7

Monstrous Moonshine

Thomas Edison once said that to invent you need a good imagination and a pile of junk. Let's see what some imagination can do.

This book has been about *Moonshine*: a diverse collection of points-of-contact between algebra, number theory and mathematical physics, which nevertheless has a common theory. The most remarkable example of Moonshine is surely the association of Hauptmoduls with elements of the Monster $\mathbb{M}$. It is to this we finally turn.

The reader should reread the introductory chapter, which quickly sketches the basics of Monstrous Moonshine. In this chapter we explore this in more detail. The original article [**111**] is still very readable and contains a wealth of information not found in other sources. Other reviews are [**107**], [**410**], [**73**], [**154**], [**412**], [**249**], [**75**], [**469**], [**78**], [**237**] and the introductory chapter in [**201**], and each has its own emphasis.

7.1 The Monstrous Moonshine Conjectures

Recall from the introductory chapter the *McKay equation*

$$196\,884 = 196\,883 + 1. \tag{7.1.1}$$

The number on the left is the first nontrivial coefficient of the j-function, and the numbers on the right are the dimensions of the smallest irreducible representations of the Fischer–Griess Monster $\mathbb{M}$. On the one side, we have a modular function; on the other, a sporadic finite simple group. Monstrous Moonshine explores this completely unexpected connection between finite groups and modular functions.

The world is full of coincidences, and it isn't always clear how seriously they should be regarded. For instance, at the heart of Monstrous Moonshine is a holomorphic $c = 24$ VOA; the conjectured number of holomorphic $c = 24$ VOAs [**488**] is 71, and this is the largest prime dividing $\|\mathbb{M}\|$. There are 26 sporadics, 26 generators in a presentation of the Bimonster discussed shortly, and 26 conjugacy classes in the largest Mathieu group M_{24}. Are any of those numbers related to the 24 of Section 2.5.1, the k-group $\mathbb{Z}_{48}$ of the integers or the number (24) of 24-dimensional even self-dual lattices?[1]

Nor is physics immune to such thoughts. The great physicist Dirac noticed [**140**] that the ratio of the electrostatic to gravitational force between the proton and electron in a

[1] Perhaps this Mathieu group remark is related somehow to the fact that for subgroups G of $\mathrm{SL}_3(\mathbb{C})$, the Euler number of a minimal resolution of the quotient singularity $\mathbb{C}^3/G$ equals the number of conjugacy classes of G [**143**], [**471**].

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

hydrogen atom is a number N of order 10^{40}. He computed that the ratio of the mass of the universe to the mass of a proton is roughly N^2, and that the ratio of the age of the universe with the time needed for light to travel across the classical radius of the electron is again roughly N. One can add that $\sqrt{N}$ is roughly Avagadro's number, so gives a measure of the minimum number of molecules needed in a macroscopic object. Dirac argued that the simple functional relation of these numbers indicates that they are all somehow physically related.

What distinguishes (7.1.1) from some of these other coincidences is that the more it was studied, the more the coincidences multiplied, and the more structure was revealed.

A noble goal for mathematics is surely to find interesting and fundamentally new theorems. Both history and common-sense suggest that to this end it is most profitable to look simultaneously at both exceptional structures and generic structures, to understand the special features of the former in the context of the latter, and to be led in this way to a new generation of exceptional and generic structures. That is the spirit in which Monstrous Moonshine should be studied.

7.1.1 The Monster revisited

Recall the finite simple group classification discussed in Section 1.1.2. The sporadics are summarised in Table 7.1 (its dates are only approximate and the list of investigators is taken from [**109**]). The Monster $\mathbb{M}$ is the largest of these 26 sporadic groups. Its existence was conjectured in 1973 by Fischer and Griess, and finally constructed (somewhat artificially) in 1980 by Griess [**263**]. Tits [**528**] showed that $\mathbb{M}$ is the automorphism group of a 196 883-dimensional commutative non-associative algebra also constructed by Griess and now called the *Griess algebra* (Griess showed only that $\mathbb{M}$ was a subgroup of that automorphism group). We now understand the Griess algebra as the first nontrivial tier (0-mode algebra) of a VOA, the *Moonshine module* $V^\natural$, lying at the heart of Monstrous Moonshine.

The Monster has 194 conjugacy classes, and so that number of irreducible representations. Its character table (and other useful information) is given in the Atlas [**109**], where we also find analogous data for the other simple groups of 'small' order. Table 7.2 gives the upper-left 0.25% or so of the character table of $\mathbb{M}$. The name '4C', for example, is given to the third smallest (hence 'C') conjugacy class of elements of order 4. Table 7.2 tells us that the dimensions of the smallest irreducible representations of $\mathbb{M}$ are 1, 196 883, 21 296 876 and 842 609 326.

The centralisers $C_G(g)$ of conjugate elements are isomorphic (why?). The centralisers for all classes of order up to 11 are given in table 2a of [**111**]. The first few are $C_{\mathbb{M}}(2\mathrm{A}) \cong 2.\mathbb{B}$, $C_{\mathbb{M}}(2\mathrm{B}) \cong 2^{25}.Co_1$, $C_{\mathbb{M}}(3\mathrm{A}) \cong 3.Fi'_{24}$, $C_{\mathbb{M}}(3\mathrm{B}) \cong 3^{13}.2.Suz$, $C_{\mathbb{M}}(3\mathrm{C}) \cong 3 \times Th$. We follow the notation of [**109**]: by, for example, '$2.\mathbb{B}$' we mean a group with $\mathbb{Z}_2$ as a normal subgroup and $\mathbb{B}$ as the quotient, or equivalently an extension of $\mathbb{B}$ by $\mathbb{Z}_2$. Of course the centraliser $C_G(g)$ has $\langle g\rangle$ as a subgroup of its centre, hence $\langle g\rangle$ is normal in $C_G(g)$ – that is, for example, the '2' in $2.\mathbb{B}$. Knowing the centraliser, the sizes of the conjugacy

Table 7.1. *The 26 sporadic groups*

Group	Exact order	Approximate order	Investigators
M_{11}	$2^4.3^2.5.11$	7.9×10^3	Mathieu (1861, 1873)
M_{12}	$2^6.3^3.5.11$	9.5×10^4	Mathieu (1861, 1873)
J_1	$2^3.3.5.7.11.19$	1.8×10^5	Janko (1965)
M_{22}	$2^7.3^2.5.7.11$	4.4×10^5	Mathieu (1861, 1873)
J_2	$2^7.3^3.5^2.7$	6.0×10^5	Hall, Janko (1960s)
M_{23}	$2^7.3^2.5.7.11.23$	1.0×10^7	Mathieu (1861, 1873)
HS	$2^9.3^2.5^3.7.11$	4.4×10^7	Higman, Sims (1968)
J_3	$2^7.3^5.5.17.19$	5.0×10^7	Janko, Higman, McKay (1960s)
M_{24}	$2^{10}.3^3.5.7.11.23$	2.4×10^8	Mathieu (1861, 1873)
McL	$2^7.3^6.5^3.7.11$	9.0×10^8	McLaughlin (1969)
He	$2^{10}.3^3.5^2.7^3.17$	4.0×10^9	Held, Higman, McKay (1960s)
Ru	$2^{14}.3^3.5^3.7.13.29$	1.5×10^{11}	Rudvalis, Conway, Wales (1973)
Suz	$2^{13}.3^7.5^2.7.11.13$	4.5×10^{11}	Suzuki (1969)
$O'N$	$2^9.3^4.5.7^3.11.19.31$	4.6×10^{11}	O'Nan, Sims (1970s)
Co_3	$2^{10}.3^7.5^3.7.11.23$	5.0×10^{11}	Conway (1968)
Co_2	$2^{18}.3^6.5^3.7.11.23$	4.2×10^{13}	Conway (1968)
Fi_{22}	$2^{17}.3^9.5^2.7.11.13$	6.5×10^{13}	Fischer (1970s)
HN	$2^{14}.3^6.5^6.7.11.19$	2.7×10^{14}	Harada, Norton, Smith (1975)
Ly	$2^8.3^7.5^6.7.11.31.37.67$	5.2×10^{16}	Lyons, Sims (1972)
Th	$2^{15}.3^{10}.5^3.7^2.13.19.31$	9.1×10^{16}	Thompson, Smith (1975)
Fi_{23}	$2^{18}.3^{13}.5^2.7.11.13.17.23$	4.1×10^{18}	Fischer (1970s)
Co_1	$2^{21}.3^9.5^4.7^2.11.13.23$	4.2×10^{18}	Conway, Leech (1968)
J_4	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$	8.7×10^{19}	Janko, Norton, Parker, Benson, Conway, Thankray (1970s)
Fi'_{24}	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$	1.3×10^{24}	Fischer (1970s)
$\mathbb{B}$	$2^{41}.3^{13}.5^6.7^2$ $.11.13.17.19.23.31.47$	4.2×10^{33}	Fischer, Sims, Leon (1970s)
$\mathbb{M}$	$2^{46}.3^{20}.5^9.7^6.11^2.13^3$ $.17.19.23.29.31.41.47.59.71$	8.1×10^{53}	Fischer, Griess (1973, 1982)

classes can be quickly determined through the formula $\|K_g\| = \|\mathbb{M}\|/\|C_{\mathbb{M}}(g)\|$. These centralisers play a large role in Section 7.3 below.

The Monster $\mathbb{M}$ has a remarkably simple presentation. As with any noncyclic finite simple group, it is generated by its involutions (i.e. elements of order 2) and so is a homomorphic image of a Coxeter group (Definition 3.2.1) – see Question 7.1.1.

Let $\mathcal{G}_{pqr}$, $p \geq q \geq r \geq 2$, be the graph consisting of three strands of lengths $p+1, q+1, r+1$, sharing a common endpoint. Label the $p+q+r+1$ nodes as in Figure 7.1 (this labelling is not standard). Given any graph $\mathcal{G}_{pqr}$, define Y_{pqr} to be the group consisting of a generator for each node, obeying the usual Coxeter group relations, together with an additional one (what Conway calls the 'spider relation'):

$$(ab_1b_2ac_1c_2ad_1d_2)^{10} = 1. \tag{7.1.2}$$

The relation (7.1.2) arises naturally in a generalisation of the Coxeter group due to Conway, called a *fabulous group*. Conway conjectured and, building on work by

Table 7.2. *The north-west corner of the Monster character table*

ch$\backslash K_g$	1A	2A	2B	3A	3B	3C	4A	4B	4C	4D	5A	5B
ρ_0	1	1	1	1	1	1	1	1	1	1	1	1
ρ_1	196883	4371	275	782	53	−1	275	51	19	−13	133	8
ρ_2	21296876	91884	−2324	7889	−130	248	1772	−52	−20	12	626	1
ρ_3	842609326	1139374	12974	55912	−221	−248	8878	782	−82	78	2451	−49
ρ_4	18538750076	8507516	123004	249458	1598	248	28796	2652	380	156	6326	76
ρ_5	19360062527	9362495	−58305	297482	1508	−247	35903	−833	63	−65	8152	27
ρ_6	293553734298	53981850	98970	1055310	−3927	3876	94874	1274	−102	−454	17423	−77
ρ_7	3879214937598	337044990	−690690	4751823	−4173	−3876	345598	−3874	−258	286	54473	98
ρ_8	36173193327999	1354188159	2864511	12616074	18954	0	701823	20383	−897	351	91124	−126
ρ_9	125510727015275	3215883115	1219435	24688454	−25375	248	1223531	19499	−661	−1365	145275	−350

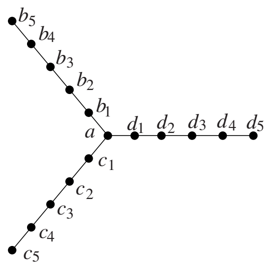

Fig. 7.1 The graph $\mathcal{G}_{555}$ presenting the Bimonster.

Ivanov [**311**], Norton proved [**451**] that $Y_{555} \cong Y_{444}$ is the *Bimonster*, the wreathed-square $\mathbb{M} \wr \mathbb{Z}_2 \cong (\mathbb{M} \times \mathbb{M}).2$ of the Monster (in fact it is a semi-direct product $(\mathbb{M} \times \mathbb{M}) \rtimes \mathbb{Z}_2$). We define the wreath product in Question 7.1.2; the wreathed-square $\mathbb{M} \wr \mathbb{Z}_2$ has $G = \mathbb{M}$ and $H = S = \mathbb{Z}_2$, where H acts on S by group multiplication. The group-theoretic significance of the wreath product is that any group G containing a normal subgroup N with quotient $G/N \cong H$ can be identified with a subgroup of $N \wr H$ with $S = H$. Thus any extension $\mathbb{M}.2$ of $\mathbb{Z}_2$ by $\mathbb{M}$ is a subgroup of the Bimonster. The Bimonster appears naturally in Section 7.3.9. A closely related presentation of the Bimonster has 26 involutions as generators and has relations given by the incidence graph of the projective plane of order 3; the Monster itself arises from 21 involutions and the affine plane of order 3. See [**112**] for details.

The groups Y_{pqr}, for $p \leq 5$, have now all been identified – see [**312**] for a unified treatment. The ones involving sporadic groups are

$$\begin{aligned}
Y_{553} &\cong Y_{443} \cong \mathbb{M} \times \mathbb{Z}_2,\\
Y_{533} &\cong Y_{433} \cong \mathbb{Z}_2 \times (2.\mathbb{B}),\\
Y_{552} &\cong Y_{442} \cong 3.(Fi'_{24}.2),\\
Y_{532} &\cong Y_{432} \cong \mathbb{Z}_2 \times Fi_{23},\\
Y_{332} &\cong \mathbb{Z}_2 \times (2.Fi_{22}).
\end{aligned}$$

The Coxeter groups of the graphs $\mathcal{G}_{555}$, $\mathcal{G}_{553}$, $\mathcal{G}_{533}$, $\mathcal{G}_{552}$ and $\mathcal{G}_{532}$ are all infinite groups of hyperbolic reflections in, for example, $\mathbb{R}^{17,1}$, and contain copies of groups such as the affine E_8 Weyl group, so there should be rich geometry here.

What role, if any, these remarkable presentations have in Monstrous Moonshine hasn't been established yet. As a first step though, [**424**] has found in the automorphism group of the Moonshine module $V^\natural$ the 21 involutions generating $\mathbb{M}$. Perhaps this can simplify the hardest part of [**201**] (see Section 7.2.1 below). Indeed, Miyamoto's simplified construction [**427**] of $V^\natural$ and proof that $\mathrm{Aut}(V^\natural) \cong \mathbb{M}$ uses Ivanov's characterisation [**311**] of $\mathbb{M}$. There is a correspondence [**425**] between certain involutions of a VOA $\mathcal{V}$ (e.g. class 2A in $\mathbb{M}$ for $V^\natural$) and certain vertex operator subalgebras of $\mathcal{V}$ isomorphic to the unique $c = 1/2$ rational VOA (the Ising model of Section 4.3.2); this technical tool has many applications, for example the association of various vertex operator superalgebras to $V^\natural$, and the VOA interpretation of McKay's $E_8{}^{(1)}$ observation in Section 7.3.6.

