Modular Moonshine II. *24 July 1994, corrected 19 Sept 1995*

Duke Math. J. 83 (1996) no. 2, 435-459.
Richard E. Borcherds,*
Mathematics department,
University of California at Berkeley,
CA 94720-3840
U. S. A.
e-mail: reb@math.berkeley.edu

Alex J. E. Ryba,
Dept of Mathematics,
Marquette University,
Milwaukee,
WI 53233,
U. S. A.
e-mail: alexr@sylow.mscs.mu.edu

The monster simple group acts on the monster vertex algebra, and the moonshine conjectures state that the traces of elements of the monster on the vertex algebra are Hauptmoduls. Ryba [R94] conjectured the existence of similar vertex algebras over fields of characteristics p acted on by the centralizers of certain elements of prime order p in the monster, and conjectured that the Brauer traces of p-regular elements of the centralizers were certain Hauptmoduls. We will prove these conjectures when the centralizer involves a sporadic group ($p \leq 11$, corresponding to the sporadic groups B, Fi'_{24}, Th, HN, He, and M_{12}).

Contents.

1. Introduction.

The original "moonshine conjectures" of Conway, Norton, McKay, and Thompson said that the monster simple group M has an infinite dimensional graded representation $V = \oplus_{n\in\mathbf{Z}} V_n$ such that the dimension of V_n is the coefficient of q^n of the elliptic modular function $j(\tau)-744 = q^{-1}+196884q+\cdots$, and more generally the McKay-Thompson series $T_g(\tau) = \sum_{n\in\mathbf{Z}} \mathrm{Tr}(g|V_n)q^n$ is a Hauptmodul for some genus 0 congruence subgroup of $SL_2(\mathbf{R})$. The representation V was constructed by Frenkel, Lepowsky, and Meurman [FLM], and it was shown to satisfy the moonshine conjectures in [B92] by using the fact that it carries the structure of a vertex algebra [B86], [FLM].

Meanwhile, Norton had suggested that there should be a graded space associated to every element g of the monster acted on by some central extension of the centralizer of g ([N], see also [Q]). It is easy to see that these graded spaces are usually unlikely to have a vertex algebra structure. Ryba suggested [R94] that these spaces might have a vertex algebra structure if they were reduced mod p (if g has prime order p). He also suggested the following definition for these vertex algebras:

$$ {}^gV = \frac{V^g/pV^g}{(V^g/pV^g)\cap(V^g/pV^g)^\perp} $$

* Supported by NSF grant DMS-9401186.

where V is some integral form for the monster vertex algebra, and V^g is the set of vectors fixed by g. He conjectured that the dimensions of the homogeneous components of ${}^gV$ should be the coefficients of certain Hauptmoduls, and more generally that if h is a p-regular element of $C_M(g)$ then

$$\mathrm{Tr}(h|{}^gV_n) = \mathrm{Tr}(gh|V_n)$$

where the trace on the left is the Brauer trace. (The numbers on the right are known to be the coefficients of a Hauptmodul depending on gh by [B92].) We will call these conjectures the modular moonshine conjectures.

We now describe the proof of the modular moonshine conjectures for some elements g given in this paper. We observe (proposition 2.3) that the definition of ${}^gV$ in [R94] is equivalent to defining it to be the Tate cohomology group $\hat{H}^0(g, V)$, or at least it would be if a good integral form V of the monster Lie algebra was known to exist. The lack of a good integral form V does not really matter much, because we can just as well use a $\mathbf{Z}[1/n]$-form for any n coprime to $|g|$, and a $\mathbf{Z}[1/2]$-form can be extracted from Frenkel, Lepowsky and Meurman's construction of the monster vertex algebra.

It is difficult to work out the dimension of $\hat{H}^0(g, V[1/2]_n)$ directly. However it is easy to work out the difference of the dimensions of $\hat{H}^0$ and $\hat{H}^1$, which can be thought of as a sort of Euler characteristic (and is closely related to the Herbrand quotient in number theory). This suggests that we should really be looking at $\hat{H}^*(g, V[1/2]) = \hat{H}^0(g, V[1/2]) \oplus \hat{H}^1(g, V[1/2])$, and it turns out for essentially formal reasons that this has the structure of a vertex superalgebra. The traces of elements h of the centralizer of g on this superalgebra are just given by the traces of the elements gh on the monster vertex algebra.

We can now complete the proof of the modular moonshine conjectures for the element g of the monster by showing that $\hat{H}^1(g, V[1/2]) = 0$. We do this for certain elements of odd prime order of the monster coming from M_{24} in section 4; this is a long but straightforward calculation. There are plenty of elements g of the monster for which $\hat{H}^1(g, V[1/2])$ does not vanish; this happens whenever some coefficient of the Hauptmodul of g is negative; for example, g of type 3B. There are also some elements of large prime order for which we have been unable to prove the modular moonshine conjectures because we have not proved that $\hat{H}^1(g, V[1/2]) = 0$ (though this is probably true), but we do at least cover all the cases when g has prime order and its centralizer involves a sporadic simple group.

The case when $p = 2$ has several extra complications, due partly to the existence of several extensions of groups by 2-groups, and due partly to the fact the FLM construction can be carried out over $\mathbf{Z}[1/2]$ but it is not clear how to do it over $\mathbf{Z}$. We deal with these extra problems in section 5 by using a $\mathbf{Z}[1/3]$-form of the monster vertex algebra. To construct this $\mathbf{Z}[1/3]$-form we need to make a mild assumption (which we have not checked) about the construction of the monster vertex algebra from an element of order 3 announced by Dong and Mason and by Montague. (In particular the proof of the modular moonshine conjectures for elements of type 2A in the monster uses this assumption.)

In section 6 we give some calculations illustrating the case when g is an element of type 7A in the monster (so the centralizer $C_M(g)$ of g is $\langle g \rangle \times He$). We give the characters and the decomposition into irreducible modular representations of the first few graded pieces of $\hat{H}^0(g, V[1/2])$.

In section 7 we discuss some open problems, in particular how one might construct a good integral form of the monster vertex algebra.

Notation.

A^G	The largest submodule of A on which G acts trivially.
A_G	The largest quotient module of A on which G acts trivially.
A, B, C	G-modules.
Aut	The automorphism group of something.
B	The baby monster sporadic simple group.
$\mathbf{C}$	The complex numbers.
$C_M(g)$	The centralizer of g in the group M.
Fi_{24}	One of Fischer's groups.
$\mathbf{F_q}$	The finite field with q elements.
g	An element of G, usually of order p.
$\langle g \rangle$	The group generated by g.
G	A group, often cyclic of prime order p and generated by g.

$\hat{H}^i(G,A)$ A Tate cohomology group of the finite group G with coefficients in the G-module A.
$\hat{H}^i(g,A)$ means $\hat{H}^i(\langle g\rangle, A)$, where $\langle g\rangle$ is the cyclic group generated by g.
$\hat{H}^*(g,A)$ The sum of the Tate cohomology groups $\hat{H}^0(g,A)$ and $\hat{H}^1(g,A)$, considered as a super module.
He The Held sporadic simple group.
HN The Harada-Norton sporadic simple group.
I The elements of a group ring of norm 0.
Im The image of a map.
Ker The kernel of a map.
$\Lambda, \hat{\Lambda}$ The Leech lattice and a double cover of the Leech lattice.
L An even lattice.
M The monster simple group.
M_{12} A Mathieu group.
M_{24} A Mathieu group.
N The norm map: $N(v) = \sum_{g\in G} g(v)$.
$N_M(g)$ The normalizer of the subgroup $\langle g\rangle$ in the group M.
p A prime, usually the order of g.
$\mathbf{R}$ The real numbers.
R_p A finite extension of the p-adic integers.
$S(a)$ $= \sum_{0\le n<p} n g^n(a)$
SL_2 A special linear group.
Th Thompson's sporadic simple group.
Tr $\mathrm{Tr}(g|A)$ is the usual trace of g on a module A if A is a module over a ring of characteristic 0, and the Brauer trace if A is a module over a field of finite characteristic.
$V[1/n]$ A $\mathbf{Z}[1/n]$-form of the monster vertex algebra.
V_Λ The integral form of the vertex algebra of $\hat{\Lambda}$.
V_n The degree n piece of V.
V^n An eigenspace of some group acting on V.
${}^gV$ A modular vertex algebra or superalgebra given by $\hat{H}^*(g, V[1/n])$ for some n coprime to $|g|$.
$\mathbf{Z}$ The integers.
$\mathbf{Z}_p$ The p-adic integers.
ω A cube root of 1 or a conformal vector.

2. Cohomology and modular representations.

In this section we summarize some basic facts about group cohomology that we will use later. For more details about Tate cohomology groups see the article [AW].

If G is a finite group acting on an abelian group A we define A^G to be the elements of A fixed by G, and A_G to be the largest quotient of A on which G acts trivially. We write N for the norm map defined by $N(a) = \sum_{g\in G} g(a)$. If n is any integer then $\hat{H}^n(G,A)$ is the Tate cohomology group of G with coefficients in A. It has the following properties.

1. $\hat{H}^0(G,A) = A^G/\mathrm{Im}(N)$.
2. $\hat{H}^{-1}(G,A) = \mathrm{Ker}(N|A_G)$.
3. If $0 \to A \to B \to C \to 0$ is an exact sequence of G modules then

$$\cdots \longrightarrow \hat{H}^{i-1}(G,C) \longrightarrow \hat{H}^i(G,A) \longrightarrow \hat{H}^i(G,B) \longrightarrow \hat{H}^i(G,C) \longrightarrow \hat{H}^{i+1}(G,A) \longrightarrow \hat{H}^{i+1}(G,B) \longrightarrow \cdots$$

   is exact.
4. There is a bilinear cup product from $\hat{H}^i(G,A) \times \hat{H}^j(G,B)$ to $\hat{H}^{i+j}(G,C)$, defined whenever we have a G-invariant bilinear map from $A \times B$ to C, and which is the obvious induced product when $i = j = 0$. $\hat{H}^*(G,\mathbf{Z})$ is a super-commutative ring under cup product. More generally if A has any G-invariant algebraic structure defined in terms of multilinear products and multilinear identities (e.g., commutative ring, Lie algebra, vertex algebra, etc.) then $\hat{H}^*(G,A) = \oplus_{n\in\mathbf{Z}} \hat{H}^n(G,A)$ is a "super" version of this algebraic structure under the cup product; this means that it satisfies the same identities as A except that we insert a factor of -1 whenever we interchange the order of two elements of odd degree. This follows from the associativity and supercommutativity properties of the cup product given in [AW]. For

example, if A is a Lie algebra, then $\hat{H}^*(G,A)$ is a Lie superalgebra (at least if A is 2-divisible so that the Lie algebra axioms can all be written as multilinear identities).

