Kac-Moody Algebras and Monstrous Moonshine

Edwin Lu

Spring 2025

1 Introduction

In this paper, we discuss the moonshine conjecture and give a detailed outline of a proof of the conjecture. Along the way, we give the basics about Kac-Moody algebras and a proof of the Weyl-Kac character formula, an infinite-dimensional version of the classical Weyl character formula for complex semisimple Lie algebras. Knowledge of the structure theory of semisimple Lie algebras is assumed, though we will recall the basic definitions and theorems.

The moonshine conjecture is a statement about the monster group and its relation to Hauptmoduls. Such a potential connection was first noticed by John McKay, when he noted that the dimension of the smallest non-trivial irreducible representation of the monster group was one less than the linear coefficient of the elliptic modular function $j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$.

The monster group G is the largest of the sporadic finite simple groups, and has order

$$\begin{aligned} &808017424794512875886459904961710757005754368000000000 \\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71. \end{aligned}$$

It contains 20 of the 26 sporadic groups as subquotients, and as such is vital for understanding many of the other sporadic groups. It was first constructed by Robert Griess as the automorphism group of the Griess algebra, which is a 196883-dimensional real commutative non-associative algebra [7].

We recall how a Hauptmodul is defined and some basics about modular functions. The special linear group $\mathrm{SL}(2,\mathbb{Z})$ acts on the upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ via fractional linear transformations: if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $A\tau = \frac{a\tau+b}{c\tau+d}$. Consider the space $\mathbb{H}/\mathrm{SL}(2,\mathbb{Z})$ under this action. Pictorially, this

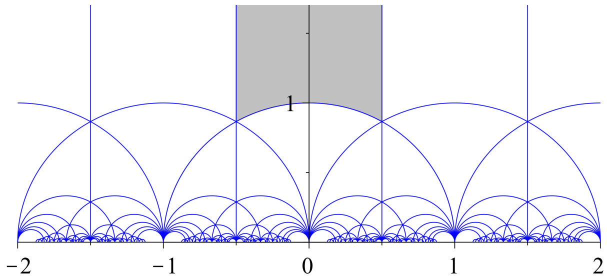

Figure 1: Fundamental domain for $\mathrm{SL}(2,\mathbb{Z})$ acting on the upper half-plane, from Wikipedia [10].

can be thought of as the greyed space above, with points on the 'boundary' of the region being identified together. We can compactify this to get a 2-sphere. It turns out that taking a discrete subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ gives a similar result. The compactification $\overline{\mathbb{H}/\Gamma}$ of $\mathbb{H}/\Gamma$ is a compact Riemann surface, which is necessarily a genus g torus for some g. In particular, we will focus on the case when $\overline{\mathbb{H}/\Gamma}$ is a sphere, in which case we say Γ is a genus 0 discrete subgroup of $\mathrm{SL}(2,\mathbb{Z})$.

When Γ is a genus 0 discrete subgroup of $\mathrm{SL}(2,\mathbb{Z})$, we can consider biholomorphic maps from $\overline{\mathbb{H}/\Gamma}$ to the Riemann sphere. Such maps can be thought of as meromorphic maps on the upper half-plane which are invariant under the action of Γ. We define a modular function of level Γ as a holomorphic function on $\mathbb{H}$ invariant under the action of Γ that also satisfies a boundedness condition as $\mathrm{Im}(z) \to \infty$.

Let $f_\Gamma(\tau)$ be a modular function of level Γ which identifies $\overline{\mathbb{H}/\Gamma}$ with the Riemann sphere. It is known that every modular function of level Γ can be written as a rational function in f_Γ [5]. Note that f_Γ is not unique, and in fact the action of any element of $\mathrm{SL}(2,\mathbb{R})$ will produce another f_Γ. There is, however, a canonical choice of f_Γ, given by considering the q-expansion of f_Γ. Under the parameter $q = e^{2\pi i\tau}$, we consider the choice of f_Γ which can be written as $q^{-1} + \sum_{n=0}^{\infty} a_n q^n$. This choice is called the Hauptmodul for Γ, and is denoted $J_\Gamma(\tau)$. The most notable case of this is when $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, in which case we call J_Γ the elliptic modular function, and denote it $j(\tau)$. This has q-expansion $j(q) = q^{-1} + 744 + 196884q + \dots$.

The remainder of this paper is split into two chapters. Chapter 2 will review the basics of complex semisimple Lie algebras and introduce (generalized) Kac-Moody algebras, their infinite-dimensional counterparts. Many concepts can be transferred from the finite to infinite-dimensional case, such as the Weyl group, the root decomposition, and even the Weyl character formula. We spend the last portion of this chapter giving a proof of the Weyl-Kac character formula. This character formula implies the denominator identity, which we will use in part of the proof of monstrous moonshine. We also mention a more general form of the Weyl-Kac character formula involving the homology of the positive root space.

Chapter 3 then will give a more detailed introduction on the moonshine conjecture. We give a proof outline of the conjecture, and give a detailed proof of several key steps. Much of this will be based on Richard Borcherds' paper "Monstrous moonshine and monstrous Lie superalgebras" [2].

Notation

V^* Dual vector space to the complex vector space V

$\langle\,,\,\rangle$ Pairing between V and V^*

$(\,,\,)$ The non-degenerate, invariant, symmetric bilinear form on $\mathfrak{g}(A)$ associated with a symmetrization $A = DB$

$\mathfrak{g}$ A generalized Kac-Moody algebra

$\mathfrak{h}$ The Cartan subalgebra of a generalized Kac-Moody algebra $\mathfrak{g}$

$\mathfrak{n}_+$ The subalgebra of a generalized Kac-Moody algebra $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$ spanned by the positive root spaces

W The Weyl group, with elements denoted by w

$j(q)$ The elliptic modular function, with $j(q) = q^{-1} + 744 + 196884q + \dots$

$c(n)$ The coefficients of $j(q) - 744 = \sum c(n)q^n$

$GL(V)$ The infinite general group of a vector space V, which is the direct limit of the inclusions $\mathrm{GL}_n(V) \to \mathrm{GL}_{n+1}(V)$

P, P_+, P_{++} The set of integral, dominant integral, and regular dominant integral weights, respectively, given by

$$P = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}, \forall i = 1, \dots, n\}$$
$$P_+ = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}_{\geq 0}, \forall i = 1, \dots, n\}$$
$$P_{++} = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}_{>0}, \forall i = 1, \dots, n\}$$

2 Generalized Kac-Moody Algebras

Before discussing the basics of Kac-Moody algebras, we review the theory of finite-dimensional semisimple Lie algebras. This can be found in a standard textbook about Lie algebras, such as Kirillov's "An Introduction to Lie Groups and Lie Algebras".

Definition 1. A (complex) *Lie algebra* $\mathfrak{g}$ is a vector space $\mathfrak{g}$ over $\mathbb{C}$ equipped with a bilinear product $[\ ,\ ]\colon \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$, called the *Lie bracket*, which is anti-symmetric and satisfies the Jacobi identity:

$$[[x,y],z]+[[y,z],x]+[[z,x],y]=0, \forall x,y,z\in\mathfrak{g}.$$

Lie algebras arise naturally from Lie groups, by considering the tangent space at the identity. Often, studying the structure of Lie algebras and their representations, we may conclude certain information about Lie groups inducing them.