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

7.1.2 Conway and Norton's fundamental conjecture

As mentioned in the introductory chapter, the central structure in the attempt to understand equations (0.2.1) is an infinite-dimensional graded module for the Monster, $V = V_{-1} \oplus V_1 \oplus V_2 \oplus \cdots$, with graded dimension $J(\tau) = j(\tau) - 744$ (see (0.3.2)). If we let ρ_d denote the dth smallest irreducible $\mathbb{M}$-module, numbered as in Table 7.2, then the first few subspaces will be $V_0 = \rho_0$, $V_1 = \{0\}$, $V_2 = \rho_0 \oplus \rho_1$, $V_3 = \rho_0 \oplus \rho_1 \oplus \rho_2$ and $V_4 = \rho_0 \oplus \rho_0 \oplus \rho_1 \oplus \rho_1 \oplus \rho_2 \oplus \rho_3$. As we know from Section 1.1.3, a dimension can (and should) be twisted, by replacing it with the character. This gives us the graded traces

$$T_g(\tau) := \mathrm{ch}_{V_{-1}}(g)\, q^{-1} + \sum_{n=1}^{\infty} \mathrm{ch}_{V_n}(g)\, q^n, \tag{7.1.3}$$

called the *McKay–Thompson series* for this module V. Of course, $T_e = J$.

Conjecture 7.1.1 (Conway–Norton [111]) *There exists a graded $\mathbb{M}$-module V such that, for each element g of the Monster $\mathbb{M}$, the McKay–Thompson series T_g is the Hauptmodul*

$$J_{\Gamma_g}(\tau) = q^{-1} + \sum_{n=1}^{\infty} a_n(g)\, q^n \tag{7.1.4}$$

for a genus-0 group Γ_g of Moonshine-type. These groups each contain $\Gamma_0(N)$ as a normal subgroup, for some N dividing $o(g)\,\mathrm{gcd}(24, o(g))$, and the quotient group $\Gamma_g/\Gamma_0(N)$ has exponent ≤ 2.

So for each n the map $g \mapsto a_n(g)$ is a character $\mathrm{ch}_{V_n}(g)$ of $\mathbb{M}$. The quantity $o(g)$ is the order of g. We defined the groups of Moonshine-type in Definition 2.2.4 and $\Gamma_0(N)$ in (2.2.4b). By the exponent of a group we mean the smallest positive m such that $h^m = 1$ for all h in the group. [**111**] explicitly identify each of the groups Γ_g. The first 50 coefficients $a_n(g)$ of each T_g are given in [**413**]. Together with the recursions given in Section 7.1.4 below, this allows one to effectively compute arbitrarily many coefficients $a_n(g)$ of the Hauptmoduls. It is also this that uniquely defines V, up to equivalence, as a graded $\mathbb{M}$-module.

There are around 8×10^{53} elements in the Monster, so naively we may expect about 8×10^{53} different Hauptmoduls T_g. However, a character evaluated at g and at hgh^{-1} will always be equal, so $T_g = T_{hgh^{-1}}$. Hence there can be at most 194 distinct T_g (one for each conjugacy class). All coefficients $a_n(g)$ are integers (as are in fact most entries of the character table of $\mathbb{M}$). This implies that $T_g = T_h$ whenever the cyclic subgroups $\langle g \rangle$ and $\langle h \rangle$ are equal (why?). In fact, the total number of distinct McKay–Thompson series T_g arising in Monstrous Moonshine turns out to be only 171.

Of those many redundancies among the T_g, only one is unexpected (and unexplained): the McKay–Thompson series of two unrelated classes of order 27, namely 27A and 27B, are equal. It would be interesting to understand what general phenomenon (if any) is responsible for $T_{27\mathrm{A}}(\tau) = T_{27\mathrm{B}}(\tau)$. But as we know from Section 5.3.3, the McKay–Thompson series $T_g(\tau)$ are actually specialisations of 1-point functions and as such are functions of not only τ but of all $\mathbb{M}$-invariant vectors v in $V^\natural$. What we call $T_g(\tau)$

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

is really the specialisation $T_g(\tau, \mathbf{1})$ of this function $T_g(\tau, v)$. All 194 T_g (one for each conjugacy class) will be linearly independent, if we include this $v \in (V^\natural)^{\mathbb{M}}$ dependence. Thus the equality $T_{27\mathrm{A}}(\tau) = T_{27\mathrm{B}}(\tau)$ should be regarded as an accidental redundancy caused by specialisation, and is not of any deep significance. Plenty of other Norton's series $N_{(g,h)}(\tau)$ (Section 7.3.2) will likewise be accidentally equal. Modular aspects of the 1-point functions $T_g(\tau, v)$ are studied in [**155**].

Recall that there are two different conjugacy classes of order 2 elements: 2A and 2B. Class 2B corresponds to $\Gamma_0(2)$ and gives the Hauptmodul J_2 in (2.2.17a), while class 2A corresponds to $\Gamma_0(2)+$, where for any prime p we define

$$\Gamma_0(p)+ := \left\langle \Gamma_0(p), \frac{1}{\sqrt{p}} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \right\rangle. \tag{7.1.5}$$

Similarly, (2.2.17b) corresponds to an order 13 element in $\mathbb{M}$, but J_{25} in (2.2.17c) doesn't equal any T_g. Recall that there are exactly 616 Hauptmoduls of Moonshine-type with integer coefficients [**121**], so most of these don't arise as T_g. Recently [**110**], a fairly simple characterisation has been found of the groups arising as Γ_g in Monstrous Moonshine:

Proposition 7.1.2 [**110**] *A subgroup G of* $\mathrm{SL}_2(\mathbb{R})$ *equals one of the modular groups Γ_g appearing in Conjecture 7.1.1, iff:*

(i) *G is genus* 0*;*
(ii) *G has the form '* $\Gamma_0(n||h) + e, f, g, \ldots$*';*
(iii) *the quotient of G by $\Gamma_0(nh)$ is a group of exponent ≤ 2; and*
(iv) *each cusp $\mathbb{Q} \cup \mathrm{i}\infty$ can be mapped to $\mathrm{i}\infty$ by an element of* $\mathrm{SL}_2(\mathbb{R})$ *that conjugates the group to one containing $\Gamma_0(nh)$.*

The notation in (ii) is a little too technical to explain here, but it is given in [**111**] or [**110**]. We now understand the significance, in the VOA or CFT framework, of transformations in $\mathrm{SL}_2(\mathbb{Z})$ (see especially Section 5.3.6), but (ii) emphasises that many modular transformations relevant to Moonshine are more general (called *Atkin–Lehner involutions*). Monstrous Moonshine will remain mysterious until we can understand its Atkin–Lehner symmetries. This isn't a hopeless task – for example, [**433**] provides an early attempt at studying string theories with Atkin–Lehner symmetries, as well as its possible physical significance. Some of these involutions appear naturally in Weil's Converse Theorem (see e.g. page 64 of [**90**]). Perhaps a topological interpretation for the groups Γ_g not contained in $\mathrm{SL}_2(\mathbb{Z})$, in the spirit of Section 2.4.3, will help us understand their relevance in VOAs and the meaning of Atkin–Lehner involutions to CFT. This proposition is the answer to an important question, but unfortunately their proof of this characterisation is by exhaustion, and so by itself doesn't contribute anything conceptually.

7.1.3 E_8 and the Leech

There are other less important conjectures in [**111**]. We've already seen easy-to-understand relations of E_8 and the Leech lattice Λ to the J-function: (0.5.1) (explained

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

in Section 3.2.3) and (0.5.2) (explained in Question 2.2.7). There is another way E_8 and Λ can be related to modular functions.

Lattices are related to groups through their automorphism groups, which are always finite for positive-definite lattices. The automorphism group $\mathrm{Aut}(\Lambda) = Co_0$ of the Leech lattice has order about 8×10^{18}, and is a central extension by $\mathbb{Z}_2$ of Conway's simple group Co_1. Several other sporadic groups are also involved in Co_0, as we'll see in Section 7.3.1. To each automorphism $\alpha \in Co_0$, let θ_α denote the theta function of the sublattice of Λ fixed by α. Conway–Norton also associate with each automorphism α a certain function $\eta_\alpha(\tau)$ of the form $\prod_i \eta(a_i\tau)/\prod_j \eta(b_j\tau)$ built out of the Dedekind eta function (2.2.6b). Both θ_α and η_α are constant on each conjugacy class in Co_0, of which there are 167. [**111**] remarks that the ratio $\theta_\alpha/\eta_\alpha$ always seems to equal some McKay–Thompson series $T_{g(\alpha)}$.

It turns out that this observation isn't quite correct [**366**]. For each automorphism $\alpha \in Co_0$, the subgroup of $\mathrm{SL}_2(\mathbb{R})$ that fixes $\theta_\alpha/\eta_\alpha$ is indeed always genus 0, but for exactly 15 conjugacy classes in Co_0, $\theta_\alpha/\eta_\alpha$ is not the Hauptmodul. Nevertheless, this construction proved useful for establishing Moonshine for M_{24} [**407**].

Similarly, one can ask this for the E_8 root lattice, whose automorphism group is the Weyl group of the Lie algebra E_8 (of order 696 729 600). The automorphisms of the lattice E_8 that yield a Hauptmodul were classified in [**95**]. On the other hand, Koike established a Moonshine of this kind for the groups $\mathrm{PSL}_2(\mathbb{F}_7)$, $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathcal{A}_5$ and $\mathrm{PSL}_2(\mathbb{F}_3)$, of order 168, 60 and 12, respectively [**356**].

7.1.4 Replicable functions

A conjecture in [**111**] that played an important role in ultimately proving the main conjecture involves the *replication formulae*. Conway–Norton want to think of the Hauptmoduls T_g as being intimately connected with $\mathbb{M}$; if so, then the group structure of $\mathbb{M}$ should somehow directly relate different T_g. Considering the power map $g \mapsto g^n$ leads to the following.

It was well known classically that $J(\tau)$ (equivalently, $j(\tau)$) has the property that

$$s(\tau) := J(p\tau) + J\left(\frac{\tau}{p}\right) + J\left(\frac{\tau+1}{p}\right) + \cdots + J\left(\frac{\tau+p-1}{p}\right) \qquad (7.1.6a)$$

is a polynomial in $J(\tau)$, for any prime p. The proof is straightforward, and is based on the principle that the easiest way to construct a function invariant with respect to some group G is by averaging it over the group: $\sum_{g\in G} f(g.x)$. Here $f(x)$ is $J(p\tau)$ and G is $\mathrm{SL}_2(\mathbb{Z})$, and we'll average over finitely many cosets rather than infinitely many elements. First, writing Γ for $\mathrm{SL}_2(\mathbb{Z})$, note that

$$\Gamma\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}\Gamma = \begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}\Gamma \cup \bigcup_{i=0}^{p-1}\begin{pmatrix} 1 & i \\ 0 & p\end{pmatrix}\Gamma = \{A \in M_{2\times 2}(\mathbb{Z}) \mid \det(A) = p\}. \qquad (7.1.6b)$$

In Question 7.1.4 you show that this implies (7.1.6a) is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. Hence $s(\tau)$ equals a rational function $Q(J(\tau))/P(J(\tau))$ of $J(\tau)$, as in (0.1.7). Because the only poles of J are at the cusps, the same applies to $s(\tau)$. This implies that the denominator polynomial $P(z)$ must be trivial (recall that $J(\mathbb{H}) = \mathbb{C}$). QED

The map $J(\tau) \mapsto s(\tau)$ in (7.1.6a) is called a 'Hecke operator', and is an important ingredient of modular theory. More generally, the same argument says

$$\sum_{ad=n, 0\leq b<d} J\left(\frac{a\tau+b}{d}\right) = Q_n(J(\tau)), \tag{7.1.7}$$

where Q_n is the unique polynomial for which $Q_n(J(\tau)) - q^{-n}$ has a q-expansion with only strictly positive powers of q. For example, $Q_2(x) = x^2 - 2a_1$ and $Q_3(x) = x^3 - 3a_1x - 3a_2$, where we write $J(\tau) = \sum_n a_n q^n$. These equations (7.1.7) can be rewritten into recursions such as $a_4 = a_3 + (a_1^2 - a_1)/2$, or collected together into the remarkable expression (3.4.7a).

Conway and Norton conjectured that these formulae have an analogue for any McKay–Thompson series T_g. In particular, (7.1.7) becomes

$$\sum_{ad=n, 0\leq b<d} T_{g^a}\left(\frac{a\tau+b}{d}\right) = Q_{n,g}(T_g(\tau)), \tag{7.1.8a}$$

where $Q_{n,g}$ plays the same role for T_g that Q_n plays for J. For example, we get

$$T_{g^2}(2\tau) + T_g\left(\frac{\tau}{2}\right) + T_g\left(\frac{\tau+1}{2}\right) = T_g(\tau)^2 - 2a_1(g),$$

$$T_{g^3}(3\tau) + T_g\left(\frac{\tau}{3}\right) + T_g\left(\frac{\tau+1}{3}\right) + T_g\left(\frac{\tau+2}{3}\right) = T_g(\tau)^3 - 3a_1(g)\,T_g(\tau) - 3a_2(g).$$

These are called the replication formulae. Again, these yield recursions like $a_4(g) = a_2(g) + (a_1(g)^2 - a_1(g^2))/2$, or can be collected into the expression

$$p^{-1}\exp\left[-\sum_{k>0}\sum_{\substack{m>0\\ n\in\mathbb{Z}}} a_{mn}(g^k)\frac{p^{mk}q^{nk}}{k}\right] = T_g(z) - T_g(\tau). \tag{7.1.8b}$$

This looks a lot more complicated than (3.4.7a), but you can glimpse the Taylor expansion of $\log(1 - p^m q^n)$ there and in fact for $g = e$, (7.1.8b) reduces to (3.4.7a).

Axiomatising (7.1.8a) leads to Conway and Norton's notion of *replicable function* [**449**], [**6**].

Definition 7.1.3 *Let f be any function of the form $f(\tau) = q^{-1} + \sum_{n=1}^{\infty} b_n q^n$, and write $f^{(1)} = f$ and $b_n^{(1)} = b_n$. Let $Q_{n,f}$ be the unique (degree n) polynomial such that the q-expansion of $Q_{n,f}(f(\tau)) - q^{-n}$ has only positive powers of q. Use*

$$\sum_{ad=n, 0\leq b<d} f^{(a)}\left(\frac{a\tau+b}{d}\right) = Q_{n,f}\big(f^{(1)}(\tau)\big), \tag{7.1.9}$$

to recursively define each $f^{(n)}$. If each $f^{(n)}$ has a q-expansion of the form $f^{(n)}(\tau) = q^{-1} + \sum_{k=1}^{\infty} b_k^{(n)} q^k$ – that is, no fractional powers of q arise – then we call f replicable.

