

MODULAR MOONSHINE, III

RICHARD E. BORCHERDS

CONTENTS

1. Introduction	129
Notation	131
2. Representations of $\mathbf{Z}_p[G]$	133
3. The $\mathbf{Z}[1/2]$ -form of the monster Lie algebra	139
4. The modular moonshine conjectures for $p \geq 13$	142
5. Calculation of some cohomology groups	146
6. Elements of type $3B$, $5B$, $7B$, and $13B$	149
7. Open problems and conjectures	151

1. Introduction. This paper is a continuation of the earlier paper [BR], so we only briefly recall results that were discussed in more detail there. In [BR] we constructed a modular superalgebra for each element of prime order in the monster and worked out the structure of this superalgebra for some elements in the monster. In this paper we work out the structure of this superalgebra for the remaining elements of prime order.

A. Ryba conjectured [R] that for each element of the monster of prime order p of type pA , there is a vertex algebra gV defined over the finite field \mathbf{F}_p and acted on by the centralizer $C_M(g)$ of g in the monster group M . This has the property that the graded Brauer character $\text{Tr}(h|{}^gV) = \sum_n \text{Tr}(h|{}^gV_n)q^n$ is equal to the Hauptmodul $\text{Tr}(gh|V) = \sum_n \text{Tr}(g|V_n)q^n$. (Here V is the graded vertex algebra acted on by the monster constructed by I. Frenkel, J. Lepowsky, and A. Meurman [FLM].) In [BR] the vertex superalgebra gV was defined for any element $g \in M$ of odd prime order to be the sum of the Tate cohomology groups $\hat{H}^0(g, V[1/2]) \oplus \hat{H}^1(g, V[1/2])$ for a suitable $\mathbf{Z}[1/2]$ -form $V[1/2]$ of V . It was also shown that $\text{Tr}(h|{}^gV) = \text{Tr}(h|\hat{H}^0(g, V[1/2])) - \text{Tr}(h|\hat{H}^1(g, V[1/2]))$ was equal to the Hauptmodul of $gh \in M$. Hence to prove the modular moonshine conjecture for an element g of type pA , it is enough to prove that $\hat{H}^1(g, V[1/2]) = 0$. In [BR] this was shown by explicit calculation for the elements of type pA for $p \leq 11$, using the fact that these elements commute with an element of type $2B$. For $p \geq 13$ this method does not work, because these elements do not commute with an element of type $2B$. The first main theorem of this paper is Theorem 4.1, which states that if g is an element of prime order $p \geq 13$ not of type $13B$, then

Received 31 October 1994.

Author's work supported by National Science Foundation grant number DMS-9401186 and by a Royal Society research professorship.