We give some important constructions of Lie algebras:

Example 1. Given a (complex) vector space V, the space $\mathfrak{gl}(V)$ of endomorphisms of V forms a Lie algebra under the Lie bracket $[x,y]=x\circ y-y\circ x$ for $x,y\in\mathfrak{gl}(V)$.

Example 2. A central example in the theory of semisimple Lie algebras is the Lie algebra $\mathfrak{sl}(2,\mathbb{C})$. This is the Lie algebra consisting of traceless 2-by-2 matrices, with Lie bracket given by the matrix commutator. The standard basis for $\mathfrak{sl}(2,\mathbb{C})$ consists of the three elements

$$h=\begin{bmatrix}1&0\\0&-1\end{bmatrix}, e=\begin{bmatrix}0&1\\0&0\end{bmatrix}, f=\begin{bmatrix}0&0\\1&0\end{bmatrix},$$

which have relations $[e,f]=h$, $[h,e]=2e$, and $[h,f]=-2f$.

Example 3. Given two Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$, their *direct sum* $\mathfrak{g}\oplus\mathfrak{h}$ is a Lie algebra, with Lie bracket given by $[(x_1,y_1),(x_2,y_2)]=([x_1,x_2],[y_1,y_2])$.

Definition 2. Given a Lie algebra $\mathfrak{g}$, an *ideal* of $\mathfrak{g}$ is a subspace $\mathfrak{h}\subset\mathfrak{g}$ such that $[\mathfrak{h},\mathfrak{g}]\subset\mathfrak{h}$, i.e. for any $x\in\mathfrak{h}$ and $y\in\mathfrak{g}$, we have that $[x,y]\in\mathfrak{h}$.

Definition 3. For a Lie algebra $\mathfrak{g}$, a *Lie algebra representation* of $\mathfrak{g}$ on a vector space V is a Lie algebra homomorphism $\rho\colon\mathfrak{g}\to\mathfrak{gl}(V)$, i.e. a linear map ρ which satisfies $\rho([x,y])=[\rho(x),\rho(y)]=\rho(x)\rho(y)-\rho(y)\rho(x)$ for all $x,y\in\mathfrak{g}$.

Importantly, we have the *adjoint representation* of $\mathfrak{g}$, which is a representation of $\mathfrak{g}$ on itself. The adjoint representation is given by $\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, $\mathrm{ad}(x)(y) = [x, y]$ for all $x, y \in \mathfrak{g}$.

Definition 4. A Lie algebra $\mathfrak{g}$ is said to be *simple* if its only ideals are 0 and itself. Equivalently, $\mathfrak{g}$ is simple precisely when its adjoint representation is irreducible, i.e. has no nontrivial subrepresentations.

Definition 5. A Lie algebra $\mathfrak{g}$ is said to be *semisimple* if it can be written as the direct sum of simple Lie algebras.

Semisimple Lie algebras have a nice structure, known as the root decomposition. This leads into the classification of semisimple Lie algebras via Dynkin diagrams. We introduce several definitions needed to describe this decomposition.

Definition 6. An element $x \in \mathfrak{g}$ is called *semisimple* if $\mathrm{ad}\, x\colon \mathfrak{g} \to \mathfrak{g}$ is a semisimple operator. A subalgebra $\mathfrak{g}$ is *toral* if it is commutative, i.e. satisfies $[\mathfrak{g}, \mathfrak{g}] = 0$, and consists only of semisimple elements. A *Cartan subalgebra* of $\mathfrak{g}$ is a maximal toral subalgebra $\mathfrak{h}$ of $\mathfrak{g}$.

Lemma 2.1. *([9], Corollary 6.36) Every semisimple Lie algebra $\mathfrak{g}$ has a Cartan subalgebra.*

Theorem 2.2. *([9], Theorem 6.38) Let $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan subalgebra of a semisimple Lie algebra. Define $\mathfrak{g}_\alpha := \{x \in \mathfrak{g} \mid [h, x] = \langle \alpha, h\rangle x, \forall h \in \mathfrak{h}\}$. Then, there exists a decomposition*

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathfrak{h}^* \setminus \{0\}} \mathfrak{g}_\alpha,$$

called the ***root decomposition*** *of $\mathfrak{g}$. The set $\Delta = \{\alpha \in \mathfrak{h}^* \setminus \{0\} \mid \mathfrak{g}_\alpha \neq 0\}$ is called the* ***root system*** *of $\mathfrak{g}$.*

Example 4. For $\mathfrak{sl}(2, \mathbb{C})$, recall that $[h, f] = -2f$ and $[h, e] = 2e$. We thus have the root decomposition $\mathfrak{sl}(2, \mathbb{C}) = \mathbb{C}f \oplus \mathbb{C}h \oplus \mathbb{C}e$, with $\mathbb{C}h$ the Cartan subalgebra and $\mathbb{C}f$, $\mathbb{C}e$ the root spaces.

Each semisimple Lie algebra also comes equipped with a non-degenerate, invariant, symmetric bilinear form $(\ ,\ )$ satisfying a number of properties, called the *Killing form*. This form is non-degenerate on $\mathfrak{h}$, and so induces an isomorphism $\mathfrak{h} \to \mathfrak{h}^*$ via $x \mapsto (x, -)$. This isomorphism induces a symmetric bilinear form on $\mathfrak{h}^*$, which we also call the Killing form, and is also denoted by $(\ ,\ )$. See pages 101, 120-124 of [9] for more. Picking non-zero $h \in \mathfrak{h}^*$ such that $(h, \alpha) \neq 0$ for each $\alpha \in \Delta$, we get a polarization $\Delta = \Delta_+ \coprod \Delta_-$, where $\Delta_+ = \{\alpha \in \Delta \mid (h, \alpha) > 0\}$, and $\Delta_- = \{\alpha \in \Delta \mid (h, \alpha) < 0\}$. We say a root $\alpha \in \Delta_+$ is *simple* if it cannot be written as a sum of two positive roots, and denote the set of simple roots by Π. Note that such a polarization (and hence choice of Δ_+) depends on the choice of h.

Definition 7. Given an ordering of the simple roots $\Pi = \{\alpha_1, \ldots, \alpha_n\}$, we define the *Cartan matrix* $A = (a_{ij})$ of $\mathfrak{g}$ by $a_{ij} = \frac{2(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}$.

The Cartan matrix uniquely classifies $\mathfrak{g}$ up to isomorphism, and in fact, it is possible to classify the set of matrices appearing as the Cartan matrix of a semisimple Lie algebra [9]. It turns out that a Cartan matrix is necessarily positive definite, with 2's along the diagonal and nonpositive integers otherwise.

