a nondegenerate symmetric bilinear form on $A \simeq \mathbb{C}^{2l}$ $(l \geqq 1)$ with a polarization $A = A^+ \oplus A^-$ into maximal isotropic subspaces. Let $GL(A^+) = GL(l)$ act on A^- via the dual representation (i.e., $g \in GL(A^+)$ acts as $(g^t)^{-1}$ on A^-), and if $g \in GL(A^+)$ has finite order N, set $\eta = e^{2\pi i/N}$ and

$$A^{\pm}_{k,g} = \{a \in A^{\pm} \mid ga = \eta^k a\} , \tag{2.6}$$

$$A_{k,g} = A^+_{k,g} \oplus A^-_{k,g} \tag{2.7}$$

for $k \in \mathbb{Z}$. Next define

$$A(\mathbb{Z}, g)^{\pm} = A^{\pm}_{0,g} + \sum_{n \gtrless 0} A_{n,g} \otimes t^{n/N} , \tag{2.8}$$

$$A\left(\mathbb{Z} + \frac{1}{2}, g\right)^{\pm} = A^{\pm}_{N/2,g} + \sum_{n - 1/2 \gtrless 0} A_{n,g} \otimes t^{n/N - 1/2} \tag{2.9}$$

($A^{\pm}_{N/2,g} = 0$ if N is odd) where t is an indeterminant and $n \in \mathbb{Z}$.

With $Z = \mathbb{Z}$ or $\mathbb{Z} + \frac{1}{2}$, set $A(Z, g) = A^+(Z, g) \oplus A^-(Z, g)$. Then there is a polarization of $A(Z, g)$ with respect to the extension of $(\cdot, \cdot)$ to $A(Z, g)$ given by $(a(m), b(n)) = (a, b)\delta_{m+n,0}$ for $a, b \in A$. Here we have set $a(m) = a_{(m)} \otimes t^m$ if $Z = \mathbb{Z}$, $m \in \frac{1}{N}\mathbb{Z}$, $a_{(m)}$ being the component of a in $A_{g,m}$; and similarly if $Z = \mathbb{Z} + \frac{1}{2}$.

There is an infinite-dimensional Clifford algebra $C(A(Z, g))$ with generators $A(Z, g)$ and relations $a(m)b(n)+b(n)a(m)=(a(m), b(n))$. Thus if $T(\cdot)$ denotes tensor algebra then we have

$$CA(Z, g)=T(A(Z, g))/\{a(m)b(n)+b(n)a(m)-(a(m), b(n))\}\ , \tag{2.10}$$

where $a, b\in A$ and $m, n\in\mathbb{Q}$. Let $C^+(A(Z, g))$ be the subalgebra of $C(A(Z, g))$ generated by $A^+(Z, g)$, and let $\mathbf{1}_{Z,g}$ span a 1-dimensional $C^+(A(Z, g))$-module annihilated by $A^+(Z, g)$ and with 1 acting as the identity. Define

$$CM(Z, g)=C(A(Z, g))\otimes_{C^+(A(Z,g))}\mathbb{C}\mathbf{1}_{Z,g}\ . \tag{2.11}$$

There are linear isomorphisms $CM(Z, g)\simeq\Lambda(A^-(Z, g))$ ($\Lambda(\cdot)$ denotes the exterior algebra), so we obtain four spaces $CM^r(Z, g)$, where $r=0$ or 1 refers to $\Lambda^{\text{even}}(A^-(Z, g))$ or $\Lambda^{\text{odd}}(A^-(Z, g))$ respectively.

Write $CM(Z)$ and $CM^r(Z)$ instead of $CM(Z, g)$ and $CM^r(Z, 1)$ in case $g=1$. Similarly write $\mathbf{1}_Z$ instead of $\mathbf{1}_{Z,1}$. Then G acts on $CM^r(Z)$ naturally such that $g\mathbf{1}_Z=\mathbf{1}_Z$ and $ga(m)g^{-1}=(ga)(m)$ for $g\in G$, $a\in A$ and $m\in\frac{1}{2}\mathbb{Z}$.

From now on, we consider a finite subgroup $G\leqq SO(l, \mathbb{R})$ embedded in the standard way in $GL(A^+)$. Thus $g\in G$ acts on $A=A^+\oplus A^-$ as (g, g).

Theorem 2.1 ([DM]). *Let $V=CM^0(\mathbb{Z}+\frac{1}{2})\oplus CM^0(\mathbb{Z})$. Then there is a linear map Y: $V\to(\mathrm{End}\ V)[[z, z^{-1}]]$ and an element $\omega\in CM^0(\mathbb{Z}+\frac{1}{2})$ such that $(V, Y, \mathbf{1}_{\mathbb{Z}+\frac{1}{2}}, \omega)$ is a* VOA *with central charge l which is holomorphic if $8|l$. Moreover the natural action of G on V identifies G with a group of automorphisms of V.*

Theorem 2.2 ([DM]). *Let the notation be as in Theorem* 2.1 *and let $8|l$. For each $g\in G$ there is $\varepsilon_g=0$ or 1 and a 1-dimensional $C_G(g)$-module N_g such that*

$$V(g)=CM^0\left(\mathbb{Z}+\frac{1}{2}, g\right)\oplus CM^{\varepsilon_g}(\mathbb{Z}, g)\otimes N_g \tag{2.12}$$

satisfies the following: there is a linear map Y_g: $V\to(\mathrm{End}\ V(g))[[z^{1/N}, z^{-1/N}]]$ ($N=$ order of g) such that $(V(g), Y_g)$ is the unique irreducible g-twisted V-module.

Furthermore assume that the space of G-invariants on A^+ is non-zero. Then for $g, h\in G$ there are invertible linear maps $\varphi(h)$: $V(h^{-1}gh)\to V(g)$ which intertwine the corresponding Y-maps, that is

$$\varphi(h)\,Y_{h^{-1}gh}(u, z)\varphi(h)^{-1}=Y_g(hu, z) \tag{2.13}$$

for $v\in V$. If h commutes with g then $\varphi(h)$ coincides with the natural action of h on $V(g)$.

From now on we assume that indeed $G\leqq SO(l, \mathbb{R})$ has non-trivial invariants on A^+, and that $24|l$.

