Journal of Pure and Applied Algebra 44 (1987) 191-214
North-Holland

SPORADIC GROUPS, CODE LOOPS AND NONVANISHING COHOMOLOGY

Robert L. GRIESS, Jr.
Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Communicated by E.M. Friedlander and S. Priddy
Received 21 November 1985

Dedicated to Jack McLaughlin on the occasion of his sixtieth birthday

1. Introduction

I intend to discuss a number of interesting 2-locals in sporadic groups and show how code loops, which are certain Moufang loops, may be used to describe the subgroups abstractly. Existence proofs of parabolic subgroups of sporadics which are independent of the existence proofs of the sporadics have not existed in every case. When available, some such demonstrations of existence have been ad hoc. This paper partially alleviates that problem. It is, I believe, the first systematic attempt to describe some of the more complicated parabolics by a unified theme. I was moved to attempt this by Conway's use of a loop invented by Parker to describe a parabolic of shape $2^{2+11+22}(S_3\times M_{24})$ in the monster [8]. The first direct construction of this parabolic is due to J. Tits, whose notes (see [35], especially III and IV, and preprint of [37]) were circulated months before Conway's work was publicized. They may well have influenced Conway's construction of the monster, though they do not contain the loop concept.

Extension-theoretic matters arise naturally in the course of the discussion. In particular, nonsplit extensions are often relevant here. By contrast, the parabolic subgroups of groups of Lie type are split extensions because of the Levi factors and one can obtain many of their properties easily because of the (B,N)-structure.

For some time, I have been fascinated by the connection between sporadic groups and exceptional degree 1 and 2 cohomology. It is a pleasure to acknowledge Jack McLaughlin's many observations which directed my attention to aspects of this phenomenon and his mastery of cohomology of groups.

In Section 2, I review basic matters about code loops and set up notation to study maps on them.

In Section 3, I discuss a few results about generic behavior of cohomology groups for naturally defined families of groups and modules and examples of nonvanishing cohomology in sporadic groups.

In Section 4, the important example of the loop $\mathbb{O}_{16}$ is discussed. Its occurrence as a double basis of the Cayley numbers has been well known for some time. The group $\mathrm{Aut}(\mathbb{O}_{16})$ is a nonsplit extension of an elementary abelian 2-group of order 8 by $\mathrm{GL}(3,2)$. Basic structure information about this group is surprisingly easy to obtain from the loop point of view.

In Section 5, a general nonsplitting result for subgroups of $\mathrm{Aut}(L)$, for L a code loop, is obtained. Other nonsplitting results for group extensions are discussed.

In Section 6, the extensions of $\mathrm{GL}(3,2)$ over $\mathbb{Z}_4^3$ which occur as maximal 2-locals in sporadics are analyzed. Since Alperin's early results on these extensions were never published, I give a proof of his result and include additional details about the nonsplit extension.

In Section 7, constructions of several other sporadic parabolics as maps on loops are achieved. I believe that this style of construction will apply to other cases.

A basic reference for parabolics in sporadic groups is [29].

2. Code loops

In this section, we review some basic definitions and results about code loops, the class of Moufang loops of interest.

Definition. A *loop* is a set L with binary composition $L\times L\to L$ such that there is an identity and for all $x\in L$ there is $y\in L$ such that $xy=yx=1$.

Definition. The loop L is *Moufang* if one (hence all) of the following identities holds:

(a) $xy\cdot zx=(x\cdot yz)x$,

(b) $(xy\cdot z)y=x(y\cdot zy)$,

(c) $x(y\cdot xz)=(xy\cdot x)z$

for all $x,y,z\in L$.

The nonzero real Cayley numbers from a Moufang loop.

We are interested in loops which are extensions of elementary abelian 2-groups by $\mathbb{Z}_2$. There are two equivalent formulations, (I) and (II) below. The first is due to R. Parker and the second to this author in [22], where the *equivalence of the two procedures* was demonstrated. I call such a loop a *code loop*.