5. If G is a cyclic group generated by an element g we will also write the cohomology groups $\hat{H}^i(G,A)$ as $\hat{H}^i(g,A)$. In this case $\hat{H}^2(g,\mathbf{Z})$ has a canonical element (depending on the generator g) such that cup product by this element is an isomorphism from $\hat{H}^i(g,A)$ to $\hat{H}^{i+2}(g,A)$. In particular there are essentially only 2 different cohomology groups, $\hat{H}^0$ and $\hat{H}^1$, as all the others are isomorphic to one of these two, so we define $\hat{H}^*(g,A)$ to be $\hat{H}^0(g,A) \oplus \hat{H}^1(g,A)$. As in 4 above, if A has some algebraic structure, then $\hat{H}^*(g,A) = \hat{H}^0(g,A) \oplus \hat{H}^1(g,A)$ has a super version of this algebraic structure, with $\hat{H}^0$ and $\hat{H}^1$ being the even and odd parts. Notice that the algebra product from $\hat{H}^1 \times \hat{H}^1$ to $\hat{H}^0$ depends on the choice of generator g because it uses the isomorphism from $\hat{H}^2$ to $\hat{H}^0$. In particular if $g \in G$ and A has an algebra structure invariant under G, then the natural action of the normalizer $N_G(g)$ on $\hat{H}^*(g,A)$ need not preserve the algebra structure (unless of course $\hat{H}^1(g,A) = 0$). The centralizer $C_G(g)$ always preserves the algebra structure. We always regard $\hat{H}^*(g,A)$ as a supermodule, and in particular when we take the trace of an element h on it we multiply the trace on $\hat{H}^1$ by -1, i.e., $\mathrm{Tr}(h|\hat{H}^*(g,A))$ is defined to be $\mathrm{Tr}(g|\hat{H}^0(g,A)) - \mathrm{Tr}(g|\hat{H}^1(g,A))$. (The trace will always be the Brauer trace, which takes values in a field of characteristic 0.)
6. $\hat{H}^*(G,A)$ is a $|G|$-torsion module, and in particular if multiplication by $|G|$ is an isomorphism on A then $\hat{H}^*(G,A)$ vanishes.

We let $\mathbf{Z}_p$ be the ring of p-adic integers.

Lemma 2.1. *If A is a free $\mathbf{Z}[1/n]$ module acted on by a p-group G with $(p,n) = 1$ then the natural map from $\hat{H}^*(G,A)$ to $\hat{H}^*(G, A \otimes \mathbf{Z}_p)$ is an isomorphism.*

Proof. This follows by looking at the long exact sequence of $0 \to A \to A \otimes \mathbf{Z}_p \to A \otimes (\mathbf{Z}_p/\mathbf{Z}[1/n]) \to 0$, if we observe that multiplication by p is an isomorphism on $\mathbf{Z}_p/\mathbf{Z}[1/n]$ so the cohomology of $A \otimes (\mathbf{Z}_p/\mathbf{Z}[1/n])$ vanishes. This proves lemma 2.1.

Now suppose that G is a cyclic group of order p generated by g. Recall ([CR] p. 690) that there are exactly 3 indecomposable finitely generated modules over the group ring $\mathbf{Z}_p[G]$ which are free as $\mathbf{Z}_p$ modules; these are:

1. The 1-dimensional module $\mathbf{Z}_p$ (with g acting trivially). The cohomology groups of G with coefficients in $\mathbf{Z}_p$ are $\hat{H}^0(g,\mathbf{Z}_p) = \mathbf{Z}/p\mathbf{Z}$, $\hat{H}^1(g,\mathbf{Z}_p) = 0$, as can be easily checked by explicit calculation.
2. The group ring $\mathbf{Z}_p[G]$. All cohomology groups of this module are trivial as it is a projective module.
3. The module I, which is the kernel of the natural map from $\mathbf{Z}_p[G]$ to $\mathbf{Z}_p$. The cohomology groups of I can be worked out from the long exact sequence of $0 \to I \to \mathbf{Z}_p[G] \to \mathbf{Z}_p \to 0$, and are given by $\hat{H}^0(g,I) = 0$, $\hat{H}^1(g,I) = \mathbf{Z}/p\mathbf{Z}$.

The next proposition is the main tool for calculating the Brauer characters of the modular vertex algebras we will construct.

Proposition 2.2. *Suppose that A is a finitely generated free module over $\mathbf{Z}_p$ (or over $\mathbf{Z}$) acted on by a group G containing an element g of order p in its center. Then the Brauer character of the virtual modular representation $\hat{H}^*(g,A) = \hat{H}^0(g,A) - \hat{H}^1(g,A)$ of $G/\langle g\rangle$ is given by*

$$\mathrm{Tr}(h|\hat{H}^*(g,A)) = \mathrm{Tr}(gh|A)$$

for any p-regular element h of G. (The left hand trace is the Brauer trace, and the right hand one is the usual trace.)

Proof. We can assume that G is the product of the cyclic groups generated by g and h. We adjoin the $|h|$'th roots of 1 to $\mathbf{Z}_p$ to obtain an unramified extension R_p of $\mathbf{Z}_p$. It is sufficient to prove the proposition for the module $A \otimes R_p$ because both sides are unaffected by tensoring A by R_p. (The Brauer trace of the cohomology groups is of course calculated by regarding them as modules over the residue class field of R_p.) We can decompose $A \otimes R_p$ into eigenspaces for h, and as both traces are additive on modules we can assume that h acts on $A \otimes R_p$ as multiplication by some fixed root of unity ζ.

Both sides of proposition 2.2 are additive on short exact sequences (the additivity for the left hand side follows from the "exact hexagon" of Tate cohomology). The only irreducible representations of $Q \otimes R_p[g]$ over the quotient field $Q \otimes R_p$ of R_p are $Q \otimes R_p$ and $Q \otimes I \otimes R_p$, which implies that the module A can be

built from $I \otimes R_p$, R_p, and finite modules by taking repeated extensions. By additivity it is then sufficient to prove proposition 2.2 in the cases when A is $I \otimes R_p$ or R_p or a finite module. The case when A is finite is trivial as both sides are zero (the dimensions of $\hat{H}^0(g, A)$ and $\hat{H}^1(g, A)$ are equal because the Herbrand quotient $|\hat{H}^0(g, A)|/|\hat{H}^0(g, A)|$ is 1 for finite modules A).

We have reduced the proof of proposition 2.2 to checking the 2 cases when $A \otimes R_p$ is R_p or $I \otimes R_p$, and where h acts as multiplication by ζ. If $A \otimes R_p$ is R_p, then $\hat{H}^0(g, R_p) = R_p/pR_p$, and $\hat{H}^1(g, A \otimes R_p) = 0$, so $\mathrm{Tr}(h|\hat{H}^*(R_p)) = \zeta$, which is equal to $\mathrm{Tr}(gh|R_p) = \mathrm{Tr}(h|R_p)$. If $A \otimes R_p$ is the group ring $R_p[g]$, then both cohomology groups are 0 and the trace of gh on $R_p[g]$ is also 0 as the eigenvalues of gh are ζ multiplied by every p'th root of 1 (including 1). Finally the case when $A \otimes R_p = I \otimes R_p$ follows from the previous two cases and the exact sequence

$$0 \longrightarrow I \otimes R_p \longrightarrow R_p[g] \longrightarrow R_p \longrightarrow 0$$

because both traces are additive on short exact sequences. This proves proposition 2.2.

If A is a finitely generated free module over a ring R with a bilinear form $(,)$, then we say this form is self dual if every linear map f from A to R is of the form $f(a) = (a, b)$ for some fixed $b \in A$. If the form is symmetric and R is the ring of integers this is equivalent to saying that A is a unimodular lattice. We say the bilinear form is nonsingular if there is no nonzero element a with $(a, b) = 0$ for all $b \in A$. We say that a submodule B of A is primitive if A/B is torsion free.

Proposition 2.3. *Suppose A is a free $\mathbf{Z}$ or $\mathbf{Z}_p$ module acted on by the finite group G of order p with an invariant self dual symmetric bilinear form $(,)$. Then $N(A)$ is the set of all elements $a \in A^G$ such that $p|(a, b)$ for all $b \in A^G$. In particular the bilinear form $(,)$ induces a nonsingular bilinear form on $\hat{H}^0(G, A)$.*

Proof. We will prove this when A is a free $\mathbf{Z}$-module; the proof when A is a free $\mathbf{Z}_p$ module is similar. We think of A as a lattice in the real vector space $A \otimes \mathbf{R}$, which also has a nonsingular bilinear form induced by that of A. Note that $A \otimes \mathbf{R}$ is the orthogonal direct sum of the subspaces $A^G \otimes \mathbf{R}$ and $\mathrm{Ker}(N)$, so the bilinear form is nonsingular on each of these subspaces. The map N is just p times orthogonal projection onto the subspace $(A \otimes \mathbf{R})^G$. Hence $\frac{1}{p}N(A)$ is just the orthogonal projection of A into $(A \otimes \mathbf{R})^G$. The sublattice A^G is also primitive because if na is fixed by G for some nonzero $n \in \mathbf{Z}$ then so is a. On the other hand, the set of vectors $a \in A^G$ such that $p|(a, b)$ for all $b \in A^G$ is the same as $p(A^{G\prime})$ (where B' means the dual of the lattice B, i.e., the set of all vectors of $B \otimes \mathbf{R}$ which have integral inner product with all elements of B). For any nonsingular primitive sublattice B of A, and in particular for $B = A^G$, B' is the projection of A into $B \otimes \mathbf{R}$ because the bilinear form on A is self dual. (As B is a primitive sublattice of A the natural map from A' to B' is surjective, so as A is self dual and can be identified with A' we see that the projection from A to B' is surjective.) This proves proposition 2.3.

There is a similar but slightly more complicated result for $\hat{H}^1$.

Proposition 2.4. *Suppose A is a free $\mathbf{Z}$ or $\mathbf{Z}_p$ module with an invariant self dual symmetric bilinear form $(,)$ acted on by the finite group G generated by g of order p. Define a bilinear form $\langle a, b\rangle$ on A by $\langle a, b\rangle = (S(a), b)$ where $S(a) = \sum_{0 \le n < p} ng^n(a)$. Then A_G is the quotient of A by the set C of all elements $a \in \mathrm{Ker}(N)$ such that $p|\langle a, b\rangle$ for all $b \in \mathrm{Ker}(N)$. In particular the bilinear form $\langle , \rangle$ induces a nonsingular antisymmetric bilinear form on $\hat{H}^1(G, A)$.*

Proof. Some easy calculations show (even if we do not assume $(,)$ is self dual) that $\langle , \rangle$ is antisymmetric mod$p$, that $S(a) - S(g(a)) = N(a) - pa$, that $N(S(a)) = (p-1)pN(a)/2$, and that the kernel of the map from A to A_G (i.e., the module generated by elements of the form $a - g(a)$) is contained in C.