2.1 Infinite-Dimensional Lie Algebras

A semisimple Lie algebra being classified by its Cartan matrix naturally begs the question of what happens if we change the Cartan matrix. It turns out that Lie algebras associated with matrices that are not positive-definite will be infinite-dimensional. These infinite-dimensional Lie algebras, called (generalized) Kac-Moody algebras, retain many properties of the finite-dimensional case, including the existence of a root decomposition.

We now introduce many definitions involving Kac-Moody algebras, many of them analogous to their finite-dimensional counterparts, with the goal of proving the Weyl-Kac denominator identity. This gives an expression for the denominator of the Weyl-Kac character formula (which is analogous to the Weyl character formula in the finite-dimensional case), which will be an important tool in the proof of monstrous moonshine. Much of this can be found in Kac's "Infinite dimensional Lie algebras".

Definition 8. A *Borcherds-Cartan matrix* is a real square matrix A satisfying the following properties:

- $a_{ii} = 2$ or $a_{ii} \leq 0$
- for $i \neq j$, $a_{ij} \leq 0$, and if $a_{ii} = 2$, we additionally have $a_{ij} \in \mathbb{Z}$
- $a_{ij} = 0$ implies $a_{ji} = 0$.

Given a Borcherds-Cartan matrix A, we may construct a Lie algebra $\mathfrak{g}(A)$. Let A be an n-by-n matrix with rank ℓ. First, consider a vector space $\mathfrak{h}$, and sets $\Pi = \{\alpha_1, \ldots, \alpha_n\} \subset \mathfrak{h}^*$ and $\Pi^\vee = \{\alpha_1^\vee, \ldots, \alpha_n^\vee\} \subset \mathfrak{h}$ such that

- Π and $\Pi^\vee$ are linearly independent,
- $\langle \alpha_i^\vee, \alpha_j \rangle = a_{ij}$, $i, j = 1, \ldots, n$,
- $n - \ell = \dim \mathfrak{h} - n$.

Remark. Note that the sets Π and $\Pi^\vee$ are **not** dual.

Proposition 2.3. *([8], Proposition 1.1) For any A, there exists a triple $(\mathfrak{h}, \Pi, \Pi^\vee)$ satisfying the above.*

We now construct a Lie algebra $\tilde{\mathfrak{g}}(A)$ with generators e_i, f_i, and $\mathfrak{h}$ for $i = 1, \ldots, n$, and the following relations (called the *Serre relations*):

- $[e_i, f_j] = \delta_{ij}\alpha_i^\vee$, $i, j = 1, \ldots, n$,
- $[\mathfrak{h}, \mathfrak{h}] = 0$,
- $[h, e_i] = \langle \alpha_i, h \rangle e_i$, $[h, f_i] = -\langle \alpha_i, h \rangle f_i$, $i = 1, \ldots, n$ and $h \in \mathfrak{h}$.

Lemma 2.4. *([8], Theorem 1.2) There exists a unique ideal τ of $\tilde{g}(A)$ with $\tau \cap \mathfrak{h} = 0$ such that τ contains every ideal of $\tilde{g}(A)$ whose intersection with $\mathfrak{h}$ is trivial.*

Definition 9. We set $\mathfrak{g}(A) = \tilde{\mathfrak{g}}(A)/\tau$ to be the *generalized Kac-Moody algebra* associated with A.

Example 5. One of the simplest examples of a (infinite-dimensional) Kac-Moody algebra has Borcherds-Cartan matrix $A = \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix}$. The Kac-Moody algebra $\mathfrak{g}(A)$ has root multiplicities for small roots as seen in Figure 2 below from page 214 of [8].

TABLE H_2

α	$-(\alpha\|\alpha)$	mult α	α	$-(\alpha\|\alpha)$	mult α
(1, 1)	1	1	(15, 11)	149	23750
(2, 2)	4	1	(16, 11)	151	25923
(3, 2)	5	2	(13, 12)	155	30865
(3, 3)	9	3	(14, 12)	164	45271
(4, 3)	11	4	(13, 13)	169	55853
(4, 4)	16	6	(15, 12)	171	60654
(5, 4)	19	9	(16, 12)	176	74434
(6, 4)	20	9	(17, 12)	179	84121
(5, 5)	25	16	(18, 12)	180	87547
(6, 5)	29	23	(14, 13)	181	91257
(7, 5)	31	27	(15, 13)	191	135861
(6, 6)	36	39	(14, 14)	196	165173
(7, 6)	41	60	(16, 13)	199	185526
(8, 6)	44	73	(17, 13)	205	233487
(9, 6)	45	80	(15, 14)	209	271860
(7, 7)	49	107	(18, 13)	209	271702
(8, 7)	55	162	(19, 13)	211	292947
(9, 7)	59	211	(16, 14)	220	409725
(10, 7)	61	240	(15, 15)	225	492420
(8, 8)	64	288	(17, 14)	229	569358
(9, 8)	71	449	(18, 14)	236	732180
(10, 8)	76	600	(16, 15)	239	815214
(11, 8)	79	720	(19, 14)	241	874650
(12, 8)	80	758	(20, 14)	244	972117
(9, 9)	81	808	(21, 14)	245	1006994
(10, 9)	89	1267	(17, 15)	251	1242438
(11, 9)	95	1754	(16, 16)	256	1476973
(12, 9)	99	2167	(18, 15)	261	1752719
(10, 10)	100	2278	(19, 15)	269	2298090
(13, 9)	101	2407	(17, 16)	271	2458684
(11, 10)	109	3630	(20, 15)	275	2808958
(12, 10)	116	5130	(21, 15)	279	3207547
(11, 11)	121	6559	(22, 15)	281	3426450
(13, 10)	121	6555	(18, 16)	284	3783712
(14, 10)	124	7554	(17, 17)	289	4456255
(15, 10)	125	7936	(19, 16)	295	5411212
(12, 11)	131	10531	(20, 16)	304	7217527
(13, 11)	139	15204	(18, 17)	305	7453376
(12, 12)	144	19022	(21, 16)	311	9005900
(14, 11)	145	19902			

Figure 2: Table of root multiplicities for the Kac-Moody algebra with Borcherds-Cartan matrix $A = \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix}$

Theorem 2.5. *([8], page 6) Let A be a Borcherds-Cartan matrix, $\mathfrak{g}(A)$ its associated generalized Kac-Moody algebra. Let $Q = \sum_{i=1}^{n} \mathbb{Z}\alpha_i$ be the root lattice, and define $\mathfrak{g}_\alpha = \{x \in \mathfrak{g}(A) \mid [h, x] = \langle \alpha, h \rangle x, \forall h \in \mathfrak{h}\}$. Then, we have the decomposition*

$$\mathfrak{g}(A) = \bigoplus_{\alpha \in Q} \mathfrak{g}_\alpha,$$

called the root decomposition *of* $\mathfrak{g}(A)$. *When $\mathfrak{g}_\alpha \neq 0$ (and $\alpha \neq 0$), we say α is a* root.