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

Proposition 7.1.4 [**6**] *Suppose f is of the form $f(\tau) = q^{-1} + \sum_{n=1}^{\infty} a_n q^n$, and define $Q_{n,f}$ as in Definition 7.1.3. Define $H_{m,n}$ by*

$$Q_{n,f}(f(\tau)) = q^{-n} + \sum_{n=1}^{\infty} n H_{n,m}\, q^m.$$

Then f is replicable iff $H_{n,m} = H_{r,s}$ holds whenever $mn = rs$ and $\gcd(n, m) = \gcd(r, s)$.

The proof isn't hard: if f is replicable, with replicates $f^{(n)} = q^{-1} + \sum_k a_k^{(n)} q^k$, then

$$H_{n,m} = \sum_{d|\gcd(n,m)} \frac{1}{d} a^{(d)}_{nm/d^2}$$

and the $H_{n,m} = H_{r,s}$ property is manifest. See Question 7.1.5 for the converse.

Equation (7.1.8a) conjectures that the McKay–Thompson series are replicable. In particular, we have $(T_g)^{(n)}(\tau) = T_{g^n}(\tau)$. [**123**] proved that the Hauptmodul of any genus-0 modular group of Moonshine-type is replicable, provided its coefficients are rational. Incidentally, if the coefficients $b_k^{(1)}$ are irrational, then Definition 7.1.3 should be modified to include Galois automorphisms (see section 8 of [**114**]). Replication in positive genus is discussed in [**510**].

Conversely, Norton has conjectured:

Conjecture 7.1.5 *Any replicable function with rational coefficients is either a Hauptmodul for a genus-0 modular group of Moonshine-type, or is one of the 'modular fictions' $f(\tau) = q^{-1} = \exp[-2\pi i \tau]$, $f(\tau) = q^{-1} + q = 2\cos[2\pi\tau]$, $f(\tau) = q^{-1} - q = -2i\sin[2\pi\tau]$.*

This conjecture seems difficult and is still open.

As is manifest in (7.1.8a), replication concerns the power map $g \mapsto g^n$ in $\mathbb{M}$. Can Moonshine see more of the group structure of $\mathbb{M}$? One step in this direction is explored in Section 7.3.6, where McKay models products of conjugacy classes using Coxeter–Dynkin diagrams. A different idea is given in Section 7.3.2. It would be very desirable to find other direct connections between the group operation in $\mathbb{M}$ and, for example, the McKay–Thompson series.

Question 7.1.1. Let G be a finite simple group, and let $K \neq \{e\}$ be any nontrivial conjugacy class. Prove that K generates G. Why is any noncyclic finite simple group a homomorphic image of a (possibly infinite) Coxeter group?

Question 7.1.2. Let G, H be any groups, and S any finite set on which H acts. By the wreath product $G \wr H$ we mean the set of all pairs (f, h), where f is any function from $S \to G$ and $h \in H$. Group multiplication is given by $(f, h)(f', h') = (f'', hh')$, where $f'' : S \to G$ is defined by $f''(s) = f(s) f'(h^{-1}.s)$.
(a) Verify that $G \wr H$ is a group. Compute its order.
(b) Find a normal subgroup in $G \wr H$, isomorphic to $G \times \cdots \times G$ ($\|S\|$ times). Identify the quotient of $G \wr H$ by this normal subgroup.
(c) Find a subgroup of $G \wr H$ isomorphic to H.

Question 7.1.3. Note that the dimensions 196 883 and 21 296 876 – see (0.2.1) – exactly divide the order of the Monster – see (0.2.2). Is this (i) merely a coincidence; (ii) a mysterious property of $\mathbb{M}$ perhaps relevant to Moonshine; or (iii) does it have a more mundane explanation?

Question 7.1.4. Prove (7.1.6b). Use that to prove that the sum $s(\tau)$ in (7.1.6a) is invariant under $\mathrm{SL}_2(\mathbb{Z})$.

Question 7.1.5. Complete the proof of Proposition 7.1.4.

Question 7.1.6. Suppose $f(\tau) = q^{-1} + \sum_{k=1}^{N} a_k q^k$ is a replicable Laurent polynomial. Prove that f is a modular fiction: $f(\tau) = q^{-1}$ or $f(\tau) = q^{-1} \pm q$.

Question 7.1.7. As we know from Section 3.2.3, $j^{\frac{1}{3}}$ is the graded dimension of the $E_8{}^{(1)}$-module $L(\omega_0)$. Thus j is the graded dimension of $L(\omega_0) \otimes L(\omega_0) \otimes L(\omega_0)$, on which the Lie group $(E_8(\mathbb{C}) \times E_8(\mathbb{C}) \times E_8(\mathbb{C})) \rtimes \mathcal{S}_3$ acts. Explain why $L(\omega_0) \otimes L(\omega_0) \otimes L(\omega_0)$ cannot be the $\mathbb{M}$-module V whose graded characters (7.1.3) are the McKay–Thompson series (ignoring the irrelevant constant 744).

7.2 Proof of the Monstrous Moonshine conjectures

At first glance, any deep significance to the Moonshine conjectures seems very unlikely: they constitute after all a finite set of very specialised coincidences. The whole point though is to try to understand *why* such seemingly incomparable objects as the Monster and the Hauptmoduls can be so related, and to try to extend and apply this understanding to other contexts. Establishing the truth (or falsity) of the conjectures was merely meant as an aid to uncovering the meaning of Monstrous Moonshine. Indeed, in proving them, important new algebraic structures were formulated. We sketch this proof in this section.

The main Conway–Norton conjecture was attacked almost immediately. Thompson showed [**524**] (see also [**476**]) that if $g \mapsto a_n(g)$ is a character for all sufficiently small n (apparently $n \leq 1300$ is sufficient), then it will be for all n. He also showed that if certain congruence conditions hold for a certain number of $a_n(g)$ (all with $n \leq 100$), then all $g \mapsto a_n(g)$ will be *virtual* characters (i.e. differences of true characters of $\mathbb{M}$). Atkin, Fong and Smith (see [**511**] for details) used that and a computer to prove that indeed all $a_n(g)$ were virtual characters (they didn't quite get to $n = 1300$ though). But their work doesn't say anything more about the underlying (possibly virtual) representation V, other than its existence, and so adds no light to Moonshine. It plays no role in the following.

We want to prove Conjecture 7.1.1, that is, show that the McKay–Thompson series $T_g(\tau)$ of (7.1.3) equals the Hauptmodul $J_{\Gamma_g}(\tau)$ in (7.1.4). First, we need to construct the infinite-dimensional module V of $\mathbb{M}$. This we discuss in Section 7.2.1. Borcherds' strategy was to bring in Lie theory, by associating with the module V a 'Monster Lie algebra'. This example of a Borcherds–Kac–Moody algebra is described in Section 7.2.2. Next, we go from the Monster Lie algebra to the replication formula, and conclude the

Table 7.3. *The first few homogeneous spaces of the Moonshine module $V^\natural$*

	$\mathbb{M}$-module
$V_0^\natural$	ρ_0
$V_1^\natural$	0
$V_2^\natural$	$\rho_0 \oplus \rho_1$
$V_3^\natural$	$\rho_0 \oplus \rho_1 \oplus \rho_2$
$V_4^\natural$	$2\rho_0 \oplus 2\rho_1 \oplus \rho_2 \oplus \rho_3$
$V_5^\natural$	$2\rho_0 \oplus 3\rho_1 \oplus 2\rho_2 \oplus \rho_3 \oplus \rho_5$
$V_6^\natural$	$4\rho_0 \oplus 5\rho_1 \oplus 3\rho_2 \oplus 2\rho_3 \oplus \rho_4 \oplus \rho_5 \oplus \rho_6$
$V_7^\natural$	$4\rho_0 \oplus 7\rho_1 \oplus 5\rho_2 \oplus 3\rho_3 \oplus \rho_4 \oplus 3\rho_5 \oplus \rho_6 \oplus \rho_7$
$V_8^\natural$	$7\rho_0 \oplus 11\rho_1 \oplus 7\rho_2 \oplus 6\rho_3 \oplus 3\rho_4 \oplus 4\rho_5 \oplus 2\rho_6 \oplus 2\rho_7 \oplus \rho_8$

proof. In the final subsection, we explain the need for a second proof, and suggest what it may involve.

Thanks largely to Borcherds, the Monstrous Moonshine conjectures opened a door to mathematical riches far beyond what Conway and Norton could have originally hoped. For his work in Monstrous Moonshine and related topics, Richard Borcherds was awarded the Fields medal in 1998.

7.2.1 The Moonshine module $V^\natural$

The first essential step in the proof of the Monstrous Moonshine conjectures was the construction by Frenkel–Lepowsky–Meurman [**200**] of a graded infinite-dimensional representation $V^\natural$ of $\mathbb{M}$. They conjectured (correctly) that it is the representation V in (0.3.1). As we know, $V^\natural$ has a very rich algebraic structure: it is in fact a VOA. A somewhat simpler construction of $V^\natural$ is now available [**427**]; in particular, the fundamental fact that $\mathrm{Aut}(V^\natural) \cong \mathbb{M}$ seems much clearer.

Each homogeneous space $V_n^\natural$ of $V^\natural$ is a finite-dimensional $\mathbb{M}$-module – see Table 7.3. Being a finite group, $\mathbb{M}$ only has finitely many (in fact exactly 194) irreducible representations, whereas $J(\tau)$ has infinitely many coefficients a_n, which grow polynomially with n. As can already be observed in the table, the decompositions of $V_n^\natural$ into irreducible $\mathbb{M}$-modules become increasingly complicated, with ever-increasing multiplicities. Thus the fact that 196 884 almost equals 196 883 is of no special significance, other than that it made it easier to anticipate that j and $\mathbb{M}$ are related.

Now, $V^\natural$ was constructed before VOAs had been defined. It was natural for Frenkel–Lepowsky–Meurman to use vertex operators to try to construct the $\mathbb{M}$-module V of (0.3.1), because there were already vertex operator constructions associated with lattices, affine algebra modules and string theory, and all of these have connections to modular functions. Borcherds' definition [**68**] of vertex algebras abstracted out algebraic properties of $V^\natural$ as well as those older vertex operator constructions.

As we discuss in Sections 4.3.4 and 5.3.6, the Moonshine module $V^\natural$ was constructed as the orbifold of the Leech lattice VOA $\mathcal{V}(\Lambda)$ by the ± 1-symmetry of Λ – more precisely, by an involution in $\mathrm{Aut}(\mathcal{V}(\Lambda))$ restricting to the automorphism -1 of Λ. This orbifold construction implies that $V^\natural$ is the direct sum of an invariant part $V^\natural_+ := \mathcal{V}(\Lambda)^1_+$ and a twisted part $V^\natural_- := \mathcal{V}(\Lambda)^{-1}_+$ (recall (4.3.16)). The underlying vector spaces can be (and usually are) chosen to be real, and in fact later we speculate that they can be taken to be $\mathbb{Z}$-modules (Conjecture 7.3.3).

The orbifold serves two purposes. First, it removes the constant term '24' from the graded dimension $J + 24$ of $\mathcal{V}(\Lambda)$. This means that the Lie algebra $V^\natural_1$ vanishes, giving $V^\natural$ a chance to have a finite automorphism group (Section 5.2.1). Second, this orbifold construction enhances the symmetry from the discrete part of $\mathrm{Aut}(\mathcal{V}(\Lambda))$, which is an extension of Co_0 by $(\mathbb{Z}_2)^{24}$, to all of $\mathbb{M}$. In particular, that discrete part of $\mathrm{Aut}(\mathcal{V}(\Lambda))$ preserves the decomposition $V^\natural = V^\natural_+ \oplus V^\natural_-$ and is isomorphic to the centraliser $C_{\mathbb{M}}(2\mathrm{B})$. An additional automorphism of $V^\natural$, an involution σ mixing $V^\natural_\pm$ and related to 'triality', was constructed by hand. A theorem of Griess [**263**] shows that together they generate $\mathbb{M}$. See [**201**] for more details. Establishing this symmetry enhancement is the most difficult part of [**201**].

A major claim of [**201**] is that $V^\natural$ is a 'natural' structure (hence their notation). This has been uncontested. We have $V^\natural_0 = \mathbb{C}\mathbf{1}$, as usual, and $V^\natural_1 = 0$. Hence the space $V^\natural_2$ will be a commutative non-associative algebra with product $u \times v := u_1 v$ and identity $\frac{1}{2}\omega$ (Question 5.2.3). In fact, it is the 196 883-dimensional Griess algebra [**263**] extended by an identity element, which is known to have automorphism group exactly $\mathbb{M}$ [**528**]. Using this, the automorphism group of $V^\natural$ can be seen to equal the Monster $\mathbb{M}$. The only irreducible module for $V^\natural$ is itself – such a VOA is called holomorphic (Section 5.3.1). Together with Zhu's Theorem 5.3.8, this implies that its graded dimension must be a modular function for $\mathrm{SL}_2(\mathbb{Z})$, and in fact $j(\tau) - 744$ (Question 5.3.4).

All arguments relating $V^\natural$ to $\mathbb{M}$ are complicated by the bipartite structure $V^\natural_\pm$ built into $V^\natural$. In particular, not all elements of $\mathrm{Aut}(V^\natural)$ are equally accessible. For example, [**201**] could prove Conjecture 7.1.1 when $g \in \mathbb{M}$ preserves $V^\natural_\pm$ – equivalently, for any $g \in \mathbb{M}$ commuting with some element in class 2B – but not for the other $g \in \mathbb{M}$. Perhaps the work of [**424**] will make the Monster's action on $V^\natural$ more uniformly accessible.

Conjecturally, there are 71 holomorphic VOAs with central charge $c = 24$ [**488**]. Recall that the Leech lattice Λ is the unique even self-dual positive-definite lattice of dimension 24 containing no norm-squared 2-vectors [**113**]. Under the lattice$\leftrightarrow$VOA correspondence mentioned at the end of Section 5.2.2, we are led to the following:

Conjecture 7.2.1 [**201**] *The Moonshine module $V^\natural$ is the unique holomorphic VOA $\mathcal{V}$ with central charge $c = 24$ and with trivial $\mathcal{V}_1$.*

Proving Conjecture 7.2.1 is one of the most important and difficult challenges in the subject – the first small step towards this is [**146**]. If true, as is expected, it would tell us $V^\natural$ is a fundamental exceptional structure, on par with the Leech lattice or the E_8 Lie algebra or indeed the Monster $\mathbb{M}$. We return to this conjecture in Section 7.3.4; the analogue $A^{f\natural}$ for vertex operator superalgebras (holomorphic, $c = 12$ and $\mathcal{V}_{1/2} = 0$) is

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

known and has automorphism group Co_1 [**163**]. Although the theta series Θ_L usually doesn't determine the lattice, Λ *is* the unique lattice with theta series Θ_Λ (this follows quickly from its above-mentioned uniqueness). It is thus tempting to also conjecture that the Moonshine module is the unique VOA with graded dimension J (see Question 7.2.7).