Let $B_2(x)=x^2-x+\frac{1}{6}$ be the second Bernoulli polynomial, and for $g\in G$ of order N let

$$B(g)=\frac{1}{2}\sum_{k=0}^{N-1}B_2(k/N)\dim A^+_{k,g}\ . \tag{2.14}$$

We graded $CM(Z, g)$ as follows: the degree of the "vacuum" $\mathbf{1}_{Z,g}$ is equal to

$$c_{Z,g}=\begin{cases} B(g)+l/24 & \text{if } Z=\mathbb{Z} \\ \frac{1}{2}B(g^2)-B(g)+l/24 & \text{if } Z=\mathbb{Z}+1/2 \end{cases}. \tag{2.15}$$

Then $CM(Z, g)$ is graded using (2.15), (2.11) and the natural grading on $A(Z, g)$ which arises if we set $\deg a(n) = -n$ for $a \in A$ and $n \in \mathbb{Q}$. We may then set

$$CM(Z, g) = \coprod_n CM(Z, g)_n \tag{2.16}$$

to indicate this decomposition into graded subspaces. We emphasize that part of our theory is that $CM(Z, g)_n$ is precisely the eigenspace of $L(0)$ corresponding to the eigenvalue n. We set

$$Z(g, h, \tau) = q^{-l/24} \sum_n \operatorname{tr}(\varphi(h)|_{V(g)_n}) q^n , \tag{2.17}$$

where $V(g)$ inherits its grading form (2.16). Also $h \in G$ commutes with g, $\varphi(h)$ is as in Theorem 2.2, $q = e^{2\pi i \tau}$ and $\tau \in \{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$.

Theorem 2.3. ([M3], [DM]). *If* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *then there is a root of unity* $\sigma(\gamma^{-1}, g, h)$ *such that if* $g, h \in G$ *and* $gh = hg$ *then*

$$Z(g, h, \gamma\tau) = \sigma(\gamma^{-1}, g, h) Z((g, h)\gamma, \tau) . \tag{2.18}$$

The function σ in Theorem 2.3 is a 1-cocycle of $\Gamma = SL_2(\mathbb{Z})$ in the sense that we have the relation

$$\sigma(\gamma_1 \gamma_2, g, h) = \sigma(\gamma_1, (g, h)\gamma_2^{-1}) \sigma(\gamma_2, g, h) \tag{2.19}$$

for $\gamma_1, \gamma_2 \in SL_2(\mathbb{Z})$. Its values are thus determined by those it takes on $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

To explain what these values are, decompose A into a direct sum $X_1 \oplus \cdots \oplus X_l$ of l 2-dimensional $\mathbb{C}\langle g, h\rangle$-modules X_j which are such that $X_j = \mathbb{C} \otimes Y_j$ for an $\mathbb{R}\langle g, h\rangle$-module Y_j satisfying $\langle g, h\rangle \leqq SO(Y_j)$. This is always possible. Then choose 1-dimensional $\langle g, h\rangle$-submodules $U_j \subset X_j$ on which g, h have eigenvalues $e^{2\pi i x_j}, e^{2\pi i y_j}$ respectively, where x_i, y_i are chosen as follows. For $1 \leqq j \leqq l$,

$$\begin{aligned} &0 \leqq x_j \leqq 1/2, \ -1/2 < y_j \leqq 1/2 ; \\ &y_j \geqq 0 \quad \text{if } x_j = 0 \text{ or } 1/2 . \end{aligned} \tag{2.20}$$

Theorem 2.4. ([M3]). *Let* $(x_1, \ldots, x_l), (y_1, \ldots, y_l)$ *be the sequences associated to* g, h *respectively as above. Let* α *be the dimension of the subspace of* A^+ *on which both* g, h *act as* -1, *and let* β *be the dimension of the subspace of* A^+ *on which* g *acts as* -1. *Then*

$$\sigma(S^{-1}, g, h) = (-1)^\alpha \prod_{x_j, y_j < 1/2} e^{-2\pi i x_j y_j} , \tag{2.21}$$

$$\sigma(T^{-1}, g, h) = (-1)^{\beta/2} \prod_{x_j < 1/2} e^{-2\pi i x_j^2} . \tag{2.22}$$

Remark. (i) β is always an even integer.
(ii) $\sigma(S^{-1}, g, h) = \sigma(S^{-1}, h, g)$.
(iii) $\sigma(T^{-1}, g, h)^2 = \sigma(S^{-1}, g, g)^{-1}$.

It would be nice (though this is perhaps unrealistic) if there were a simple closed formula for $\sigma(\gamma^{-1}, g, h)$ for all $\gamma \in SL_2(\mathbb{Z})$.

3. Statement of Results

Throughout the rest of this paper we will take $l=24$ with V as in Theorem 2.1. Thus V is a self-dual VOA of central charge 24. Now let Γ_{24} be the Neimeier lattice of rank 24 whose root system is of type D_{24} (cf. [V]). In [DM] we call this the spin lattice, and it is shown that V is isomorphic (as VOA) to the *bosonic theory* based on Γ_{24}. That is we have the *boson-fermion correspondence* (cf. [F, DM])

$$V \simeq V_{\Gamma_{24}},$$

where $V_{\Gamma_{24}}$ is the self-dual VOA based on Γ_{24} ([B1, FLM]).

We also take $G=M_{24}$ with its usual permutation representation of dimension 24 arising form its action on 24 letters [C]. Then indeed M_{24} fixes a non-zero vector of A^+, so Theorems 2.1–2.4 of Sect. 2 apply.

Theorem A. *With previous assumptions, let g, h be a pair of commuting elements in M_{24} with $Z(g, h, \tau)$ the corresponding partition function* (2.17). *One of the following holds*:

(a) $\langle g, h\rangle$ *has a cyclic Sylow 2-subgroup and $Z(g, h, \tau)$ is a hauptmodul.*
(b) $\langle g, h\rangle$ *has a non-cyclic Sylow 2-subgroup and $Z(g, h, \tau)$ is identically zero.*

We can be more precise concerning part (a). To explain this we introduce some critical invariants associated to an element $g \in M_{24}$ considered as a permutation on 24 letters and decomposed into a product of disjoint cycles:

$$\begin{aligned} &n=n(g)=\text{longest cycle}, \\ &m=m(g)=\text{shortest cycle}, \\ &N_0=N_0(g)=nm, \end{aligned} \tag{3.1}$$

$$h=h(g)=\begin{cases} m, & m \text{ odd} \\ m/2, & m \text{ even} \end{cases}, \tag{3.2}$$

$$N=N(g)=hn.$$

Remark. (i) $n=$ order of g.
(ii) m divides n.
(iii) Either $m=1$ or $m \equiv n \pmod 2$.

Define the discrete subgroup $\Gamma_g \subset SL_2(\mathbb{R})$ as follows:

$$\Gamma_g=\Gamma_0(n|h)+\text{odd}. \tag{3.3}$$

Here we are using a modified version of the notation of Conway–Norton [CN]. Namely,

$$\Gamma_0(n|h)=\begin{pmatrix} h^{-1} & 0 \\ 0 & 1 \end{pmatrix} \Gamma_0(n/h) \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix},$$

where as usual

$$\Gamma_0(l)=\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod l \right\};$$

and the notation "odd" in (3.3) means that we adjoin to $\Gamma_0(n|h)$ all of the Atkin–Lehner involutions W_t for *odd* Hall divisors t of n/h (cf. [CN]).

Theorem B. *$Z(1, g, \tau)$ is an eigenfunction for Γ_g and each $\gamma \in \Gamma_g$ satisfies*

$$Z(1, g, \gamma\tau) = c(\gamma) Z(1, g, \tau)$$

for some h^{th} root of unity $c(\gamma)$.