Similar to in the finite-dimensional case, we have the following definitions:

Definition 10. A root α is *positive* (and we write $\alpha > 0$) if $\alpha = \sum k_i \alpha_i$ for $k_i \geq 0$. We similarly define negative roots. We denote the set of all roots, positive roots, and negative roots, by Δ, Δ_+, and Δ_-, respectively. We also have the *triangular decomposition* $\mathfrak{g}(A) = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$ for $\mathfrak{n}_+$ (respectively, $\mathfrak{n}_-$) the subalgebra generated by $e_1, \ldots, e_n$ (respectively, $f_1, \ldots, f_n$).

Definition 11. A *representation* of $\mathfrak{g}(A)$ (or $\mathfrak{g}(A)$-representation) is a vector space V with a linear map $\rho\colon \mathfrak{g}(A) \to \mathfrak{gl}(V)$ preserving the Lie bracket.

An element $x \in \mathfrak{g}(A)$ is *locally nilpotent* on V if for every $v \in V$ there exists a positive integer N satisfying $x^N(v) = 0$.

Definition 12. A $\mathfrak{g}(A)$-representation V is said to be $\mathfrak{h}$-diagonalizable if we have a weight decomposition $V = \bigoplus_{\lambda\in\mathfrak{h}^*} V_\lambda$, where $V_\lambda = \{v \in V \mid h(v) = \langle\lambda, h\rangle v, \forall h \in \mathfrak{h}\}$. The *multiplicity* of λ is $\dim V_\lambda$, denoted by $\operatorname{mult}_V \lambda$. An $\mathfrak{h}$-diagonalizable $\mathfrak{g}(A)$-representation is *integrable* if each e_i and f_i, $i = 1, \dots, n$ is locally nilpotent on V.

Definition 13. Let $\mathfrak{g}(A)$ be a generalized Kac-Moody algebra. For $i = 1, \dots, n$, we define the *fundamental reflection* $r_i\colon \mathfrak{h}^* \to \mathfrak{h}^*$ by $r_i(\lambda) = \lambda - \langle\lambda, \alpha_i^\vee\rangle\alpha_i$, $\lambda \in \mathfrak{h}^*$. The *Weyl group* W of $\mathfrak{g}(A)$ is then the subgroup of $\mathrm{GL}(\mathfrak{h}^*)$ generated by the fundamental reflections.

Proposition 2.6. *([8], Proposition 3.7) Let V be an integrable $\mathfrak{g}(A)$-module. Then, $\operatorname{mult}_V \lambda = \operatorname{mult}_V w(\lambda)$ for any $\lambda \in \mathfrak{h}^*$ and $w \in W$. In particular, the root system Δ is W-invariant, and the set $\Delta_+ \setminus \{\alpha_i\}$ is r_i-invariant.*

We say a matrix A is *symmetrizable* if $A = DB$ for a diagonal matrix D and symmetric matrix B. If A is symmetrizable, then we can construct a bilinear form on $\mathfrak{g}(A)$, akin to the Killing form in the finite-dimensional case.

Let $A = DB$ for $D = \mathrm{diag}(\varepsilon_1, \dots, \varepsilon_n)$ an invertible diagonal matrix and B symmetric. Pick a complementary subspace $\mathfrak{h}''$ to $\mathfrak{h}' := \sum_i \mathbb{C}\alpha_i^\vee$ in $\mathfrak{h}$. We can then define a symmetric bilinear form $(\ ,\ )$ on $\mathfrak{h}$ by the equations

- $(\alpha_i^\vee, \mathfrak{h}) = \langle\alpha_i, h\rangle\varepsilon_i$ for $h \in \mathfrak{h}$ and $i = 1, \dots, n$,
- $(h, h') = 0$ for $h, h' \in \mathfrak{h}''$.

Note that this is dependent on the choice of symmetrization $A = DB$.

Theorem 2.7. *([8], Theorem 2.2) Let A be symmetrizable, with a fixed decomposition $A = DB$. Then, there exists a non-degenerate invariant symmetric bilinear form $(\ ,\ )$ on $\mathfrak{g}(A)$ such that*

1. *$(\ ,\ )|_{\mathfrak{h}}$ is defined as above and is non-degenerate,*
2. *$(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$ for $\alpha + \beta \neq 0$,*

3. $(\, , \,) \colon \mathfrak{g}_\alpha \otimes \mathfrak{g}_{-\alpha} \to \mathbb{C}$ *is a non-degenerate pairing.*

As in the finite-dimensional case, this bilinear form induces an isomorphism $\mathfrak{h} \to \mathfrak{h}^*$, and hence a bilinear form on $\mathfrak{h}^*$, which we also denote $(\, , \,)$.

Definition 14. A root $\alpha \in \Delta$ is *real* if $|\alpha|^2 := (\alpha, \alpha) > 0$, and *imaginary* otherwise.

Note in the finite-dimensional case, every root is real, as we may write any root α as $\alpha = w(\alpha_i)$ for $w \in W$ and α_i a simple root. We then have that $|\alpha|^2 = |w(\alpha_i)|^2 > 0$. In the infinite-dimensional case, the distinction between real and imaginary roots allows us to show statements about each, and henceforth explicitly compute root multiplicities of a given Kac-Moody algebra.

Example 6. A central example that we will use is a generalized Kac-Moody algebra $\mathfrak{g}$ with root lattice given by the standard lattice in the two-dimensional Lorentzian space $II_{1,1}$, i.e. roots are of the form (m, n), $m, n \in \mathbb{Z}$ such that the inner product is given by

$$((m_1, n_1), (m_2, n_2)) = -m_1 n_2 - m_2 n_1,$$

and simple roots of the form $(1, n)$ for $n = -1$ or $n > 0$. Every simple root is imaginary except $(-1, 0)$, as $((1, n), (1, n)) = -2n < 0$ except for $n = -1$.

2.2 Weyl-Kac Denominator Identity

Our goal in this section is to give a proof of the Weyl-Kac character formula, which as an immediate consequence will give us the Weyl-Kac denominator identity. We first need to introduce the concept of a highest-weight representation and Verma module. The character of a highest-weight representation is a way of packaging the dimension of the weight spaces in a formula which acts nicely under sums and the Weyl group.

Definition 15. For an h-diagonalizable representation V, we define the *character* of V to be $\mathrm{ch}(V) = \sum_{\lambda \in \mathfrak{h}^*} \mathrm{mult}_V \, \lambda e^\lambda$, where e^λ is a formal symbol satisfying $e^0 = 1$ and $e^\lambda e^\mu = e^{\lambda + \mu}$.

The character evidently retains information about the multiplicities of the weights of the representation V, and is also preserved under the action of the Weyl group.

We can also easily see that computing the character of V gives complete information about the representation, as a representation is determined by the dimension of its weight subspaces.

We define

$$P = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}, \forall i = 1, \ldots, n\}$$
$$P_+ = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}_{\geq 0}, \forall i = 1, \ldots, n\}$$
$$P_{++} = \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}_{> 0}, \forall i = 1, \ldots, n\}.$$

The set P is the *weight lattice*, and allows us to describe a class of representations of $\mathfrak{g}$.