First some notation. If V is a vector space over $\mathbb{F}_2$ and $\phi: V\times V\to\mathbb{F}_2$ a function satisfying $\phi(0,x)=\phi(x,0)=0$ for all $x\in X$, we make $\hat{V}=\mathbb{F}_2\times V$ into a loop by defining $(c,x)(d,y)=(c+d+\phi(x,y),x+y)$. Use bars for the map $\hat{V}\to V$, $(c,x)\to x$. Let $p:V\to\mathbb{F}_2$ be a function with $p(0)=0$ and identify $\mathbb{F}_2$ with $\mathbb{F}_2\times 0<\hat{V}$. Define

$$N(x_1,\ldots,x_m)=\sum_{(c_i)\in\mathbb{F}_2^m} p(c_1\bar{x}_1+\cdots+c_m\bar{x}_m).$$

Note that $N(x_1,\ldots,x_m)=0$ if $\{\bar{x}_1,\ldots,\bar{x}_m\}$ is independent. Write $[x,y]$ for the commutator $(yx)^{-1}(xy)$ and $[x,y,z]$ for the associator $(x\cdot yz)^{-1}(xy\cdot z)$. Consider the conditions

(S) $x^2 = N(x)$.

(C) $[x, y] = N(x, y)$.

(A) $[x, y, z] = N(x, y, z)$.

(I) Let $V \cong \mathbb{F}_2^n$ for some $n \geq 0$ and let $\mathcal{D} \subseteq V^{\#} = V - \{0\}$ have characteristic function p. Assume the *evenness condition*: $\sum_{x \in W} p(x) = 0$ whenever $W \leq V$, dim $W \geq 4$. There exists a Moufang loop L satisfying (S), (C) and (A).

(II) Let V be a doubly even binary code and let $p(x) = \frac{1}{4}|x|$ ($= \frac{1}{4}$ the weight of x). There exists a Moufang loop L satisfying (S), (C) and (A).

The evenness condition is automatically satisfied by doubly even codes; see [22]. We call $\mathcal{D}$ the set of *odd vectors* or *odd codewords.*

We want to define certain groups of maps on loops for use in Section 7. Write $P(A)$, $PE(A)$ for the vector space of subsets, even subsets, respectively, of the set A.

Notation. A an alphabet and C a code in $P(A)$; M a code loop based on the code $\bar{M}$; V^* denotes $\mathrm{Hom}(V, \mathbb{F}_2)$ for a vector space V over $\mathbb{F}_2$; $\langle\, ,\, \rangle$ denotes the pairing of $V \times V^*$ or $V^* \times V$ into $\mathbb{F}_2$; $\langle S, T\rangle = |S \cap T| (\mathrm{mod}\ 2)$ for $S, T \in P(A)$.

Define maps

$$x(i, d), \quad i \in P(A), \quad d \in M;$$

$$y(\lambda, \mu), \quad \lambda \in P(A), \quad \mu \in \bar{M}^*;$$

$$z_\lambda, \quad \lambda \in P(A)$$

on $M^L = \mathrm{Maps}(L, M)$, for $L \subseteq A$, by declaring the image of (a_k), $k \in L$, to be (b_k), where

$$b_k = \begin{cases} a_k d, & \langle i, k\rangle = 1, \\ a_k, & = 0; \end{cases}$$

$$b_k = a_k z^{\langle \lambda, k\rangle \langle \mu, a_k\rangle};$$

$$b_k = a_k z^{\langle \lambda, k\rangle};$$

in the respective cases. Since $N(a, b, c)$ is trilinear, we may write $b \cap c$ for the linear functional $a \to N(a, b, c)$. We are identifying $P(A)$ with $P(A)^*$.