7.2.2 The Monster Lie algebra $\mathfrak{m}$

It was discovered early on that every Hauptmodul is replicable, and moreover that any replicable function is determined by its first few coefficients. An obvious approach to Conjecture 7.1.1 then is to show that the McKay–Thompson series T_g are also replicable. To get the necessary identities satisfied by their q-expansions, Borcherds used the denominator identity (Section 3.4.2) of a Lie algebra he associated with $V^\natural$.

We want to construct a Lie algebra $\mathfrak{m}$ from the Moonshine module $V^\natural = V_0^\natural \oplus V_1^\natural \oplus \cdots$. Of course, the direct choice $V_1^\natural$ is 0-dimensional, so we must modify $V^\natural$ first. Recall from Section 5.2.2 that a near-VOA $\mathcal{V}(L)$ is associated with any even *indefinite* lattice L. Let $\mathcal{V}_{1,1} := \mathcal{V}(II_{1,1})$ be the near-VOA associated with the two-dimensional even self-dual indefinite lattice $II_{1,1}$ defined in Section 1.2.1. We take both $V^\natural$ and $\mathcal{V}_{1,1}$ to be real. Define $\mathcal{V}$ to be the near-VOA $V^\natural \otimes \mathcal{V}_{1,1}$. As we know, the Monster $\mathbb{M}$ acts on $V^\natural$; extend this action to $\mathcal{V}$ by defining $\mathbb{M}$ to fix $\mathcal{V}_{1,1}$. An invariant positive-definite bilinear form on $V^\natural$ is constructed in [**201**]; extend it to $\mathcal{V}$ in the obvious way. Then the resulting form $(\star|\star)$ is $\mathbb{M}$-invariant.

The Monster Lie algebra $\mathfrak{m}$ is the quotient of $\mathcal{PV}_1$ by the radical of the form $(\star|\star)$ on $\mathcal{V}$, where the spaces $\mathcal{PV}_n$ are defined in (5.2.3). The radical contains $\mathcal{PV}_0$, so $\mathfrak{m}$ has a natural (real) Lie algebra structure (see Question 7.2.4). From the $\mathcal{V}_{1,1}$ part of $\mathcal{V}$ we get the involution ω and $\mathbb{Z}$-grading (see e.g. section 6.2 of [**323**] for details). Then by Theorem 3.3.6, a certain central extension of $\mathfrak{m}$ is some universal Borcherds–Kac–Moody algebra $\widehat{\mathfrak{g}}(A)$ – see [**72**], [**323**] for details. More precisely, its Cartan$_{BKM}$ matrix

$$A = \begin{pmatrix} 2 & 0 & \cdots & 0 & -1 & \cdots & -1 & \cdots \\ 0 & -2 & \cdots & -2 & -3 & \cdots & -3 & \cdots \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \\ 0 & -2 & \cdots & -2 & -3 & \cdots & -3 & \cdots \\ \vdots & & \vdots & & & \vdots & & \end{pmatrix} \tag{7.2.1}$$

consists for each $i, j \in \{-1, 1, 2, 3, \ldots\}$ of a block in the (i, j) spot of size $a_i \times a_j$ and with entries $-(i+j)$, where a_i are the coefficients $J(\tau) = \sum_{i=-1}^{\infty} a_i q^i$.

Theorem 7.2.2 *The Monster Lie algebra is $\mathfrak{m} = \widehat{\mathfrak{g}}(A)/\mathfrak{c}$, where A is in (7.2.1) and $\mathfrak{c}$ is the (infinite-dimensional) centre of $\widehat{\mathfrak{g}}(A)$. $\mathfrak{m}$ has Cartan subalgebra $\mathbb{R} \otimes_{\mathbb{Z}} II_{1,1} = \mathbb{R} \oplus \mathbb{R} =: \mathfrak{m}_{(0,0)}$ and simple roots $\alpha_{i,k}$ for each $i \in \{-1, 1, 2, 3, \ldots\}$ and $1 \le k \le a_i$. Only $\alpha_{-1,1}$ is real. The root-space decomposition of $\mathfrak{m}$ is $\mathfrak{m} = \oplus_{i,j=-\infty}^{\infty} \mathfrak{m}_{(i,j)}$. The Monster $\mathbb{M}$ acts on $\mathfrak{m}$ as Lie algebra automorphisms. Each root space $\mathfrak{m}_{(i,j)}$ (for $(i, j) \neq (0, 0)$) is an $\mathbb{M}$-module isomorphic to the homogeneous space $(V^\natural)_{ij+1}$, while the Cartan subalgebra*

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

$\mathfrak{m}_{(0,0)} \cong \rho_0 \oplus \rho_0$ *as an* $\mathfrak{m}$*-module. The denominator identity of* $\mathfrak{m}$ *is given in (3.4.7a). Finally,* $\mathfrak{m}$ *has a vector-space decomposition* $\mathfrak{u}^+ \oplus \mathfrak{gl}_2 \oplus \mathfrak{u}^-$ *into a sum of Lie subalgebras, where* $\mathfrak{u}^\pm$ *are free Lie algebras with countably many generators.*

The proof is given explicitly in section 6.2 of [**323**], and involves the No-Ghost Theorem (see the appendix of [**323**]) – a result first proved in string theory and special to VOAs with central charge $c = 24$. In particular, the No-Ghost Theorem establishes the $\mathbb{M}$-module isomorphisms in Theorem 7.2.2. $\mathfrak{m}$ has only one positive real root, so its Weyl group is order 2 and sends (i, j) to (j, i); it is responsible for the difference on the right side of (3.4.7a) (the j-function is the correction due to imaginary simple roots). The positive roots are $(-1, 1)$ and the α_{ij} of type (i, j), and this gives the product on the left.

Similarly, the fake Monster Lie algebra is associated in the same way with the near-VOA $\mathcal{V}(\Lambda) \otimes \mathcal{V}_{1,1}$. Though it is certainly an interesting example of a Borcherds–Kac–Moody algebra, it plays no role in the theory. Its name arose because it was initially suspected as playing a role in the Moonshine proof, but like $\mathcal{V}(\Lambda)$ doesn't carry a natural action of $\mathbb{M}$ so was discarded.

This construction of $\mathfrak{m}$ from $V^\natural$ may seem indirect. An alternate approach uses *Moonshine cohomology* [**386**] – a functor assigning to certain $c = 2$ near-VOAs a Lie algebra carrying an action of $\mathbb{M}$. To $\mathcal{V}_{1,1}$ this functor assigns $\mathfrak{m}$. This functor was anticipated in [**72**] and [**73**] and was inspired by BRST ('Becchi–Rouet–Stora–Tyutin') cohomology in string theory, or the semi-infinite cohomology of Lie theory. In particular, the standard method for obtaining the space of physical states in a string theory involves tensoring the original space $\mathcal{H}$ (a CFT with $c = 26$) with a space $\mathcal{H}_{ghosts}$ of ghosts (with $c = -26$); on $\mathcal{H} \otimes \mathcal{H}_{ghosts}$ is an operator Q obeying $Q^2 = 0$, and the space $\mathcal{H}_{phys}$ of physical states is the cohomology $H^\star = \ker Q/\mathrm{im}\, Q$. In particular, $\mathfrak{m}$ is the space H^1 for $\mathcal{H} = V^\natural \otimes \mathcal{V}_{1,1}$. The Baby Monster Lie algebra [**72**], which plays the same role for $\mathbb{B}$ as $\mathfrak{m}$ plays for $\mathbb{M}$, can be obtained in a similar way [**290**].

Because of a cohomological interpretation of denominator identities valid for any Borcherds–Kac–Moody algebra, (3.4.7a) can be 'twisted' by any $g \in \mathbb{M}$. This is how Borcherds derived (7.1.8b). These formulae are equivalent to the replication formulae (7.1.8a) conjectured in Section 7.1.4. However, these identities are obtained by more elementary means – requiring less of the theory of Borcherds–Kac–Moody algebras – in [**324**], [**331**], permitting a simplification of Borcherds' proof at this stage. In particular, in [**324**] the replication formulae (7.1.8a) appear quite naturally because $\mathfrak{u}^\pm$ are free Lie algebras.

7.2.3 The algebraic meaning of genus 0

Now, it turns out that if we verify for each conjugacy class K_g of $\mathbb{M}$ that the first, second, third, fourth and sixth coefficients of the McKay–Thompson series T_g and the corresponding Hauptmodul J_{Γ_g} agree, then $T_g = J_{\Gamma_g}$. That is precisely what Borcherds then did: he compared finitely many coefficients, and as they all equal what they should, this concluded the proof of Monstrous Moonshine!

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

However, this case-by-case verification occurred at the critical point where the McKay–Thompson series were being compared directly to the Hauptmoduls, and so provides little insight into why the T_g are genus 0. Recall that the main purpose for the proof of Conjecture 7.1.1 was not to establish its logical validity – the numerical evidence was already quite strong. Rather, the proof is supposed to help us understand how the Monster could be related to Hauptmoduls. This case-by-case verification became known as the conceptual gap. The basic problem is that $V^\natural$, $\mathfrak{m}$ and (7.1.8b) are *algebraic*, and the genus-0 property is *topological*. Fortunately, a more conceptual explanation of the equality $T_g = J_{\Gamma_g}$ – a conversion of the Hauptmodul property into an algebraic statement – has been found [**122**], replacing Borcherds' coefficient check with a general theorem.

Let p be prime. Exactly as in the argument of (7.1.6a), we find that the quantity

$$J(p\tau)^k + J\left(\frac{\tau}{p}\right)^k + J\left(\frac{\tau+1}{p}\right)^k + \cdots + J\left(\frac{\tau+p-1}{p}\right)^k \tag{7.2.2a}$$

is a degree-pk polynomial in $J(\tau)$. This uses the Hauptmodul property of J. Thus there is a polynomial $F_p(X, Y)$, of degree p in both X and Y, defined by

$$F_p(X, J(\tau)) = (X - J(p\tau)) \prod_{i=0}^{p-1} \left(X - J\left(\frac{\tau+i}{p}\right)\right). \tag{7.2.2b}$$

Indeed, the coefficients of $F_p(X, J(\tau))$ are symmetric polynomials in the roots $J(p\tau)$, $J\left(\frac{\tau+i}{p}\right)$, and so can be expressed polynomially using (7.2.2a). For example,

$$\begin{aligned} F_2(X,Y) = (X^2 - Y)(Y^2 - X) &- 393768\,(X^2 + Y^2) - 42987520\,XY \\ &- 40491318744\,(X+Y) + 120981708338256. \end{aligned}$$

Definition 7.2.3 *Consider a formal series $f(\tau) = q^{-1} + \sum_{n=1}^{\infty} b_n q^n$ ('formal' means we don't worry about whether it converges). An* order-n modular equation *for f is a monic polynomial $F_n(x, y)$ in two variables, of degree $\psi(n) := n \prod_{\text{primes } p|n}(1 + 1/p)$, such that*

$$F_n\left(f(\tau), f\left(\frac{a\tau+b}{d}\right)\right) = 0$$

for all integers $a, b, d \geq 0$ such that $ad = n$, $\gcd(a, b, d) = 1$ and $0 \leq b < d$.

This definition looks a little obscure, but it is natural. The degree $\psi(n)$ is precisely the number of those triples (a, b, d). These triples come from the coset expansion

$$\Gamma_0(K) \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \Gamma_0(K) = \bigcup_{a,b,d} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \Gamma_0(K),$$

for any K obeying $n \equiv 1 \pmod{K}$. Modular equations necessarily obey $F_n(x, y) = \pm F_n(y, x)$.

Thus $J(\tau)$ obeys a modular equation for all n. Note that this property depends crucially on it being a Hauptmodul. Conversely, does the existence of modular equations imply the Hauptmodul property? Unfortunately not: the exponential function $f(\tau) = q^{-1}$ also

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

obeys one for every n. For example, for p prime, take $F_p(x, y) = (x^p - y)(x - y^p)$ (see also Question 7.2.5).

Beautiful and unexpected is that the only functions $f(\tau) = q^{-1} + b_1 q + \cdots$ to obey modular equations for all n are $J(\tau)$ and the 'modular fictions' q^{-1} and $q^{-1} \pm q$ (which are essentially exp, cos and sin) [**360**]. More generally, we have the following:

Theorem 7.2.4 [**122**] *Let $f(\tau)$ be a formal series $q^{-1} + \sum_{n=1}^{\infty} b_n q^n$, $b_i \in \mathbb{C}$. Suppose f satisfies a modular equation of order n for all $n \equiv 1$ (mod N). Then:*

(a) *f converges to a holomorphic function on $\mathbb{H}$.*

(b) *If the symmetry group $\Gamma(f) := \{\alpha \in \mathrm{SL}_2(\mathbb{R}) \mid f(\alpha.\tau) = f(\tau)\}$ consists only of the translations $\pm \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, then $f(\tau) = q^{-1} + \xi q$ for some coefficient $\xi \in \mathbb{C}$; if the coefficient ξ is an algebraic number, then $\xi = 0$ or $\xi^{\gcd(24,N)} = 1$.*

(c) *If the symmetry group $\Gamma(f)$ does not only contain translations, then $\Gamma(f)$ is genus 0 and f is a Hauptmodul for $\Gamma(f)$. Moreover, $\Gamma(f)$ contains some subgroup $\Gamma_0(K)$, for $K|N^\infty$.*

Conversely, if f is a Hauptmodul for some subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ containing $\Gamma_0(K)$, and all coefficients b_i lie in the cyclotomic field $\mathbb{Q}[\xi_K]$, then f obeys a modular equation for every $n \equiv 1$ (mod K). For the other n coprime to K, there is also a modular equation involving twisting by the Galois group, as in (2.3.14). See [**122**] for details. The condition $K|N^\infty$ means all primes dividing K also divide N.

The denominator identity argument tells us each T_g obeys a modular equation for each $n \equiv 1$ modulo the order $N = o(g)$ of g, so Theorem 7.2.4 concludes the proof of Monstrous Moonshine, and replaces Borcherds' coefficient check.

The proof of Theorem 7.2.4 is difficult. First, it is established that f is holomorphic on $\mathbb{H}$. This implies that whenever $f(\tau_1) = f(\tau_2)$, there is a diffeomorphism α defined locally about τ_1, such that $\alpha(\tau_1) = \tau_2$ and $f(\alpha(\tau)) = f(\tau)$. The hard part of the proof is to show α extends to all of $\mathbb{H}$. Once that is done, we know α is a Möbius transformation, and the rest of the argument is reasonably straightforward.