Suppose $a \in C$; we want to deduce that $a = b - g(b)$ for some $b \in A$. We know that $N(S(a)) = 0$ (because $N(a) = 0$), and $p|(S(a), b)$ for all b with $N(b) = 0$. Hence $S(a)/p$ lies in $\mathrm{Ker}(N)'$. The submodule $\mathrm{Ker}(N)$ is a primitive nonsingular submodule of the self dual module A, so $S(a)/p$ lies in the orthogonal projection of A into $\mathrm{Ker}(N) \otimes \mathbf{R}$, i.e., $S(a)/p = b - N(b)/p$ for some $b \in A$. But this means that $S(a) = S(g(b)) - S(b)$, so that $S(a - b + g(b)) = 0$. But S is injective, as we can see by checking that it multiplies every eigenvector of g by a nonzero constant, so $a - b + g(b) = 0$. This proves proposition 2.4. (It is easy to see that $\hat{H}^1(G, A)$ has an antisymmetric $\mathbf{Z}/p\mathbf{Z}$-valued bilinear form induced from the cup product and the bilinear form on A, followed by the isomorphism from $\hat{H}^2(G, \mathbf{Z})$ to $\hat{H}^0(G, \mathbf{Z})$. The main point of the proof above is that this antisymmetric form is self dual when the form on A is self dual.)

3. Vertex superalgebras mod p.

In this section we will construct a vertex superalgebra for every element of odd prime order in the monster.

If R is a subring of the complex numbers $\mathbf{C}$, then by an R-form of the monster vertex algebra we mean a graded vertex algebra defined over R which is a free R module, and which becomes isomorphic to the FLM monster vertex algebra when it is tensored with $\mathbf{C}$, and which is acted on by the monster and contains a conformal vector (the components of whose vertex operator generate the Virasoro algebra). We say that an R-form is self dual if the natural bilinear form on the FLM algebra restricts to a self dual R-valued bilinear form on each homogeneous piece.

We let $V[1/2]$ be the $\mathbf{Z}[1/2]$-form of the monster vertex algebra constructed in theorem 3.2 below.

Theorem 3.1. *If g is an element of the monster of odd prime order p then $\hat{H}^*(g, V[1/2]) = \hat{H}^0(g, V[1/2]) \oplus \hat{H}^1(g, V[1/2])$ is a $\mathbf{Z}$-graded vertex superalgebra over $\mathbf{Z}/p\mathbf{Z}$, acted on by $C_M(g)/\langle g\rangle$. It has a nonsingular supersymmetric bilinear form that is invariant under $C_M(g)/\langle g\rangle$. If $h \in C_M(g)$ is p-regular then $\sum_{n\in\mathbf{Z}} \mathrm{Tr}(h|\hat{H}^*(g, V[1/2]_n))q^n$ is a Hauptmodul for some genus 0 subgroup of $SL_2(\mathbf{R})$, and is equal to the Hauptmodul of the element gh of M.*

Proof. The fact that $\hat{H}^*(g, V[1/2])$ is a vertex superalgebra follows from the remarks about group cohomology in the previous section. The nonsingularity of the supersymmetric bilinear form follows from propositions 2.3 and 2.4. The fact that the trace of g is a Hauptmodul follows from proposition 2.2 together with the result of [B92] that the series $\sum_{n\in\mathbf{Z}} \mathrm{Tr}(g|V_n)q^n$ is a Hauptmodul for any element $g \in M$. This proves theorem 3.1.

Remark. The bilinear form in theorem 3.1 is also compatible with the vertex algebra structure (where this notion is defined in the discussion below), but we will not use this fact.

Proposition 2.3 also shows that $\hat{H}^0(g, V[1/2])$ is isomorphic to the space ${}^gV = V^g/pV^g/((V^g/pV^g) \cap (V^g/pV^g)^\perp)$ suggested in [R94].

In the rest of this section we recall some results about vertex algebras from [B86] and give the construction of the $\mathbf{Z}[1/2]$-form $V[1/2]$ of the monster vertex algebra. The only serious use we make of vertex algebra structures is to use them to construct other modular vertex algebras, so the reader who wishes to ignore vertex algebras completely and only see the proof that the traces of various group elements are Hauptmoduls can replace the words "vertex algebra" by "graded vector space" without losing much. Similarly the conformal vectors and bilinear forms on vertex algebras are used mainly to construct conformal vectors and bilinear forms on modular vertex algebras, so the reader can ignore all the discussion of these.

We recall the definition of a vertex algebra over any commutative ring R. The definition we give here is equivalent to that given in [B86]. If V is an R module we define a vertex operator $a(z)$ on V to be a sequence of linear operators a_n for $n \in \mathbf{Z}$ on V, with the property that for any $b \in V$, $a_n b = 0$ for n sufficiently large (depending on a and b). We put these operators into the formal Laurent series $a(z) = \sum_{n\in\mathbf{Z}} z^n a_{-n-1}$. Then a vertex algebra over R is an R module V together with an element $1 \in V$ and a vertex operator $a(z)$, acting on V, for each $a \in V$, such that the following conditions are satisfied for any $a, b \in V$.

1. $1(z) = 1$, and $a(0)1 = a$ (i.e., $a_n 1 = 0$ if $n \geq 0$ and $a_{-1}1 = a$).
2. The vertex operators $a(z)$ and $b(y)$ formally commute, in the sense that we can find $n \geq 0$ (depending on a and b) such that all coefficients of monomials $x^i y^j$ of
$$(x-y)^n(a(x)b(y) - b(y)a(x))$$
are zero. (For a vertex superalgebra we replace $b(y)a(x)$ by $(-1)^{(\deg(a),\deg(b))}b(y)a(x)$.)
3. We denote the element $a_{-n-1}1$ by $D^{(n)}(a)$. Then $(D^{(n)}a)(z) = ((\frac{d}{dz})^n/n!)a(z)$.

This is similar to a definition of commutative associative algebras over R: we can define these as R modules V such that for every $a \in V$ we are given an operator a_L on V and an element $1 \in V$ with the properties that $1_L a = a_L 1 = a$, and the operators a_L and b_L commute for all $a, b \in V$. This shows that a vertex algebra can be thought of as a "commutative ring with singularities in the multiplication".

The operators $D^{(n)}$ have the properties $D^{(0)}(a) = a$, $D^{(m)} = 0$ if $m < 0$, and $D^{(m)}D^{(n)} = \binom{m+n}{m} D^{(m+n)}$.

We briefly recall the structure of the integral form V_Λ of the vertex algebra of Λ from [B86]. The lattice Λ has a certain nonsplit central extension $\hat{\Lambda}$ (in which the group operation is written multiplicatively) such

that if we denote a lifting of $a \in \Lambda$ by $e^a \in \hat{\Lambda}$, then $e^a e^b = (-1)^{(a,b)} e^b e^a$ so we get an exact sequence

$$0 \longrightarrow \pm 1 \longrightarrow \hat{\Lambda} \longrightarrow \Lambda \longrightarrow 0.$$

The automorphism group of $\hat{\Lambda}$ preserving the inner product on Λ is a nonsplit extension of the form $2^{24}.\mathrm{Aut}(\Lambda)$ which acts on the vertex algebra V_Λ of Λ (which really depends on $\hat{\Lambda}$ rather than Λ). V_Λ is graded by Λ in such a way that e^a has degree $a \in \Lambda$, it has an underlying ring structure which is "graded commutative", i.e., $ab = (-1)^{(\deg(a),\deg(b))} ba$ if a and b are homogeneous elements with Λ-degrees $\deg(a)$ and $\deg(b)$, and it has a derivation with divided powers, i.e., a set of additive operations $D^{(m)}$ for $m \in \mathbf{Z}$ such that $D^{(0)}(a) = a$, $D^{(m)} D^{(n)} = \binom{m+n}{m} D^{(m+n)}$, $D^{(m)} = 0$ if $m < 0$, and $D^{(n)}(ab) = \sum_{m \in \mathbf{Z}} (D^{(m)}(a)) D^{(n-m)}(b)$. The derivation D has Λ-degree 0; in other words $D^{(m)}(a)$ has the same Λ-degree as a. The graded-commutative ring V_Λ contains a copy of the twisted group ring of Λ which has a basis of elements denoted by e^a for $a \in \Lambda$ with the properties that $e^a e^b = \pm e^{a+b}$, $e^a e^b = (-1)^{(a,b)} e^b e^a$, and can be defined as the universal graded-commutative ring with a derivation with divided powers generated by this group ring. The subring $V_{\Lambda,0}$ of elements of V_Λ with Λ-degree 0 is generated as a commutative ring by elements of the form $(e^a)^{-1} D^{(i)}(e^a)$ for $a \in \Lambda$, $i \geq 1$.

A conformal vector of dimension (or "central charge") $c \in \mathbf{R}$ of a vertex algebra V is defined to be an element ω of V such that $\omega_0 v = D(v)$ for any $v \in V$, $\omega_1 \omega = 2\omega$, $\omega_3 \omega = c/2$, $\omega_i \omega = 0$ if $i = 2$ or $i > 3$, and any element of V is a sum of eigenvectors of the operator $L_0 = \omega_1$ with integral eigenvalues. If v is an eigenvector of L_0, then its eigenvalue is called the (conformal) weight of v. If v is an element of the monster vertex algebra V of conformal weight n, we say that v has degree $n - 1$ $(= n - c/24)$, and we write V_n for the module of elements of V of degree n.

The $\mathbf{R}$-form of the vertex algebra of any c-dimensional even lattice L has a canonical conformal vector $\omega = \sum_i a_i(1) a_i(1)/2$ of dimension c, where the elements a_i run over an orthonormal basis of $L \otimes \mathbf{R}$ and the monster vertex algebra has a conformal vector of dimension 24. If ω is a conformal vector of a vertex algebra V then we define operators L_i on V for $i \in \mathbf{Z}$ by

$$L_i = \omega_{i+1}.$$

These operators satisfy the relations

$$[L_i, L_j] = (i - j) L_{i+j} + \binom{i+1}{3} \frac{c}{2} \delta^i_{-j}$$

and so make V into a module over the Virasoro algebra. The operator L_{-1} is equal to D.