We now restrict ourselves to the case where $i \in C$, C is doubly even, $\lambda \in PE(A)$, $v \in P(A)$ of the form $i \cap j$, $i, j \in C$. Let X, Y, Z be the groups generated by, respectively, all $x(i, d)$, $y(\lambda, \mu)$, z_v. Then $YZ = Y \times Z$ is abelian and $Z \leq ZY \leq ZYX$ is a central series.

We record a few elementary calculations.

(2.1) $z_\lambda z_\mu = z_{\lambda + \mu}$.

(2.2) $[z_\lambda, x(i, d)] = 1$, $[z_\lambda, y(\mu, v)] = 1$.

(2.3) $y(\lambda,\mu)$ is linear in each variable, $Y \cong PE(A) \otimes \bar{M}^*$.

(2.4) $x(i,d)x(j,e) : (a_k) \to (b_k)$ where

$$b_k = \begin{cases} a_k & \text{if } \langle i,k\rangle = 0,\ \langle j,k\rangle = 0, \\ a_k d & \quad = 1, \qquad = 0, \\ a_k e & \quad = 0, \qquad = 1, \\ a_k \cdot dez^{N(a_k,d,e)} & \quad = 1, \qquad = 1. \end{cases}$$

Proof. Straightforward, using (A) on the fourth line.

(2.5) $x(i,d)^2 = z_i^{Nd}$.

(2.6) $[x(i,d), x(j,e)] = z_{i\cap j}^{N(d,e)}$.

(2.7) The commutator subgroup of X is $Z = \langle z_B \mid B = i \cap j$ for some $i, j \in C\rangle$ if M is noncommutative.

(2.8) $[x(i,d), y(\lambda,\mu)] = z_{i\cap\lambda}^{\langle d,\mu\rangle}$; $i \cap \lambda \in PE(A)$ if $i, \lambda \in C$.

3. Some generic behavior of cohomology and exceptional behavior within sporadic groups

Many individuals have observed that cohomology of a family of groups tends to have a regular pattern, except at the beginning of the series. Early examples of this may be seen in the work of Schur [31, 32] and Steinberg [33, 34].

It is hard to say who first articulated this general observation. McLaughlin had done so by the late 1960's. In [5], credit is given to [6] and [27] (Landazuri was a student of McLaughlin).

I am aware of the following general results which are relevant to the above situation. The first concerns behavior as the rank increases and the second as the field increases.

Theorem 3.1 (Friedlander, 1976 [15]). *Let k be a field with more than 2 elements and let $G_n(k)$ be one of* GL_n, SL_n, U_n, O_n, Sp_{2n}, SO_n *over k and let q be a prime,* $q \neq \mathrm{char}\, k$. *Then, the natural map*

$$H_i(G_n(k), \mathbb{Z}/q\mathbb{Z}) \to H_i(G_{n+1}(k), \mathbb{Z}/q\mathbb{Z})$$

is an isomorphism for certain specified values of i (when $G_n = \mathrm{GL}_n$, SL_n or U_n, $i \leq 2n$ implies isomorphism).

Theorem 3.2 (Cline–Parshall–Scott–van der Kallen, 1977 [5]). *Let G be a semisimple algebraic group defined and split over $\mathbb{F}_p$, $p>0$. Let $q = p^m$, $G(q)$ the $\mathbb{F}_q$-rational points of G, V an irreducible G-module and $V(e)$ the module obtained from V by twisting with the* eth *power of the Frobenius $x \to x^q$. Then, for $q \gg 0$ and $e \gg 0$,*

$$H^n(G, V) \cong H^n(G(q), V(e)) \cong H^n(G(q), V).$$

See also a result of Friedlander–Parshall [16].

Theorem 3.1 is the only general result I know of which suggests that the phenomenon of cohomology stabilizing as the rank increases is general. Here is a sample of evidence.

$$\dim H^1(\mathrm{SL}(n,q),\mathbb{F}_q^n)=\begin{cases}1, & (n,q)=(2,2^n),\ n\geq 2,\ (3,2);\\ 0, & \text{otherwise}.\end{cases}$$

$$\dim H^2(\mathrm{SL}(n,q),\mathbb{F}_q^n)=\begin{cases}1, & (n,q)=(3,2),(4,2),(5,2),(3,3^n),\ n\geq 2,\ (3,5);\\ 0, & \text{otherwise}.\end{cases}$$

Cf. [25], [4], [12]; see Proposition 6.2.