The kernel of this action is a subgroup Γ_g' of Γ_g of index h. Moreover, Γ_g' has genus zero, $Z(1, g, \tau)$ is a hauptmodul for Γ_g', and Γ_g' is the largest subgroup of $SL_2(\mathbb{R})$ which leaves $Z(1, g, \tau)$ invariant.

Remark. Conway–Norton have conjectured this result [CN] for the Monster.

By results in [M4], there are just two types of non-cyclic abelian groups in M_{24} which are generated by two elements and which have a cyclic 2-Sylow. These groups are denoted (loc cit.) $\mathbb{Z}_3 \times \mathbb{Z}_3 A$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 B$, having the indicated isomorphism type. We can take generators (g, h) so that in each case g has cycle decomposition $1^6 3^6$, while h is of type $1^6 3^6$ or 3^8 respectively.

Theorem C. *Let g, h generate $\mathbb{Z}_3 \times \mathbb{Z}_3 A$ or $\mathbb{Z}_3 \times \mathbb{Z}_3 B$ as above, and let $Z'(g, h, \tau) = Z(g, h, 3\tau)$. Set*

$$\Gamma_{g,h} = \Gamma_0(N(h)|3) + \ .$$

Then $Z'(g, h, \tau)$ is an eigenfunction for $\Gamma_{g,h}$ and each $\gamma \in \Gamma_{g,h}$ satisfies

$$Z'(g, h, \gamma\tau) = c(\gamma) Z'(g, h, \tau)$$

for some cube root of unity $c(\gamma)$.

The kernel of this action is a subgroup $\Gamma_{g,h}'$ of $\Gamma_{g,h}$ of index 3. Moreover $\Gamma_{g,h}'$ has genus zero, $Z(1, g, \tau)$ is a hauptmodul for $\Gamma_{g,h}'$, and $\Gamma_{g,h}'$ is the largest subgroup of $SL_2(\mathbb{R})$ which leaves $Z'(g, h, \tau)$ invariant.

Next we list the explicit q-expansions and other pertinent data.

Column 1 lists pairs (g, h) of commuting elements, giving the cycle decomposition of each element. The second column lists the "balancing number" N_0 defined via

$$N_0 = N_0(g) N_0(h) \ , \tag{3.5}$$

where $N_0(g)$ is as in (3.1). Column 3 is the group Γ_g or $\Gamma_{g,h}$ (as defined in Theorems B and C). Column 4 gives the name of the Monster class with the same group. Column 5 gives a formula for $Z(1, h, \tau)$. If h has odd order this always has the form

$$Z(1, h, \tau) = \Theta_h(\tau)/\eta_h(\tau) \ , \tag{3.6}$$

where in (3.6) $\Theta_h(\tau)$ denotes the theta-function of the sublattice of Γ_{24} fixed by $h \in M_{24}$ under the natural action of M_{24} on Γ_{24}. Also, $\eta_h(\tau)$ is as in [CN], namely, if h has cycle decomposition $1^{e_1} 2^{e_2} \ldots$, then

$$\eta_h(\tau) = \eta(\tau)^{e_1} \eta(2\tau)^{e_2} \ldots , \tag{3.7}$$

and η is the Dedekind eta-function. If h has even order the formula always takes the form (const) + "Frame shape," where by Frame shape we mean the eta-product corresponding to the indicated partition. For example if $h = 1^8 2^8$ then Table (3.4), line 2 tells us that $Z(1, h, \tau)$ is equal to 2^7 plus the eta-product $\eta(\tau)^{24}/\eta(2\tau)^{24}$. Finally, we give the explicit constant term for each $Z(1, h, \tau)$ since, unlike the Monster case, they are in general non-zero.

Table (3.4)

Pair (g, h)	N_0	*Group*	*M elt.*	*Formula*	*Const. term*
$(1, 1^{24})$	1	$\Gamma_0(1)$	$1A$	Θ_h/η_h	$\binom{48}{2}$
$(1, 1^8 2^8)$	2	$\Gamma_0(2)-$	$2B$	$(2^7)+1^{24}/2^{24}$	104
$(1, 2^{12})$	4	$\Gamma_0(2)-$	$2B$	$1^{24}/2^{24}$	-24
$(1, 1^6 3^6)$	3	$\Gamma_0(3)+$	$3A$	Θ_h/η_h	$\binom{12}{2}$
$(1, 3^8)$	9	$\Gamma_0(3\|3)$	$3C$	Θ_h/η_h	0
$(1, 2^4 4^4)$	8	$\Gamma_0(4)-$	$4C$	$1^8/4^8$	-8
$(1, 1^4 2^2 4^4)$	4	$\Gamma_0(4)-$	$4C$	$(2^5)+1^8/4^8$	24
$(1, 4^6)$	16	$\Gamma_0(4\|2)-$	$4D$	$2^{12}/4^{12}$	0
$(1, 1^4 5^4)$	5	$\Gamma_0(5)+$	$5A$	Θ_h/η_h	$\binom{8}{2}$
$(1, 1^2 2^2 3^2 6^2)$	6	$\Gamma_0(6)+3$	$6C$	$(2^3)+1^6 3^6/2^6 6^6$	2
$(1, 6^4)$	36	$\Gamma_0(6\|3)$	$6F$	$3^8/6^8$	0
$(1, 1^3 7^3)$	7	$\Gamma_0(7)+$	$7A$	Θ_h/η_h	$\binom{6}{2}$
$(1, 1^2 \cdot 2 \cdot 4 \cdot 8^2)$	8	$\Gamma_0(8)-$	$8E$	$(2^3)+1^4 4^2/2^2 8^4$	4
$(1, 2^2 10^2)$	20	$\Gamma_0(10)+5$	$10B$	$1^4 5^4/2^4 10^4$	-4
$(1, 1^2 11^2)$	11	$\Gamma_0(11)+$	$11A$	Θ_h/η_h	$\binom{4}{2}$
$(1, 2 \cdot 4 \cdot 6 \cdot 12)$	24	$\Gamma_0(12)+3$	$12E$	$1^2 3^2/4^2 12^2$	-2
$(1, 12^2)$	144	$\Gamma_0(12\|6)$	$12J$	$6^4/12^4$	0
$(1, 1 \cdot 2 \cdot 7 \cdot 14)$	14	$\Gamma_0(14)+7$	$14B$	$(2)+1^3 7^3/2^3 14^3$	-1
$(1, 1 \cdot 3 \cdot 5 \cdot 15)$	15	$\Gamma_0(15)+$	$15A$	Θ_h/η_h	$\binom{2}{2}$
$(1, 3 \cdot 21)$	63	$\Gamma_0(21\|3)+$	$21C$	Θ_h/η_h	0
$(1, 1 \cdot 23)$	23	$\Gamma_0(23)+$	$23A$	Θ_h/η_h	$\binom{2}{2}$
$(1^6 3^6, 1^6 3^6)$	9	$\Gamma_0(3\|3)$	$3C$		
$(1^4 3^6, 3^8)$	27	$\Gamma_0(9\|3)+$	*ghost*		

4. Preliminaries

First recall that the elements of M_{24} are "balanced." More precisely, the integer $N_0 = N(g)$ defined for $g \in M_{24}$ by (3.1) can also be characterized as follows: if g has cycle decomposition $r_1^{e_1} r_2^{e_2} \ldots r_t^{e_t}$ with $1 \leqq r_1 < r_2 < \cdots < r_t$ and $e_i > 0$, then each r_i divides N_0 and $\left(\frac{N_0}{r_t}\right)^{e_t} \left(\frac{N_0}{r_{t-1}}\right)^{e_{t-1}} \cdots \left(\frac{N_0}{r_1}\right)^{e_1}$ is again the cycle decomposition of g. See [K] for the relation of this to the theory of the eta-product $\eta_g(\tau)$ (3.7).