The vertex algebra of any even lattice L has a real valued symmetric bilinear form $(,)$ such that the adjoint of the operator u_n is $(-1)^i \sum_{j \geq 0} L_1^j (\sigma(u))_{2i-j-n-2}/j!$ if u has degree i, where σ is the automorphism of the vertex algebra defined by $\sigma(e^w) = (-1)^{(w,w)/2} (e^w)^{-1}$ for e^w an element of the twisted group ring of L corresponding to the vector $w \in L$. Similarly the monster vertex algebra has a real valued symmetric bilinear form $(,)$ such that the adjoint of the operator u_n is $(-1)^i \sum_{j \geq 0} L_1^j (u)_{2i-j-n-2}/j!$ if u has degree i. If a vertex algebra has a bilinear form with the properties above we say that the bilinear form is compatible with the conformal vector. If a vertex algebra does not have a conformal vector but only a $\mathbf{Z}$-grading we can still define compatible bilinear forms, because we can define the operator $L_1^j/j!$ to be the adjoint of the operator $L_{-1}^i/i! = D^{(i)}$. (If we are not in characteristic 0 we have to modify these definitions slightly by replacing $L_1^i/i!$ by a system of divided powers of L_1 satisfying some conditions.)

The integral form V_Λ of the vertex algebra of the Leech lattice contains the conformal vector $\omega = \sum_{1 \leq i \leq 24} a_i(1) a_i(1)/2$ where the a_i's run over an orthogonal basis of $\Lambda \otimes \mathbf{R}$ because we can rewrite this as $\omega = \sum_{1 \leq i < j \leq 24} a_i(1) a_j(1)(a_i', a_j') + \sum_{1 \leq i \leq 24} a_i(1) a_i(1)(a_i', a_i')/2$ where the a_i's run over a basis of Λ and the a_i''s are the dual basis. The elements a_i' have integral inner products and even norms because they all lie in Λ as Λ is unimodular. In general the same argument shows that the conformal vector of any even integral unimodular lattice lies in the integral form of its vertex algebra; this is usually false for lattices that are not unimodular and even. The bilinear form on the integral form V_Λ is self dual (section 2, (vi) of [B86]), and in fact the same is true if Λ is replaced by any even unimodular lattice.

For working out values of the bilinear form in V_Λ it is useful to note that $(a(1)b(1), c(1)d(1)) = (a,c)(b,d) + (a,d)(b,c)$ for $a, b, c, d \in \Lambda$. In particular the conformal vector ω has norm $(\omega, \omega) = \dim(\Lambda)/2 = 12$.

Theorem 3.2. *There is a* $\mathbf{Z}[1/2]$*-form* $V[1/2]$ *of the monster vertex algebra with a conformal vector and a self dual bilinear form such that* $V[1/2]$ *can be written as a direct sum of* $2^{12}.M_{24}$ *modules each of which is isomorphic to a submodule of the* $\mathbf{Z}[1/2]$*-form* $V_\Lambda[1/2]$ *of* V_Λ*.*

Proof. Frenkel, Lepowsky and Meurman construct the monster vertex algebra as a complex vector space. However their construction almost works over the integers (if we use the integral form of V_Λ above) except that they often need to decompose vector spaces into eigenspaces of abelian groups of order 2. This can be done over $\mathbf{Z}[1/2]$ (proof: $a = \frac{a+h(a)}{2} + \frac{a-h(a)}{2}$). A precise definition of this $\mathbf{Z}[1/2]$-form $V[1/2]$ of the monster vertex algebra is given implicitly in the next 2 paragraphs.

The $\mathbf{Z}[1/2]$-form $V[1/2]$ of the monster vertex algebra splits as the sum $V^0 \oplus V^1$ of the $+1$ and -1 eigenspaces of an element $h \in M$ of type 2B. As modules over $\mathrm{Aut}(\hat{\Lambda}) = 2^{24}.\mathrm{Aut}(\Lambda)$, V_Λ^0 and V^0 are isomorphic, where V_Λ^0 is the subalgebra of $V_\Lambda[1/2]$ fixed by the automorphism σ.

To construct the action of the monster on $V[1/2]$, Frenkel, Lepowsky, and Meurman split it further as $V[1/2] = V^{00} \oplus V^{01} \oplus V^{10} \oplus V^{11}$ where the V^{ij}'s are the eigenspaces of a 2^2-group in the monster containing h, and can be taken as free $\mathbf{Z}[1/2]$ modules. The modules V^0 and V^1 decompose as $V^0 = V^{00} \oplus V^{01}$, $V^1 = V^{10} \oplus V^{11}$. Frenkel, Lepowsky, and Meurman construct a triality automorphism σ that maps V^{00} to itself, transitively permutes the modules V^{01}, V^{10}, and V^{11}, and commutes with the elements of the group $2^{12}.M_{24} \subset \mathrm{Aut}(\hat{\Lambda})$. We use the isomorphism defined by σ between these 3 modules to transport the $\mathbf{Z}[1/2]$-form from V^{01} to V^{10}, and V^{11}, which defines the $\mathbf{Z}[1/2]$-form $V[1/2] = V^{00} \oplus V^{01} \oplus V^{10} \oplus V^{11}$. In particular σ commutes with $2^{12}.M_{24}$, so that V^{01}, V^{10}, and V^{11} are all isomorphic as modules over this group.

The conformal vector of $V[1/2]$ is just the conformal vector of $V^0 \subset V_\Lambda[1/2]$ (which is fixed by h). The self dual bilinear form on V_Λ induces a self dual bilinear form on V^0 over $\mathbf{Z}[1/2]$, which restricts to self dual forms on V^{01} and V^{00}, which give self dual forms on V^{10} and V^{11} by using the triality automorphism to transport the self dual form from V^{01}. This defines the self dual form on $V[1/2]$. This proves theorem 3.2.

4. A vanishing theorem for cohomology.

For every element g of the monster (or at least for those of odd order) we have constructed a vertex superalgebra $\hat{H}^*(g, V)$ acted on by $C_M(g)$ whose McKay-Thompson series are Hauptmoduls. For some elements g we will now show that the first cohomology group vanishes, so in fact we have constructed a modular vertex algebra satisfying the modular moonshine conjectures for the element g. It is certainly not true that $\hat{H}^1(g, V)$ vanishes for all elements g; by proposition 2.2 a necessary condition is that all coefficients of the Hauptmodul of g are nonnegative. This may be a sufficient condition but we do not know how to prove this in general. We will prove it is sufficient if g is an element of odd order coming from an element of M_{24}. This covers the cases of the conjugacy classes 3A, 3C, 5A, 7A, 11A, 15A, 21A, and 23A of the monster. In section 5 we will prove a similar theorem for elements of type 2A (under a mild assumption).

We will call a free R-module A acted on by a group G a permutation module if it has a basis that is closed under the action of G.

Lemma 4.1. *If* A *is a permutation module of a finite group* G *over a ring* R *with no* $|G|$ *torsion then* $\hat{H}^{-1}(G, A) = 0$*.*

Proof. We can assume that A comes from a transitive permutation representation of G, as all permutation representations are sums of transitive ones. Suppose S is the set of elements in the permutation representation, so that S is a basis for A. We have to show that $\mathrm{Ker}(N)$ is spanned by elements of the form $a - g(a)$. But $\mathrm{Ker}(N)$ is the set of elements $\sum_{s\in S} a_s s$ with $\sum_{g\in G} a_{g(s)} = 0$ (for some fixed $s \in S$), which is the set of elements with $\sum_{s\in S} a_s = 0$ because A has no $|G|$ torsion. But this space is obviously spanned by the set of elements of the form $s - g(s)$ as G acts transitively on S. This proves lemma 4.1.

Lemma 4.2. *The set of permutation modules is closed under taking sums, tensor products, and symmetric powers.*

Proof. The operations of taking sums or tensor products correspond to taking unions and products on the permutation representations. The operation of taking a symmetric n'th power of a representation corresponds to taking the set of "multisubsets" of cardinality n of a permutation representation S. (A

multisubset is like a subset except that we are allowed to take several copies of some element.) This proves lemma 4.2.

Remark. If A is a permutation module for G coming from a permutation in which every element of G acts as an even permutation then all exterior powers of A are permutation modules for G. In particular if G has odd prime order then the set of permutation modules is closed under taking exterior powers, but this is false when G has order 2.

Lemma 4.3. *If A is a free $\mathbf{Z}_p$ module acted on by the group G generated by an element g of order p, then $\hat{H}^1(g, A) = 0$ if and only if A is a permutation module of G.*

Proof. If A is a permutation module then $\hat{H}^1(g, A)$ vanishes by lemma 4.1 (using the fact that $\hat{H}^{-1}$ is isomorphic to $\hat{H}^1$ for cyclic groups). Conversely if $\hat{H}^1(g, A)$ vanishes then A is a sum of the indecomposable representations $\mathbf{Z}_p$ and $\mathbf{Z}_p[G]$ (because the other indecomposable representation $I \otimes \mathbf{Z}_p$ has nonvanishing $\hat{H}^1$ by the remarks after lemma 2.1), and these are both permutation modules of G. This proves lemma 4.3.

Lemma 4.4. *The free modules over $\mathbf{Z}_p$ acted on by $G = \mathbf{Z}/p\mathbf{Z}$ with vanishing $\hat{H}^1$ are closed under taking sums, products, and symmetric powers.*

Proof. This follows immediately from lemmas 4.2 and 4.3.

Lemma 4.5. *If g is an element of odd prime order p in $M_{24} \subset \mathrm{Aut}(\Lambda)$ (where Λ is the Leech lattice) then $\hat{H}^1(g, \Lambda) = \hat{H}^1(g, \Lambda \otimes \mathbf{Z}_p) = 0$.*

Proof. This follows from lemmas 2.1 and 4.1 and the fact that as a representation of M_{24}, $\Lambda \otimes R$ is isomorphic to the representation coming from the usual permutation representation of M_{24} whenever R contains $1/2$, and in particular whenever R is the ring of p-adic integers for p an odd prime. (Recall that the Leech lattice Λ contains a set of 24 pairwise orthogonal vectors of squared length 8 which are acted on by M_{24} as the standard permutation of M_{24} and which generate the $Z[1/2]$-module $\Lambda \otimes Z[1/2]$.) This proves lemma 4.5.

Theorem 4.6. *Suppose g is an element of odd prime order p in $\mathrm{Aut}(\Lambda)$ such that $\hat{H}^1(g, \Lambda) = 0$. Then $\hat{H}^1(g, V_\Lambda) = 0$.*

Proof. Recall from section 3 that there is an integral form V_Λ of the vertex algebra of Λ, which is graded by Λ.