A third sort of stability may be observed from this example (and others), that of stability as the characteristic increases. I do not know of any theoretical result expressing the general nature of such a phenomenon.

Examples of exceptional behavior (in the above senses) may be found in sporadic groups. If E_n denotes the nonsplit extension of $\mathrm{GL}(n,2)$ by $\mathbb{F}_2^n$, $n=3,4,5$, we find that E_3 is a maximal 2-local in $G_2(K)$, for any field K of characteristic not 2, E_4 is a maximal 2-local in .3 and E_5 (the Dempwolff extension) is a maximal 2-local in F_5. See Section 6 for more on E_3.

Certain nonsplit extensions $(2_\varepsilon^{1+2n})\Omega^\varepsilon(2n,2)$ of extraspecial 2-groups by the natural subgroup of index 2 in the outer automorphism group occur as centralizers of involutions in certain simple groups for $n\leq 4$. The list is the following.

$(n,\varepsilon)=(1,+)$:	A_6,
$(1,-)$:	none,
$(2,+)$:	PSU(4, 3),
$(2,-)$:	J_2, J_3,
$(3,+)$:	none,
$(3,-)$:	Suz,
$(4,+)$:	.1,
$(4,-)$:	none.

These extensions E are nonsplit over $\mathrm{O}_2(E)$ modulo the center if and only if $n\geq 4$ or $(n,\varepsilon)=(3,-)$. In general, more than one type of nonsplit extension exists. See an appendix of my Montreal article [24] for a discussion of these extensions.

See [23, Section 13], for a different discussion of exceptional cohomology and finite simple groups.

4. The loop $\mathbb{O}_{16}$ and nonsplit $2^3\mathrm{GL}(3,2)$

If L is the code loop afforded by the code L, a *base* of L means a set of elements $x_1,\ldots,x_n$ whose images $\overline{x_1},\ldots,\overline{x_n}$ in $\bar{L}$ form a basis for $\bar{L}$. When this happens, $x_1,\ldots,x_n$ form a set of generators for L if and only if L is not an elementary abelian 2-group. In this section, we write (± 1) instead of $\mathbb{F}_2$ for the kernel of $L \to \bar{L}$.

An important code loop is a subloop of the nonzero Cayley numbers. It is based on the unique binary Hamming code H with parameters $[7,4,3]$. One representation is the span of $\{(1111000),(1100110),(1010101)\}$ in $\mathbb{F}_2^7$. We call this loop $\mathbb{O}_{16}$ and observe that $\bar{\mathbb{O}}_{16} = \mathbb{O}_{16}/Z(\mathbb{O}_{16}) \cong H$ and if $x, y, z \in \mathbb{O}_{16}$, then:

(S) $$x^2 = \begin{cases} -1, & \bar{x} \neq 0, \\ 1, & \bar{x} = 0. \end{cases}$$

(C) $$[x,y] = \begin{cases} -1, & \text{if } \bar{x}, \bar{y} \text{ independent}, \\ 1, & \text{if } \bar{x}, \bar{y} \text{ dependent}. \end{cases}$$

(A) $$[x,y,z] = \begin{cases} -1, & \text{if } \bar{x}, \bar{y}, \bar{z} \text{ independent}, \\ 1, & \text{if } \bar{x}, \bar{y} \text{ dependent}. \end{cases}$$

Note that $\mathbb{O}_{16}$ contains the quaternion group Q_8 as any subloop of index 2.