Definition 16. Let A be a Borcherds-Cartan matrix. We say a $\mathfrak{g}(A)$-representation V is a *highest-weight representation* with *highest weight* $\Lambda \in \mathfrak{h}^*$ if there exists a non-zero vector $v \in V$ such that $\mathfrak{n}_+(v) = 0, h(v) = \Lambda(h)v$ for all $h \in \mathfrak{h}$, and v generates V as a $\mathfrak{g}(A)$-representation. The vector v is called a *highest-weight vector*.

A highest-weight $\mathfrak{g}(A)$-representation $M(\Lambda)$ with highest weight Λ is called a *Verma module* if every $\mathfrak{g}(A)$-representation with highest weight Λ is a quotient of $M(\Lambda)$.

Proposition 2.8. *([8], Proposition 9.2) For every $\Lambda \in \mathfrak{h}^*$, there exists a Verma module $M(\Lambda)$ which is unique up to isomorphism. Moreover, $M(\Lambda)$ contains a unique proper maximal subrepresentation $M'(\Lambda)$.*

We note that the proof is constructive. We define $U(\mathfrak{g}(A))$ to be the universal enveloping algebra of $\mathfrak{g}(A)$ as follows: consider the tensor algebra $T(\mathfrak{g}(A))$, and mod out by the ideal generated by $[x, y] - xy + yx$ for $x, y \in \mathfrak{g}(A)$. We then set $M(\Lambda) = U(\mathfrak{g}(A))/J(\Lambda)$, where $J(\Lambda)$ is the left ideal of $U(\mathfrak{g}(A))$ generated by $\mathfrak{n}_+$ and elements of the form $h - \Lambda(h)$ for $h \in \mathfrak{h}$. We can quickly see this makes $M(\Lambda)$ a highest-weight representation with highest weight Λ. For a full proof see [8].

We set $L(\Lambda) := M(\Lambda)/M'(\Lambda)$, which by the proposition is the unique highest-weight irreducible representation of highest weight Λ.

Example 7. For $\Lambda = 0$, we see by uniqueness that $L(0)$ must be the trivial representation, as the trivial representation is an irreducible representation of $\mathfrak{g}(A)$ with highest weight 0.

We are now ready to state the character formula. Pick an element $\rho \in \mathfrak{h}^*$ such that $\langle \rho, \alpha_i^\vee \rangle = 1$ for all $i = 1, \ldots, n$. Let $\Lambda \in P_+$, and let s be a finite sum of pairwise orthogonal imaginary simple roots which are orthogonal to Λ. Set $\varepsilon(s) = (-1)^m$ for m the number of simple roots used in the finite sum above, and define $S = e^{\Lambda+\rho} \sum_s \varepsilon(s) e^s$.

Theorem 2.9. *Let A be a symmetrizable Kac-Moody algebra, with $L(\Lambda)$ the irreducible $\mathfrak{g}(A)$-representation with highest weight $\Lambda \in P_+$. Then, if W is the Weyl group of $\mathfrak{g}(A)$, we have*

$$\operatorname{ch} L(\Lambda) = \frac{\sum_{w \in W} \det(w) e^{-\rho} w(S)}{\prod_{\alpha>0} (1 - e^{-\alpha})^{\operatorname{mult}\alpha}}.$$

Corollary 2.9.1.

$$e^\rho \prod_{\alpha>0} (1 - e^{\alpha})^{\operatorname{mult}\alpha} = \sum_{w \in W} \det(w) w(S).$$

This corollary immediately follows by setting $\Lambda = 0$, and noting $L(0)$ is the trivial representation. This equation is called the Weyl-Kac denominator identity, and will be used in the next section.

We now present a proof of the Weyl-Kac character formula. We follow the proof in [8]. Briefly, we will compute the character of the Verma module $M(\Lambda)$, and relate it to the character of the corresponding highest-weight irreducible representation $L(\Lambda)$.

Lemma 2.10. $\operatorname{ch} M(\Lambda) = e^\Lambda \prod_{\alpha>0} (1 - e^{-\alpha})^{-\operatorname{mult}\alpha}$.

Proof. We construct a basis of the space $M(\Lambda)_\lambda$ as such: let $\beta_1, \beta_2, \ldots$ be the positive roots of $\mathfrak{g}(A)$, with $e_{\beta_s i_s}$, $1 \leq i_s \leq \operatorname{mult}\beta_s = m_s$ a basis of $\mathfrak{g}_{-\beta_s}$. Let $v \in M(\Lambda)$ be a highest-weight vector. Then, ranging over positive integers n_{ij} satisfying $\sum_i (\sum_j n_{ij}) \beta_i = \Lambda - \lambda$, the vectors $e_{\beta_{11}}^{n_{11}} \ldots e_{\beta_{1m_1}}^{n_{1m_1}} e_{\beta_{21}}^{n_{21}} \ldots e_{\beta_{2m_1}}^{n_{2m_1}} \ldots (v_\Lambda)$ form a basis of $M(\Lambda)_\lambda$ by the Poincaré-Birkhoff-Witt theorem. Thus, a combinatorial argument tells us

$$\operatorname{ch} M(\Lambda) = e^\Lambda \prod_{\alpha>0} (1 + e^{-\alpha} + e^{-2\alpha} + \ldots)^{\operatorname{mult}\alpha} = e^\Lambda \prod_{\alpha>0} (1 - e^{-\alpha})^{\operatorname{mult}\alpha}.$$

□

We assume the following lemma without proof. For a proof, see [8] pages 151-152.

Lemma 2.11. *Let V be a highest weight $\mathfrak{g}(A)$-representation of highest weight Λ. Then,*

$$\operatorname{ch} V = \sum_{\lambda \in \mathfrak{h}^*} [V : L(\lambda)] \operatorname{ch} L(\lambda).$$

This allows us to compute the character of $L(\Lambda)$ in terms of characters of Verma modules $M(\lambda)$.

Lemma 2.12.

$$\operatorname{ch} L(\Lambda) = \sum_{\substack{\lambda \leq \Lambda \\ |\lambda+\rho|^2 = |\Lambda+\rho|^2}} c_\lambda \operatorname{ch} M(\lambda)$$

for some $c_\lambda \in \mathbb{Z}$, with $c_\Lambda = 1$.

Proof. Set $B(\Lambda) = \{\lambda \leq \Lambda \ : \ |\lambda + \rho|^2 = |\Lambda + \rho|^2\}$, and order the elements of $B(\Lambda)$ as $\lambda_1, \lambda_2, \ldots$ so that $\lambda_i \geq \lambda_j$ implies $i \leq j$. Then, the previous lemma implies

$$\operatorname{ch} M(\lambda_i) = \sum_{\lambda_j \in B(\Lambda)} c_{ij} \operatorname{ch} L(\lambda_j)$$

such that the matrix (c_{ij}) is upper-triangular with ones along the diagonal. Solving this system for $L(\lambda_j)$ proves the lemma. □

Lemma 2.13. *Let $\Lambda \in P_{++}, \lambda \in P_+$ with $\lambda < \Lambda$. Then,* $(\Lambda, \Lambda) - (\lambda, \lambda) > 0$.

