MONSTROUS MOONSHINE

J. H. CONWAY AND S. P. NORTON

A quick summary of the recent amazing discoveries about the Fischer-Griess "MONSTER" simple group.

Section 1. *History.*

In 1973 Bernd Fischer and Bob Griess independently produced evidence for a new simple group *M* of order

246.32O.59 .7⁶ .11² .13³ .17.19.23.29.31.41.47.59.71

 $= 8080, 17424, 79451, 28758, 86459, 90496, 17107, 57005, 75436, 80000, 00000.$

We proposed to call this group the MONSTER and conjectured that it had a representation of degree 196883. In a remarkable piece of work, Fischer, Livingstone and Thome [6] have recently computed the entire character table on this assumption. The MONSTER has not yet been proved to exist, but Thompson [18] has proved its uniqueness on similar assumptions.

Here are some observations (roughly in chronological order) that are now known not to be mere coincidences:—

- (A) M. J. T. Guy observed a certain symmetry in the character table of the monomial group $2^{12} M_{24}$ of [5].
- (B) We pointed out long ago that the elements of M_{24} have "balanced" cycleshapes, so that $a^{\alpha} b^{\beta} c^{\gamma}$... is the same as $(N/a)^{\alpha} (N/b)^{\beta} (N/c)^{\gamma}$... for some N. Example 1^2 .2.4.8², for which $N = 8$.
- (C) For each prime *p* with (p —1)|24 there is a conjugacy class (called *p—* below) of elements of M, with centraliser of form p^{1+2d} . G_p , where p . G_p is the centraliser of a corresponding automorphism of the Leech Lattice. [The symbol p^{1+2d} denotes an extraspecial p-group, and $2d = 24/(p-1)$.]
- (D) For the same p, there is a second class $p +$, and the characters of $p +$ and $p -$ in the minimal faithful representation differ by p^d . (Similar properties were observed for elements of order *2p.)*
- (E) Ogg [15] noticed that the primes p dividing $|M|$ are just those for which the function field determined by the normaliser of $\Gamma_0(p)$ in $PSL_2(\mathbb{R})$ has genus zero. (t)

Received 8 May, 1979.

[BULL. LONDON MATH. Soc., 11 (1979), 308-339]

f Very recently A. Pizer [16] has shown that these primes are the only ones that satisfy a certain conjecture of Hecke (1936, op. cit.) relating modular forms of weight 2 to quaternion algebra theta-series.

(F) McKay noticed that one of the coefficients in the g-series

$$
j = q^{-1} + 744 + 196884q + 21493760q^{2} + \dots = \sum a_{r} q^{r}, \text{ say,}
$$

is $196883+1$, and Thompson [17] found that the later a_r are also simple linear combinations of the character degrees f_r of M :-

 $a_{-1} = f_1$, $a_1 = f_1 + f_2$, $a_2 = f_1 + f_2 + f_3$, $a_3 = 2f_1 + 2f_2 + f_3 + f_4$.

Our Tables 1 and 1a, extracted from [6] and [19], give f, and a,.

(G) Finally, the Lie group E_8 has dimension $248 = 744/3$.

Section 2. The main conjectures

As usual, we write Γ for the group $PSL_2(\mathbb{Z})$ of all linear fractional transformations

$$
z \to \frac{az+b}{cz+d} \quad (a, b, c, d \in \mathbb{Z}, ad-bc=1)
$$

and $\Gamma_0(N)$ for the congruence subgroup of all elements with $N|c$. The modular group Γ acts on the upper half-plane, and leaves invariant the field of rational functions of *i*. Various other discrete subgroups of $PSL_2(\mathbb{R})$ give rise to function fields that are of genus zero and so can be expressed in terms of a single function analogous to*^j .* For instance this happens for $\Gamma_0(N)$ in the cases $N \leq 10$.

In all cases that concern us, the group contains the map $z \rightarrow z+1$, so that the functions can be written in terms of $q = e^{2\pi i z}$. We call such a function *normalised* if its q-series begins q^{-1} +0+aq +bq²+..., so that the normalised function for Γ is not *i*, but $J = j - 744$.

Thompson proposed that the coefficients in the g-series for *J* be replaced by the representations of *M* that they "suggest", so that we obtain a formal series

$$
H_{-1}q^{-1}+0+H_1q+H_2q^2+H_3q^3+\dots
$$

in which the *Hr* are certain representations of *M* that we call its *head representations. H*, has degree a_r , as in Table 1a, and, for example, H_{-1} is the trivial representation (degree 1), while H_1 is the sum of this and the degree 196883 representation.

Thompson also suggested that on replacing the *Hr* by their character values *Hr(m)* for various elements *m* of *M* we obtain other functions that might be worth investigating. We have now evaluated these to the q^{10} term for every $m \in M$, and the results fully justify this idea. In fact we conjecture:—

The series

$$
T_m = q^{-1} + 0 + H_1(m)q + H_2(m)q^2 + \dots
$$

is the normalised generator of a genus zero function field arising from a group between $\Gamma_0(N)$ and its normaliser in $PSL_2(\mathbb{R})$. The modular groups that arise have a certain *natural parameterisation, described later, and there are many formulae for the modular functions in terms of the eigenvalues of certain automorphisms of the Leech Lattice.*

The correspondence between MONSTER conjugacy classes and the genus zero function fields described above is quite remarkable, and at one stage we conjectured that it was essentially 1 to 1. Although this is now disproved, the following points deserve mention:—

- (0) A MONSTER element and its inverse have the same Thompson series, as do the two distinct conjugacy classes of elements of order 27.
- (1) Although there are no further equalities between these series, there are some linear dependences, for example

$$
T_{6+} + 2T_{6-} = T_{6+2} + T_{6+3} + T_{6+6}
$$

(and similarly for other 4-groups found from Table 3). Oliver Atkin has verified our guess that there are exactly enough of these dependences to bring the dimension down to 163. (See Section 8.)

- (2) From column 3 of "Antwerp IV s Table 5" [1] one can extract the genus of all function fields corresponding to involutory subgroups of the normaliser of $\Gamma_0(N)$ for $N \le 300$. The last genus zero entry in that table is for the normaliser of $\Gamma_0(119)$, and indeed 119 is the largest order of any element of M. All genus zero cases but three, the "ghost elements" 25Z, 49Z, 50Z of our Table 2, correspond to elements of M . There is some hope of making the correspondence exact by adding functional conditions, because the modular functions in just these three cases have abnormal product formulae. Of course, this correspondence includes observation E.
- (3) Our parametrisation for the modular groups suggests various relations between the classes, illustrated in our Table 3, and various identities between the corresponding modular functions, of which observations D and G are consequences.
- (4) There are various correspondences between automorphisms of the Leech Lattice and MONSTER classes, which give rise to interesting formulae for the appropriate modular functions. Fixed-point-free automorphisms play a special role here, and there are connections with observation C. We can also deduce observation B from observation A and properties of the modular functions concerned.
- (5) Of course the condition that *Hr* be a MONSTER representation of degree *ar* does not determine *H*, uniquely (for example, each *H*, could be a multiple of the trivial representation). Even when we restrict attention to cases with small multiplicities ambiguities soon arise. However, the additional properties noted above have resolved these up to H_{10} , and, in principle, completely. One of the decompositions suggested in [17] has had to be altered.
- (6) Had our conjectures been available some time ago they would have afforded an easy route to the computation of the MONSTER character table. It has not escaped our attention that the BABY MONSTER characters have not yet been found, and that the conjectures might help us to find them! Perhaps they could later be verified using the Brauer-Tate theorem.
- (7) The resulting notations $T_m = T_{n|h+e,f,g}$, and $t_m = T_m + constant$ for certain modular functions are convenient in their own right, and happily generalise some that have already been used (e.g., Birch [4]).