We will show that the sum of the degree-λ pieces $V_{\Lambda,\lambda}$ of V_λ for λ running over the elements of some orbit of G on Λ has vanishing first cohomology, which will prove theorem 4.6. If λ is not fixed by g then the sum of the spaces $V_{\Lambda,g^i(\lambda)}$ is a free module over the group ring of G and so all its cohomology groups vanish. Hence we may assume that λ is fixed by g. In this case, $V_{\Lambda,\lambda}$ is isomorphic to the degree 0 piece $V_{\Lambda,0}$ as a G module (under multiplication by e^λ). (At this point we are implicitly using the fact that g has odd order to deduce that g fixes e^λ whenever g fixes λ; if g has even order we need to be more careful.) Hence we have reduced the proof of theorem 4.6 to showing that $\hat{H}^1(g, V_{\Lambda,0}) = 0$, or equivalently to showing that $\hat{H}^1(g, V_{\Lambda,0} \otimes \mathbf{Z}_p) = 0$.

By assumption on g and by lemma 4.3 we can choose a basis $a_1, \ldots, a_{24}$ of $\Lambda \otimes \mathbf{Z}_p$ such that the action of g on $\Lambda \otimes \mathbf{Z}_p$ is given by some permutation representation on this basis. The ring $V_{\Lambda,0}$ is the polynomial ring over $\mathbf{Z}_p$ generated by the elements $e^{-a_j} D^{(i)}(e^{a_j})$ for $i \geq 1$, $1 \leq j \leq 24$. This polynomial ring, considered as a representation of G over $\mathbf{Z}_p$, is a direct sum of products of symmetric powers of $\Lambda \otimes \mathbf{Z}_p$, so by lemma 4.4 its first cohomology vanishes. This proves theorem 4.6. (Warning: $V_{\Lambda,0}$ is strictly larger than the polynomial ring generated by the elements $D^{(i)}(a_j)$ for $i \geq 1$, $1 \leq j \leq 24$.)

Theorem 4.7. *Suppose g is an element of the monster of type 3A, 3C, 5A, 7A, 11A, or 23A, and let $V[1/2]$ be the $\mathbf{Z}[1/2]$-form of the monster vertex algebra constructed in 3.2. Then $\hat{H}^1(g, V[1/2]) = 0$.*

Proof. The element g in the monster commutes with an element h of type 2B because it can be seen from the monster character table in [C] that the monster always has an element of order $2p$ (and type 6C, 6F, 10B, 14B, 22B, or 46A) whose square is in the conjugacy class pA or 3C of g and whose p'th power is of type 2B. The centralizer of h is a group with structure $2^{1+24}.Co_1$, which contains a split extension of M_{24} by a 2-group of the form $2^{1+24}.2^{12}$. We can identify g with an element of this M_{24} group.

In particular we can consider g to be an element of $\mathrm{Aut}(\hat{\Lambda})$, so that it acts on the integral form V_Λ of the vertex algebra of the Leech lattice Λ. The 1st cohomology of g with coefficients in any direct summand of $V_\Lambda \otimes \mathbf{Z}[1/2]$ must also vanish, as it is a direct summand of $\hat{H}^1(g, V_\Lambda[1/2]) = 0$. By theorem 3.2, $V[1/2]$ is a direct sum of modules (V^{00}, V^{01}, V^{10}, and V^{11}) which are isomorphic as modules over g to direct summands of $V_\Lambda[1/2]$, so $\hat{H}^1(g, V[1/2]) = 0$. This proves theorem 4.7.

Corollary 4.8. *(The modular moonshine conjectures [R94] for the primes 3, 5, 7, 11, 23.) Suppose g is an element of order p in one of the conjugacy classes 3A, 3C, 5A, 7A, 11A, or 23A of the monster. Then there is a vertex algebra ${}^gV = \oplus_n {}^gV_n$ defined over the field with p elements with the following properties.*

1. *If g is not in the class 3C then ${}^gV_2$ contains a conformal vector (generating an action of the mod p Virasoro algebra) and has a nonsingular bilinear form compatible with the vertex algebra structure.*
2. *${}^gV$ is acted on by the group $C_M(g)/\langle g\rangle$, and this action preserves the conformal vector and the bilinear form.*
3. *The Brauer trace $\sum_n \mathrm{Tr}(h|{}^gV_n)q^n$ of any p-regular element h of $C_M(g)/\langle g\rangle$ on ${}^pV$ is a Hauptmodul, and is equal to the Hauptmodul of the element gh of the monster.*

Everything in corollary 4.8 except for the existence of a conformal vector follows from 4.7 and other things stated above. To show the existence of a conformal vector it is sufficient to show that the image of the conformal vector ω in $V[1/2]$ is nonzero, and to do this it is sufficient to find some vector fixed by g that has nonzero inner product with $\omega (\mathrm{mod} p)$. We let $a_1, \dots a_{24}$ be an orthonormal base of $\Lambda \otimes \mathbf{Z}_p$ corresponding to a set acted on by M_{24}, and the element g fixes at least one of the a_i's (as g is not of type 3C), say a_1. Then the conformal vector ω is $\sum a_i(1)a_i(1)/2$ which has nonzero inner product 1 with the element $a_1(1)a_1(1)$ mod$p$. This proves 4.8.

The head representation $\hat{H}^0(g, V[1/2]_1)$ containing the conformal vector ω splits slightly differently depending on whether $p > 3$ or $p \le 3$. If $p > 3$ then ω has norm $12 \bmod p$, which is nonzero so that $\hat{H}^0(g, V[1/2]_1)$ splits as the orthogonal direct sum of a 1-dimensional space spanned by ω and its orthogonal complement (and this splitting is obviously invariant under $C_M(g)$). If $p = 3$ and g is an element of type $3A$ then ω has norm $12 \equiv 0 \bmod 3$ so it is contained in its orthogonal complement, and $\hat{H}^0(g, V[1/2]_1)$ has a composition series of the form 1.781.1 (as a $C_M(g)/\langle g\rangle = Fi'_{24}$ module). The Atlas [C] states that the 781 dimensional module has an algebra structure mod 3, but this seems to be a mistake and the construction there only gives an algebra structure on 1.781.1 mod 3.

When g is in the class 3C then the vertex algebra $\hat{H}^0(g, V[1/2])$ does not have a conformal vector, and in fact not only is the image of ω equal to zero, but the whole degree 1 space $\hat{H}^0(g, V[1/2]_1)$ is zero. However we can turn $\hat{H}^0(g, V[1/2])$ into a better vertex algebra by "compressing" it. If we look at the series $q^{-1} + 248q^2 + 4124q^5 + \cdots$ we see that only every 3rd term of the graded space $\hat{H}^0(g, V[1/2])$ is nonzero. Hence we change the grading of the piece of degree $3n-1$ to n. We also change the vertex operator $v(x)$ of $v \in \hat{H}^0(g, V[1/2])$ to $v(x^{1/3})$. It is easy to check that this defines a new vertex algebra structure on $\hat{H}^0(g, V[1/2])$, (because if we are in characteristic 3 then $x - y = (x^{1/3} - y^{1/3})^3$), whose homogeneous degrees are the coefficients of $1 + 248q + 4124q^2 + \cdots$. The compression of the vertex algebra $\hat{H}^0(g, V[1/2])$ is probably isomorphic to the vertex algebra $V_{E_8}/3V_{E_8}$ (the vertex algebra of the E_8 lattice reduced mod 3) which is acted on by the finite group $E_8(\mathbf{F_3})$, because both vertex algebras have the same graded dimension and are both acted on by the Thompson group. (It is well known that the Thompson group $C_M(g)/\langle g\rangle$ is contained in $E_8(\mathbf{F_3})$.) Warning: the vertex algebra $V_{E_8}/3V_{E_8}$ can be lifted to characteristic 0, but the the action of the Thompson group does not lift to an action on the vertex algebra V_{E_8}.

5. The case $p = 2$.

In this section we will extend the proof of the modular moonshine conjectures (Corollary 4.8) to cover the case of the elements of type 2A in the monster, to obtain a vertex algebra over $\mathbf{F_2}$ acted on by the baby monster. The proof is similar to the cases for elements of odd order, except that there are several extra technical complications, and we have to use one assertion which we have not completely proved.

The theorems in this section depend on the following assumption about the monster vertex algebra. We have not rigorously verified this, but we sketch how its verification should go.

Assumption 5.1. *There is a $\mathbf{Z}[1/3]$-form $V[1/3]$ of the monster vertex algebra with a self dual bilinear form such that $V[1/3]$ can be written as a direct sum of $2.M_{12}.2$ modules each of which is isomorphic to a submodule of the $\mathbf{Z}[1/3]$-form $V_\Lambda[1/3]$ of V_Λ.*

We outline a possible proof of 5.1. (Roughly speaking, this outline would become a correct proof if Dong, Mason or Montague do not need to divide by any integer other than 3 in their constructions.) We obviously cannot use the FLM construction of the monster vertex algebra, which writes V as the sum of the eigenspaces of an element of type 2B, because this involves inverting 2 and gives a 2-divisible module whose cohomology vanishes. Instead we use the construction of the monster vertex algebra as a sum of eigenspaces of an element of type 3B, due independently to Dong and Mason [DM] and Montague [M]. This should produce a $\mathbf{Z}[1/3,\omega]$-form $V[1/3,\omega]$ of the monster vertex algebra as follows, where ω is a cube root of 1 satisfying $\omega^2+\omega+1=0$. We first note that modules over $\mathbf{Z}[1/3,\omega]$ can be written as the sums of eigenspaces of any group $\langle h\rangle$ of order 3 acting on them, because $a=\frac{a+h(a)+h^2(a)}{3}+\frac{a+\omega h(a)+\omega^2 h^2(a)}{3}+\frac{a+\omega^2 h(a)+\omega h^2(a)}{3}$. The vertex algebra $V[1/3,\omega]$ is a sum of 3 submodules V^0, V^1, and V^2, which are the eigenspaces of an element h of type 3B. The space V^0 is isomorphic to the subspace of $V_\Lambda[1/3,\omega]$ fixed by an element of order 3 coming from a fixed point free element of order 3 of $\mathrm{Aut}(\Lambda)$, and this defines the $\mathbf{Z}[1/3,\omega]$-form of V^0. The spaces V^i each split into the sum of 3 subspaces V^{ij} which are the eigenspaces of a group $(\mathbf{Z}/3\mathbf{Z})^2$ in the monster, and Dong and Mason and Montague show that there is a group $SL_2(\mathbf{F_3})$ acting transitively on the spaces V^{ij} for $(i,j)\neq(0,0)$. We use this group to transport the $\mathbf{Z}[1/3,\omega]$-form from V^{01} and V^{02} to V^{ij} for $i\neq 0$. This defines the $\mathbf{Z}[1/3,\omega]$-form on the monster vertex algebra (and it also has a self dual $\mathbf{Z}[1/3,\omega]$ bilinear form and a conformal vector, coming from the same structures on V_Λ).