Proof. Write $\lambda = \Lambda - \beta$ for $\beta = \sum_i k_i \alpha_i$ with $k_i \geq 0$ not all zero. Then, $(\Lambda, \Lambda) - (\lambda, \lambda) = (\Lambda - \lambda, \Lambda + \lambda) = (\Lambda + \lambda, \beta) = \sum_i \frac{1}{2} k_i (\alpha_i, \alpha_i) \langle \Lambda + \lambda, \alpha_i^\vee \rangle$. As $(\alpha_i, \alpha_i) > 0$, we get $(\Lambda, \Lambda) - (\lambda, \lambda) > 0$. □

We are now ready to prove the Weyl-Kac character formula.

Proof. (of Theorem 2.9). We prove the case where $a_{ii} = 2$ for each $i = 1, \ldots n$, in which case there are no imaginary simple roots and $S = e^{\Lambda+\rho}$. The proof in the general case is similar, see (section 11.13 in Kac). Set $R = \prod_{\alpha > 0} (1 - e^{-\alpha})^{\operatorname{mult} \alpha}$, so that $R \operatorname{ch} M(\lambda) = 1$ by Lemma 2.10. Multiplying both sides of Lemma 2.13 by $e^\rho R$, we get

$$e^\rho R \operatorname{ch} L(\Lambda) = \sum_{\substack{\lambda \leq \Lambda \\ |\lambda+\rho|^2 = |\Lambda+\rho|^2}} c_\lambda e^{\lambda+\rho}, \tag{1}$$

for some $c_\lambda \in \mathbb{Z}$ with $c_\Lambda = 1$.

Notice that the left-hand side is W-skew-invariant, i.e. $w(e^\rho R \operatorname{ch} L(\Lambda)) = \det(w) e^\rho R \operatorname{ch} L(\Lambda)$. We can see this by checking the statement for $w = r_i$ a fundamental reflection. By Proposition 2.6, the set $\Delta_+ \setminus \{\alpha_i\}$ is r_i-invariant. Then,

$$\begin{aligned} r_i(e^\rho R) &= e^{\rho-\alpha_i} r_i(1-e^{-\alpha_i}) r_i \left(\prod_{\alpha \in \Delta_+ \setminus \{\alpha_i\}} (1-e^{-\alpha})^{\operatorname{mult}\alpha} \right) \\ &= e^\rho e^{-\alpha_i}(1-e^{\alpha_i}) \prod_{\alpha \in \Delta_+ \setminus \{\alpha_i\}} (1-e^{-\alpha})^{\operatorname{mult}\alpha} \\ &= e^\rho (e^{-\alpha_i}-1) \prod_{\alpha \in \Delta_+ \setminus \{\alpha_i\}} (1-e^{-\alpha})^{\operatorname{mult}\alpha} \\ &= -e^\rho R = \det(r_i) e^\rho R. \end{aligned}$$

Since $L(\Lambda)$ is integrable, Proposition 2.6 tells us that the dimension of its weight spaces is invariant under the Weyl group, and hence $w(\operatorname{ch} L(\Lambda)) = \operatorname{ch} L(\Lambda)$. This shows that $e^\rho R \operatorname{ch} L(\Lambda)$ is W-skew-invariant.

Thus, the coefficients on the right-hand side of equation 1 satisfy $c_\lambda = \det(w) c_\mu$ if $w(\lambda+\rho) = \mu+\rho$ for some $w \in W$. Let λ be such that $c_\lambda \neq 0$, so $c_{w(\lambda+\rho)-\rho} \neq 0$ for any $w \in W$. Hence, $w(\lambda+\rho)-\rho \leq \Lambda$. Consider $\mu \in \{w(\lambda+\rho)-\rho \mid w \in W\}$ such that the height of $\Lambda - \mu$ is minimal. Certainly, $\mu+\rho \in P_+$ and $|\mu+\rho|^2 = |\Lambda+\rho|^2$. Applying (previous lemma) to $\Lambda+\rho \in P_{++}$ and $\mu+\rho$, we get that $\mu = \Lambda$. Hence, $c_\lambda \neq 0$ implies $\lambda+\rho = w(\Lambda+\rho)$ for some $w \in W$, so $c_\lambda = \det(w)$. Yet since $w(\Lambda+\rho) = \Lambda+\rho$ implies $w = 1$, we get that

$$\sum_{\substack{\lambda \leq \Lambda \\ |\lambda+\rho|^2 = |\Lambda+\rho|^2}} c_\lambda e^{\lambda+\rho} = \sum_{w \in W} \det(w) e^{w(\Lambda+\rho)},$$

as desired.

□

2.3 Homology

We now introduce another tool to be used in the proof of monstrous moonshine.

Recall $\mathfrak{n}_+$ is the subspace of $\mathfrak{g}$ spanned by the positive root spaces. Let $\Lambda^i(\mathfrak{n}_+)$ be the ith exterior power of $\mathfrak{n}_+$. We define $H_i(\mathfrak{n}_+)$ to be the ith homology of the complex $\Lambda^\bullet(\mathfrak{n}_+)$ with maps $\Lambda^\bullet(\mathfrak{n}_+) \to \Lambda^{\bullet-1}(\mathfrak{n}_+)$ given as in the bar resolution. We then set $\Lambda(\mathfrak{n}_+) = \Lambda^0(\mathfrak{n}_+) \ominus \Lambda^1(\mathfrak{n}_+) \oplus \Lambda^2(\mathfrak{n}_+) \ominus \dots$ as the virtual vector space given by the alternating sum of the exterior powers. We similarly set $H(\mathfrak{n}_+) = H_0(\mathfrak{n}_+) \ominus H_1(\mathfrak{n}_+) \oplus H_2(\mathfrak{n}_+) \ominus \ldots$.

This definition immediately tells us that $\Lambda(\mathfrak{n}_+) = H(\mathfrak{n}_+)$. This statement will be a vital fact in the next section. It also gives a more general form of the Weyl-Kac denominator formula, which can be used to give another proof of the denominator identity.

The ith homology group $H_i(\mathfrak{n}_+)$ can be computed explicitly, as seen in Garland and Lepowsky [6]. Garland and Lepowsky show that $H_i(\mathfrak{n}_+)$ is explicitly the subspace of $\Lambda^i(\mathfrak{n}_+)$ spanned by the homogeneous vectors of $\Lambda^i(\mathfrak{n}_+)$ whose degrees r satisfy $(r+\rho)^2 = \rho^2$. We can use this fact to compute the homology groups, given information about the simple roots.

Example 8. Consider the generalized Kac-Moody algebra described in Example 6. We may pick ρ to be the vector $(-1, 0)$, as $(\rho, (1, n)) = -n = -(1, n)^2/2$. Hence, for $(r+\rho)^2 = \rho^2$, we must have that $r+\rho$ has norm 0. Thus, $r+\rho$ is of the form $(0, n)$ or $(m, 0)$, meaning r is of the form $(1, n)$ or $(m, 0)$. Computing H_i is thus equivalent to finding elements of $\Lambda^i(\mathfrak{n}_+)$ of these degrees.