I remark that $\mathbb{O}_{16}$ forms a double basis for the Cayley numbers. Form the algebra $\mathbb{R}[\mathbb{O}_{16}]$ with basis $\mathbb{O}_{16}$ and let $\langle z \rangle = Z(\mathbb{O}_{16})$. Define $C = \mathbb{R}[\mathbb{O}_{16}]/(z+1)$. Then $\dim C = 8$, C has an involution $*$ fixing 1 and -1 based on $x \to zx \equiv -x$ if $x \in \mathbb{O}_{16} - \langle z \rangle$. Then $(ab)^* = b^* a^*$, $cc^* > 0$ if $c \neq 0$ and $cc^* \in \mathbb{R}$, for all a, b, c. Thus, C is a normed real division algebra, and is in fact the Cayley numbers [10].

A pleasant way to write $\mathbb{O}_{16}$ is the following. The elements are ± 1 and $\pm x$, where x ranges over the days of the week. Define Monday · Tuesday = Thursday and require the multiplication to be preserved by the natural 7-cycle on the days of the week. The rest of the multiplication table follows from centrality of ± 1 and the rules (S), (C) and (A); it is given in Table 1 below.

I thank George Glauberman for explaining this to me and pointing out the reference [10].

Call an automorphism α of a code loop L *diagonal* if it is trivial on $\bar{L}$. This means that α may be identified with $\beta \in \mathrm{Hom}(\bar{L}, \mathbb{F}_2)$ by $(c,x)^\alpha = (c + \beta(x), x)$. The group of

Table 1. Multiplication in $\mathbb{O}_{16}$

Let $1, \ldots, 8$ represent 1, Monday, Tuesday, ..., Sunday. Thus, $\mathbb{O}_{16} = \{\pm 1, \pm 2, \ldots, \pm 8\}$. The (i,j)-entry below represents the product of i and j. For example, Tuesday · Monday = − Thursday and Saturday · Tuesday = − Friday.

1	2	3	4	5	6	7	8
2	−1	5	8	−3	7	−6	−4
3	−5	−1	6	2	−4	8	−7
4	−8	−6	−1	7	3	−5	2
5	3	−2	−7	−1	8	4	−6
6	−7	4	−3	−8	−1	2	5
7	6	−8	5	−4	−2	−1	3
8	4	7	−2	6	−5	−3	−1

diagonal automorphism is denoted Diag(L) or Inn(L) and is a normal subgroup of Aut(L).

Lemma 4.1. (i) *Let* x_1, x_2, x_3 *be a base of* $\mathbb{O}_{16}$. *Every element of* $\mathbb{O}_{16}$ *has a unique expression* $\pm x_1^{e_1} x_2^{e_2} x_3^{e_3}$, *where* $e_i \in \{0, 1\}$, $i = 1, 2, 3$.

(ii) *If* x_1, x_2, x_3 *and* y_1, y_2, y_3 *are bases of* $\mathbb{O}_{16}$, *then* $\pm x_1^{e_1} x_2^{e_2} x_3^{e_3} \to \pm y_1^{e_1} y_2^{e_2} y_3^{e_3}$, *for* $e_i \in \{0, 1\}$, $i = 1, 2, 3$, *is an automorphism of* $\mathbb{O}_{16}$.

(iii) *If* $\alpha \in \mathrm{Aut}(\mathbb{O}_{16})$ *and* $|\alpha| = 2$, *there exists a base* x_1, x_2, x_3 *of* $\mathbb{O}_{16}$ *such that*

(a) $\alpha : x_1 \to -x_1$, $x_2 \to x_2$, $x_3 \to x_3$ *if* α *is diagonal*;