We now reduce this $\mathbf{Z}[1/3,\omega]$-form to a $\mathbf{Z}[1/3]$-form. We have an operation of complex conjugation on V^0 coming from complex conjugation on $V_\Lambda\otimes\mathbf{Z}[1/3,\omega]$, and the action of $SL_2(\mathbf{F_3})$ can be used to transfer this to complex conjugation on all the spaces $V^{ij}\oplus V^{2i,2j}$, and hence to $V[1/3,\omega]$. This conjugation preserves the vertex algebra structure and commutes with the monster, and satisfies $\overline{\omega v}=\bar\omega\bar v$. Any element of $V[1/3,\omega]$ can be written uniquely in the form $a+\omega b$ with a and b fixed by conjugation, because finding a and b involves solving the 2 linear equations $v=a+b\omega$, $\bar v=a+\bar\omega v$, and there is a unique solution for a and b because the determinant of this system of equations is $\omega-\bar\omega$ which is a unit in $\mathbf{Z}[1/3,\omega]$. Hence if we define $V[1/3]$ to be the fixed points of the conjugation, we see that $V[1/3]\otimes\mathbf{Z}[1/3,\omega]=V[1/3,\omega]$. Hence $V[1/3]$ is a $\mathbf{Z}[1/3]$-form for the monster vertex algebra. This completes the arguments for assumption 5.1.

Theorem 5.2. *If we assume that 5.1 is correct then there is a vertex algebra defined over $\mathbf{F_2}$ acted on by the baby monster, such that the McKay-Thompson series of every element of the baby monster is a Hauptmodul. The vertex algebra has a conformal vector and a compatible self dual bilinear form, also invariant under the baby monster.*

Proof. We will only give details for parts of the argument that differ significantly from the proof of corollary 4.8. We choose an element $g\in M_{24}\subset\mathrm{Aut}(\Lambda)$ of order 2 and trace 8. (There is a unique conjugacy class of such elements in M_{24}.)

The first step is to prove that $\hat H^1(g,\Lambda)=\Lambda_{\langle g\rangle}/\mathrm{Ker}(N)=0$, which we do by direct calculation as follows. We can assume that g acts on Λ in the usual coordinates by acting as -1 on the first 8 coordinates and as $+1$ on the last 16. Then $\mathrm{Ker}(N)$ is the sublattice of Λ of vectors whose last 16 coordinates vanish. This lattice is a copy of the E_8 lattice with norms doubled (so it has 240 vectors of norm 4 and so on). It is generated by its norm 4 vectors and the centralizer of g acts transitively on these norm 4 vectors, so to prove that $\Lambda_{\langle g\rangle}=\mathrm{Ker}(N)$ we only need to prove that one of these norm 4 vectors is of the form $v-g(v)$ for some vector $v\in\Lambda$. We can do this by taking v to be the vector $(1^{23},-3)$. Therefore $\hat H^1(g,\Lambda)=0$.

From this it follows as in theorem 4.6 that $\hat H^1(\hat g,V_\Lambda)=0$, provided we show that g lifts to an element in $\mathrm{Aut}(\hat\Lambda)$ which we denote by $\hat g$, such that $\hat g$ also has order 2 and $\hat g$ fixes every element e^a of the twisted group ring of Λ corresponding to an element a of Λ fixed by g. (If g is of odd order the existence of a good element $\hat g$ is trivial, but for some elements of even order, for example those of trace 0, a lift with these properties does not exist.) Lemma 12.1 of [B92] says that such a lift $\hat g$ exists provided that $(v,g(v))$ is even for all elements $v\in\Lambda$, which follows because $(v,g(v))=((v-g(v),v-g(v))-(v,v)-(g(v),g(v)))/2$, and $(v,v)=(g(v),g(v))$ is even while $v-g(v)\in\mathrm{Ker}(N)$ has norm divisible by 4. Hence $\hat H^1(\hat g,V_\Lambda)=0$.

In particular any submodule of $V_\Lambda[1/3]$ invariant under $\hat g$ also has vanishing $\hat H^1$, so by assumption 5.1 $\hat H^1(\hat g,V[1/3])=0$. We can now follow the argument proving corollary 4.8 to construct a vertex algebra satisfying the conditions of theorem 5.2. This proves theorem 5.2.

Remark. In the proof of theorem 5.2 we should really have checked that the 2 vertex algebras constructed by Frenkel-Lepowsky-Meurman and by Dong-Mason-Montague are isomorphic as modules over the monster,

so that the traces of elements of the monster are Hauptmoduls. Dong and Mason have announced [DM] that these two vertex algebras are indeed isomorphic as vertex algebras acted on by the monster. It would also be easy to show that they are isomorphic as modules over the monster (but not as vertex algebras) by using the results of [B92] to calculate the character of the Dong-Mason-Montague algebra.

It seems likely that $V[1/2]$ and $V[1/3]$ both come from a conjectural integral form V of the monster vertex algebra by tensoring with $\mathbf{Z}[1/2]$ or $\mathbf{Z}[1/3]$; see lemma 7.1.

If we look at the McKay-Thompson series for the element 2B of the monster we see that the coefficients are alternating, which suggests that $\hat{H}^0$ vanishes for half the homogeneous pieces of V, and $\hat{H}^1$ vanishes for the other half. The next theorem shows that this is indeed the case.

Theorem 5.3. *Assume that 5.1 is correct. If $\hat{g}$ is an element of type 2B in the monster, then $\hat{H}^0(\hat{g}, V[1/3]_n)$ vanishes if n is even, and $\hat{H}^1(\hat{g}, V[1/3]_n)$ vanishes if n is odd.*

Proof. By using the argument in the last few paragraphs of the proof of theorem 5.2 we see that it is sufficient to prove the same result for the cohomology with coefficients in V_Λ for a suitable element $\hat{g}$ of $\mathrm{Aut}(\hat{\Lambda})$. We will take g to be the automorphism -1 of Λ, and take its lift $\hat{g}$ in $\mathrm{Aut}(\hat{\Lambda})$ to be the element taking e^a to $(-1)^{(a,a)/2}(e^a)^{-1}$ in the group ring. It is easy to check that $\hat{g}$ is an automorphism of order 2. As a graded $\hat{g}$ module, V_Λ is the tensor product of the twisted group ring and the module $V_{\Lambda,0}$ as in theorem 4.6. The twisted group ring is a sum of infinitely many free modules over the group ring and one copy of $\mathbf{Z}$ (spanned by 1), so its 0'th cohomology group is $\mathbf{Z}/2\mathbf{Z}$, and its first cohomology vanishes. Hence $H^*(\hat{g}, V_\Lambda) = H^*(\hat{g}, V_{\Lambda,0})$. We let ω be the involution of $V_{\Lambda,0}$ that is the product of $\hat{g}$ and the involution acting as -1^n on the piece of degree n. As multiplying the action of $\hat{g}$ by -1 exchanges H^0 and H^1, we see that to prove theorem 5.3 we have to show that $H^1(\omega, V_{\Lambda,0}) = 0$. To do this it is sufficient to show that $V_{\Lambda,0}$ is a permutation module for ω.

We now complete the proof of theorem 5.3 by finding an explicit basis of $V_{\Lambda,0}$ described in terms of S-functions, on which ω acts as a permutation. If we choose a basis $a_1, \dots, a_{24}$ of Λ, then $V_{\Lambda,0}$ is the polynomial ring generated by the elements $h_{i,n} = e^{-a_i} D^{(n)} e^{a_i}$, $1 \le i \le 24$, $n \ge 1$. The element $\hat{g}$ takes $h_{i,n}$ to $e^{a_i} D^{(n)} e^{-a_i}$, so $\omega(h_{i,n}) = e_{i,n}$, where $e_{i,n} = (-1)^n e^{a_i} D^{(n)} e^{-a_i}$. From the relation

$$\sum_m D^{(m)}(e^{a_i}) D^{(n-m)}(e^{-a_i}) = D^{(n)}(e^{a_i} e^{-a_i}) = 0$$

for $n \ge 1$ we find that

$$\sum_{0 \le m \le n} (-1)^m e_{i,m} h_{i,n-m} = 0$$

for $n \ge 1$, which recursively defines the $e_{i,n}$'s in terms of the $h_{i,n}$'s. If we identify the $h_{i,n}$'s with the n'th complete symmetric function (see [Mac], page 14) then the ring generated by the $h_{i,n}$'s for some fixed i is the ring of all symmetric functions. By the formulas 2.6' and 2.7 on page 14 of [Mac] we see that the $e_{i,n}$'s are then identified with the elementary symmetric functions, and ω with the canonical involution ω of [Mac]. The ring of all symmetric functions is spanned by the S-functions s_λ for permutations λ [Mac, p. 24, formulas 3.1 and 3.3], and the action of ω on the S-functions is given by

$$\omega(s_\lambda) = s_{\lambda'}$$

[Mac, p. 28, formula 3.8] where λ' is the conjugate partition of λ [Mac, p. 2]. Therefore the ring generated by the $h_{i,n}$'s for any fixed i is a permutation module for ω, and therefore so is $V_{\Lambda,0}$ because it is the tensor product of 24 permutation modules. This proves theorem 5.3.

Of course, as we are working in characteristic 2, there is really no difference between a vertex algebra and a vertex superalgebra, so the superalgebra associated to 2B can be considered as a vertex algebra with dimensions given by the coefficients of the series $q^{-1} + 276q + 2048q^2 + \cdots$. However it seems more natural to think of it as a superalgebra.

This superalgebra is acted on by the group $2^{24}.Co_1$. The next paragraph suggests that the 2^{24} may act trivially, so that we get an action of Co_1, but we have not proved this.

We can also ask if this superalgebra can be lifted to characteristic 0. It turns out that there is a vertex superalgebra (constructed below) with the right grading acted on by $\mathrm{Aut}(\Lambda)$. In fact this superalgebra has

2 different natural actions of $\mathrm{Aut}(\Lambda)$, one faithful, and one for which the center of $\mathrm{Aut}(\Lambda)$ acts trivially. Unfortunately we do not know of an integral form invariant under either action of $\mathrm{Aut}(\Lambda)$, but it seems reasonable to guess that both actions have invariant integral forms, and the reduction mod 2 of either integral form is the mod 2 vertex superalgebra above. (This requires that the 2^{24} acts trivially on this mod 2 vertex algebra.)