For $H_0(\mathfrak{n}_+)$, we see that $\Lambda^0(\mathfrak{n}_+) = \mathbb{R}$ is a one-dimensional space of degree $(0, 0)$, and hence $H_0(\mathfrak{n}_+)$ is one-dimensional with character 1. For $H_1(\mathfrak{n}_+)$, we have that $\Lambda^1(\mathfrak{n}_+) = \mathfrak{n}_+$, which has no elements of degree $(m, 0)$. The space of elements of degree $(1, n)$ is the simple root space generated by the simple root of degree $(1, n)$. For $i \geq 2$, $\Lambda^i(\mathfrak{n}_+)$ has no elements of degree $(1, n)$, since each element has degree (m, n) for $m \geq 2$. The only elements of $\mathfrak{n}_+$ of degree (m, n) for $n \leq 0$ must be of degree $(1, -1)$. Hence, for an element to be of degree $(m, 0)$, it must be the exterior product of elements of $\mathfrak{n}_+$ of degrees $(1, -1)$ and $(m-1, 1)$. Thus, $H_2(\mathfrak{n}_+)$ is the sum of pieces of the form $M_{m-1,1}$ for $m \geq 2$ and $H_3(\mathfrak{n}_+) = 0$, where $M_{m-1,1}$ is the space of degree $(m-1, 1)$ in $\mathfrak{g}$.

3 Monstrous Moonshine

In this chapter, we give a brief summary of the moonshine conjecture, including an outline of its proof and a proof of a key step using the Weyl-Kac denominator identity. This will primarily follow Richard Borcherds' paper [2].

Monstrous moonshine, also known as the moonshine conjectures, is a conjecture relating the monster group and the elliptic modular function.

The monster group G is the largest of the sporadic finite simple groups, and has order

$$808017424794512875886459904961710757005754368000000000$$
$$= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

The smallest non-trivial irreducible representation of the monster group is of dimension 196883. John McKay first observed that this dimension is one less than the linear coefficient of the elliptic modular function $j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$. Explicitly, the q-expansion of the j-function is given by

$$j(q) = \frac{(1 + 240 \sum_{n>0} \sigma_3(n) q^n)^3}{q \prod_{n>0} (1 - q^n)^2 4},$$

where $\sigma_3(n) = \sum_{d|n} d^3$ is the sum of the cubes of the divisors of n. Thompson then later showed that the other non-constant coefficients of the j-function are simple linear combinations of dimensions of the irreducible representations of M. For instance, $21493760 = 1 + 196883 + 21296876$ and $864299970 = 2 \cdot 1 + 2 \cdot 196883 + 21296876 + 842609326$, where $1, 196883, 21296876, 842609326$ are the degrees of the four smallest irreducible representations of M.

This suggested a deeper connection between the monster group and the j-function. Indeed, Frenkel, Lepowski, and Meurman [3],[4] were able to construct an infinite-dimensional graded representation $V = \oplus_{n \in \mathbb{Z}} V_n$ of the monster. This representation satisfies that the dimension of V_n corresponds with the degree n coefficient of $j(q) - 744$, i.e. $\dim V_n = c(n)$, where $c(n)$ satisfies $j(q) - 744 = \sum_n c(n) q^n$. The moonshine conjecture says that for any element $g \in M$, the Thompson series $T_g(q) = \sum_n \mathrm{Tr}(g|_{V_n}) q^n$ is a Hauptmodul for a genus 0 discrete subgroup of $\mathrm{SL}(2, \mathbb{R})$.

We will now give a very brief outline for the proof of monstrous moonshine, and give a detailed explanation of one step of the proof which uses the Weyl-Kac denominator identity from chapter 2.

Proof Outline:

Step 1. Constructing the Monster Lie algebra. This is a generalized Kac-Moody algebra M satisfying the following:

- M is $\mathbb{Z}^2$-graded. In fact, the root lattice of M forms the standard lattice in the two-dimensional Lorentzian space $II_{1,1}$, i.e. roots are of the form (m,n), $m,n \in \mathbb{Z}$ such that the inner product is given by $((m_1,n_1),(m_2,n_2)) = -m_1n_2 - m_2n_1$.

- M is a representation of G, with $M_{m,n} \cong V_{mn}$ as representations for $(m,n) \neq (0,0)$, and $M_{0,0}$ isomorphic to $\mathbb{R}^2$ as the trivial representation.

The existence of such a Kac-Moody algebra is shown using the no-ghost theorem from string theory. See sections 5 and 6 of [2] for a proof of the no-ghost theorem and a proof of this step. Now, using the Weyl-Kac denominator identity, we may show that the simple roots of M are of the form $(1,n)$ for $n=-1$ or $n \in \mathbb{Z}_{>0}$, and hence is precisely the Kac-Moody algebra described in Example 6.

Step 2. The Thompson series $T_g(\tau)$ is completely replicable. Using the homology of the Monster Lie algebra, we show that $T_g(\tau)$ is completely replicable, in other words satisfies the identity

$$p^{-1}\exp\left(-\sum_{i>0}\sum_{m>0,n\in\mathbb{Z}}\mathrm{Tr}(g^i|_{V_{mn}})p^{mi}q^{ni}/i\right) = \sum_{m\in\mathbb{Z}}\mathrm{Tr}(g|_{V_m})p^m - \sum_{n\in\mathbb{Z}}\mathrm{Tr}(g|_{V_n})q^n$$

in formal variables p, q.

Step 3. Completely replicable functions are Hauptmoduls. This follows by a computation done by Alexander et al. which computes all completely replicable functions with integer coefficients [1]. It can then be shown that all such functions are Hauptmoduls.

We now present a proof of step 2 of the outline. We first prove the fact stated in step 1 about the simple roots of M.

Theorem 3.1. *The simple roots of the monster Lie algebra M are of the form $(1,n)$ for $n=-1$ or $n \in \mathbb{Z}_{>0}$, each with multiplicity $c(n)$.*

We first show the following lemma:

Lemma 3.2. *Let $c(n)$ be the coefficient of q^n in $j(q)-744$. Then,*

$$p^{-1}\prod_{m>0,n\in\mathbb{Z}}(1-p^mq^n)^{c(mn)} = j(p) - j(q). \tag{2}$$

The proof of this lemma uses the notion of the mth Hecke operator T_m. This is defined as follows: for $m \in \mathbb{Z}$ and a Laurent series $f(q) = \sum_{n\in\mathbb{Z}} a(n)q^n$, we define

$$T_m f(q) = \sum_{n\in\mathbb{Z}} \sum_{\substack{k>0 \\ k|m,k|n}} \frac{a(mn/k^2)}{k} q^n.$$

An important property of this operator is that modular functions are sent to modular functions.