Lemma 4.1. *Let $c_{Z,g}$ be as in* (2.15). *Then*

$$c_{z,g}=\begin{cases} 1+\dfrac{2}{N_0(g)}, & Z=\mathbb{Z} \\ 1-\dfrac{1}{N_0(g)}, & Z=\mathbb{Z}+\frac{1}{2},\ n(g)\ \text{odd} \\ 1+\dfrac{2}{N_0(g)}, & Z=\mathbb{Z}+\frac{1}{2},\ n(g)\ \text{even},\ m(g)>1 \\ 1, & Z=\mathbb{Z}+\frac{1}{2},\ n(g)\ \text{even},\ m(g)=1 \end{cases}.$$

Proof. Let $B(g)$ be as in (2.14). We claim that

$$B(g)=\frac{2}{N_0(g)}. \tag{4.1}$$

The "contribution" to $B(g)$ made by a single cycle of length s is equal to

$$\frac{1}{2}\sum_{t=0}^{s-1}\left(\frac{t^2}{s^2}-\frac{t}{s}+\frac{1}{6}\right)=\frac{1}{12s}.$$

So if g has cycle decomposition $r_1^{e_1}r_2^{e_2}\ldots r_t^{e_t}$ then

$$B(g)=\frac{1}{12}\sum_{i=1}^{t}\frac{e_i}{r_i}=\frac{1}{12N_0(g)}\sum_{i=1}^{t}e_ir_i=\frac{2}{N_0(g)}$$

as $\sum_{i=1}^{t}e_ir_i=24$. So (4.1) holds.

As $l=24$, we are done by (2.15) if $Z=\mathbb{Z}$. We also have

$$N_0(g)=\begin{cases} N_0(g^2), & n(g)\ \text{odd} \\ 4N_0(g^2), & n(g)\ \text{even},\ m(g)>1 \\ 2N_0(g^2), & n(g)\ \text{even},\ m(g)=1 \end{cases}. \tag{4.2}$$

Now if $Z=\mathbb{Z}+\frac{1}{2}$ we are done by (4.2) and (2.15). The lemma is proved. □

There is an important consequence of Lemma 4.1 for the partition functions $Z(g, h, \tau)$, namely

Lemma 4.2. (i) *If $n(g)$ is odd then $Z(g,h,\tau)=q^{\frac{-1}{N_0(g)}}+$ higher powers.*
(ii) *If $n(g)$ is even then $Z(g,h,\tau)$ is holomorphic at ∞.*

Proof. This follows from Lemma 4.1, (2.17) and the accompanying discussion of the grading of $CM(Z, g)$. □

Lemma 4.3. *We have*

$$Z(1,g,\tau)=T_2\eta_g(\tau)^2/\eta_g(\tau)^2,$$

where T_2 is the Hecke operator corresponding to 2.

Proof. This is a basic result of [M3] – see in particular (7.13) of that paper and the attendant discussion. □

Corollary 4.4. *All poles of $Z(1, g, \tau)$ are at the cusps.*

Proof. This is because $\eta_g(\tau)$ does not vanish in the upper half-plane. □

Corollary 4.5. *$Z(1, g, \tau)$ is a modular function on $\Gamma_0(N(g))$.*

Proof. It is well-known [K] that if $\pi = r_1^{e_1} r_2^{e_2} \ldots r_t^{e_t}$ is a partition of some multiple of 24 then the corresponding eta-product is a modular form of level l, where l satisfies $r_i | l$ for $i = 1, \ldots, t$, and also $l \sum_{i=1}^{t} \frac{e_i}{r_i} \equiv 0 \pmod{24}$. Thus if $g \in M_{24}$ then $\eta_g(\tau)$ is certainly a form on $\Gamma_0(N_0(g))$ by balance. Moreover if $m(g)$ is even then $\eta_g(\tau)^2$ is a form on $\Gamma_0(N_0(g)/2)$. Now the lemma follows from Lemma 4.3 together with Definitions (3.1) and (3.2). □

Now it is well-known [O] that the cusps of $\Gamma_0(N(g))$ may be taken to be rationals of the form $\frac{a}{c}$, where $c | N(g)$ and $(a, c) = 1$. We call the cusp $\frac{a}{c}$ *odd* in case c is divisible by the 2-part of $n(g)$, and otherwise $\frac{a}{c}$ is called an *even cusp* of $\Gamma_0(N(g))$.

Lemma 4.6. *$Z(1, g, \tau)$ is holomorphic at all even cusps.*

Proof. Let $\frac{a}{c}$ be an even cusp, and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lie in $SL_2(\mathbb{Z})$. By (2.18) we have

$$Z(1, g, \gamma\tau) = \sigma(\gamma^{-1}, 1, g) Z(g^c, g^d, \tau) . \tag{4.3}$$

Now g^c has even order by construction, so according to Lemma 4.2 (ii), $Z(g^c, g^d, \tau)$ is holomorphic at ∞. As γ: $\infty \mapsto \frac{a}{c}$, then $Z(1, g, \tau)$ is holomorphic at $\frac{a}{c}$ as required. □

Lemma 4.7. *The poles of $Z(1, g, \tau)$ are precisely at the odd cusps of $\Gamma_0(N(g))$.*

Proof. All poles are cuspidal by Corollary 4.4, hence are among the odd cusps by Lemma 4.6. But if $\frac{a}{c}$ is an odd cusp then from (4.3) and Lemma 4.2 (i) we see that $Z(1, g, \tau)$ indeed has a pole at $\frac{a}{c}$ since $\sigma(\gamma^{-1}, 1, g)$ never vanishes. □

Lemma 4.8. *Let g, h be commuting elements of M_{24}.*

(i) *Suppose that $\langle g, h \rangle$ has a non-cyclic Sylow 2-subgroup. Then in the 24-dimensional permutation representation of M_{24} there are 1-dimensional $\langle g, h \rangle$-invariant subspaces U_1, U_2, U_3, U_4 such that g acts as 1 on U_1, U_2, and as -1 on U_3, U_4 whereas h acts as 1 on U_2, U_3, and as -1 on U_1, U_4.*