In [**120**] it is shown that if f obeys a modular equation for any n, all of whose prime divisors are congruent to 1 (mod N), then either $f = q + \xi q^{-1}$ for some ξ, or f is the Hauptmodul for a group containing some $\Gamma(N')$. However, computer calculations by [**102**] indicate that the hypothesis of these theorems can be considerably weakened:

Conjecture 7.2.5 [**102**], [**120**] *Let $f(\tau) = q^{-1} + \sum_{n=1}^{\infty} b_n q^n$ be a formal series and p, p' any two distinct primes. If f satisfies modular equations for both p and p', then f converges in $\mathbb{H}$ to a holomorphic function, and either $f(\tau) = q^{-1} + \xi q$ for $\xi^{\gcd(p-1,p'-1)+1} = \xi$, or f is the Hauptmodul for a genus-0 group containing $\Gamma(N)$ for N coprime to pp'.*

This conjecture is completely out of reach at present.

Finding modular equations was a passion of Ramanujan, who filled his notebooks with them. See [**82**] for an application of Ramanujan's modular equations (namely, for the function $p(\tau) = \frac{\mathrm{d}}{\mathrm{d}\tau} \log \eta(\tau)$) to computing the first billion or so digits of π.

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

In Section 1.7.2 we show that although radicals can be used to solve (i.e. find closed expressions for the roots of) arbitrary polynomials of degree 4 or less, they are inadequate to solve all polynomials of degree 5 or higher. However, much as the relation $\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta)$ yields the solution to cubics, a modular equation relating τ and 5τ for $\sqrt{\theta_3/\eta}$ can be used to solve quintic polynomials (see e.g. chapter 7 of [**464**]).

Many of the applications of the j-function have to do with its modular equations. For instance, recall from Theorem 1.7.1 that each abelian extension of $\mathbb{Q}$ lies inside some cyclotomic field $\mathbb{Q}[\xi_n]$, in other words is generated by the values of the exponential function $\exp[2\pi\mathrm{i}\alpha]$ when α is rational. Likewise, the abelian extensions of the imaginary quadratic fields $\mathbb{Q}[\sqrt{-d}]$ are generated by the values of $J(\tau)$ for special τ. See [**117**] for a review of this part of what is called class field theory. Modular equations are used to establish properties of those special values of $J(\tau)$ (see Question 7.2.2).

Generalising a little a definition of McKay (recall Conjecture 7.1.5), we get:

Definition 7.2.6 *By a* modular fiction *we mean any function of the form* $f(\tau) = q^{-1} + \xi q$, *where either* $\xi = 0$ *or* $\xi^{24} = 1$.

The point is that these behave like the modular functions T_g – more precisely [**122**], these are precisely the non-Hauptmoduls with cyclotomic integer coefficients, which obey (Galois-twisted) modular equations for each n (see [**122**] for more details). Perhaps, exceptional though they are, they shouldn't be ignored. This suggests the following:

Problem *What is the VOA-related question, for which* '24' *is the answer?*

More precisely, out of which VOA-like structure can we obtain the modular fictions, in a way analogous to how the T_g are obtained from $V^\natural$? That structure would complete Moonshine for the modular fictions. Incidentally, it is manifest in the proof of Theorem 7.2.4 that this 24 arises there through the usual exponent-2 property of Section 2.5.1.

7.2.4 Braided #7: speculations on a second proof

Monstrous Moonshine began with the challenge to understand how the Monster (the right side of (7.1.1)) could be related conceptually to modular functions (the left side of (7.1.1)). We have seen that VOAs constitute a bridge between the two sides: the Monster is the symmetry of a VOA $V^\natural$ whose graded dimension is the J-function.

That argument is still the only proof we have of Monstrous Moonshine. But does that put our finger on the essence of the mystery? The indirect argument sketched in the previous three subsections leaves the special role of the Monster unclear. As we'll see shortly, it also ignores what CFT has tried to teach us regarding modularity. It should also be remarked that a VOA is quite a complicated beast – do we really need all of its rich structure, if all we care about is Moonshine? Is there a simpler explanation that, by requiring less machinery, is both more general and more conceptual and that more directly connects $\mathbb{M}$ to a Hauptmodul property?

For these reasons, we should look for a second proof of Monstrous Moonshine. But what would it look like? To get a hint, let's recall the CFT explanation of modularity.

Two essentially equivalent formulations of quantum field theory are:

(i) The Hamiltonian formulation (canonical quantisation), which presents us with a state space V, carrying a representation of the symmetry algebra of the theory, and includes among other things a Hamiltonian (energy operator) H.
(ii) The Feynman formulation, which interprets the amplitudes using path integrals.

In RCFT, the Hamiltonian formulation describes concretely the space V, graded by H, on which we take the trace $\mathrm{tr}_V q^H$, and hence gives us the coefficients of our q-expansions. The Feynman path formalism, on the other hand, interprets these graded traces as functions over moduli spaces, and hence makes their modularity manifest. According to RCFT, *the modularity in Moonshine is the conjunction of these two formulations.*

On the Hamiltonian side of CFT, the space V is a module for the chiral algebra (VOA) $\mathcal{V}$. As such, it is a module of the Virasoro algebra (3.1.5) (giving us the Hamiltonian $H = L_0$), as well as possibly other algebras (e.g. Kac–Moody) and groups (e.g. $\mathbb{M}$). In our hypothetical second proof, we would like to avoid the full VOA structure, but probably the presence of $\mathfrak{Vir}$ is fundamental if we want to give meaning to the coefficients in the q-expansion, that is the grading of the modules. Thanks to the theory of VOAs, we understand fairly well the Virasoro side. The remainder of this subsection will be devoted to the more mysterious question: what is the key ingredient of the Feynman side?

In any treatment of RCFT (e.g. [**436**], [**207**], [**131**], [**530**], [**32**]), we read that $\mathcal{V}$-characters (5.3.13) are '1-point functions on the torus'. By this is meant that they are chiral blocks in $\mathfrak{B}_{\mathcal{V}}^{(1,1)}$ for the torus with one marked point, with that point labelled with the 'vacuum' module $\mathcal{V}$ itself (see e.g. Sections 4.3.3 and 5.3.4 for the physical description). Verlinde's formula tells us that space has dimension equal to the number of irreducible modules M of the chiral algebra $\mathcal{V}$, and indeed the characters χ_M form a natural basis for it. As explained in Section 2.1.4, its (enhanced) mapping class group $\widehat{\Gamma}_{1,1}$ is the braid group $\mathcal{B}_3$. Thus $\mathcal{B}_3$ will act on the characters of the RCFT. From this, using (1.1.10a), we obtain the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$.

To see this $\mathcal{B}_3$ action explicitly, we have to undo a simplification we performed in Definition 5.3.6. The 1-point functions χ_M are actually functions of the triple (τ, v, z), where τ lies in the Teichmüller space $\mathbb{H}$ of the torus with 1 puncture, $v \in \mathcal{V}$ is the insertion state and $z \in \mathbb{C}$ is a local coordinate at the puncture. Explicitly, as explain in Section 5.3.4, for $v \in \mathcal{V}_{[k]}$ we get

$$\chi_M(\tau, v, z) := \mathrm{tr}_M Y(v, e^{2\pi \mathrm{i} z})\, q^{L_0 - c/24} = e^{-2k\pi \mathrm{i} z}\, \mathrm{tr}_M o(v)\, q^{L_0 - c/24}, \tag{7.2.3a}$$

using the notation of Section 5.3.3 (compare with (5.3.13)). The group $\widehat{\Gamma}_{1,1}$ is (like any mapping class group) generated by the Dehn twists, and as mentioned we obtain

$$\widehat{\Gamma}_{1,1} = \langle \sigma_1, \sigma_2 \,|\, \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle \cong \mathcal{B}_3, \tag{7.2.3b}$$

where σ_i are the Dehn twists of Figure 2.8. The action of σ_i on the characters is then

$$\sigma_1.\chi_M(\tau, v, z) = e^{-2\pi \mathrm{i} k/12}\, \chi_M(\tau + 1, v, z), \tag{7.2.4a}$$

$$\sigma_2.\chi_M(\tau, v, z) = e^{-2\pi \mathrm{i} k/12}\, \chi_M\left(\frac{\tau}{1-\tau}, \frac{v}{(1-\tau)^k}, z\right), \tag{7.2.4b}$$

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

so in particular we get

$$(\sigma_1\sigma_2\sigma_1)^2.\chi_M(\tau, v, z) = e^{-2\pi \mathrm{i}k/2}\,\chi_M(\tau, (-1)^k v, z), \tag{7.2.4c}$$

$$(\sigma_1\sigma_2\sigma_1)^4.\chi_M(\tau, v, z) = e^{-2\pi \mathrm{i}k}\,\chi_M(\tau, v, z). \tag{7.2.4d}$$

The combination $(\sigma_1\sigma_2\sigma_1)^4$, which is trivial in the (unenhanced) mapping class group $\Gamma_{1,1} \cong \mathrm{SL}_2(\mathbb{Z})$, here equals the Dehn twist about the puncture, which for the logarithmic parameter z of course sends z to $z+1$. The actions of σ_i on τ and v are determined from the homomorphism $\mathcal{B}_3 \to \mathrm{SL}_2(\mathbb{Z})$ given by (1.1.11b) at $w=-1$. This should be very reminiscent of Section 2.4.3.

Of course here the state v comes from the vacuum sector $\mathcal{V}$ so the conformal weight k is an integer. We are in the situation of Section 2.4.3, where our $\mathcal{B}_3$ action collapses to one of $\mathrm{PSL}_2(\mathbb{Z})$, since the centre (7.2.4c) acts trivially. This is why the z-dependence of χ_M could be safely ignored in Definition 5.3.6. As before, the more interesting case is when the weight k of the modular form is not integral. Here, that will happen when we insert states from other $\mathcal{V}$-modules, that is when we consider chiral blocks from the other $\mathfrak{B}_M^{(1,1)}$. In CFT these are equally fundamental. In this case, $v \in M$ will have rational conformal weight $k \in h_M + \mathbb{N}$, and here the Dehn twist about the puncture will typically not act trivially. As happened with the Dedekind eta function in (2.4.14), we will then see nontrivial $\mathcal{B}_3$ actions[2] (involving e.g. the $S_{(a)}$ of Figure 6.4).

It should be clear that in RCFT, modularity is a topological effect. Zhu's Theorem 5.3.8 generalises the appearance of $\mathrm{SL}_2(\mathbb{Z})$ in RCFT to any RVOA, but as we recall from Section 5.3.5, the proof follows closely the intuition of RCFT: modularity in VOAs arises through that $\mathrm{SL}_2(\mathbb{Z})$ action on the space of chiral blocks, which is inherited from the topological $\widehat{\Gamma}_{1,1}$-action mentioned above, once we drop (as Zhu did) the dependence on z.

A toy model of this idea is provided by the proof in Section 2.4.2 of the modularity of θ_3: we can interpret this action of $\mathrm{SL}_2(\mathbb{Z})$ as an action of $\mathcal{B}_3$. Note that this action of $\mathrm{SL}_2(\mathbb{Z})$ on the Heisenberg group H is really the action of $\mathcal{B}_3$ on the group $\mathbb{R}^2$ given in (2.4.15b); it factors through to $\mathrm{SL}_2(\mathbb{Z})$ because $\mathbb{R}^2$ is abelian.

The relation of the Hamiltonian ($\mathfrak{Vir}$) side to that of Feynman ($\mathcal{B}_3$) is that the Virasoro algebra acts naturally on the enhanced moduli space $\widehat{\mathcal{M}}_{1,1}$ (see Section 3.1.2), whose mapping class group is $\mathcal{B}_3$. This $\mathfrak{Vir}$-action leads to the KZ equations, which are partial differential equations obeyed by the chiral blocks in $\mathfrak{B}_{\mathcal{V}}^{(1,1)}$, that is by the VOA characters. The monodromy group of those equations is $\widehat{\Gamma}_{1,1} \cong \mathcal{B}_3$, and thus $\mathcal{B}_3$ acts on $\mathfrak{B}_{\mathcal{V}}^{(1,1)}$.

Of course the reason Borcherds chose a different route in [**72**] is that we need more than merely modularity: we need the genus-0 property. But as we will see in Section 7.3.3, Norton has proposed a possible relationship between the Monster and the genus-0 property, and his method also involves the $\mathcal{B}_3$ action given in (2.4.15b). Finally, we argue in Section 6.3.3 that the $\Gamma_{\mathbb{Q}}$-action associated with $\mathcal{B}_3$ underlies the Galois action in RCFT. In all of these examples, the modular group arose from an underlying appearance of the braid group $\mathcal{B}_3$. Is this the same $\mathcal{B}_3$? We suggest that this braid group action (together

[2] The thought that, for example, topological field theory really sees $\mathcal{B}_3$ and not $\mathrm{SL}_2(\mathbb{Z})$ is also made in [**404**].

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

with a compatible Virasoro action) somehow underlies Moonshine, and pursuing this thought would lead to a second, more conceptual proof of Monstrous Moonshine.

Question 7.2.1. Verify that any replicable function is uniquely determined by finitely many coefficients.

Question 7.2.2. (a) Verify that $J(\tau)$ obeys a modular equation for every $n = 2, 3, 4, \ldots$ (b) Suppose $\tau_0 = r + \mathrm{i}\sqrt{s}$ for rational r, s, where $s > 0$. Use part (a) to prove that $J(\tau_0)$ is an algebraic number.

Question 7.2.3. Verify that any replicable function obeys a modular equation.

Question 7.2.4. Prove that $\mathcal{PV}_1/\mathrm{rad}(\star|\star)$ is a Lie subalgebra of $\mathcal{PV}_1/\mathcal{PV}_0$.

Question 7.2.5. For each n, find the modular equations obeyed by the modular fictions (a) $f(\tau) = q^{-1}$; (b) $f(\tau) = q^{-1} + q$; (c) $f(\tau) = q^{-1} - q$.

Question 7.2.6. Arguably, what makes two-dimensional quantum field theory so unique is the possibility of braid statistics. Could those braid groups directly be responsible for the $\mathcal{B}_3$ action of Section 7.2.4?

Question 7.2.7. Call any VOA $\mathcal{V}$ obeying the hypotheses of Corollary 6.2.5, 'nice'. Prove that a nice $\mathcal{V}$ is holomorphic iff its graded dimension $\chi_{\mathcal{V}}(\tau)$ is invariant under $\tau \mapsto -1/\tau$. Use this to show, for the class of nice VOAs, that Conjecture 7.2.1 is true iff $V^\natural$ is the unique nice VOA with graded dimension $J(\tau)$.

7.3 More Monstrous Moonshine

We give in this section a quick sketch of further developments and conjectures. As we know, Moonshine is an area where it is much easier to conjecture than to prove.

7.3.1 Mini-Moonshine

It is natural to ask about Moonshine for other groups. Of course any subgroup of $\mathbb{M}$ automatically inherits Moonshine by restriction, but this isn't at all interesting. A very accessible sporadic is M_{24} – see, for example, chapters 10 and 11 of [**113**]. Most constructions of the Leech lattice start with M_{24}, and most constructions of the Monster involve the Leech lattice. Thus we are led to the following natural hierarchy of (most) sporadics:

- M_{24} (from which we can get $M_{11}, M_{12}, M_{22}, M_{23}$); which leads to
- $Co_0 \cong 2.Co_1$ (from which we get $HJ, HS, McL, Suz, Co_3, Co_2$); which leads to
- $\mathbb{M}$ (from which we get $He, Fi_{22}, Fi_{23}, Fi'_{24}, HN, Th, \mathbb{B}$).