We can construct this superalgebra in characteristic 0 easily as the vertex superalgebra of the odd 12-dimensional unimodular lattice with no roots D_{12}, which is the set of vectors $(x_1, \dots, x_{24})$ in $\mathbf{R}^{24}$ such that all the x_i's are integers or all are integers $+1/2$, and their sum is even. This vertex superalgebra is acted on by the spinor group $Spin_{12}(\mathbf{R})$. The group $\mathrm{Aut}(\Lambda)$ in $SO_{24}(\mathbf{R})$ can be lifted to the spin group as it has vanishing Schur multiplier, so we get an action of $\mathrm{Aut}(\Lambda)$ on the vertex algebra. The reason why we get two actions is that there are two conjugacy classes of embeddings of $\mathrm{Aut}(\Lambda)$ in $SO_{24}(\mathbf{R})$ (which are interchanged by a reflection). The spin group does not act faithfully because an element of order 2 in the center acts trivially, and it is not hard to check that for exactly one of the classes of embeddings of $\mathrm{Aut}(\Lambda)$ in $SO_{24}(\mathbf{R})$ the element $-1 \in \mathrm{Aut}(\Lambda)$ lifts to the element of $Spin_{24}(\mathbf{R})$ acting trivially.

The existence of these two actions of $\mathrm{Aut}(\Lambda)$ has the curious consequence that every second coefficient of $q^{-1} + 276q + 2048q^2 + \cdots$ is in a natural way the dimension of 2 different representations of $\mathrm{Aut}(\Lambda)$, in which the nontrivial element of the center acts as either $+1$ or -1. For example 2048 decomposes as either $1771 + 276 + 1$ or $2024 + 24$.

6. Example: the Held group.

We give some numerical tables to illustrate the case when g is an element of type 7A in the monster, with centralizer $\langle g \rangle \times He$. First we give the 7-modular character table of He (taken from [R88]), followed by the modular characters of the first few head characters of $\hat{H}^0(g, V[1/2])$ (which can be read off from [CN] table 4). The bottom line gives the corresponding conjugacy classes in the monster group (the one whose Hauptmodul is given by the coefficients of the head characters).

	1A	2A	2B	3A	3B	4A	4B	4C	5A	6A	6B	8A	10A	12A	12B	15A	17A	17B
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	50	10	2	5	−1	2	2	−2	0	1	−1	0	0	−1	−1	0	−1	−1
	153	9	−7	0	3	−3	1	1	3	0	−1	1	−1	0	1	0	0	0
	426	26	10	3	−3	−2	2	2	1	−1	1	−2	1	1	−1	−2	1	1
	798	38	14	6	3	6	−2	2	−2	2	−1	0	−2	0	1	1	−1	−1
	1029	−35	21	21	0	−7	−3	1	4	1	0	−1	0	−1	0	1	$\frac{1-\sqrt{17}}{2}$	$\frac{1+\sqrt{17}}{2}$
	1029	−35	21	21	0	−7	−3	1	4	1	0	−1	0	−1	0	1	$\frac{1+\sqrt{17}}{2}$	$\frac{1-\sqrt{17}}{2}$
	1072	16	−16	10	−2	0	0	0	−3	−2	2	0	1	0	0	0	1	1
	1700	20	4	−10	5	0	−4	−4	0	2	1	0	0	0	−1	0	0	0
	3654	−10	38	−9	3	2	−2	−2	4	−1	−1	2	0	−1	1	1	−1	−1
	4249	9	−7	−8	−5	−3	1	1	−1	0	−1	1	−1	0	1	2	−1	−1
	6154	−70	−22	−2	7	6	2	2	4	2	−1	−2	0	0	−1	−2	0	0
	6272	−64	0	35	8	−8	0	0	−3	−1	0	0	1	1	0	0	−1	−1
	7497	81	−7	0	3	−3	1	−3	−3	0	−1	−1	1	0	1	0	0	0
	13720	−56	56	−14	7	0	8	0	−5	−2	−1	0	−1	0	−1	1	1	1
	14553	9	−7	0	−9	9	−7	1	3	0	−1	1	−1	0	−1	0	1	1
	17493	21	21	−21	0	−7	−3	5	−7	3	0	1	1	−1	0	−1	0	0
	23324	−196	28	14	−7	0	4	−4	−1	2	1	0	−1	0	1	−1	0	0
H_{-1}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
H_0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_1	51	11	3	6	0	3	3	−1	1	2	0	1	1	0	0	1	0	0
H_2	204	20	−4	6	3	0	4	0	4	2	−1	2	0	0	1	1	0	0
H_3	681	57	9	15	0	1	9	1	6	3	0	1	2	1	0	0	1	1
H_4	1956	92	−12	30	0	0	12	0	6	2	0	2	2	0	0	0	1	1
H_5	5135	207	15	41	8	7	15	−1	10	9	0	3	2	1	0	1	1	1
H_6	12360	312	−24	66	0	0	24	0	10	6	0	4	2	0	0	1	1	1
H_7	28119	623	39	111	0	7	39	3	19	11	0	5	3	1	0	1	1	1
H_8	60572	932	−52	146	11	0	52	0	22	14	−1	6	2	0	1	1	1	1
H_9	125682	1674	66	222	0	18	66	−2	32	18	0	8	4	0	0	2	1	1
H_{10}	251040	2464	−96	336	0	0	96	0	40	16	0	8	4	0	0	1	1	1
	7A	14A	14B	21A	21C	28A	28B	28C	35A	42A	42C	56A	70A	84A	84C	105A	119A	119A

The values for the first 50 head characters can be extracted from the tables in [MS], by looking up the values of the head characters in the monster conjugacy classes listed in the last line. The paper [MS] also gives the decompositions of the first 50 head characters of the monster into irreducibles, which can be compared with the next table. (The top left corners of both tables are very similar.)

The next table gives the decomposition of the first few head characters H_i of $\hat{H}^0(g, V[1/2])$ into irreducible characters. The columns correspond to the irreducible characters arranged in order of their degrees (which are given in the first row). For example the 5th row means that the composition factors of the head representation H_2 are the representations of dimension 1, 50, and 153.

	1	50	153	426	798	1029	1029	1072	1700	3654	4249	6154	6272	7497	13720	14553	17493	23324
H_{-1}	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_2	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_3	2	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H_4	2	3	2	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
H_5	4	5	3	2	1	0	0	1	1	0	0	0	0	0	0	0	0	0
H_6	4	7	5	3	1	0	0	3	1	0	1	0	0	0	0	0	0	0
H_7	7	12	8	7	3	0	0	5	2	1	2	0	0	0	0	0	0	0
H_8	8	16	13	9	4	0	0	9	4	1	4	1	0	1	0	0	0	0
H_9	12	25	18	17	8	0	0	15	7	4	7	1	0	2	0	1	0	0
H_{10}	14	35	29	26	11	0	0	27	12	6	15	4	1	4	0	2	0	0
H_{11}	23	53	43	45	21	0	0	43	22	13	25	7	2	8	1	4	1	0
H_{12}	26	75	67	68	29	0	0	74	37	21	48	16	4	14	1	9	2	1
H_{13}	40	114	99	114	50	0	0	119	62	41	79	27	8	26	3	18	5	3
H_{14}	49	161	155	174	72	0	0	202	106	68	144	58	16	44	6	32	10	6
H_{15}	71	243	233	290	119	0	0	328	176	124	244	99	28	74	13	58	20	14
H_{16}	88	348	358	446	173	0	0	543	292	204	422	186	53	124	22	103	35	28
H_{17}	128	519	543	723	279	1	1	876	484	355	700	319	91	206	43	176	64	54
H_{18}	161	752	831	1121	408	1	1	1425	785	578	1179	562	160	335	72	300	110	100
H_{19}	231	1125	1263	1793	643	4	4	2280	1271	969	1927	937	270	542	129	500	190	180
H_{20}	298	1637	1932	2769	951	6	6	3656	2043	1560	3159	1591	457	868	215	824	315	313

Notice that the multiplicities of nontrivial representations of small dimension have a tendency to start off with some of the values of the series $1, 1, 2, 3, 5, 7, \ldots$ which are the values $p(n)$ of the partition function. The same is true for the multiplicities of representations of the monster in the monster vertex algebra, and in that case it can be explained using the Virasoro algebra, and the fact that the Verma modules for the Virasoro algebra with $c = 24$, $h > 0$ are irreducible and have graded dimensions $1, 1, 2, 3, 5, 7, \ldots, p(n), \ldots$. (The irreducible factor of the Verma module with $c = 24$, $h = 0$ has pieces of dimension $p(n) - p(n-1) = 1, 0, 1, 1, 2, 2, 4, 4, 7, \ldots$, which more or less accounts for the initial multiplicities of the trivial character.) For our modular vertex algebras this explanation does not work so well, because the Verma modules are usually reducible over finite fields. We can get a small amount of information by examining how the Verma modules decompose, but this does not seem to be enough to account for why the numbers in the table above are so similar to the numbers we get when we look at the monster vertex algebra. On the other hand, if g has large prime order then the corresponding numbers do not seem to be similar to those for the monster; for example, if g has order 71 then the dimensions of the H_i's start off $1, 0, 1, 1, 1, \ldots$, which cannot be the dimensions corresponding to any representation of the Virasoro algebra in characteristic 0.

Silly question: why do the representations of dimension 1029 appear so late in the head characters?

7. Open problems and conjectures.

1. Can the information about modular representations be used to calculate the $|g|$-modular character tables of $C_M(g)$? The mod 7 character table of He has already been worked out in [R88], so the next simplest case is the mod 5 character table of the Harada-Norton group HN. For example, by cutting up the mod 5 vertex algebra of HN using the mod 5 Virasoro algebra we find that HN has representations over $\mathbf{F_5}$ of dimensions 1, 133, 626 and 2451 (which are probably irreducible). Unfortunately it seems to be difficult to get useful information like this from the later head representations, because we run into the problem that Verma modules over the Virasoro algebra mod p are not irreducible.
2. Does the monster vertex algebra have an integral form V such that each homogeneous piece is self dual under the natural bilinear form? It is easy to construct some monster invariant integral form by taking some integral form and taking the intersections of its conjugates under the action of the monster, but this will be far too small. The following lemma shows that we are quite close to constructing such an integral form.

Lemma 7.1. *Suppose that the spaces $V[1/2] \otimes \mathbf{Z}[1/6]$ and $V[1/3] \otimes \mathbf{Z}[1/6]$ are isomorphic as vertex algebras*

acted on by the monster. Then there exists an integral form of the monster vertex algebra with a compatible self dual integral bilinear form.

Dong and Mason [DM] have announced that these two vertex algebras are isomorphic over the complex numbers, but their description of the proof (which has not appeared yet) sounds as if it might be hard to carry out over $\mathbf{Z}[1/6]$.