Section 3. *The normaliser of* $\Gamma_0(N)$.

It is a curious fact that the divisors *h* of 24 are precisely those numbers *h* for which $xy \equiv 1 \pmod{h}$ implies $x \equiv y \pmod{h}$. We shall use this fact to give a simple description of the normaliser of $\Gamma_0(N)$ in $PSL_2(\mathbb{R})$ which does not seem to be generally known. Let *h* be the largest divisor of 24 for which $h^2|N$, and let $N = nh$.

Then from the rather complicated description of the normaliser in [3] it can be deduced that it consists exactly of the matrices

$$
\binom{ae\ b/h}{cn\ de}\ =\ \binom{a\ b}{c\ d}\, , \text{ say, for } e\bigg|\frac{n}{h}\, ,
$$

with the understandings that the determinant of the matrix is $e > 0$, and that $r\|s$ means that *r\s* and *(r,s/r) =* 1. (We call *r* an *exact, unitary,* or *Hall* divisor of *s.)*

Since these matrices can be multiplied by the rule

$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix}_{e} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}_{e} = u \text{ times } \begin{cases} au\alpha + bx\gamma & av\beta + bw\delta \\ cw\alpha + dv\gamma & cx\beta + du\delta \end{cases}_{vw}
$$

(where $e = uv$, $\varepsilon = uw$, $n/h = uvwx$, and u, v, w, x are coprime) they do indeed form a group, up to scalar multiplication.

Moreover, the conditions for
$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix}_e
$$
 to be in $\Gamma_0(N)$ are simply that

$$
b \equiv c \equiv 0 \pmod{h}
$$

and also

 $e = 1 = ad - bc(n/h)$, so that $ad \equiv 1 \pmod{h}$

whence

$$
a \equiv d \pmod{h}
$$

by our "defining property of 24 ".

So we see that $\begin{bmatrix} c & d \end{bmatrix} \in I_0(V)$ just when $e = 1$ and $\begin{bmatrix} c & d \end{bmatrix}$ is congruent modulo *h* to an invertible scalar multiple of the identity. It follows that $\begin{bmatrix} c & d \end{bmatrix}$ and $\begin{bmatrix} \gamma & \delta \\ \gamma & \delta \end{bmatrix}$ lie in the same (left *or* right) coset of $\Gamma_0(N)$ just when

 $e = \varepsilon$ and $a \equiv k\alpha$, $b \equiv k\beta$, $c \equiv k\gamma$, $d \equiv k\delta \pmod{h}$

for some *k* invertible mod *h,* and so this set of matrices really does normalise $\Gamma_0(N)$.

From the indices given in the last theorem of Atkin-Lehner [3], we see that it is the full normaliser in $PSL_2(\mathbb{R})$, while the normaliser in $PSL_2(\mathbb{C})$ or $PGL_2(\mathbb{R})$ can be obtained simply by removing the condition *e >* 0.

Section 4. *Subgroups of the normaliser*

A number of subgroups deserve special mention.

(0) The map $z \to -1/Nz$, which we call the Fricke involution, is in the normaliser, and extends $\Gamma_0(N)$ to a group we call the Fricke group, in which $\Gamma_0(N)$ has index 2.

(1) Provided $N = nh$, where $h/24$ and h^2/N the matrices

$$
\binom{a \ b/h}{cn \ d} = \binom{a \ b}{c \ d} \Big\} \quad \text{of determinant 1}
$$

form a group, even when *h* is not the largest divisor of 24 with this property. Since this group is a conjugate of $\Gamma_0(n/h)$ by $\binom{h}{0}$ we shall call it $\Gamma_0(n/h)$.

(2) The set W_e of all matrices of the form

$$
\begin{pmatrix} ae & b \\ cN & de \end{pmatrix} = \begin{pmatrix} a & bh \\ ch & d \end{pmatrix}_e
$$
, where $e||N$, and the determinant is e

is a single coset of $\Gamma_0(N)$. We have the relations

$$
W_e^2 \equiv 1
$$
, $W_e W_f \equiv W_f W_e \equiv W_g \pmod{\Gamma_0(N)}$, where $g = \frac{e}{(e, f)} \cdot \frac{f}{(e, f)}$

which show that these cosets form a subgroup of the normaliser that we call *the involutory normaliser.* They are called the *Atkin-Lehner involutions* for $\Gamma_0(N)$, and we can regard the Fricke involution as the special case W_N .

 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}_e$ with a given value of *e* forms a $\begin{pmatrix} h & 0 \\ 0 & h \end{pmatrix}_e$ single coset of $r_0(n|n)$, which is of course the conjugate by $\begin{pmatrix} 0 & 1 \end{pmatrix}$ of an Atkin-Lehner involution for $\Gamma_0(n/h)$. We shall therefore call w_e an Atkin-Lehner involution for $\Gamma_0(n|h)$, and this time the Fricke involution is $w_{n/h}$.

In this language we can summarise our results:—

The full normaliser of $\Gamma_0(N)$ *in* $PSL_2(\mathbb{R})$ *is obtained by adjoining to the group* $\Gamma_0(n|h)$ [which is a conjugate of $\Gamma_0(n|h)$] its Atkin-Lehner involutions [which are conjugate to those of $\Gamma_0(n/h)$].

(4) We shall use the notation

$$
\Gamma_0(n|h)+e,f,g,\ldots
$$

for the group obtained from $\Gamma_0(n|h)$ by adjoining its particular Atkin-Lehner involutions w_e, w_f, w_g, \ldots . We further abbreviate this notation (and similar notations later) by:—

- (i) omitting " $|h$ " when $h = 1$
- (ii) writing $\Gamma_0(n|h)$ + when *all e* $\|n|h\|$ are present
- (iii) writing $\Gamma_0(n|h)$ when *no e* (except 1) is present.

Of course, the " $-$ " in (iii) is optional, but is often included for greater clarity.

Section 5. *The modular groups for elements of M*

If $m \in M$ and $q = e^{2\pi i z}$, then the Thompson series

$$
T_m = q^{-1} + 0 + H_1(m) \cdot q + H_2(m) \cdot q^2 + \dots
$$

(in which $H_r(m)$ is the character of the rth head representation at m) defines a function of z which determines four subgroups of $PSL_2(\mathbb{R})$ with varying degrees of interest:

- *F(m)* consists just of the elements of $PSL_2(\mathbb{R})$ that fix T_m ,
- $E(m)$ of the elements that multiply it by hth roots of 1,
- *D(m)* of the elements that multiply it by *any* roots of 1,
- $C(m)$ of elements that convert it to functions $(AT_m + B)/(CT_m + D)$.

We call *F(m)* the *fixing group* and *C(m)* the *converting group,* and use the term *eigengroup* for *E(m)* rather than for the *distended eigengroup D(m)* because the latter seems to be of less interest in this context.

Now an element $m \in M$ determines a number N in any of three ways:

- (1) as the *level* of the group *F(m),*
- (2) as the *least N* with $z \rightarrow z/(Nz+1)$ in $F(m)$,
- (3) as the *unique N* with $z \rightarrow -1/Nz$ in $C(m)$.

Having determined N, we write $h = N/n$, where n is the order of m, and observe that in fact *h* is always an integer, $h|24$, and $h^2|N$.