It can thus be argued that we could approach problems in Monstrous Moonshine by first addressing in order M_{24} and Co_1, which should be much simpler. Indeed, Moonshine for M_{24} has been completely established in [**153**].

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

Largely by trial and error, Queen [**466**] established Moonshine for the following groups (all essentially centralisers of elements of $\mathbb{M}$): Co_0, Th, $3.2.Suz$, $2.HJ$, HN, $2.\mathcal{A}_7$, He, M_{12}. In particular, to each element g of these groups, there corresponds a series $Q_g(\tau) = q^{-1} + \sum_{n=0}^{\infty} a_n(g)q^n$, which is a Hauptmodul for some modular group of Moonshine-type, and where each $g \mapsto a_n(g)$ is a virtual character. For Co_0, $3.2.Suz$, $2.HJ$ and $2.\mathcal{A}_7$, it is only a virtual character. Other differences with Monstrous Moonshine are that there can be a preferred nonzero value for the constant term a_0, and that although $\Gamma_0(N)$ will be a subgroup of the fixing group, it won't necessarily be normal.

For example, Queen's series Q_e for Co_0 is the Hauptmodul (2.2.17a) for the genus-0 group $\Gamma_0(2)$. Checking the tables in [**109**], we see that 276, 299, 1771, 2024 and 8855 are dimensions of irreducible modules of the Conway group Co_1 (hence its $\mathbb{Z}_2$-extension Co_0), and 24 is the dimension of the Co_0 representation associated with the Leech lattice (it's only a projective representation of Co_1). We find $11\,202 = 8855 + 1771 + 299 + 276 + 1$, and the ambiguity $2048 = 1771 + 276 + 1 = 2024 + 24$ is resolved in favour of the latter by considering other character values and comparing to the list of Hauptmoduls. That a virtual character is needed for Co_0 is clear from the minus signs in (2.2.17a). This Hauptmodul is better known as the McKay–Thompson series $T_{2\mathrm{B}}$ (and the centraliser of 2B involves Co_0, which isn't a coincidence), but about half of Queen's Hauptmoduls Q_g for Co_0 do not arise as T_g for $\mathbb{M}$. Nevertheless, next subsection we see how to interpret them through the Moonshine for $\mathbb{M}$.

The Hauptmodul for $\Gamma_0(2)+$ looks like

$$q^{-1} + 4372q + 96256q^2 + 12\,40002q^3 + \cdots \tag{7.3.1a}$$

and we find the relations

$$4372 = 4371 + 1, \quad 96\,256 = 96\,255 + 1, \quad 1\,240\,002 = 1\,139\,374 + 4371 + 2 \cdot 1, \tag{7.3.1b}$$

where 1, 4371, 96 255 and 1 139 374 are all dimensions of irreducible representations of the Baby Monster $\mathbb{B}$. Thus we may expect Moonshine for $\mathbb{B}$. This should actually fall into Queen's scheme because (7.3.1a) is the McKay–Thompson series associated with class 2A of $\mathbb{M}$, and the centraliser of an element in 2A is a double cover of $\mathbb{B}$.

However, there can't be a VOA $\mathcal{V} = \oplus_n \mathcal{V}_n$ with graded dimension (7.3.1a) and automorphism $\mathbb{B}$, because, for example, the $\mathbb{B}$-module $\mathcal{V}_3$ doesn't contain $\mathcal{V}_2$ as a submodule (recall Question 5.2.1). Nevertheless, Höhn deepened the analogy between $\mathbb{M}$ and $\mathbb{B}$ by constructing a vertex operator superalgebra $V\mathbb{B}^\natural$ of central charge $c = 23.5$, called the *shorter Moonshine module*, closely related to $V^\natural$ (see e.g. [**289**]). Like $V^\natural$ it is holomorphic (i.e. it has only one irreducible module), with automorphism group $\mathbb{Z}_2 \times \mathbb{B}$ and graded dimension

$$\chi_{V\mathbb{B}^\natural}(\tau) = q^{-47/48}\left(1 + 4371q^{3/2} + 96256q^2 + 1143745q^{5/2} + \cdots\right). \tag{7.3.2a}$$

Of course the strange $-47/48$ is $-c/24$; the half-integer powers of q come from the odd (i.e. fermionic) part of $V\mathbb{B}^\natural$. Just as $\mathbb{M}$ is the automorphism group of the Griess algebra $V_2^\natural$, so is $\mathbb{B}$ the automorphism group of the algebra $(V\mathbb{B}^\natural)_2$. Just as $V^\natural$ is associated

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

with the Leech lattice Λ, so is $V\mathbb{B}^\natural$ associated with the shorter Leech lattice O_{23}, the unique 23-dimensional positive-definite self-dual lattice with no vectors of length-squared 2 or 1 (see chapter 6 of [**113**]). The automorphism group of O_{23} is a central extension of Co_2 by $\mathbb{Z}_2$. The relation between (7.3.2a) and (7.3.1a) will be clearer next subsection.

Similarly, Duncan [**163**] constructs a vertex operator superalgebra $A^{f\natural}$ with $c = 12$ and automorphism group Co_1. Again it is holomorphic, and has graded superdimension

$$\chi_{A^{f\natural}}(\tau) = q^{-1/2}\left(1 + 276\,q - 2048\,q^{3/2} + 11202\,q^2 - 49152\,q^{5/2} + \cdots\right), \quad (7.3.2b)$$

i.e. is given by (2.2.17a) with $\tau \mapsto \tau/2$ and hence is fixed by a genus-0 subgroup of $\mathrm{SL}_2(\mathbb{R})$ (see Question 7.3.1). It is the unique 'nice' holomorphic vertex operator superalgebra with $c = 12$ and no elements with conformal weight $1/2$, in perfect analogy with the conjectured uniqueness of $V^\natural$ (Conjecture 7.2.1). The algebra $A^{f\natural}$ plays the same role for Co_1 that $V^\natural$ plays for $\mathbb{M}$. In particular, just as $V^\natural$ is obtained from a $\mathbb{Z}_2$-orbifold, so is $A^{f\natural}$, and this removes the constant term and enhances the symmetry. From this construction of $A^{f\natural}$, it is then straightforward (see Theorem 7.1 in [**163**]) to compute explicit finite expressions for the Thompson twists of (7.3.2b) by $g \in Co_1$, using Frame shapes as described in [**111**]. In this way, a genus-0 Moonshine for Co_1 is established (as expected, the arguments are far simpler than that for $\mathbb{M}$).

There has been no interesting Moonshine rumoured for the remaining six sporadics (the *pariahs* J_1, J_3, Ru, ON, Ly, J_4). There is some sort of weaker Moonshine for any group that is an automorphism group of a vertex operator algebra (so this means any finite group [**152**]!). Many finite groups of Lie type should arise as automorphism groups of VOAs associated with affine algebras except defined over finite fields. But apparently the known finite group examples of genus-0 Moonshine are limited to those involved with $\mathbb{M}$.

7.3.2 Twisted #7: Maxi-Moonshine

In an important announcement [**450**], on par with [**111**], Norton unified and generalised Queen's work. Unfortunately he called it 'Generalised Moonshine', but we won't (recall the diatribe in Section 3.3.1).

About a third of the McKay–Thompson series T_g will have some negative coefficients. In Section 7.3.5 we see that Borcherds interprets them as dimensions of superspaces (which automatically come with signs). Norton proposed that, although $T_g(-1/\tau)$ will not usually be another McKay–Thompson series, it will always have nonnegative integer q-coefficients, and these can be interpreted as ordinary dimensions. In the process, he extended the $g \mapsto T_g$ assignment to commuting pairs $(g, h) \in \mathbb{M} \times \mathbb{M}$.

Conjecture 7.3.1 (Norton [**450**]) *To each pair $g, h \in \mathbb{M}$, $gh = hg$, we have a function $N_{(g,h)}(\tau)$ such that*

$$N_{(g^a h^c,\, g^b h^d)}(\tau) = \alpha\, N_{(g,h)}\left(\frac{a\tau + b}{c\tau + d}\right), \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad (7.3.3)$$

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

for some root of unity α *(of order dividing* 24*, and depending on* g, h, a, b, c, d*).* $N_{(g,h)}(\tau)$ *is either constant, or generates the modular functions for a genus-0 subgroup of* $\mathrm{SL}_2(\mathbb{R})$ *containing some* $\Gamma(M)$*. Constants* $N_{(g,h)}(\tau)$ *arise when all elements of the form* $g^a h^b$ *(for* $\gcd(a, b) = 1$*) are 'non-Fricke' (defined below). Each* $N_{(g,h)}(\tau)$ *has a* $q^{\frac{1}{M}}$*-expansion for that* M*; the coefficients of this expansion are characters evaluated at* h *of some central extension of the centraliser* $C_{\mathbb{M}}(g)$*. Simultaneous conjugation of* g, h *leaves the function unchanged:* $N_{(aga^{-1},aha^{-1})}(\tau) = N_{(g,h)}(\tau)$*.*

We call $N_{(g,h)}(\tau)$ the *Norton series*. An element $g \in \mathbb{M}$ is called *Fricke* if the group Γ_g fixing T_g contains an element sending 0 to $\mathrm{i}\infty$. In terms of the notation of Conjecture 7.1.1, $g \in \mathbb{M}$ is Fricke iff the invariance group Γ_g contains the *Fricke involution* $\tau \mapsto -1/(M\tau)$. The identity e is Fricke, as are 120 of the 171 Γ_g. For example, the classes pA, for p prime, are Fricke, while the classes pB are not.

The McKay–Thompson series are recovered by the $g = e$ specialisation: $N_{(e,h)}(\tau) = T_h(\tau)$. Unlike the McKay–Thompson series, the Norton series can have cyclotomic integer coefficients, and the groups fixing them may not contain $\Gamma_0(M)$. If g is Fricke, then clearly $N_{(g,e)}(\tau) = T_g(\tau/M)$. The action (7.3.3) of $\mathrm{SL}_2(\mathbb{Z})$ is related to its natural action on the fundamental group $\mathbb{Z}^2$ of the torus, as we saw in Section 6.3.1, as well as a natural action of the braid group, as we'll see next subsection.

For example, when $\langle g, h\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and g, h, gh are all in class 2A, then

$$N_{(e,g)}(\tau) = N_{(e,h)}(\tau) = T_g(\tau) = q^{-1} + 4372q + 96256q^2 + \cdots, \qquad (7.3.4a)$$

$$N_{(g,e)}(\tau) = N_{(h,e)}(\tau) = T_g(\tau/2) = q^{-1/2} + 4372q^{1/2} + 96256q + \cdots, \qquad (7.3.4b)$$

$$N_{(g,h)}(\tau) = \sqrt{J(\tau) - 984} = q^{-1/2} - 492q^{1/2} - 22590q^{3/2} + \cdots, \qquad (7.3.4c)$$

$$N_{(g,g)}(\tau) = N_{(h,h)}(\tau) = q^{-1/2} + 4372q^{1/2} - 96256q + \cdots. \qquad (7.3.4d)$$

Hence $N_{(g,e)}(\tau + 1) = \mathrm{i}\, N_{(g,g)}(\tau)$, giving us an example of a nontrivial α in (7.3.3).

The basic tool we have for approaching Moonshine conjectures is the theory of VOAs, so we need to understand Norton's suggestion from that point of view. This is done using twisted modules (Section 5.3.6). For each $g \in \mathbb{M}$, there is a unique g-twisted module of $V^\natural$ [**150**] – call this twisted module $V^\natural(g)$. This generalises the holomorphicity of $V^\natural$ mentioned in Section 7.2.1. Given any automorphism $h \in \mathrm{Aut}(V^\natural)$ commuting with g, we can perform Thompson's trick (5.3.23) and write

$$q^{-1}\mathrm{tr}_{V^\natural(g)} h\, q^{L_0} =: \mathcal{Z}(g, h; \tau). \qquad (7.3.5)$$

Then $\mathcal{Z}(g, h) = N_{(g,h)}$.

[**150**] proves that, whenever the subgroup $\langle g, h\rangle$ generated by g and h is cyclic, then $N_{(g,h)}$ will be a Hauptmodul satisfying (7.3.3). This will happen, for instance, whenever the orders of g and h are coprime. [**150**] proves this by reducing it to Conjecture 7.1.1 (which is now a theorem). Extending [**150**] to all commuting pairs g, h is one of the most pressing tasks in Moonshine.

Höhn [**290**] verified Conjecture 7.3.1 for g in class 2A and $h \in C_{\mathbb{M}}(g) \cong 2.\mathbb{B}$. In particular, those 247 functions $N_{(g,h)}(2\tau)$ are Hauptmoduls for genus-0 groups of Moonshine-type (see Question 7.3.1). The proof mirrors that of [**72**] fairly closely. There is a simple relation between the twisted module $V^\natural(g)$ and the shorter Moonshine module $V\mathbb{B}^\natural$, and from this the 286 Thompson twists of (7.3.2a) can be obtained [**290**]. Verifying Conjecture 7.3.1 for g in class 2B should likewise be possible.

More satisfying though would be a uniform proof of Conjecture 7.3.1, for example, by considering the full orbifold $V^\natural/\mathbb{M}$. It appears that the 3-cocycle α corresponding to this orbifold (recall the cohomological twist of Section 5.3.6) will have to be nontrivial – in fact, its order in $H^3(\mathbb{M}, \mathbb{C}^\times)$ should be a multiple of 12 [**408**]. Suggestive is that the permutation orbifold $\mathbb{M}^{\otimes n}/\langle g\rangle$ gives a natural interpretation of the left-half of the definition (7.1.9) of a replicable function.

The orbifold theory for M_{24} is established in [**153**] (the relevant series $\mathcal{Z}(g, h)$ had already been constructed in [**407**]). Next up should be the orbifold theory for Conway's group Co_1, but that seems out of reach right now, in spite of [**163**].

As has been alluded to elsewhere in this book, the subfactor approach complements that of VOAs. In particular, orbifolds seem more accessible for them [**157**], [**332**].

7.3.3 Why the Monster?

That $\mathbb{M}$ is associated with *modular functions* can be explained mathematically by it being the automorphism group of the vertex operator algebra $V^\natural$. But what is so special about that group $\mathbb{M}$ that these modular functions T_g and $N_{(g,h)}$ should be Hauptmoduls? In fact, every group known to have rich genus-0 Moonshine properties is contained in the Monster. To what extent can we derive $\mathbb{M}$ from Monstrous Moonshine? Our understanding of this seemingly central role of $\mathbb{M}$ is still poor.