(ii) *Suppose that g has odd order and h has even order. Then there are subspaces U_5, U_6 such that g is 1 on U_5, U_6, h is 1 on U_5, -1 on U_6.*

Proof. Straightforward. □

Lemma 4.9. *Let $g, h \in M_{24}$ be as in either* (i) *or* (ii) *of Lemma* 4.8. *Then for $r = 0$ or 1, the graded trace of h on $CM^r(\mathbb{Z}, g)$ is identically zero.*

Proof. As discussed following (2.11), there are isomorphisms of graded $\langle h\rangle$-modules $CM^r(\mathbb{Z}, g)\simeq\Lambda(A(\mathbb{Z}, g)^-)$. Moreover from (2.8) we get

$$\Lambda(A(\mathbb{Z}, g)^-)\simeq\Lambda(A_{0,g}^-)\otimes\Lambda\left(\sum_{l<0}A_{l,g}\otimes t^{l/n(g)}\right),$$

where $A_{0,g}^-$ is the subspace of A^- fixed by g.

Now h acts on A^-, and by Lemma 4.8 there are eigenvectors for h in A^- corresponding to the eigenvalues 1 and -1. The existence of the eigenvalue 1 means that $\Lambda^0(A(\mathbb{Z}, g)^-)\simeq\Lambda^1(A(\mathbb{Z}, g)^-)$ as $\langle h\rangle$-modules (cf. [DM], (7.5)), whereas the -1 eigenvalue forces the trace of h on $\Lambda(A_{0,g}^-)$ (and hence on $\Lambda(A(\mathbb{Z}, g)^-)$ to be zero (cf. [M3], Lemma 2.3)). The lemma follows. □

Lemma 4.10. *Let $g, h\in M_{24}$ be as in* (i) *of Lemma* 4.8. *Then the graded trace of h on $CM^0(\mathbb{Z}+\frac{1}{2}, g)$ is identically zero.*

Proof. The proof is essentially that of the previous lemma. We just use (2.9), the action of h on $A_{n(g)/2,g}^-$, and Lemma 4.8 (i). □

We next consider the 1-cocycle σ. Recall the generators $S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ of $SL_2(\mathbb{Z})$.

Lemma 4.11. (i) $\sigma(T^{-1}, g, h)$ *is independent of h.*

(ii) $\sigma(T^{-r}, g, h)=\sigma(T^{-1}, g, h)^r$.

(iii) $$\sigma(T^{-1}, g, 1)=\begin{cases}e^{-2\pi i/N_0(g)}, & n(g)\text{ odd}\\ 1, & n(g)\text{ even, } m(g)=1\\ e^{4\pi i/N_0(g)}, & n(g)\text{ even, } m(g)>1\end{cases}.$$

Proof. (i) follows from (2.22) and (ii) is a consequence of the 1-cocycle property (2.19). Finally, (iii) can be computed from (2.22), but it is quicker to use identity (2.18) together with Lemmas 4.1 and 4.2. We leave the easy details to the reader. □

Lemma 4.12. *Let $x\in M_{24}$ either have odd order; or have even order which is not a power of 2 and satisfies $m(x)=1$. Then if $\langle g, h\rangle=\langle x\rangle$ and $\gamma\in SL_2(\mathbb{Z})$ then $\sigma(\gamma^{-1}, g, h)$ is a root of unity of odd order.*

Proof. Because of the cocycle property, it is enough to prove the lemma for $\gamma=S$ or T.

If $\gamma=T$ then the result follows from Lemma 4.11 (iii) since if $m(x)=1$ then $m(g)=1$ too.

So assume that $\gamma=S$. If x has odd order then the result is clear from (2.21). Otherwise x is one of the elements $1^2\cdot 2^2\cdot 3^3\cdot 6^2$ or $1\cdot 2\cdot 7\cdot 14$ in M_{24}, in particular $n(x)$ is square-free. In each case the integer α which intervenes in (2.21) is even, and we see from that formula that if $\sigma(S^{-1}, g, h)$ is *not* an odd root of unity then $\langle g\rangle=\langle h\rangle=\langle x\rangle$ (recall that each of the pairs (x_j, y_j) in (2.21) occur an *even* number of times). So we may take $g=x$, $h=x^b$ for some b coprime to $n(g)$. Now the result is an easy calculation using (2.21). □

Of course we can in principle calculate $\sigma(\gamma^{-1}, g, h)$ for all $\gamma \in SL_2(\mathbb{Z})$, $g, h \in M_{24}$ using (2.21) and (2.22). Though we wish in general to avoid explicit calculations, we illustrate with an example that we use later.

Lemma 4.13. *Let* $\gamma = \begin{pmatrix} -1 & -1 \\ 4 & 3 \end{pmatrix}$ *and* $g = 2 \cdot 4 \cdot 6 \cdot 12$. *Then* $\sigma(\gamma^{-1}, 1, g) = 1$.

Proof. We have $\gamma = ST^4ST$, so the cocycle property (2.19) yields

$$\sigma(\gamma^{-1}, 1, g) = \sigma(T^{-1}S^{-1}T^{-4}, g, 1)\sigma(S^{-1}, 1, g)$$
$$= \sigma(T^{-1}, g^4, g^{-1})\sigma(S^{-1}, g, g^4)\sigma(T^{-4}, g, 1)\sigma(S^{-1}, 1, g) .$$

The last term is 1 by (2.21), and a calculation similarly yields $\sigma(S^{-1}, g, g^4) = 1$. On the other hand Lemma 4.11 yields $\sigma(T^{-1}, g^4, g^{-1}) = e^{-2\pi i/3}$ and also $\sigma(T^{-4}, g, 1) = e^{16\pi i/24}$. The lemma follows. □

The partition functions satisfy a crucial symmetry property:

Proposition 4.14. *Let g and h commute and have coprime orders, and assume that g has odd order. Then*

$$Z(g, h, N_0(g)\tau) = Z(1, gh, \tau) .$$

Proof. Bearing in mind the definition (2.17) of $Z(g, h, \tau)$, let us first concentrate on the first summand of $V(g)$ in (2.12), more precisely we consider the space $CM(\mathbb{Z}+\frac{1}{2}, g)$. Since g has odd order, the discussion in Sect. 2 shows that as q-graded $C_{M_{24}}(g)$-module we have

$$CM\left(\mathbb{Z}+\frac{1}{2}, g, \tau\right) = CM\left(\mathbb{Z}+\frac{1}{2}, g\right) \simeq q^{-1/N_0(g)} \Lambda\left(\sum A_{l,g} \otimes q^{l/n-1/2}\right) ,$$

where l runs over all integers satisfying $l/n > 1/2$, and we have also set $n = n(g)$.