Then we conjecture:-

- $E(m)$ has the form $\Gamma_0(n|h) + e, f, g, \ldots$
- *F(m)* is a certain subgroup of index *h* in this.

[It is easy to see that $C(m)$ is the normaliser of $F(m)$ in $PSL_2(\mathbb{R})$, and we are not very interested in $D(m)$, which is occasionally larger than $E(m)$.] To specify $F(m)$ exactly it will suffice of course to specify the eigenvalue λ by which a given element of $E(m)$ multiplies T_m . We believe:-

- (0) $\lambda = 1$ for elements of $\Gamma_0(N)$, so is constant on cosets of $\Gamma_0(N)$,
- (1) $\lambda = 1$ for all the Atkin-Lehner involutions of $\Gamma_0(N)$ inside $E(m)$,

(2)
$$
\lambda = e^{-2\pi i/h}
$$
 for the coset $\begin{pmatrix} 1 & 1 \ 0 & 1 \end{pmatrix}$ ₁ (i.e., $e = 1$, $a \equiv b \equiv d \equiv 1$, $c \equiv 0 \pmod{h}$),
\n(3) $\lambda = e^{\pm 2\pi i/h}$ for the coset $\begin{pmatrix} 1 & 0 \ 1 & 1 \end{pmatrix}$ (i.e., $e = 1$, $a \equiv c \equiv d \equiv 1$, $b \equiv 0 \pmod{h}$),

the sign in (3) being + if $z \rightarrow -1/Nz$ is in $E(m)$, - if not.

It can be checked that the cosets in (2) and (3) generate $\Gamma_0(n|h)$, so that (0-3) completely determine λ , and therefore the exact fixing group $F(m)$.

We shall use the symbol

$$
n|h+e,f,g,\ldots
$$

as a name for the set of MONSTER elements *m* for which *E(m)* has the form

 $\Gamma_0(n|h) + e, f, g, \ldots$.

By the remarks in Section 2, this set is a union of one or two conjugacy classes, and we loosely call it a *class.* We abbreviate its name in similar ways to those in which we abbreviate the names for groups.

Section 6. *Relations between the classes*

Our parametrisation shows up a number of relations between the classes. In particular, the power maps are very simply expressed:—

The dth power of n| $h + e, f, g, \ldots$ *is of class n'*| $h' + e', f', g', \ldots$ *, where n' = n|*(n,d), $h' = h/(h,d)$, and e', f', g', \ldots are the divisors of n'/h' among the numbers e, f, g, \ldots .

In the case that $d|h$ we call m the dth harmonic of m^d , and we call the elements with $h = 1$ the *fundamental* elements. The general element, of class $n|h + e, f, g, ...$ is therefore the *h*th harmonic of a fundamental one of class $(n/h) + e, f, g, ...$ [In a slight divergence from musical terminology, fundamentals are their own first harmonics, rather than zeroth harmonics.]

If m' is the *dth* harmonic of m , then for an appropriate choice of the functions t_m and $t_{m'}$ we have

$$
t_m(z) = [t_m(dz)]^{1/d}
$$

$$
E(m')
$$
 is the conjugate of $E(m)$ by $\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$

F(m') contains the corresponding conjugate of *F(m)* to index *d.*

If *M + e* is the class obtained from class *M* under symmetrisation by a further Atkin-Lehner involution w_e , then for an appropriate choice of the functions t_M and t_{M+e} we have

 $t_{M+e} = t_M(z) + k/t_M(z)$ $E(M+e) = E(M)$ extended by w_e

 $F(M + e)$ contains $F(M)$ to index 2.

Each line of Table 3 illustrates a number of such relationships, and makes a simultaneous choice of the appropriate functions. The typical line starts with the symbol for a fundamental element of class *m* followed by a formula for the appropriate *tm,* and then gives the Atlas names for all harmonics of *m* (including *m* itself), followed in parentheses by their symmetrisations (with the relevant constants *k).*

Some lines also give, after a semicolon, additional product formulae for the fundamental t_m (with different constants), and at the end of the table there are some cases of "pseudoharmonics", for which $t_m(z) = [t_m(dz)]^{1/d}$, but our other conditions for harmonics are not all satisfied.

Thus the first line of the table tells us that *\A* and 3C are the first and third harmonics of the identity, with functions $t_{1A} = j$, $t_{3C} = (j(3z))^{1/3}$. From the second line, 2B, 4D, 6F, 8F, 12J, 24J are the harmonics of 2-, with symmetrisations

$$
t_{2A} = t_{2B} + 4096/t_{2B}, \quad t_{4B} = t_{4D} + 64/t_{4B}.
$$

The symbol $1^{24}/2^{24}$ tells us that the appropriate function to use for class 2B is

$$
\eta(z)^{24}/\eta(2z)^{24} = T_{2B} - 24,
$$

and so a product formula for its dth harmonic is $[\eta(dz)/\eta(2dz)]^{24/d}$.

The table is complete for all harmonics, pseudoharmonics, and symmetrisations within M, and displays all product formulae for the t_m in terms of factors $\eta(kz)$.

Section 7. *Relations with the Leech Lattice*

There are several correspondences between automorphisms of the Leech Lattice L (see [13], [5]) and elements of M. Because L is a rational lattice, we can use Frame's "generalised permutation" notation, [7], in which we say that an automorphism π has shape $a^{\alpha} b^{\beta}$.../c^{*y*} d^{δ} ... meaning that its eigenvalues can be obtained by removing those of a permutation of cycle-shape $c^{\gamma}d^{\delta}$... from those of one of shape $a^{\alpha} b^{\beta}$...

We then write

 $\eta_{\pi}(z)$ for $\eta(az)^{\alpha} \eta(bz)^{\beta}$... $/\eta(cz)^{\gamma} \eta(dz)^{\delta}$...

 L_{π} for the sublattice of L fixed by π , and

 $\theta_n(z)$ for the θ -function of L_n , namely $\sum u_n q^n$,

where u_n is the number of vectors of norm $2n$ in L_n .

Then it seems that there is always a class of elements π_1 in M whose Thompson *series has a form* $\theta_{\pi}(z)/\eta_{\pi}(z)$.

Some of the product formulae in Table 3 arise in this way from cases in which π acts fixed-point-freely on L, so that $\theta_{\pi} = 1$. But to understand some of the others, we shall need to study the groups $p \cdot G_p$ of our observation (C) in more detail.

If π is a fixed-point-free automorphism of L of prime order p, its eigenvalues must be the $p-1$ primitive pth roots of unity, each repeated $24/(p-1) = 2d$ times. [The fact that this number is even follows either from a case-by-case analysis $\binom{p-2}{2d} = 24.12.6.4.2$ or from later statements.] Now since π and the complex number $e_n = e^{2\pi i/p}$ have the same minimal polynomial $t^{p-1} + t^{p-2} + ... + t + 1$ over \mathbb{Z} . we can define $v.f(e_p) = v.f(\pi)$ for each $v \in L$ and each polynomial $f(t) \in \mathbb{Z}[t]$, and so turn L into a 2d-dimensional lattice over $\mathbb{Z}[e_n]$. The automorphisms of L that preserve this structure are just those that commute with π , and they form the group p.G_p of observation (C).

[We use an extended form of the notation first introduced in [5], under which the symbols

while A.B just means a group with a normal subgroup of type A whose quotient has type B.]