The most interesting approach to this important question is due to Norton, and was first (cryptically) stated in [**450**]: the Monster is probably the largest (in a sense) group with the 6-transposition property. A *k-transposition group G* is one generated by a conjugacy class K of involutions, where the product gh of any two elements of K has order $\leq k$. For example, take K to be the transpositions in the symmetric group $\mathcal{S}_n$, that is, K is the set of all permutations $(i\,j)$. Since $\pi\circ(i\,j)\circ\pi^{-1} = (\pi\,i, \pi\,j)$, K is a conjugacy class in $\mathcal{S}_n$. An easy induction on n confirms that $\mathcal{S}_n$ is generated by K. Moreover, $(i\,j)(k\ell)$ has order 1, 2, 3, respectively iff the set $\{i, j\}\cup\{k, \ell\}$ has cardinality 2, 4, 3. Thus $\mathcal{S}_n$ is a 3-transposition group (this example is the source of the name 'k-transposition'). The Monster $\mathbb{M}$ is 6-transposition, for the choice of class $K = 2\text{A}$ (see Section 7.3.6 for more details). Transposition groups were used in the finite simple group classification by Fischer to great effect. The simplest relation known to this author, of the number '6' to genus 0, is given in Question 7.3.2.

The group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the free product $\mathbb{Z}_3 * \mathbb{Z}_2$ generated by an order 3 element $u = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ and an order 2 element $v = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. A transitive action of Γ on a finite set X with one distinguished point $x_0 \in X$ is equivalent to specifying a finite index subgroup Γ_0 of Γ. In particular, Γ_0 is the stabiliser $\{g \in \Gamma \mid g.x_0 = x_0\}$ of x_0, X can be identified with the cosets $\Gamma_0\backslash\Gamma$ and x_0 with the coset Γ_0. (If we avoid specifying x_0, then Γ_0 will be identified only up to conjugation.) As an abstract group, Γ_0 will be

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

a free product of a certain number of $\mathbb{Z}_2$'s, $\mathbb{Z}_3$'s and $\mathbb{Z}$'s (e.g. $\mathcal{F}_n = \mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}$ n times).

To such an action, we can associate a directed graph $\mathcal{G}$: its vertices are labelled by the set X, and we draw a solid edge directed from x to $u.x$, and a dotted undirected edge between x and $v.x$. Choose any spanning tree $\mathcal{T}$ of $\mathcal{G}$ (i.e. a connected subgraph of $\mathcal{G}$ containing all vertices of $\mathcal{G}$ and the minimum possible number ($\|X\| - 1$) of edges). Then the Reidemeister–Schreier method (see e.g. the appendix to [**292**] or section I.3 of [**103**]) gives a presentation for Γ_0, with one generator for every edge in $\mathcal{G}$ not in $\mathcal{T}$.

We are more interested though in a triangulation of the closed surface $\Gamma_0\backslash\overline{\mathbb{H}}$, called a (modular) *quilt*, which we can canonically associate with the action of Γ in X. The definition, originally due to Norton and further developed by Parker, Conway and Hsu, is somewhat involved and will be avoided here (but see especially chapter 3 of [**292**]). It is so-named because there is a polygonal 'patch' covering every cusp of $\Gamma_0\backslash\mathbb{H}$, and the closed surface is formed by sewing together the patches along their edges ('seams'). There are a total of $2n$ triangles and n seams in the triangulation, where n is the index $\|\Gamma_0\backslash\Gamma\| = \|X\|$. The boundary of each patch has an even number of edges, namely the double of the corresponding cusp width. The formula (2.2.16) for the genus g of $\Gamma_0\backslash\mathbb{H}$ in terms of the index n and the numbers n_i of Γ_0-orbits of fixed points of order i, can be interpreted in terms of the data of the quilt (see (6.2.3) of [**292**]), and we find in particular that if every patch of the quilt has at most six sides, then the genus will be 0 or 1, and genus 1 only exceptionally.

The quilt picture was specifically designed for one class of these Γ-actions (actually an $\mathrm{SL}_2(\mathbb{Z})$-action, but this doesn't matter). Fix a finite group G (we're most interested in the choice $G = \mathbb{M}$). Recall from (2.4.15) the right action of $\mathcal{B}_3$ on triples $(g_1, g_2, g_3) \in G^3$, and the equivalent reduced action of $\mathcal{B}_3$ on G^2. We will be interested in this action on the subset of G^3 where all $g_i \in G$ are involutions. The modular group $\mathrm{SL}_2(\mathbb{Z})$ is related to $\mathcal{B}_3$ by (1.1.10a). From this, we can get an action of $\mathrm{SL}_2(\mathbb{Z})$ in two ways: either (i) by restricting to commuting pairs g, h; or (ii) by identifying each pair (g, h) with all conjugates (aga^{-1}, aha^{-1}). Norton's $\mathrm{SL}_2(\mathbb{Z})$ action (7.3.3) arises from the $\mathcal{B}_3$ action of (2.4.15b), when we combine both (i) and (ii).

The number of sides in each patch of the corresponding quilt is determined by the orders of the g, h in these pairs. Taking G to be the Monster, and the involutions g_i from class 2A, then each patch will have ≤ 6 sides, and the corresponding genus will be 0 (usually) or 1 (exceptionally). In this way we can relate the Monster with a genus-0 property. This approach to genus 0 faces the same challenge of any other: how to incorporate the Atkin–Lehner involutions of Proposition 7.1.2(ii).

Based on the $\mathcal{B}_3$ actions (2.4.15), Norton hopes for some analogue of Moonshine valid for noncommuting pairs. Although the resulting series are always modular, they may not be Hauptmoduls, their fixing group may not contain some $\Gamma(N)$, and the coefficients won't always be cyclotomic integers. CFT considerations ('higher-genus orbifolds') alluded to in Section 6.3.1 suggest that this might be more natural to do using, for example, noncommuting quadruples $(g_1, g_2, h_1, h_2) \in \mathbb{M}^4$ obeying $g_1 h_1 g_1^{-1} h_1^{-1} = h_2 g_2 h_2^{-1} g_2^{-1}$; the role of $\mathrm{SL}_2(\mathbb{Z})$ is then played by higher-genus mapping class groups.

An important question is, how much does Monstrous Moonshine determine the Monster? How much of $\mathbb{M}$'s structure can be deduced from, for example, McKay's $\widehat{E}_8$ Dynkin diagram observation (Section 7.3.6), and/or the (complete) replicability of the T_g, and/or Conjecture 7.3.1, and/or Modular Moonshine in Section 7.3.5 below? A small start towards this is taken in [**452**], where some control on the subgroups of $\mathbb{M}$ isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ (p prime) is obtained, using only the properties of the $N_{(g,h)}$. See also chapter 8 of [**292**].

7.3.4 Genus 0 revisited

Tuite [**532**] suggests a very intriguing reformulation of the genus-0 property, directly in terms of VOAs. Assume the uniqueness conjecture: $V^\natural$ is the only $c = 24$ VOA with graded dimension J (Section 7.2.1). He argues from this that, for each $g \in \mathbb{M}$, the McKay–Thompson series T_g will be a Hauptmodul iff the only orbifolds of $V^\natural$ are the Leech lattice VOA $\mathcal{V}(\Lambda)$ and $V^\natural$ itself. More precisely, orbifolding $V^\natural$ by $\langle g \rangle$ should be $V^\natural$ if g is Fricke, and $\mathcal{V}(\Lambda)$ if g is non-Fricke ('Fricke' is defined in Section 7.3.2).

In, for example, [**313**], this analysis is extended to the genus-0 property of some Norton series $N_{(g,h)}$, when the subgroup $\langle g, h \rangle$ is not cyclic (thus going beyond [**150**]), although again assuming the uniqueness conjecture. Tuite is thus suggesting that the genus-0 property of the Monstrous Moonshine functions T_g and $N_{(g,h)}$ seems to be equivalent to a single principle. These arguments emphasise the importance of establishing the uniqueness conjecture of $V^\natural$. Unfortunately, that still seems out of reach.

7.3.5 Modular Moonshine

Consider an element $g \in \mathbb{M}$. We know from [**466**], [**450**], [**150**] that there is a Moonshine for the centraliser $C_{\mathbb{M}}(g)$ of g in $\mathbb{M}$, governed by the g-twisted module $V^\natural(g)$. Unfortunately, $V^\natural(g)$ is not usually itself a VOA, so the analogy with $\mathbb{M}$ is not perfect. Ryba found it interesting that, for $g \in \mathbb{M}$ of prime order p, Norton's series $N_{(g,h)}$ can be transformed into a McKay–Thompson series (and has all the associated nice properties) whenever h is *p-regular* (i.e. h has order coprime to p) – as we know, in this case $\langle g, h \rangle$ is cyclic. This special behaviour of p-regular elements suggested to him to look at modular representations, for reasons we'll soon see.

Let's begin by reviewing the basics of modular representations and Brauer characters (see also [**446**], [**308**]). A *modular representation* ρ of a group G is a representation defined over a field of positive characteristic p dividing the order $\|G\|$ of G. This is precisely the class of finite-dimensional representations where the usual properties break down. Such representations possess many special (that is to say, unpleasant) features.

For one thing, they are no longer completely reducible, so Theorem 1.1.2 breaks down. For a simple example, let p be any prime and consider $G = \mathbb{Z}_p$; then over any field of characteristic p, the map

$$a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \tag{7.3.6}$$

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

defines a two-dimensional representation of G that is indecomposable but not irreducible. It's not irreducible because it maps the x-axis to itself, and so contains the one-dimensional identity representation as a subrepresentation. Before, given a representation we could simplify it enough merely by writing it as a direct sum of indecomposables, but here there are far too many indecomposables. In other words, there are other more complicated ways to combine irreducibles than direct sum. The familiar role of irreducibles as direct summands is replaced here by their role as composition factors. It is completely analogous to, and simpler than, the role of simple groups in finite group theory (recall Section 1.1.2). Completely reducible representations (as in Theorem 1.1.2) are equivalent to a representation with blocks down the diagonal and zero-blocks above and below the diagonal; the diagonal blocks are its irreducible summands. On the other hand, a modular representation ρ is equivalent to a matrix with zero-blocks below the diagonal; the blocks along the diagonal (e.g. two copies of the trivial representation (1) for the representation in (7.3.6)) are the composition factors, and the blocks above the diagonal describe how these glue together.

Another complication is that the familiar character χ_ρ of (1.1.5) loses its usefulness. As we saw at the end of Section 1.1.3, very different modular representations can have identical characters. Instead, the more subtle *Brauer character* $\beta(\rho)$ is used. It can be defined as follows. Let m be the order $\|G\|$ of G, and write $m = p^a p'$ where p and p' are coprime. Let K be the cyclotomic field $\mathbb{Q}[\xi_m]$, and let $R = \mathbb{Z}[\xi_m]$ be the ring of cyclotomic integers. A finite field k of characteristic p can be obtained from R by choosing any prime ideal $\mathfrak{p}$ of R containing pR; then $k = R/\mathfrak{p}$. This construction of k defines a ring homomorphism $\phi_\mathfrak{p} : R \to k$. In particular, put $\xi := \xi_{p'} \in R$; then $\overline{\xi} = \phi_\mathfrak{p}(\xi)$ will be a primitive p'th root of unity in k.

Suppose ρ is some n-dimensional modular representation of G over k. Let $G_{p'}$ be the set of all p-regular elements in G. The field k defined above is big enough that the $n \times n$ matrix $\rho(g)$, for any $g \in G_{p'}$, is diagonalisable over k. More precisely, its n eigenvalues (counting multiplicities) are all p'th roots of unity in k, and so can be written as $\overline{\xi}^{\ell_i}$ for some integers ℓ_i, $1 \leq i \leq n$.

The Brauer character $\beta(\rho)$ of ρ is defined to be

$$\beta(\rho)(g) := \sum_{i=1}^{n} \xi^{\ell_i} \in R \subset \mathbb{C}, \qquad \forall g \in G_{p'}.$$

It is a well-defined class-function on $G_{p'}$, and in fact the Brauer characters form a basis for the space of class functions on $G_{p'}$. Two representations have the same Brauer character iff they have the same composition factors. Brauer characters were introduced by Brauer and his student Nesbitt in 1937. Apart from their role in modular representations, they also relate p-subgroups of G with properties of the usual character table. See Question 7.3.4 for an example.

Theorem 7.3.2 ([**484**], [**79**], [**77**]) *Let $g \in \mathbb{M}$ be any element of prime order p, for any p dividing $\|\mathbb{M}\|$. Then there is a vertex operator superalgebra ${}^g\mathcal{V} = \oplus_{n\in\mathbb{Z}} {}^g\mathcal{V}_n$ defined over the finite field $\mathbb{F}_p$ and carrying a (projective) representation of the centraliser $C_\mathbb{M}(g)$.*

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

If $h \in C_{\mathbb{M}}(g)$ is p-regular, then the graded Brauer character

$$R(g, h; \tau) := q^{-1} \sum_{n \in \mathbb{Z}} \beta({}^g\mathcal{V}_n)(h)\, q^n$$

equals the McKay–Thompson series $T_{gh}(\tau)$. Moreover, for g belonging to any conjugacy class in $\mathbb{M}$ except 2B, 3B, 5B, 7B *or* 13B*, this is in fact an ordinary VOA (i.e. the 'odd' part vanishes), while in those remaining cases the graded Brauer characters of both the odd and even parts can be expressed separately using McKay–Thompson series.*

We defined vertex operator superalgebras in Section 5.1.3. The centralisers $C_{\mathbb{M}}(g)$ in the theorem are quite nice: for example, for groups of type 2A, 2B, 3A, 3B, 3C, 5A, 5B, 7A, 11A these are extensions of the sporadic groups $\mathbb{B}$, Co_1, Fi'_{24}, Suz, Th, HN, HJ, He and M_{12}, respectively. The proof for $p = 2$ is not complete as it relies on a still-unproven hypothesis. The conjectures in [**484**] concerning modular analogues of the Griess algebra for several sporadic groups follow from Theorem 7.3.2.

Can these modular ${}^g\mathcal{V}$'s be interpreted as a reduction mod p of (super)algebras in characteristic 0? What can we say about elements g of composite order in $\mathbb{M}$?