It follows from this (cf. [M4]) that the graded trace of h on $CM(\mathbb{Z}+\frac{1}{2}, g, N_0(g)\tau)$ is equal to

$$q^{-1} \prod_{l \in \mathbb{Z}, l \geqq 0} \prod_{k} \prod_{j=1}^{k} (1 + e^{2\pi i\alpha} q^{(l+j/k-1/2)N_0(g)}) , \tag{4.4}$$

where k runs over the cycles of g in its cycle decomposition on 24 letters, and where $e^{2\pi i\alpha}$ is a typical eigenvalue of h on the corresponding g-eigenspace.

As h has order coprime to the order of g then each g-eigenspace is a rational $\langle h \rangle$-module, so h has a Frame shape $1^{f_1}2^{f_2} \ldots$, $f_i \in \mathbb{Z}$ on each g-eigenspace. Then the "contribution" of a cycle of length s from this Frame shape to (4.4) is given by (assuming that s is odd for a moment):

$$1 + q^{s(l+j/k-1/2)N_0(g)} .$$

(If s is even the plus sign becomes minus.) So we see that (4.4) is equal to (taking h of odd order for now):

$$q^{-1} \prod_{l \geqq 0} \prod (1 + q^{s(l+j/k-1/2)N_0(g)}) ,$$

where the second product ranges over the various choices for k, j, s corresponding to the 24-dimensional representation of M_{24}. Now

$$s(l+j/k-1/2)N_0(g)=\frac{sN_0(g)}{k}(kl+j-k/2)\,.$$

By balance, $N_0(g)/k$ ranges over the cycle lengths of g as k does, so $sN_0(g)k$ ranges over the cycle lengths of gh. And for fixed k, $kl+j-k/2$ ranges over $r-1/2>0, r\in\mathbb{Z}$. The upshot is that the graded trace of h on $CM(\mathbb{Z}+\frac{1}{2}, g, N_0(g)\tau)$ is equal to

$$q^{-1}\prod_{r\geqq 0}\prod_{t}(1+q^{t(r-1/2)})\,,$$

where t ranges over the cycles of gh. But this is precisely the trace of gh on $CM(\mathbb{Z}+\frac{1}{2}, 1, \tau)$. If h has even order the same argument applies as long as certain plus signs are replaced by minus as explained above.

It remains to treat second summand of $V(g)$ in (2.12), and as before we consider the full exterior algebra $CM(\mathbb{Z}, g)\otimes N_g$, where N_g is a1-dimensional representation of $C_{M_{24}}(g)$ as discussed in [DM] and [M3, Sect. 8] (where it is denoted by $\chi(g,\cdot)$).

There are two cases to deal with. First, if h has even order then, since g has odd order, Lemma 4.9 shows that h has trace 0 on $CM^r(\mathbb{Z}, g)$ for $r=0, 1$, and similarly gh has trace 0 on $CM^r(\mathbb{Z}, 1)$. So in this case the proposition is proved.

If h has odd order then one computes from the description of N_g (loc cit.) that $N_g(h)=1$. The argument in the first part of the proof then shows that the graded trace of h on $CM(\mathbb{Z}, g, N_0(g)\tau)\otimes N_g$ is equal to that of gh on $CM(\mathbb{Z}, 1, \tau)$. Since the trace of h on $CM^r(\mathbb{Z}, g, \tau)$ is independent of $r=0, 1$, the proposition now follows in its entirety. □

5. The Case $h(g)=1$

We deal in this section with the proof of Theorem B in case $h(g)=1$, and also show how Theorem A reduces to proving Theorems B and C.

Lemma 5.1. *Part* (b) *of Theorem A holds.*

Proof. Take g, h commuting elements of M_{24} with $\langle g, h\rangle$ having non-cyclic Sylow 2-subgroup. Comparing Lemmas 4.9 and 4.10 with (2.12) and (2.17), the result follows immediately. □

Now suppose that $\langle g, h\rangle$ has a cyclic Sylow 2-subgroup. By [M4] either $\langle g, h\rangle$ is of type $\mathbb{Z}_3\times\mathbb{Z}_3 A$ or $\mathbb{Z}_3\times\mathbb{Z}_3 B$ and we are in the situation of Theorem C, or else $\langle g, h\rangle=\langle x\rangle$ is itself cyclic.

In this latter situation, let Δ be the largest subgroup of $SL_2(\mathbb{R})$ which leaves $Z(1, x, \tau)$ invariant. We can find $\gamma\in SL_2(\mathbb{Z})$ such that $(g, h)\gamma=(1, x)$, in which case $\gamma\Delta\gamma^{-1}$ is the largest subgroup of $SL_2(\mathbb{R})$ which leaves $Z(g, h, \tau)$ invariant – as one sees easily from (2.18). The upshot is that Theorem A is a consequence of Theorems B and C.

For the rest of this section, then, we will fix $g\in M_{24}$ such that $h(g)=1$ (cf. (3.2)). We then let $n=n(g)$, $N_0=N_0(g)$, etc. In order to prove Theorem B in this case we must establish.

Theorem 5.2. *$\Gamma_g=\Gamma_0(n)+$odd is the largest subgroup of $SL_2(\mathbb{R})$ which leaves $Z(1, g, \tau)$ invariant. Moreover, Γ_g has genus zero and $Z(1, g, \tau)$ is a hauptmodul for Γ_g.*

Lemma 5.3. *Theorem* 5.2 *holds if n is a power of* 2.

Proof. Because $h(g)=1$ then $N=n$, so as n is a power of 2 then $\Gamma_0(n)$ has only one odd cusp (which is equivalent to ∞). By Lemma 4.2 (i) and Lemma 4.7, $Z(1, g, \tau)$ has a pole of order 1 at ∞ and no other poles in a fundamental domain for $\Gamma_0(n)$. Since $Z(1, g, \tau)$ is a function on $\Gamma_0(n)$ (Corollary 4.5) then $\Gamma_0(n)$ must have genus zero and $Z(1, g, \tau)$ is a hauptmodul for $\Gamma_0(n)$.

Finally, we must show that $\Gamma_0(n)$ is the largest subgroup of $SL_2(\mathbb{R})$ leaving $Z(1, g, \tau)$ invariant. If β leaves $Z(1, g, \tau)$ invariant then from the above argument we see that β fixes the cusp ∞ of $\Gamma_0(n)$, so $\beta=\delta\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}$ for some $r\in\mathbb{R}$ and $\delta\in\Gamma_0(n)$. So we may take $\beta=\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}$. As $Z(1, g,\tau)=q^{-1}+\cdots$ then we must have $r\in\mathbb{Z}$, so $\beta\in\Gamma_0(n)$ as required. □

We refer the reader to [CN] for information concerning the Atkin–Lehner involutions W_e of $\Gamma_0(N)$. We call W_e an *odd* Atkin–Lehner involution of $\Gamma_0(N)$ in case e is odd.