When we factor by the ideal generated by $e_n - 1$, $\mathbb{Z}[e_n]$ becomes the field of order p, and so *L* becomes a vector space *L(p)* of dimension *Id* over this, or equivalently an elementary abelian group of order *p 2d.* It follows that *Gp* has an action on this group, so that there exists a group p^{2d} . G_p . Moreover, a suitable complex multiple of the inner product on *L* yields a symplectic inner product on $L(p)$, so that there exists a group p^{1+2d} . G_p with the property that for $x, y \in p^{1+2d}$ we have

$$
x^{-1}y^{-1}xy = m^{\bar{x}\cdot\bar{y}}
$$

where *m* is the central element of p^{1+2d} and \bar{x} . \bar{y} the symplectic inner product of the images of *x* and *y* in *L(p).*

Now it happens that the centraliser in M of an element *m* of class *p—* is a group p^{1+2d} . G_p of just this form. The particular cases are

It appears that if π is an automorphism of L whose p-part is the central element of $p.G_p$, then the element π_1 of M considered above can be taken as an element of p^{1+2d} . G_p whose p-part is the central element of this group, and which has the same image in G_n as π does.

However, it seems that the correspondence between π and π_1 is not the only one of interest. If π is an element of p . G_p of Frame-shape $a^{\alpha}b^{\beta}$..., there is usually an element π_n of *M* with product formula

$$
a^{\alpha} b^{\beta} \dots / (p a)^{\alpha} (p b)^{\beta} \dots
$$

Thus, if π is the automorphism $x \to -x$ of L, regarded as an element of 2. G_2 , it has Frame-shape $2^{24}/1^{24}$, so that π_2 has product formula

$$
(2^{24}/1^{24})/(4^{24}/2^{24}) = 2^{48}/1^{24} 4^{24}
$$

which we see from Table 3 corresponds to MONSTER class $4+$. In these calculations, the Frame-shape to use is that corresponding to the representation of $p \cdot G_p$ on a 2*d*-dimensional lattice over $\mathbb{Z}[e_n]$.

There appear to be similar correspondences $\pi \rightarrow \pi_n$ for non-prime *n*—we shall not go into more detail here. Since $p \cdot G_p$ (or more generally $n \cdot G_n$) is not always a rational group, the automorphisms involved are not always expressible in Frame's notation, and the obvious generalisation of our remarks (which works!) involves η -functions evaluated at points of the form $nz+(a/b)$. A number of such formulae, not all obtainable in this way, are given in Table 3a.

We show in Section 11 that the number of product formulae of this type for a given function T_m (+constants) is at most equal to the number of finite values taken by *Tm* at cusps. The formulae of Tables 3 and 3a show that this bound is attained for all functions T_m except those corresponding to the three ghost elements 25Z, 49Z, 50Z. The "missing" formulae in these cases are also given in Table 3a; they involve a slightly generalised kind of η -function.

Michael Guy's symmetry of $2^{12} M_{24}$ shows that that group has an element of shape $(2a)^{\alpha}(2b)^{\beta} \dots/a^{\alpha} b^{\beta} \dots$ whenever M_{24} has one of shape $a^{\alpha} b^{\beta} \dots$. The "balance" property of M_{24} now follows from the fact that the corresponding η -function product formula is inverted by the Fricke involution $z \to -1/2Nz$. (See Section 11.)

A more complicated formula apparently enables us to compute t_m for any m in the centraliser $G_1 = 2^{1+24}$. C_1 of an element of class 2-. We regard m as the image of two elements π and $-\pi$ of the central extension $G_0 = 2^{1+24}$. C_0 of G_1 , and can then define $\eta_{\pi}, L_{\pi}, \theta_{\pi}$ as above, since the quotient group C_0 acts on the Leech Lattice. Also, since any vector *v* of L_n has a natural image in the group 2^{24} , it may be called symmetric or skew according as the two corresponding elements of 2^{1+24} are fixed or interchanged on conjugating by π . If we define

$$
\theta_{\pi}^{-}(z) = \sum_{v \in L_{\pi}} \pm q^{\text{norm}(v)} \quad (+ \text{ for symmetric } v, - \text{ for skew } v)
$$

then our formula is

$$
t_m(z) = \frac{1}{2} \left(\frac{\theta_{\pi}^{}(z) + \delta_{\pi} \cdot \theta_{\pi}(2z)}{\eta_{\pi}(z)} + \frac{\theta_{-\pi}^{}(z) + \delta_{-\pi} \cdot \theta_{-\pi}(2z)}{\eta_{-\pi}(z)} \right)
$$

where δ_{π} is the value at π of the unique character of degree 2^{12} for G_0 that restricts irreducibly to the extraspecial group 2^{1+24} .

We make the following remarks:

- (0) t_m is well-defined by the formula, since it is symmetric in π and $-\pi$.
- (1) Classes of G_1 that fuse in M should yield the same function T_m , but the formula may well give different constant terms for t_m .
- (2) It follows from its expression in terms of eigenvalues that the coefficient of q^n in $1/\eta_{\pi}(z)$ is a character of G_0 , and it can be seen that the coefficients in θ_{π} ⁻(z)+ δ_{π} . θ_{π} (2z) are characters of G₀ obtained by induction from linear characters of various subgroups. These remarks entail that the coefficients in our formula are characters of G_1 .
- (3) We have not been able to find similar formulae for the centralisers of elements of classes $3 -$, $5 -$, $7 -$, and $13 -$. If this could be done, it would, in virtue of the Brauer-Tate theorem, go a long way towards establishing our main conjecture that the coefficients of the T_m are characters of M.

Section 8. *The replication and other formulae*

Let us write $J(z) = T_1(z) = j(z) - 744 = q^{-1} + a_1 q + a_2 q^2 + ...$ Then for any prime number *p* the expression

$$
K(z) = J(pz) + J\left(\frac{z}{p}\right) + J\left(\frac{z+1}{p}\right) + \dots + J\left(\frac{z+p-1}{p}\right)
$$

= $q^{-p} + a_1 q^p + a_2 q^{2p} + \dots + p\{a_p q + a_{2p} q^2 + \dots\}$

is invariant under Γ , which permutes its $p+1$ arguments. Since it has no poles inside the upper half-plane, it is actually a polynomial in *J,* whose coefficients can be found from the leading terms. We deduce that there is an identity of the form

$$
\frac{1}{p} \{J^p(z) - J(pz)\} = f(J) + a_p q + a_{2p} q^2 + \dots
$$

Such identities exist also for composite multipliers, and apparently always have character valued versions, which we call *replication formulae,* obtained by replacing each a_r , by a suitable value of H_r . Here are the first few cases:—

$$
\frac{1}{2}\lbrace T^2 - T_{(2)}(2z)\rbrace = \lbrace H_2 q + H_4 q^2 + ... \rbrace + H_1 \quad \text{(duplication)}
$$
\n
$$
\frac{1}{3}\lbrace T^3 - T_{(3)}(3z)\rbrace = \lbrace H_3 q + H_6 q^2 + ... \rbrace + H_1 T + H_2 \quad \text{(triplication)}
$$
\n
$$
\frac{1}{4}\lbrace T^4 - T_{(4)}(4z) - T_{(2)}(z) - T_{(2)}(z + \frac{1}{2})\rbrace
$$
\n
$$
= \lbrace H_4 q + H_8 q^2 + ... \rbrace + H_1 T^2 + H_2 T + (H_3 - \frac{1}{2}H_1^2)
$$
\n
$$
\frac{1}{3}\lbrace T^5 - T_{(5)}(5z)\rbrace
$$
\n
$$
= \lbrace H_5 q + H_{10} q^2 + ... \rbrace + H_1 T^3 + H_2 T^2 + (H_3 - H_1^2) T + (H_4 - H_2 H_1).
$$

where $T = T_m(z)$, $T_{(n)} = T_{m^n}$, and $H_r = H_r(m)$. To obtain the *n*-plication formula, set

$$
K(z) = \sum J\left(\frac{nz + dr}{d^2}\right)
$$
, summed over $d|n$ and $0 \le r \le d$

and replace a, by $H_r(m^{n/d})$ inside $K(z)$ and by $H_r(m)$ outside (including appearances in the coefficients of f).