Conjecture 7.3.3 (Borcherds [77]) *Choose any $g \in \mathbb{M}$ and let n denote its order. Then there is a $\frac{1}{n}\mathbb{Z}$-graded superspace ${}^g\widehat{\mathcal{V}} = \oplus_{i \in \frac{1}{n}\mathbb{Z}} {}^g\widehat{\mathcal{V}}_i$ over the ring of cyclotomic integers $\mathbb{Z}[e^{2\pi \mathrm{i}/n}]$. It is often (but probably not always) a vertex operator superalgebra – in particular, ${}^1\widehat{\mathcal{V}}$ is an integral form of the Moonshine module $V^\natural$. Each ${}^g\widehat{\mathcal{V}}$ carries a representation of a central extension of $C_{\mathbb{M}}(g)$ by $\mathbb{Z}_n$. Define the graded trace*

$$B(g, h; \tau) = q^{-1} \sum_{i \in \frac{1}{n}\mathbb{Z}} \mathrm{ch}_{{}^g\widehat{\mathcal{V}}_i}(h)\, q^i .$$

If $g, h \in \mathbb{M}$ commute and have coprime orders, then $B(g, h; \tau) = T_{gh}(\tau)$. If all q-coefficients of T_g are nonnegative, then the 'odd' part of ${}^g\widehat{\mathcal{V}}$ vanishes, so it is an ordinary space, and should equal the g-twisted module $V^\natural(g)$ of [**150**]. *If g has prime order p, then the reduction mod p of ${}^g\widehat{\mathcal{V}}$ is the modular vertex operator superalgebra ${}^g\mathcal{V}$ of Theorem 7.3.2.*

More precisely, ${}^g\widehat{\mathcal{V}}$ is to be a free module over the ring $\mathbb{Z}[e^{2\pi \mathrm{i}/n}]$, and each graded piece is finite-dimensional over that ring. When we say ${}^1\widehat{\mathcal{V}}$ is an integral form for $V^\natural$, we mean that ${}^1\widehat{\mathcal{V}}$ has the same structure as a VOA, with everything defined over $\mathbb{Z}$, and tensoring it with $\mathbb{C}$ gives $V^\natural$. Borcherds' conjecture, which beautifully tries to explain Theorem 7.3.2, is completely open. It provides the analogue for $V^\natural$ of the surprising Lie algebra Theorems 1.5.4 and 3.4.1.

7.3.6 McKay on Dynkin diagrams

McKay found other relationships with Lie theory [**411**], [**75**], [**247**], reminiscent of his A–D–E correspondence with finite subgroups of $\mathrm{SU}_2(\mathbb{C})$ (see Section 2.5.2). As we see from Table 7.2, $\mathbb{M}$ has two conjugacy classes of involutions. Let K be the smaller

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

one, called '2A' in [**109**] (the alternative, class '2B', has almost 100 million times more elements). The product of any two elements of K will lie in one of nine conjugacy classes: namely, 1A, 2A, 2B, 3A, 3C, 4A, 4B, 5A, 6A. These conjugacy classes are of elements of orders 1, 2, 2, 3, 3, 4, 4, 5, 6. It is remarkable that, for such a complicated group as $\mathbb{M}$, that list stops at only 6 – as we know from Section 7.3.3, we call $\mathbb{M}$ a 6-transposition group for this reason. The punchline: McKay noticed that those nine numbers are precisely the labels a_i of the affine E_8 diagram (see Figure 3.2). Thus we can attach a conjugacy class of $\mathbb{M}$ to each vertex of the $E_8{}^{(1)}$ diagram. A direct interpretation of the *edges* in the $E_8{}^{(1)}$ diagram, in terms of $\mathbb{M}$, is unfortunately not yet known, though [**247**], [**365**] establish how to unambiguously assign classes to the nodes.

We can't get the affine E_7 labels in a similar way, but McKay noticed that an order 2 folding of affine E_7 gives the affine F_4 diagram, and we can obtain its labels using the Baby Monster $\mathbb{B}$ (the second largest sporadic). In particular, let K now be the smallest conjugacy class of involutions in $\mathbb{B}$ (also labelled '2A' in [**109**]); the conjugacy classes in KK have orders 1, 2, 2, 3, 4 ($\mathbb{B}$ is a 4-transposition group) – these are the labels of $F_4{}^{(1)}$. Of course we'd prefer $E_7{}^{(1)}$ to $F_4{}^{(1)}$, but perhaps that *two*-folding has something to do with the fact that an order-2 central extension of $\mathbb{B}$ is the centraliser of an element $g \in \mathbb{M}$ of order 2.

Now, the *triple*-folding of affine E_6 is affine G_2. The Monster has three conjugacy classes of order 3. The smallest of these ('3A') has a centraliser that is a *triple* cover of the Fischer group $Fi_{24}'.2$. Taking the smallest conjugacy class of involutions in $Fi_{24}'.2$, and multiplying it by itself, gives conjugacy classes with orders 1, 2, 3 ($Fi_{24}'.2$ is a 3-transposition group) – and those not surprisingly are the labels of $G_2{}^{(1)}$!

McKay's $E_8{}^{(1)}$, $F_4{}^{(1)}$, $G_2{}^{(1)}$ observations still have no explanation. In [**247**] these patterns are extended, by relating various simple groups to the $E_8{}^{(1)}$ diagram with deleted nodes. More recently, [**365**] relate the $E_8{}^{(1)}$ observation to VOAs, by applying [**425**] to the lattice VOA $\mathcal{V}(\sqrt{2}E_8)$; the connection with $V^\natural$ is plausible but not yet completely established. As we know from Section 1.5.4, the folding of Coxeter–Dynkin diagrams arises when we restrict to the invariant subalgebras of automorphisms, so perhaps that provides a clue how to attack the $F_4{}^{(1)}$ and $G_2{}^{(1)}$ observations.

7.3.7 Hirzebruch's prize question

Algebra is the mathematics of structure, and so of course it has a profound relationship with every area of mathematics. Therefore the trick for finding possible fingerprints of Moonshine in, say, geometry is to look there for modular functions. And that search quickly leads to the elliptic genus.

We briefly discuss this in Section 5.4.2, where we mention several deep relationships between elliptic genera and the material covered elsewhere in this book. Let us simply mention here that the genus of a manifold will typically involve negative coefficients and be the graded dimension of a vertex operator superalgebra. This certainly doesn't preclude Moonshine-like behaviour – for example, Moonshine for Co_1 involves as we know the vertex operator superalgebra $A^{f\natural}$. However, the genera of even-dimensional

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

projective spaces has nonnegative integer coefficients [**400**]; it would be interesting to study the representation-theoretic questions associated with them.

Hirzebruch's 'prize question' (page 86 of [**287**]) asks for the construction of a 24-dimensional manifold M with Witten- or $\widehat{A}$-genus J (after being normalised by η^{24}). We would like $\mathbb{M}$ to act on M by diffeomorphisms, and the twisted Witten genera to be the McKay–Thompson series T_g. See also [**151**]. It would also be nice to associate Norton's series $N_{(g,h)}$ with this Moonshine manifold. Constructing such a manifold would realise the geometry underlying Monstrous Moonshine, and as such is perhaps the remaining Holy Grail in the subject.

Hirzebruch's question was partially answered by Mahowald–Hopkins [**399**], who constructed a manifold with Witten genus J, but couldn't show it would support an effective action of $\mathbb{M}$. Related work is [**21**], who constructed several actions of $\mathbb{M}$ on, for example, 24-dimensional manifolds (but none of which could have genus J), and [**364**], who showed the graded dimensions of the subspaces $V^\natural_\pm$ of the Moonshine module are twisted $\widehat{A}$-genera of Milnor–Kervaire's manifold M_0^8 (the $\widehat{A}$-genus is the specialisation of elliptic genus to the cusp $\mathrm{i}\infty$).

Related to elliptic genus is elliptic cohomology, which is described beautifully in [**499**]. Mason's constructions [**407**] associated with Moonshine for the Mathieu group M_{24} have been interpreted as providing a geometric model ('elliptic system') for elliptic cohomology $\mathrm{Ell}^*(BM_{24})$ of the classifying space of M_{24} [**523**], [**154**].

7.3.8 Mirror Moonshine

There has been a second conjectured relationship between geometry and Monstrous Moonshine. Calabi–Yau manifolds (see e.g. [**299**]) are a class of complex manifolds with an unusually rich mathematical structure – for example, in dimensions 1 and 2 they are elliptic curves and K3 surfaces, respectively. Specifying a Calabi–Yau manifold X means choosing a complex structure, as well as a Kähler class $[\omega] \in H^2(X, \mathbb{C})$. In the case of an elliptic curve (i.e. a torus), this corresponds to choosing parameters $\tau, \sigma \in \mathbb{H}$. Mirror symmetry [**291**] says that most Calabi–Yau manifolds come in closely related pairs, where the roles of the complex structure and Kähler structure are switched. In the case of elliptic curves, it relates the pair (τ, σ) to the pair (σ, τ) and implies the modularity of certain generating functions for Gromov–Witten invariants – see [**132**] for a review. This unexpected modularity is, of course, reminiscent of Moonshine, and it is tempting to look for a concrete connection.

Consider a one-parameter family X_λ of Calabi–Yau manifolds, with mirror X^* given by the resolution of an orbifold X/G for G finite and abelian. Then the Hodge numbers $h^{1,1}(X)$ and $h^{2,1}(X^*)$ will be equal, and more precisely the moduli space of (complexified) Kähler structures on X will be locally isometric to the moduli space of complex structures on X^*. The 'mirror map' $\lambda(q)$, which can be defined using the Picard–Fuchs equation [**438**], is a canonical map between those moduli spaces. For example, $x_1^4 + x_2^4 + x_3^4 + x_4^4 + \lambda^{-1/4} x_1 x_2 x_3 x_4 = 0$ is such a family of K3 surfaces, where $G = \mathbb{Z}_4 \times \mathbb{Z}_4$. Its mirror

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

map is given by

$$\lambda(q) = q - 104q^2 + 6444q^3 - 311\,744q^4 + 13\,018\,830q^5 - 493\,025\,760q^6 + \cdots . \tag{7.3.7}$$

Lian–Yau [**385**] noticed that the reciprocal $1/\lambda(q)$ of the mirror map in (7.3.7) equals the McKay–Thompson series $T_{2A}(\tau) + 104$. After looking at several other examples with similar conclusions, they proposed their *Mirror Moonshine Conjecture*: The reciprocal $1/\lambda$ of the mirror map of a one-parameter family of K3 surfaces with an orbifold mirror will be a McKay–Thompson series (up to an additive constant).

A counterexample (and more examples) are given in section 7 of [**544**]. In particular, although there are relations between mirror symmetry and modular functions (see e.g. [**266**] and [**275**]), there doesn't seem to be any special relation with $\mathbb{M}$. Doran [**158**] 'demystifies the Mirror Moonshine phenomenon' by finding necessary and sufficient conditions for $1/\lambda$ to be a modular function for a modular group commensurable with $\mathrm{SL}_2(\mathbb{Z})$.

This focus on K3 surfaces is not significant. Calabi–Yau 3-folds are the real meat of mirror symmetry, but it is much harder to find explicit families. Some of the interesting number theory of Calabi–Yau manifolds and mirror symmetry is reviewed in [**571**].

7.3.9 Physics and Moonshine

The physical side of Moonshine (namely, perturbative string theory and conformal field theory) was noticed early on, and has profoundly influenced the development of Moonshine and VOAs. This effectiveness of physical interpretations isn't magic – it merely tells us that finite-dimensional objects are sometimes seen much more clearly when studied through infinite-dimensional structures (often by being 'looped'). Of course Monstrous Moonshine, which teaches us to study the finite group $\mathbb{M}$ via its infinite-dimensional module $V^\natural$, fits perfectly into this picture.

Throughout this book we've described various points-of-contact between mathematics and physics. Because $V^\natural$ is so mathematically special, it may be expected that it corresponds somehow to interesting physics. Although there have been some attempts to directly interpret Monstrous Moonshine in the context of physics, we still have no evidence Nature concurs.

There is a $c = 24$ RCFT whose anti-holomorphic chiral algebra is trivial, and whose holomorphic one, as well as the state space $\mathcal{H}$, are both $V^\natural$ (this is possible because $V^\natural$ is holomorphic). This RCFT is nicely described in [**142**]; its symmetry is the Monster. The Bimonster $\mathbb{M} \wr \mathbb{Z}_2 = (\mathbb{M} \times \mathbb{M}) \rtimes \mathbb{Z}_2$ (Section 7.1.1) is the symmetry of a $c = \overline{c} = 24$ RCFT with state space $\mathcal{H} = V^\natural \otimes \overline{V^\natural}$. The paper [**119**] finds the D-branes (boundary states) of lowest mass for this theory; they are in one-to-one correspondence $g \mapsto \|g\rangle\!\rangle$ with the elements of $\mathbb{M}$. The Bimonster permutes them: $(h, k).\|g\rangle\!\rangle = \|hgk^{-1}\rangle\!\rangle$, while the remaining involution sends $\|g\rangle\!\rangle$ to $\|g^{-1}\rangle\!\rangle$. Most interestingly, their 'overlaps' $\langle\!\langle g\|q^{\frac{1}{2}(L_0+\bar{L}_0-\frac{c}{24})}\|h\rangle\!\rangle$ equal the McKay–Thompson series $T_{g^{-1}h}$. We largely ignored D-branes (surfaces on which endpoints of open strings rest) in Chapter 4, but they are a

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press

natural ingredient in string theory. Much as every natural property of the Wess–Zumino–Witten string translates nicely into Lie theory, it would appear that the same holds with the string theory $\mathcal{H} = V^\natural \otimes \overline{V^\natural}$ and the Monster $\mathbb{M}$. Surely it would be interesting to continue that investigation. Other suggestions for the physics of Monstrous Moonshine are [**99**], [**274**], [**96**], [**260**], [**281**].

Question 7.3.1. Let $f(\tau)$ be a Hauptmodul for some genus-0 group Γ. For any $a > 0$, prove that $f(a\tau)$ is fixed by a genus-0 group (call it Γ_a), and any modular function for Γ_a will be a rational function in $f(a\tau)$.

Question 7.3.2. Let G be any group with exponent $k < 6$ (i.e. $g^k = e$ for all $g \in G$). Suppose there are a set of functions $N_{(g,h)}(\tau)$ associated with every commuting pair $g, h \in G$, with the property that equation (7.3.3) always holds with $\alpha = 1$. Prove that each of these functions is fixed by a genus-0 subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Question 7.3.3. Assume for simplicity that $g \in \mathbb{M}$ is such that $C_{\mathbb{M}}(g)$ acts linearly (i.e. nonprojectively) on the twisted module $V^\natural(g)$. Then for $h \in C_{\mathbb{M}}(g)$ of order n, the q-coefficients of $\mathcal{Z}(g, h)$ all lie in the field $\mathbb{Q}[\xi_n]$. Fix any Galois automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q})$, and let $\sigma\mathcal{Z}(g, h)$ denote the q-expansion obtained by formally applying σ term-by-term to $\mathcal{Z}(g, h)$: $\sigma(\sum_i a_i q^i) = \sum_i \sigma(a_i) q^i$. Show that $\sigma\mathcal{Z}(g, h)$ equals another series $\mathcal{Z}(g', h')$, for some $g' \in \mathbb{M}$, $h' \in C_{\mathbb{M}}(g')$.

Question 7.3.4. Consider the usual representation ρ of $G = \mathcal{S}_3$ by 3×3 permutation matrices, associating with $\pi \in \mathcal{S}_3$ the matrix $\rho(\pi)$ obtained from the identity matrix by applying π to the components of each column. For example,

$$\rho(123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Show that ρ is completely reducible when considered as a modular representation over characteristic 2, but is not completely reducible when considered as a modular representation over characteristic 3. For both characteristic 2 and 3, compute its Brauer character using the definition given in Section 7.3.5.

https://doi.org/10.1017/9781009401548.008 Published online by Cambridge University Press