Lemma 5.4. *The group generated by the odd Atkin–Lehner involutions of* $\Gamma_0(N)$ *is transitive on the odd cusps of* $\Gamma_0(N)$.

Proof. Let a/c be an odd cusp of $\Gamma_0(N)$. So $c|N$ and N/c is odd, moreover $(a, c)=1$. Let $e=N/c$.

Now g has order N, so g^c has odd order e and by a property of M_{24}, g^c has square-free order. Thus $(ae, c)=1$ and we can find integers u, v such that $aue-vc=1$.

Set

$$W_e=\begin{pmatrix}ae & v\\ N & ue\end{pmatrix}=\begin{pmatrix}a & v\\ c & ue\end{pmatrix}\begin{pmatrix}e & 0\\ 0 & 1\end{pmatrix} \tag{5.1}$$

which has determinant e. Indeed W_e is an odd Atkin–Lehner involution. As W_e: $\infty\mapsto ae/N=a/c$, the lemma follows. □

Proposition 5.5. $Z(1, g, W_e\tau)=Z(1, g, \tau)$ *for each add Atkin–Lehner involution* W_e *of* $\Gamma_0(N)$.

This being the case, it follows from Lemmas 4.7 and 5.4 that $Z(1, g, \tau)$ is a function on $\Gamma_0(N)+\text{odd}$ with a simple pole at ∞ and no other poles in a fundamental domain for $\Gamma_0(N)+\text{odd}$. Then Theorem 5.2 follows as in the proof of Lemma 5.3.

So to prove Theorem 5.2, it is enough to establish Proposition 5.5. To this end, let $\gamma=\begin{pmatrix}a & v\\ c & ue\end{pmatrix}\in SL_2(\mathbb{Z})$ be as in (5.1). By (2.18) we get

$$Z(1, g, W_e\tau)=\sigma(\gamma^{-1}, 1, g)Z(g^c, g^{ue}, e\tau)\,. \tag{5.2}$$

Now g^c has odd order e while g^{ue} has order c. Furthermore $N_0(g^c)=n(g^c)=e$, so we may apply Proposition 4.14 to conclude that $Z(g^c, g^{ue}, e\tau)=Z(1, g, \tau)$. As a consequence, to complete the proof of the proposition we see from (5.2) that we must establish

Lemma 5.6. *With previous notation, we have*

$$\sigma(\gamma^{-1}, 1, g)=1\,.$$

Proof. We have already established that

$$Z(1, g, W_e\tau)=\sigma(\gamma^{-1}, 1, g)Z(1, g, \tau)\,,$$

so as W_e acts as involution then certainly $\sigma(\gamma^{-1}, 1, g)=\pm 1$.

Suppose first that g has odd order, or else even order which is not a power of 2 and such that $m(g)=1$. Then Lemma 4.12 tells us that $\sigma(\gamma^{-1}, 1, g)$ is a root of unity of odd order. So it must be 1 in this case, as required.

After Lemma 5.3 we may assume that $m(g)=2$ and $n(g)$ is even but not a power of 2. The only possibilities are $g=2^210^2$ or $2\cdot 4\cdot 6\cdot 12$. In the second case we may take $\gamma=\begin{pmatrix}-1 & -1\\ 4 & 3\end{pmatrix}$, in which case the present lemma follows from Lemma 4.13. In case $g=2^210^2$ then we may take $\gamma=\begin{pmatrix}1 & 2\\ 2 & 5\end{pmatrix}$, and we invite the reader to again verify the lemma for themselves as in the proof of Lemma 4.13. (To this end, note that $\gamma=TST^2ST^3$.) □

This complete the proof of Theorem 5.2.

6. The Case $h(g)>1$

In this section we complete the proof of Theorem B. Throughout we fix $g\in M_{24}$ such that $h=h(g)>1$, and let $N_0=N_0(g)$, $n=n(g)$, etc. Note that as $h(g)$ divides 24 then if h is odd it must be equal to 3.

We shall give a precise formulation for the action of Γ_g on $Z(1, g, \tau)$:

Theorem 6.1. *There is a group homomorphism*

$$c\colon \Gamma_g=\Gamma_0(n|h)+\text{odd}\to\{h^{\text{th}}\text{ roots of unity}\}$$

defined by $Z(1, g, \gamma\tau)=c(\gamma)Z(1, g, \tau)$. *Moreover*

$$c\left(\begin{pmatrix}1 & 1/h\\ 0 & 1\end{pmatrix}\right)=e^{-2\pi i/h}\,, \tag{6.1}$$

$$c\left(\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}\right)=\begin{cases}e^{-2\pi i/h}, & n\text{ odd}\\ e^{2\pi i/h}, & n\text{ even}\end{cases}\,, \tag{6.2}$$

$$c(w)=1,\quad \text{for all odd Atkin–Lehner involutions } w \text{ of } \Gamma_0(n|h). \tag{6.3}$$

Remarks. (i) According to [CN] the elements $\begin{pmatrix}1 & 1/h\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}$ generate $\Gamma_0(n|h)/\Gamma_0(N)$, and the homomorphism c is determined completely by (6.1)–(6.3).

(ii) Conway–Norton have conjectured exactly this result for Monster elements [CN, Sect. 5]. (But note: the signs $\pm$ in (6.2) are the opposite of those proposed in [CN].)

(iii) Theorem 6.1 in case $h=1$ was established in Sect. 5.

We proceed in a sequence of lemmas.

Lemma 6.2. *Equation* (6.2) *holds.*

Proof. $\gamma=\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}\in\Gamma_0(n)$, so (2.18) yields

$$Z(1, g, \gamma\tau)=\sigma(\gamma^{-1}, 1, g)Z(1, g, \tau)\,,$$

so we must compute $\sigma(\gamma^{-1}, 1, g)$ $(=c(\gamma)$ in the notation of Theorem 6.1).

Now $\gamma=ST^{-n}S$, so using Theorem 2.4 and the cocycle property we find that

$$c(\gamma)=\sigma(S^{-1}, g, 1)\sigma(T, g, 1)^n\,.$$

Again $\sigma(S, g, 1)=1$ by Theorem 2.4, while Lemma 4.11 (iii) shows that

$$\sigma(T, g, 1)^n=\begin{cases} e^{2\pi in/N_0}, & n \text{ odd}\\ e^{-4\pi in/N_0}, & n \text{ even}\end{cases}.$$

Now (6.2) follows from this and (3.2). □

Lemma 6.3. *Equation* (6.1) *holds.*

Proof. In this case, if $\gamma=\begin{pmatrix}1 & 1/h\\ 0 & 1\end{pmatrix}$ then $Z(1, g, \gamma\tau)=Z(1, g, \tau+1/h)$. To evaluate this we use the nature of $Z(1, g, \tau)$.