Comparing powers of *q* we obtain many identities, for example

$$
H_4 = H_3 + H_1^{2-}
$$

\n
$$
H_6 = H_4 + H_2 H_1
$$

\n
$$
H_8 = H_5 + H_3 H_1 + H_2^{2-}
$$

\n
$$
H_9 = H_5 + H_3 H_1 + H_2^{2} + H_1^{[21]}
$$

\n
$$
H_{10} = H_6 + H_4 H_1 + H_3 H_2
$$

\n
$$
H_{12} = H_7 + H_5 H_1 + H_4 H_2 + H_3^{2-}
$$

\n
$$
H_{12} = H_6 + H_4 H_1 + 2H_3 H_2 + H_2 H_1^{2}
$$

from the duplication and triplication formulae, where

$$
H_r^{2-} = \frac{1}{2} \{ H_r^{2}(m) - H_r(m^2) \} H_r^{[21]} = \frac{1}{3} \{ H_r^{3}(m) - H_r(m^3) \}.
$$

Although it seems that the *a*-plication and *b*-plication formulae agree at H_{ab} , we get new relations in other cases when there are two formulae for the same H_n . For example, our two formulae for H_{12} show that H_7 can be expressed in terms of H_1,H_2,H_3,H_5 , and similar methods show that the same is in fact true of all H_n . We can also find a number of relations, of increasing complexity, between H_1, H_2, H_3 , and $H₅$.

When the fixing group $F(m)$ contains the involution w_p , the two sides of

$$
T_m(z) + T_m\left(\frac{z}{p}\right) + T_m\left(\frac{z+1}{p}\right) + \ldots + T_m\left(\frac{z+p-1}{p}\right) = T_{m,p}(z)
$$

will have the same invariance group and leading terms, and must therefore be equal. Between this *compression formula* and the corresponding replication formula we can eliminate some terms to get an *expansion formula,* of which the prototype is

$$
J(z) + J(2z) = T_{2+}^2(z) + T_{2+}(z) - 2H_1(2+).
$$

Some other instances, providing expressions for T_m as roots of polynomials involving T_{m} , have been used in Table 4a.

There are other types of compression formula in which the symmetrisation involves some Atkin-Lehner involution or is achieved in other ways, for example

$$
T_{2+}(z) = T_{2-}(z) - T_{2-}\left(\frac{z}{2}\right) - T_{2-}\left(\frac{z+1}{2}\right)
$$

$$
T_{4+}(z) = T_{4-}(z) + T_{8+}\left(\frac{z}{2}\right) + T_{8+}\left(\frac{z+1}{2}\right).
$$

 $\mathbf{1}$

The same type of argument can be used to establish the linear relations between the T_m that were mentioned in Section 2. If N is one of 6, 10, 12, 18, and W_a , W_b , W_c are the three Atkin-Lehner involutions for $\Gamma_0(N)$, then the functions

$$
T_{N+} \hspace{1cm} T_{N+} \hspace{1cm} T_{N+0} \hspace{1cm} T_{N+b} \hspace{1cm} T_{N+c}
$$

have the respective forms

$$
f, f+f(W_a z)+f(W_b z)+f(W_c z), f+f(W_a z), f+f(W_b z), f+f(W_c z)
$$

and so we have

$$
2T_{N-} + T_{N+} = T_{N+a} + T_{N+b} + T_{N+c}.
$$

The relation

$$
2T_{30+15} + T_{30+} = T_{30+6}, 10, 15 + T_{30+3}, 5, 15 + T_{30+2}, 15, 30
$$

is exactly similar, and there are two more equations

$$
2T_{8-} = T_{4-} + T_{4|2} \qquad 2T_{16-} = T_{8-} + T_{8|2}
$$

which can be regarded as four-group relations of this type in which the missing terms correspond to functions that symmetrise to zero. The last relation

$$
T_{12+3} + T_{12|2+} - T_{12|2+2} - T_{12|2+6} = 2(T_{12-} + T_{24+} - T_{24+8} - T_{24+24})
$$

is more difficult, but since $\Gamma_0(24)$ has genus 1 we can use the theory of elliptic functions to show that the difference between the two sides has no poles, and so is zero. The last three relations were discovered by Atkin, who has also shown that there are no more.

Section 9. *Moonshine for other groups.*

Various groups G, often derived in some way from centralisers of elements of *M,* have moonshine properties of their own. In other words, to each element $g \in G$ there corresponds a series

$$
t_g = q^{-1} + h_0(g) + h_1(g) \cdot q + h_2(g) \cdot q^2 + \dots
$$

defining the modular function for which the fixing group $F(g)$ contains some $\Gamma_0(N)$

and determines a function field of genus zero. Most of the properties we found for *M* extend, though there are some differences:

- (1) The fixing group does not always contain $\Gamma_0(N)$ *normally*.
- (2) The Fricke involution need not lie in the converting group.
- (3) The replication formulae need certain modifications.
- (4) There are additional multiplicative properties for certain groups, and for these the most natural $h_r(g)$ are *generalised* characters.

Multiplicative moonshine. We discuss (4) first. The group G_p of Section 7 has a central element -1, and two algebraically conjugate representations ϕ_+ and ϕ_- of degree $2d = \frac{24}{p-1}$, except that $\phi_+ = \phi_-$ for $p = 2$. For this group, *every* t_g has a multiplicative formula:

$$
t_g = \frac{1}{q} \prod_{p \nmid n} \text{char}_{\pm}(q^n)
$$

in which

$$
char_{\pm}(q)=(1-q\epsilon_1)(1-q\epsilon_2)\dots(1-q\epsilon_{2d})
$$

where the ε 's are the eigenvalues of g in the representation ϕ_{\pm} , and the sign is the Legendre symbol (n/p) . With this definition it can readily be shown that $h_r(-g)$ is a character, while *hr(g)* is only a *generalised* character, but certain properties of the replication formulae show us that it would be wrong to exchange the two functions. However, there is a bonus: for these groups $h_0(-g) = -h_0(g)$ is also a character of *G*, namely that afforded by the basic representation ϕ_{+} .

Immaterial moonshine. For the groups 2B, $3F_{24}$ ', E, F, H, M_{12} of Table 2a, we seem always to get proper characters, and the constant term $h_0(g)$ is immaterial, just as in *M.*

The fixing groups of the new modular functions are less restricted than those that arise from M. For example, in *2B* there is an involution corresponding to the function $(j - 1728)^{\frac{1}{2}}$, and which we therefore call 2|2, but although W_4 is in the eigengroup, it is not in the fixing group and therefore has eigenvalue -1 rather than $+1$. A seventh root, 14|2, of this element arises in both *IB* and *H,* and has similar properties. In *F* there is an element we call 5|5, since its fixing group has index 5 in $\Gamma_0(5|5)$, but the latter is not the eigengroup, and does not even contain the fixing group normally. Our naming system rapidly breaks down, and in fact it seems that the possible fixing groups are *all* the discrete extensions of $\Gamma_0(N)$ for which the corresponding function field has genus zero. We shall say more about such groups in a moment.