Proof. We denote $V[1/2] \otimes \mathbf{Z}[1/6]$ by $V[1/6]$, so we can assume that $V[1/6]$ contains $V[1/2]$ and $V[1/3]$ as subalgebras, and we define V to be $V[1/2] \cap V[1/3]$. It is obvious that V is a $\mathbf{Z}$-form of the monster vertex algebra, and we just have to check that the bilinear form on V is self dual. The embeddings of $V[1/2]$ and $V[1/3]$ into $V[1/6]$ preserve the conformal vector (as this is the only degree 2 vector ω fixed by the monster such that the operator ω_1 multiplies every vector by its degree), so the embeddings preserve the action of the Virasoro algebra. The bilinear forms are determined by the grading and vertex algebra structure and the action of the Virasoro algebra, so the embeddings also preserve the bilinear forms on all 4 algebras. If we look at the embedding of V into $V[1/2]$ we see that the bilinear form on V is self dual over $\mathbf{Z}_p$ for any odd prime p (as the bilinear form on $V[1/2]$ is self dual over $\mathbf{Z}[1/2]$), and similarly if we look at the embedding into $V[1/3]$ we see that the bilinear form on V is self dual over $\mathbf{Z}_p$ for any $p \neq 3$. Hence the symmetric bilinear form on V is self dual over all rings of p-adic integers, and is therefore self dual over $\mathbf{Z}$. This proves lemma 7.1.

It may be possible to prove that the vertex algebras $V[1/2]$ and $V[1/3]$ are isomorphic over $\mathbf{Z}[1/6]$ either by carrying out the proof suggested in [DM] over $\mathbf{Z}[1/6]$, or by constructing the monster vertex algebra as a sum of eigenspaces of an element of the monster of type 6B. This element corresponds to a fixed point free element of order 6 in $\mathrm{Aut}(\Lambda)$ (of trace 12) whose cube and square are the elements of orders 2 and 3 in $\mathrm{Aut}(\Lambda)$ used to construct $V[1/2]$ and $V[1/3]$.

The integral form V would give integral forms for all the homogeneous spaces V_n, and in particular would give an integral form on the Griess algebra V_1. This cannot be the same as the integral form constructed by Conway and Norton in [C85], because the one in [C85] contains the element $\omega/2$ (which is denoted by 1 there). It seems possible that Conway and Norton's integral form is spanned by $\omega/2$ together with the elements of V_1 which have integral inner product with $\omega/2$. Notice that the bilinear form used in [C85] is half the bilinear form on V_1.

3. Assume the integral form V exists. Is $\hat{H}^1(g, V)$ zero whenever g is an element of the monster whose Hauptmodul has no negative coefficients? (Theorem 4.7 shows this for some elements of odd order.) If the coefficients of the Hauptmodul for g alternate in sign, do the groups $\hat{H}^0(g, V_{2n})$ and $\hat{H}^1(g, V_{2n+1})$ vanish? (Theorem 5.3 proves this for elements of type 2B.)
4. What happens if g is an element of composite order? For example, if we look at the Hauptmodul for an element of type 4B we see that it starts off $q^{-1} + 52q + 834q^3 + 4760q^5$, and the coefficient 52 of q^1 is the dimension of the Lie algebra F_4, and the centralizer of an element of type 4B is of the form $(4 \times F_4(\mathbf{F_2})).2$. This suggests there should be a modular vertex algebra corresponding to elements of type 4B, whose "compression" should be the reduction mod 2 or 4 of a vertex algebra for F_4 defined over $\mathbf{Z}$, in the same way that the compression of the vertex algebra for elements of type 3C is the reduction mod 3 of an algebra for E_8. (See the end of section 4.)
5. We can construct Lie algebras and superalgebras which have much the same relation to our modular vertex algebras as the monster Lie algebra [B92] has to the monster vertex algebra. We do this by using the $\mathbf{Z}_p$-forms of the monster vertex algebra to put $\mathbf{Z}_p$-forms on the monster Lie algebra (with a self dual symmetric invariant bilinear form), and then take the Tate cohomology of this $\mathbf{Z}_p$-form of the monster Lie algebra, which by the comments at the beginning of section 2 produces a Lie superalgebra. (Of course if we have a good integral form of the monster Lie algebra we can use this directly and not worry about $\mathbf{Z}_p$-forms.) The Lie algebras and superalgebras we get are similar to generalized Kac-Moody algebras, except that they are over fields of characteristic p rather than characteristic 0: they have a root system, a Cartan subalgebra, an invariant nonsingular symmetric bilinear form, a Cartan involution, and a $\mathbf{Z}$-grading with finite dimensional homogeneous pieces. Their structure as $C_M(g)$ modules can be described as follows: they have a $\mathbf{Z}^2$-grading, such that the piece of degree (m, n) is isomorphic to ${}^gV_{mn}$ if $(m, n) \neq (0, 0)$, and the piece of degree $(0, 0)$ (the Cartan subalgebra) is 2-dimensional and acted on trivially by $C_M(g)$. This suggests that there should be some sort of theory of "generalized Kac-Moody algebras mod$p$", which could be applied to study these algebras. For example, we could ask for the

Lie algebra homology groups of the positive degree subalgebras (which in characteristic 0 is equivalent to asking for the simple roots). Notice that many of these modular Lie algebras cannot be obtained by reducing some integral form of a generalized Kac-Moody algebra mod$p$, because the denominator formula shows that some of the simple roots would then have negative multiplicity.

6. The modules $\hat{H}^*(g, V[1/2])$ are acted on not just by the centralizer of g but by the normalizer $N_M(g)$ of g. What are the traces of elements of the normalizer of g that are not in the centralizer? It may be possible to do this by extending proposition 2.2 to the case when the subgroup $\langle g \rangle$ is only normal and not central. (Notice that if $\hat{H}^1(g, V[1/2])$ is nonzero then elements of the normalizer do not necessarily preserve the algebra structure on $\hat{H}^*(g, V[1/2])$.)
7. Give a complete proof of assertion 5.1.
8. Can the modular vertex algebras ${}^gV$ be lifted to characteristic 0 in some way? The answer to the strong form of this question is usually "no": it is easy to check that it is usually impossible to lift ${}^gV$ to a vertex algebra in characteristic 0 that is acted on by $C_M(g)$. However Queen [Q] found strong evidence that ${}^gV$ could be lifted to some $C_M(g)$ representation in characteristic 0 (which cannot carry an invariant vertex algebra structure). The representations that Queen found evidence for are now called twisted sectors. Perhaps these representations have some sort of "twisted" vertex algebra structure, where the vertex operators $a(z)$ have branch points of order p at the origin. It might be possible to use some sort of analogue of Witt vectors for vertex algebras to construct these. (But there is one serious obstruction to any canonical way of lifting some ${}^gV$'s to characteristic 0: the automorphism group in characteristic 0 is sometimes a *nonsplit* central extension of the automorphism group in characteristic p.) On the other hand we have seen (in the remarks at the end of sections 4 and 5) that if g is of type 3C or 2B then ${}^gV$ can probably be lifted to a vertex algebra in characteristic 0, which is not acted on by $C_M(g)$. Dong, Li and Mason [DLM] have recently made some progress on this question by constructing a twisted sector that is probably a lift to characteristic zero of the space ${}^gV$ when g is of type $2A$.
9. If $p = 3, 5, 7$, or 13 and g is an element of type pB in the monster corresponding to the group $\Gamma_0(p)$ then the group $C_M(g)/O_p(C_M(g))$ contains an element of order 2 in its center. We conjecture that this element of order 2 acts as $+1$ on $\hat{H}^0(g, V[1/2])$ and as -1 on $\hat{H}^1(g, V[1/2])$. This would imply that the graded modular characters of both $\hat{H}^0$ and $\hat{H}^1$ can be expressed as a linear combination of 2 Hauptmoduls. These are the only elements of prime order in the monster not already covered by theorems 4.7, 5.2, 5.3, and question 3 above, so an affirmative answer to this question and question 3 would mean that we would have a complete description of the modular characters of both $\hat{H}^0(g, V)$ and $\hat{H}^1(g, V)$ for all elements g of prime order in the monster.

References.

[AW] M. F. Atiyah, C. T. C. Wall, Cohomology of finite groups, in "Algebraic number theory", editors J. W. S. Cassels and A. Fröhlich, Academic Press 1967.

[B86] R. E. Borcherds, Vertex algebras, Kac-Moody algebras, and the monster. Proc. Natl. Acad. Sci. USA. Vol. 83 (1986) 3068-3071.

[B92] R. E. Borcherds, Monstrous moonshine and monstrous Lie superalgebras, Invent. Math. 109, 405-444 (1992).

[C] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Clarendon Press, Oxford, 1985.

[C85] J. H. Conway, A simple construction for the Fischer-Griess monster group, Invent. Math. 79 (1985) p. 513-540.

[CN] J. H. Conway, S. Norton, Monstrous moonshine, Bull. London. Math. Soc. 11 (1979) 308-339.

[CR] C. W. Curtis and I. Reiner, "Methods of representation theory Vol 1", Wiley Interscience, 1981 and 1990.

[DLM] C. Dong, H. Li, G. Mason, Some twisted sectors for the moonshine module, to appear in Contemporary Math.

[DM] C. Dong and G. Mason, On the construction of the moonshine module as a $\mathbf{Z}_p$-orbifold, Santa Cruz preprint, 1992. To appear in: Proc. 1992 Joint Summer Research Conference on Conformal Field Theory, Topological Field theory and Quantum Groups, Mount Holyoke, 1992, Contemporary Math.

[FLM] I. B. Frenkel, J. Lepowsky, A. Meurman, Vertex operator algebras and the monster, Academic press 1988.

[Mac] I. G. Macdonald, "Symmetric functions and Hall polynomials", Oxford University press, 1979.

[MS] J. McKay, H. Strauss, The q-series of monstrous moonshine and the decomposition of the head characters, Comm. in Alg. (1990) 18, 253-278.

[M] P. Montague, Third and Higher Order NFPA Twisted Constructions of Conformal Field Theories from Lattices, preprint, submitted to Nuc. Phys. B.

[N] S. P. Norton, Generalized Moonshine, Proc. Symp. Pure Math. 47 (1987) p. 208-209.

[Q] L. Queen, Some relations between finite groups, Lie groups, and modular functions, PhD thesis, Cambridge University, England, 1980.

[R88] A. J. E. Ryba, Calculation of the 7-modular characters of the Held group. J. Algebra, 117, 240-255, 1988.

[R94] A. J. E. Ryba, Modular Moonshine?, 1994 preprint.