If g has cycle decomposition $r_1^{e_1}r_2^{e_2}\ldots$, then $m=m(g)$ divides each r_i, so the eta-product $\eta_g(\tau)^2$ takes the form

$$\eta_g(\tau)^2=q^2\sum_{l=0}^{\infty}a_lq^{ml}\,. \tag{6.4}$$

Case 1: m odd. In this case we have $h=m=3$ and n is odd. So $\eta_g(\tau)^2$ has odd level and some weight k (as a modular form), so that

$$T_2\eta_g(\tau)^2=q\sum_{l=0}^{\infty}a_{2l}q^{ml}+2^{k-1}q^4\sum_{l=0}^{\infty}a_lq^{2ml}\,. \tag{6.5}$$

Because $h=3$ we see that replacing τ by $\tau+1/h$ merely multiplies expression (6.5) by $e^{2\pi i/h}$, whereas the same operation multiplies (6.4) by $e^{4\pi i/h}$. Now (6.1) holds in this case by Lemma 4.3.

Case 2: m even. In this case $m=2h$ by (3.2) and $\eta_g(\tau)^2$ has even level. So now

$$T_2\eta_g(\tau)^2=q\sum_{l=0}^{\infty}a_lq^{hl}\,,$$

as we see from (6.4), and the result follows as before. □

It remains to deal with the odd Atkin–Lehner involutions of $\Gamma_0(n|h)$. In our situation, there is only one class of elements in M_{24} for which n/h has an odd divisor greater than 1, namely $g=3\cdot 21$, where $n=21$, $h=3$.

In this case the only non-trivial Atkin–Lehner involution is

$$W_7=\begin{pmatrix}1/3 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 7 & 0\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & 1\end{pmatrix}=S\begin{pmatrix}21 & 0\\ 0 & 1/3\end{pmatrix}.$$

Now (2.18) yields

$$Z(1, g, W_7\tau)=\sigma(S^{-1}, 1, g)Z(g, 1, 63\tau)\,.$$

But $\sigma(S^{-1}, 1, g)=1$ by Theorem 2.4, and since $N_0(g)=63$ then $Z(g, 1, 63\tau)=Z(1, g, \tau)$ by Proposition 4.14. This completes the proof of Theorem 6.1.

Lemma 6.4. *Let Γ_g' be the kernel of the homomorphism c of Theorem* 6.1. *Then Γ_g' acts transitively on the odd cusps of $\Gamma_0(N)$.*

Proof. Certainly Γ_g' acts on the odd cusps of $\Gamma_0(N)$ by Lemma 4.7, while the stabilizer of the cusp ∞ is generated by $\begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}$. After Theorem 6.1, in particular (6.1), it is enough to show that $|\Gamma_g'\colon \Gamma_0(N)|$ is equal to the number of odd cusps.

Now the order $|\Lambda\colon \Gamma_0(N)|$ of the full normalizer $\Lambda=\Gamma_0(n|h)+$ of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ (modulo $\Gamma_0(N)$) is well-known (cf. [O]). It is equal to $2^r h^2 s$, where r is the number of distinct prime factors of N, and (in our case) $s=2/3$ if $3|h$ and is otherwise 1. Let us note at this point that g is one of the possibilities: 3^8, 6^4, 12^2, 4^6, $3\cdot 21$.

Now if N is odd then $\Gamma_g=\Gamma_0(n|h)+$, whereas if N is even then in each case $n/h=2$ and then $|\Lambda:\Gamma_g|=2$. So we get

$$|\Gamma_g'\colon \Gamma_0(N)|=\begin{cases} 2^{r+1}, & n \text{ odd, } (h=3) \\ 2^r h/3, & n \text{ even, } 3|h \\ 2^{r-1}h, & n \text{ even, } 3\nmid h. \end{cases}$$

Explicitly, we have the table

g	3^8	6^4	12^2	4^6	$3\cdot 12$
$\lvert\Gamma_g'\colon \Gamma_0(N)\rvert$	4	4	8	2	8

On the other hand the number of cusps of $\Gamma_0(N)$ is just $\sum_{c|N}\phi((c, N/c))$, and we calculate that in each case we have number of odd cusps $=\frac{1}{2}\sum_{c|N}\phi((c, N/c))$, and that this coincides with the index $|\Gamma_g'\colon \Gamma_0(N)|$. The lemma follows. □

Theorem B is an immediate consequence of Theorem 6.2 and Lemma 6.4.

The proof of Theorem C is completely analogous, and we leave details to the interested reader.

References

[B1] Borcherds, R.E.: Vertex algebras, Kac–Moody algebras, and the Monster. Proc. Natl. Acad. Sci. USA **83**, 3068–3071 (1986)

[B1] Borcherds, R.E.: Monstrous moonshine and monstrous Lie superalgebras. Invent. Math. **109**, 405–444 (1992)

[C] Conway, J.H.: Three lectures on exceptional groups. In: Finite Simple Groups. ed. by Higman, G., Powell, M.B., London/New York: Academic Press, 1971, pp. 215–247

[CN] Conway, J.H., Norton, S.: Monstrous moonshine. Bull. Lond. Math. Soc. **11**, 308–339 (1979)

[DGH] Dixon, L., Ginsparg, P., Harvey, J.: Beauty and the beast: Superconformal symmetry in a Monster module. Commun. Math. Phys. **119**, 285 (1988)

[DM] Dong, C., Mason, G.: Nonabelian orbifolds and the boson-fermion correspondences. Commun. Math. Phys., to appear

[F] Frenkel, I.B.: Two constructions of affine Lie algebra representations and boson-fermion correspondence in quantum field theory. J. Funct. Anal. **44**, 259–327 (1981)

[FLM] Frenkel, I.B., Lepowsky, J., Meurman, A.: Vertex Operator Algebras and the Monster. Pure and Applied Math., Vol. **134**, New York: Academic Press, 1988

[K] Koike, M.: On McKay's conjecture. Nagoya Math. J. **95**, 85–89 (1984)
[M1] Mason, G.: Finite groups and modular functions. Proc. Symp. Pure. Math. **47**, 181–210 (1987)
[M2] Mason, G.: G-elliptic systems and the genus zero problem for M_{24}. Bull. Am. Math. Soc. **25**, No. 1, 45–53 (1991)
[M3] Mason, G.: Hecke operators and conformally-invariant orbifold models. Preprint, UCSC, 1992
[M4] Mason, G.: On a system of elliptic modular forms attached to the large Mathieu group. Nagoya Math. J. **118**, 177–193 (1990)
[M5] Mason, G.: Frame shapes and rational characters of finite groups. J. Algebra **89**, 237–248 (1984)
[O] Ogg, A.: Modular functions. Proc. Symp. Pure. Math. **37**, 521–532 (1979)
[Tu] Tuite, M.: Monstrous Moonshine from orbifolds. Commun. Math. Phys. **146**, 277–309 (1992)
[V] Venkov, B.: Even unimodular 24-dimensional lattices. Chap. 18, Sphere Packing, Lattices and Groups, by Conway, J.H., Sloane, N.J.A., Berlin, Heidelberg, New York: Springer, 1988

Communicated by N.Yu. Reshetikhin