When algebraic irrationalities arise in the coefficients, there are new problems, like the need to distinguish between ϕ_+ and ϕ_- above. We have noticed that when *Tg* involves quadratic irrationalities, and G is derived from the centraliser of an element of order p in M, then the part ${H_n q + H_{2n}q^2 + ...}$ of the *n*-plication formula must be replaced by its algebraic conjugate whenever $(n/p) = -1$. Presumably this rule has a natural extension to other groups and higher degree irrationalities, if indeed these arise.

Abstract replication. If $T = q^{-1} + H_1 q + H_2 q^2 + ...$ generates a genus zero function field corresponding to some group containing $\Gamma_0(N)$, there will usually be several groups G with elements g for which $T = T_{g}$. We say that these elements have *type T,* and call T a *type* (even if there is no g with $T = T_e$).

The replication formulae, as just amended, can now be used to *define* certain functions $T_{(2)}$, $T_{(3)}$, ..., $T_{(n)}$, which we call the *duplicate*, *triplicate*, *,..., n-plicate* of T. Of course, if *T* is the type of some $m \in M$, these will just be the types of the square, cube, ..., nth power of *m,* so that our abstract definition has captured at least something of the multiplication in *M.*

If *G* is derived from the centraliser of some element of M of order *s,* and $T = T_g$, then it seems that indeed $T_{(n)} = T_{g^n}$ whenever $(n, s) = 1$. But if $(n, s) > 1$, then n-plication often yields an element in another group, usually the Monster itself. For example, the quintuplicate of the type T_{515} is $J(z)$, and so corresponds to the identity element, not of *F,* but of *M.* Since *J(z)* is its own n-plicate for every *n,* we call it the identity type, and say that T_{515} has replication order 5, while elements of any order *n* prime to 5 in *F* have replication order *5n.*

Many questions arise about this abstract replication of modular functions. Is the *a*-plicate of the *b*-plicate equal to the *ab*-plicate? Does every type have a welldefined and finite replication order? What is the proper treatment of algebraic irrationalities? And so on.

It is a famous assertion of Galois that *PSL2(p)* has a subgroup of index *p* only for $p = 2, 3, 5, 7, 11$. We have already mentioned the types $t_{2,12}, t_{3,13}, t_{5,15}$, and remark that $t_{7/7}$ and $t_{11/11}$ arise respectively in Held's group and M_{12} . The exact correspondence of these with the Galois exceptions appears to be significant.

Finally, we ask whether the sporadic simple groups that may not be involved in *M* (those discovered by Lyons, O'Nan, Rudvalis, and the three Janko groups J_1 , J_3 $J₄$) have moonshine properties. There is an exceptional involutory automorphism of the algebraic curve for $\Gamma_0(37)$ that might be relevant for the Lyons group. Is there a similar period three automorphism for the case $\Gamma_0(67) + ?$

Section 10. *The genus zero problem*

Helling [9] has shown that the groups $\Gamma_0(n)$ + for square-free *n* are maximal discrete groups, and that every discrete group Δ commensurable with Γ can be conjugated into one of these groups. Moreover, if the function field for Δ is of genus zero, so is that for $\Gamma_0(n)$ +, and it is easy to see that the conjugating element can be taken in the form $z \rightarrow (pz+q)/r$ where p, q, r are integers with no common factor.

The question as to which groups between $\Gamma_0(N)$ and its involutory normaliser $\Gamma_0(N)$ + give genus zero is an old one. Fricke ([8], p. 367, but accidentally omitting 59) lists cases when the Fricke normaliser $\Gamma_0(N) + N$ gives genus zero, and Ogg [15] has used techniques from algebraic geometry to show that Fricke's list (with 59 inserted) is complete for primes (and offers a bottle of Jack Daniels' for an explanation of why the primes that arise are just those dividing *\M*!) More recently, Kluit [12] has shown that there are no cases other than those appearing in Table 5 of [1], which are of course just the cases with $h = 1$ in our Table 2. See also Kluit [11].

The corresponding discussion for the non-involutory part of the normaliser does not seem to be available in the literature. However, our remark that the full normaliser of $\Gamma_0(N)$ is conjugate to the involutory normaliser of $\Gamma_0(n/h)$ makes a fairly elegant discussion possible. In particular, the largest N for which the full normaliser of $\Gamma_0(N)$ has genus zero is $N = 24^2.119 = 68544$.

However, we are concerned also with groups not containing any $\Gamma_0(N)$ normally, and the correct requirements seem to be:—

- (1) Δ contains some $\Gamma_0(N)$.
- (2) the function field for Δ has genus zero.
- (3) the translation $z \rightarrow z+k$ is in Δ exactly when k is an integer.
- (4) the coefficients in the canonical Hauptmodul T for Δ are algebraic integers.

We conjecture that there are only finitely many groups with these properties. Larissa Queen has computed the first few terms of T_g for all g in various finite groups *(E, F, H, M12,* ...) and for the elements of smallest order in the infinite Lie group $E_8(\mathbb{R})$. In most cases the corresponding modular groups are easily identified. On the basis of these results we conjecture that there will be three or four hundred cases in all (171) of which appear in M). It would be very interesting to have a complete list, and to study the replication maps between them.

Section 11. *Description of the tables*

Table 1, copied from [6], gives the degrees f_i of the irreducible characters of M.

Table 1a gives first, copied from [19], the coefficients $a_0 - a_{24}$ in the *q*-series for *j*. Beside this are given the decomposition numbers for the Head characters H_{-1} to H_0 in terms of the MONSTER irreducibles ordered as in Table 1.

Table 2 is our class list for the MONSTER. Its columns give:-

The term ATLAS refers to the Atlas of Finite Groups that we are preparing with R. T. Curtis and R. A. Parker, in which classes of elements of order *n* in any group are named *nA, nB, nC,* ... in descending order of their centraliser sizes. The number *D* can be used to find the index of one of the groups *F(m)* in another that contains it.

Table 2a supplements Table 2 by giving structural details of the centralisers of elements of small order. It also gives decimal forms for the centraliser orders that were too long to fit in Table 2 itself.

Table 3 gives all products for t_m expressible only in terms of $n(kz)$ for various k. It also illustrates various relations between the classes in a way described in more detail in Section 6. This table can be used to derive a formula for any class in any line from one for the fundamental class.

Table 3a gives additional product formulae involving $\eta(kz+c)$, $c \neq 0$, and some transformation rules for such functions. The three formulae for 25Z, 49Z, 50Z involve a further generalisation explained in the table.

If $\pi(z)$ is one of the product formulae for *m* in Table 3 or 3a, then $\pi(z) = T_m - k$, and since $\pi(z)$ does not vanish in the interior of the upper half-plane, T_m must take the value *k* at a *cusp*. Since T_m takes the value ∞ at the cusp i ∞ , the number of such product formulae for a given *m* is therefore at most C— 1, where *C,* given in Table 2, is the number of equivalence classes of cusps under *F(m).* Study of Tables 3 and 3a shows that the bound is always attained, so that no more such formulae are to be expected.