We now give a sketch of the proof. Multiplying the left-hand side by p and taking the logarithm gives

$$\begin{aligned}
\sum_{m>0}\sum_{n\in\mathbb{Z}} c(mn)\log(1-p^m q^n) &= -\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{k>0} c(mn)p^{mk}q^{nk}/k \\
&= -\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{\substack{k>0 \\ k|m,k|n}} c(mn/k^2)p^m q^n/k \\
&= -\sum_{m>0} T_m\left(\sum_{n\in\mathbb{Z}} c(n)q^n\right)p^m \\
&= -\sum_{m>0} T_m\left(j(q)-744\right)p^m.
\end{aligned}$$

Let $f_m(q) = T_m(j(q) - 744)$, which is a modular function as stated above, and hence a polynomial in $j(q)$. Taking $\exp$ of the expression above, multiplying by $\mathfrak{p}^{-1}$, and expanding the Taylor series, we may write the left hand side of equation (2) as $\sum_{m\geq -1} g_m(q)p^m$, where each $g_m(q)$ is a polynomial in $j(q)$. On the other hand, each coefficient of p^m on the right-hand side of equation 2 is either constant (when $m \neq 0$) or of the form $744 - j(q)$ (when $m = 0$) and is hence also a polynomial in $j(q)$. Now, any polynomial in $j(q)$ is determined by the coefficients of the terms of non-positive degrees, so we only need to check that the coefficients of q^n for $n \leq 0$ are the same. Yet this is obvious by expanding the product $p^{-1}\prod_{m>0,n\in\mathbb{Z}}(1-p^m q^n)^{c(mn)}$ and computing the coefficients of q^{-1} and q^0.

Proof. (of Theorem 3.1) Let N be the generalized Kac-Moody algebra with root lattice $II_{1,1}$ and simple roots as in the theorem. It suffices to show that the multiplicity of the root (m,n) of N is $c(mn)$. Set $p = e^{(1,0)}$ and $q = e^{(0,1)}$. Applying the denominator identity to N, we get

$$e^\rho \prod_{m>0,n\in\mathbb{Z}} (1-p^m q^n)^{\mathrm{mult}(m,n)} = \sum_{w\in W} \det(w)w(S).$$

We may take $\rho = (-1, 0)$ as in Example 6. This allows us to write $e^\rho = p^{-1}$. Recall $S = e^\rho \sum_s \varepsilon(s) e^s$, where s are elements which can be written as a finite sum of pairwise orthogonal imaginary simple roots. Yet for $n_1, n_2 \in \mathbb{Z}_{>0}$, $((1, n_1), (1, n_2)) = -n_1 - n_2 \neq 0$, so there are no pairwise orthogonal imaginary simple roots. Hence, the sum will be taken over simple imaginary roots $s = (1, n)$, $n \in \mathbb{Z}_{>0}$, and we get

$$\begin{aligned} S &= e^\rho (1 - \sum_{n>0} c(n) p q^n) \\ &= p^{-1}(1 - p(j(q) - q^{-1} - 744)) \\ &= p^{-1} - j(q) + q^{-1} + 744. \end{aligned}$$

The final thing to note is that the Weyl group W of N consists of two elements, where the non-trivial one sends (m, n) to (n, m), and in particular interchanges p and q. Thus, the sum on the right-hand side of the denominator identity becomes

$$(p^{-1} - j(q) + q^{-1} + 744) - (q^{-1} - j(p) + p^{-1} + 744) = j(q) - j(p),$$

which by the previous lemma precisely tells us that $c(mn) = \mathrm{mult}(m, n)$. $\square$

We are now ready to prove step 2.

Proof. The previous lemma allows us to compute the homology groups $H_i(\mathfrak{n}_+)$ for M and their characters. Example 6 tells us that $H_0(\mathfrak{n}_+) = \mathbb{R}$ with character 1, $H_1(\mathfrak{n}_+) = \sum_n V_n p q^n$ with character $\sum_n c(n) p q^n = p(j(q) - 744)$, $H_2(\mathfrak{n}_+) = p \sum_{m>0} V_m p^m$ with character $p(j(p) - 744) - 1$, and $H_i(\mathfrak{n}_+) = 0$ for $i \geq 3$. This tells us that

$$H(\mathfrak{n}_+) = p \left(\sum_m V_m p^m - \sum_n V_n q^n \right).$$

We thus have

$$p^{-1} \Lambda(\mathfrak{n}_+) = \sum_m V_m p^m - \sum_n V_n q^n. \quad (3)$$

We have the natural isomorphism $\Lambda(U) \cong \exp(-\sum_{i>0} \psi^i(U)/i)$ for U finite-dimensional or infinite-dimensional and graded by L (provided that the homogeneous pieces are finite dimensional). ψ^i are the Adams' operations, which are maps of representations determined by the equality $\mathrm{Tr}(g|_{\psi^i(U)}) = \mathrm{Tr}(g^i|_U)$. Taking the g-trace of the equation 3, we get

$$p^{-1} \exp \left(-\sum_i > 0 \sum_{m>0, n \in \mathbb{Z}} \mathrm{Tr}(g^i|_{V_{mn}}) p^{mi} q^{ni}/i \right) = \sum_{m \in \mathbb{Z}} \mathrm{Tr}(g|_{V_m}) p^m - \sum_{n \in \mathbb{Z}} \mathrm{Tr}(g|_{V_n}) q^n,$$

which is exactly the statement that $T_g(\tau)$ is completely replicable. $\square$

Acknowledgements

Special thanks to my advisor Professor Isabel Vogt for her guidance and encouragement. I would also like to thank my peers Ameer Muhialdeen and Semir Mujevic for being great friends, and without whom these past two years would've been much tougher to get through.

References

[1] D. Alexander, C. Cummins, J. McKay, and C. Simons. Completely replicable functions. In *Groups, combinatorics & geometry (Durham, 1990)*, volume 165 of *London Math. Soc. Lecture Note Ser.*, pages 87–98. Cambridge Univ. Press, Cambridge, 1992.

[2] Richard E. Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Invent. Math.*, 109(2):405–444, 1992.

[3] I. B. Frenkel, J. Lepowsky, and A. Meurman. A natural representation of the Fischer-Griess Monster with the modular function J as character. *Proc. Nat. Acad. Sci. U.S.A.*, 81(10):3256–3260, 1984.

[4] Igor Frenkel, James Lepowsky, and Arne Meurman. *Vertex operator algebras and the Monster*, volume 134 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988.

[5] T. Gannon. The algebraic meaning of genus-zero, 2005.

[6] Howard Garland and James Lepowsky. Lie algebra homology and the Macdonald-Kac formulas. *Invent. Math.*, 34(1):37–76, 1976.

[7] Robert L. Griess, Jr. The friendly giant. *Invent. Math.*, 69(1):1–102, 1982.

[8] Victor G. Kac. *Infinite-dimensional Lie algebras*. Cambridge University Press, Cambridge, third edition, 1990.

[9] Alexander Kirillov, Jr. *An introduction to Lie groups and Lie algebras*, volume 113 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2008.

[10] Wikipedia contributors. j-invariant — Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/J-invariant#/media/File:ModularGroup-FundamentalDomain.svg, 2025. [Online; accessed April 30, 2025].