It is also possible to see from these tables how the Atkin-Lehner involutions transform the t_m . The well-known formulae

$$
\eta(z+1)=\varepsilon.\eta(z), \quad \eta(-1/z)=\eta(z)\sqrt{\left(\frac{z}{i}\right)}=\eta(z).z^{\frac{1}{2}}.\varepsilon^{-3},
$$

where $\varepsilon = e^{2\pi i/24}$, imply that for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ we have *\c d!*

$$
\eta\left(\frac{az+b}{cz+d}\right)=\eta(z)\cdot(cz+d)^{\frac{1}{2}}\cdot\varepsilon^{f(a,\,b,\,c,\,d)}.
$$

and using this one can show that to within algebraic factors that largely cancel in our calculations, the elements of $\Gamma_0(N)$ leave all $\eta(\varepsilon z)$ (e||N) fixed, while the Atkin-Lehner involutions of $\Gamma_0(N)$ permute them in the obvious way. For instance, when $N = 6$, we find that W_2 interchanges $\eta(z)$ with $\eta(2z)$ and $\eta(3z)$ with $\eta(6z)$ to within such algebraic factors, and therefore fixes the product formula $1^4 2^4/3^4 6^4 = t_{6+2}$ but inverts $1^6 3^6 / 2^6 6^6 = t_{6+3}$ of Table 3. [A more detailed calculation shows that W_2 takes t_{6+3} to 81/ t_{6+3} .]

Table 4 gives numbers $H_{-1}(m)$, ..., $H_{10}(m)$ for each $m \in M$. For $r \neq 0$, $H_r(m)$ is the coefficient of q^r in T_m (i.e. the value of the rth head character at m), while $H_0(m)$ is the Rademacher constant for T_m . The Rademacher constant of a modular function f is the complex number c for which $f + c$ lies in a certain complex vector space. This is the unique space that is invariant under the positive elements of $PGL_2(\mathbb{Q})$ and has codimension 1 in the space of *all* modular functions belonging to groups commensurable with F.

Table 4a provides sufficient additional formulae to identify T_m for every $m \in M$. Several of these are consequences of our expansion and compression formulae (Section 8), while others involve the θ -functions of certain 2-dimensional lattices. The Table is self-explanatory. Some of the formulae are due to Fricke, and some to Atkin.

Table 1

Table 1a. Coefficients of the j-function, and head character decompositions.

MONSTROUS MOONSHINE 327

Table **2.** *Class list of M.*

 $\sim 10^{-1}$

 \mathcal{L}

 \sim

centraliser structure and order											class
(MONSTER)	8080 17424 79451 28758 86459 90496 17107 57005 75436 80000 00000										1A
(BABY)	2.B				8305 96296 24528 52382 35516 10880 00000						2A
(Conway)	$2^{1+24}C_1$								13 95118 39126 33632 81715 20000		2B
(Fischer)	$3.F_{24}$								37656 17127 57198 51638 78400		3A
(Suzuki)	3^{1+12} . 2. Sz								1429 61507 75402 49600		3B
(Thompson, Smith)	$3 \times E$								272 23783 16636 16000		3C
(Conway)	4.2 ²² . C_3								8317 58427 33096 96000		4A
	${4 \times F_4(2)}.2$								26 48901 28269 31200		4B
	4.2^{15} . 2^8 . $S_6(2)$								4870 49291 36640		4C
	4.2 ¹² . $G_2(4)$.2								824 43239 42400		4D
(Harada, Norton)	$5 \times F$								1 36515 45600 00000		5A
(Hall, Janko)	5^{1+6} . 2. HJ								9 45000 00000		5B
(Fischer)	$3 \times 2. F_{22}.2$								77474 10198 52800		6A
(Suzuki)	$6.$ Sz								269 00729 85600		6B
	2^{1+12} . 3 ² . $U_4(3)$. 2								48 15794 99520		6C
	$2.3^{1+8}.2^{1+6}.U_4(2)$								13 06069 40160		6D
	2.3^{1+4} . 2^{1+6} . $U_4(2)$									16124 31360	6E
	$3 \times 2^{1+8}$. A_9									2786 91840	6F
(Held)	$7 \times H$								2 82127 10400		7A
	7^{1+4} . 2. A_7									847 07280	7B
	$8.2^7.2^6. U_3(3).2$									7927 23456	8A
(Mathieu)	8.2^{10} . M_{12}									7785 67680	8B
(Tits)	$8\times{}^2F\,{}^{'}_4(2)$									1437 69600	8C
	$8.2^9.2^4. A_6$									235 92960	8D
	$[2^{22}3]$									125 82912	8E
	$8.2^6. U_3(3)$									30 96576	8F
	$9.3^{1+4}.S4(3)$									566 87040	9A 9B
	[2 ⁴ 3 ¹¹] 5×2 . HS. 2									28 34352 8870 40000	10A
(Higman, Sims)	$5 \times 2^{1+8}$. $(A_5 \times A_5)$. 2									184 32000	10B
	$2.5^{1+4}.2^{1+4}.A_5$									120 00000	10C
(Hall, Janko)	5×2 . HJ									60 48000	10D
	$2.5^{1+2}.2^{1+4}.A_5$									4 80000	10E
(Mathieu)	$11 \times M_{12}$									10 45440	11A

Table 2a. Additional information for small order elements.

 \overline{a}

 \sim

 $\hat{\mathbf{r}}$

 ~ 200

 \mathcal{L}^{\pm}

class	formulae	
8D	$(1\frac{1}{4})^4 2^2/4^4 8^2$	
9 B	$(1\frac{1}{3})^3/9^3$	
16B	$(1\frac{1}{4})^2$ 2 . 8^2 /4 ³ 16 ²	
18A	$(1\frac{1}{3})^3(2\frac{1}{3})^31.2/3^46^4$	
18D	$(1\frac{1}{3})^2$ 6.9/(2 ² / ₃)3.18	
18D	$(2\frac{2}{3})^2$ 9/(1 ¹ / ₃)18 ²	
18E	$(1\frac{1}{3})(2\frac{2}{3})2.9/1^218^2$	
24D	$(1\frac{1}{4})^2(3\frac{1}{4})^2 2^2 6^2 8.24/4^5 12^5$	
24H	$(1\frac{1}{4})(3\frac{3}{4})$ 6.8/2.4.12.24	
25A	$(1\frac{1}{3})(1\frac{4}{3})/1.25$	
27AB	$(1\frac{1}{3})(3\frac{2}{3})/1.27$	
32A	$(1\frac{1}{4})(2\frac{3}{4})$ 2.16/1.4.8.32	
32B	$(1\frac{1}{2})(1\frac{7}{2})4^216^2/2.8^432$	
36B	$(1\frac{1}{3})(4\frac{1}{3})18/(2\frac{2}{3})9.36$	
36B	$(2\frac{3}{3})^5$ 3 . 12 . 18/ $(1\frac{1}{3})^2$ $(4\frac{1}{3})^2$ 6 ² 9 . 36	
36D	$(1\frac{1}{3})(4\frac{2}{3})2.18/1.6^236$	
40CD	$(1\frac{1}{4})(5\frac{3}{4})8.10/4^220^2$	
50A	$(1\frac{1}{5})(1\frac{4}{5})(2\frac{1}{5})(2\frac{4}{5})/5^2 10^2$	
54A	$(1\frac{1}{3})(2\frac{1}{3})(3\frac{2}{3})(6\frac{2}{3})/3.6.9.18$	
25Z	$(1\frac{1}{5})(1\frac{2}{5})/(1\frac{3}{5})25$	(4 forms)
49 Z	$(1\frac{2}{7})(1\frac{3}{7})(1\frac{4}{7})(1\frac{5}{7})/7^4$	(3 forms)
50Z	$5^2 10^2/(1\frac{1}{5})(2\frac{4}{5})1.50$	(4 forms)

Table 3a. *Additional product formulae.*

All formulae except those for 25Z, 49Z, 502 are $\left(\sqrt{a}\right)$ valid up to a constant factor when $\binom{N}{b}$ is the preted as $\eta\left(Nz+\frac{a}{b}\right)$. All formulae are valid under the interpretation

$$
\left(N\frac{a}{b}\right)=q^{N/24}\prod_{n=1}^{\infty}\left(1-u^{n}q^{nN}\right)
$$

where

$$
u = e^{2\pi i a/b}
$$

and

 $n\bar{n} \equiv 1 \pmod{b}$ if $(n, b) = 1$, $\bar{n} \equiv n \pmod{b}$ if $(n, b) \neq 1$.

All formulae except those for 25Z, 49Z, 50Z have two algebraically conjugate forms, while these cases yield the numbers indicated. The conjugate forms can be found by applying the permutations

$$
\begin{array}{c}\n(\frac{1}{3}, \frac{2}{3}), (\frac{1}{4}, \frac{3}{4}), (\frac{1}{5}, \frac{2}{5}, \frac{4}{5}, \frac{3}{5}), \\
(\frac{1}{7}, \frac{3}{7}, \frac{2}{7}, \frac{6}{7}, \frac{4}{7}, \frac{5}{7}), (\frac{1}{8}, \frac{3}{8})(\frac{5}{8}, \frac{7}{8}).\n\end{array}
$$

There are some useful transformations:—

 $(N^1_2) = (2N)^3/(N)(4N)$
 $(N^1_3)(N^2_3) = (3N)^4/(N)(9N)$
 $(N^1_4)(N^2_4) = (4N)^8/(2N)^3(8N)^3$ = *(5N)6 /(N)(25N)* $=(7N)^8/(N)(49N)$

Table 4. *Values of head characters.*

÷,

 $\sim 10^{-1}$

 $\ddot{}$

MONSTROUS MOONSHINE

70A	$70B$	71A	$78A$	$78B$	84A	$84B\,$	84C	87A	88A	92A	93A	94A	95A
									ŀ				
	$-\frac{5}{12}$				0	0	0		0		O		
	O				0		0						
					0	0					o		
						0	0		0		0		
							0						
	0					0	0						
							0						
							0						
					0	0		2	0	2			
					0		0	2		2	0	2	2
4		4	$\overline{2}$		0	$\bf{0}$	0	\overline{c}	0	$\overline{2}$	0	$\overline{2}$	$\overline{2}$
	$104A$	$105A$		110A		119A			$25\rm Z$		49Z		$50\ Z$
													3
													4
													5
													6
													8
											l 1		10
											13		12

Table 4a. Further formulae for the t_m .

Here η_n denotes $\eta(nz)$, and $\theta(a,b,c)$ denotes $\sum q^{1(\alpha x^2 + bxy + cy^2)}$, while $\theta_x(a,b,c)$ or $\theta_y(a,b,c)$ would be the same sum restricted to odd values of x or y respectively. We use $S(d,N)$ for $T_{N+}(z) + T_{N+}(dz)$.

Section 12. *Postscript.*

It seems to follow from Kac $[10]$ that the properties of E_8 noted in Section 9 are suitably generalised forms of certain identities of MacDonald [14], for which the appropriate framework is the theory of Lie superalgebras, which are a kind of graded Lie algebra.

Is there a Lie superalgebra that "explains" the MONSTER? Our own tentative investigations of this possibility have not yet proved fruitful, but it is at least consistent with the discovery made by one of us some time ago that the 196883-dimensional representation admits a natural commutative algebra structure. There are difficulties concerned with the portion of the Lie superalgebra corresponding to the $q⁰$ term, which should either be 0-dimensional or infinite-dimensional. Perhaps a more "twisted" kind of algebra is needed?

Most explanations of *M* along these lines suggest that it is embedded in an infinite group M^1 that should be more "natural". Unfortunately there are difficulties with this possibility as well. M^1 can hardly be an infinite Lie group, and we can find no real evidence for the existence of an infinite discrete group with the required properties.

Another possibility is that M is a Galois group. However, although there are many pairs of mutually algebraic fields in sight, for example $\mathbb{C}(j)$ and $\mathbb{C}(j, t_2, ..., t_{119+})$, all the most obvious pairs, including this one, have either been rendered extremely unlikely or actually disproved. However, such an explanation could carry with it an understanding of the "genus zero" property, which would follow if all the Riemann surfaces corresponding to the T_m were quotients of a universal surface of genus zero.

References

- 1. B. J. Birch and W. Kuyk, ed. *Modular Functions of One Variable IV,* Proc. Intern. Summer School (Antwerp, 1972, Springer).
- 2. J. H. Conway, R. T. Curtis, S. P. Norton and R. A. Parker, *An Atlas of Finite Groups,* in preparation.
- **3.** A. O. L. Atkin and J. Lehner, "Hecke Operators on $\Gamma_0(m)$ ", *Math. Ann.*, 185 (1970), 134–160.
- 4. B. J. Birch, "Some calculations of Modular Relations", *in Modular Functions of One Variable,* I, (Antwerp, 1973, Springer).
- 5. J. H. Conway, "Three Lectures on Exceptional Groups" (Chapter VII of *Finite Simple Groups,* edited by M. B. Powell and G. Higman).
- 6. B. Fischer, D. Livingstone, M. P. Thorne, *The characters of the "Monster" simple group* (Birmingham, 1978).
- 7. J. S. Frame, "Computation of the characters of the Higman-Sims group and its automorphism group", /. *Algebra,* 20 (2) (1972), 320-349.
- 8. R. Fricke, *Die Elliptische Funktionen undlhre Anwendungen, 2-ter Teil* (Teubner, Leipzig, 1922).
- 9. H. Helling, "On the commensurability class of rational modular group", /. *London Math. Soc,* (2)2(1970), 67-72.
- 10. V. G. Kac, "Infinite dimensional algebras, Dedekind's η -function, Classical Möbius function, and the Very Strange Formula", *Advances in Mathematics,* 30 (2) (1978), 85-136.
- 11. P. G. Kluit, "On the Normaliser of $\Gamma_0(n)$ ", *in Modular Functions of One Variable, V* (Bonn, 1976, Springer), 239–246.
- 12. P. G. Kluit, Doctoral Dissertation, Antwerp, 1979.
- 13. J. Leech, "More notes on Sphere Packings", *Can. J. Math.,* 19 (1967), 251-267.
- 14. I. G. MacDonald, "Affine Root Systems and Dedekind's η -function", *Invent. Math.*, 15 (1972), 91-143.
- 15. A. P. Ogg, "Automorphismes des Courbes Modulaires", *Seminaire Delange-Pisot, Poitou,* (7), 1974.
- 16. A. Pizer, "A note on a conjecture of Hecke", *Pacific J. Math., to appear.*
- 17. J. G. Thompson, "Some Numerology between the Fischer-Griess Monster and the Elliptic Modular Function", *Bull. London Math. Soc,* 11 (1979), 352-353.
- 18. J. G. Thompson, "Uniqueness of the Fischer-Griess Monster", *Bull. London Math. Soc,* 11 (1979).
- 19. H. S. Zuckerman, "The computation of the smaller coefficients of /(T)" , *Bull. Amer. Math. Soc,* 45 (1939), 917-919.

Department of Pure Mathematics and Mathematical Statistics,

University of Cambridge,

16 Mill Lane, Cambridge CB2 1SB.