(b) $\alpha : x_1 \to x_2$, $x_3 \to x_3$ *if* α *is not diagonal.*

Proof. (i) is obvious. As for (ii), one only needs (i) and to observe that (S), (C), (A) and centrality of $\{\pm 1\}$ form a set of defining relations for $\mathbb{O}_{16}$. In (iii), if α is non-trivial on $\overline{\mathbb{O}_{16}} := \mathbb{O}_{16}/Z(\mathbb{O}_{16})$, there is a basis $\bar{x}_1, \bar{x}_2, \bar{x}_3$ of $\overline{\mathbb{O}_{16}}$ with $\alpha : \bar{x}_1 \leftrightarrow \bar{x}_2$, $\bar{x}_3 \leftrightarrow \bar{x}_3$. Lift $\bar{x}_1$ to $x_1 \in \mathbb{O}_{16}$ and define $x_2 = x_1^{\alpha}$. If a lift $x_3 \in \mathbb{O}_{16}$ of $\bar{x}_3$ satisfies $x_3^{\alpha} \neq x_3$, $x_3^{\alpha} = -x_3$. Note that $(x_1 x_2)^{\alpha} = x_2 x_1 = -x_1 x_2$. So, we replace x_3 by $x_1 x_2 x_3$ to get (iii).

Theorem 4.2. $\mathrm{Aut}(\mathbb{O}_{16})$ *is a non-split extension* $2^3 \cdot L_3(2)$.

Proof. Let $Z = Z(\mathbb{O}_{16}) \cong \mathbb{Z}_2$, $A = \mathrm{Aut}(\mathbb{O}_{16})$ and K the kernel of the natural map $A \to \mathrm{Aut}(\mathbb{O}_{16}/Z)$. Then $K \cong \mathrm{Hom}(\mathbb{O}_{16}/Z, Z) \cong \mathbb{Z}_2^3$.

From Lemma 4.1, $A/K \cong L_3(2)$. Lemma 4.1 implies that every involution of $A - K$ is conjugate in A. However, a split extension $X = 2^3 \cdot L_3(2)$ has two classes of involutions outside $O_2(X)$ since the Jordan canonical form of such an involution, t, in its action on $O_2(X)$, is

$$\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix},$$

whence $H^1(\langle t \rangle, O_2(X)) \cong \mathbb{Z}_2$.

A variation on the loop $\mathbb{O}_{16}$ is $\mathscr{L} = \mathbb{O}_{16} \times \mathbb{Z}_2$, which is a code loop afforded by the code $\tilde{H} \subseteq \mathbb{F}_2^8$ spanned by our binary Hamming code $H \subseteq \mathbb{F}_2^7 \subseteq \mathbb{F}_2^8$ and (1 1 1 1 1 1 1 1).

Lemma 4.2. (i) $Z(\mathscr{L}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(ii) $A = \mathrm{Aut}(\mathscr{L})$ *contains* $\mathrm{Aut}\,\mathbb{O}_{16}$ *and has structure* $O_2(A) \cong (\mathbb{Z}_2^3)^2 \times \mathbb{Z}_2$, $A \geq (\mathrm{Aut}\,\mathbb{O}_{16}) \times Z_2$ *and* $A^{\circ} = \{a \in A \mid a \text{ is trivial on } Z(\mathscr{L})\} \geq \mathrm{Aut}(\mathbb{O}_{16})$ *and* $O_2(A^{\circ})$ *is a direct sum of two modules, each isomorphic to* $O_2(\mathrm{Aut}\,\mathbb{O}_{16})$.

(iii) A *does not contain a copy of* GL(3, 2).

5. Nonvanishing degree 2 cohomology

I have been interested in ways to find nonsplit extesions, both because of my general interest in group extension theory and my wish to understand subgroups of finite simple groups. The code loop situation provides new applications. Just for fun, I will review my criteria.

(I) ('The permutation trick', 1970 [19]). Let G be a subgroup of Σ_n and suppose that G has an involution t which moves 4 (mod 8) letters and lies in every subgroup of index 2 in G. Then, the preimage $\hat{G}$ of G in a covering group of Σ_n is nonsplit; in fact, if $Z=\mathrm{Ker}(\hat{G}\to G)$, $Z\leq \hat{G}'\cong Z(\hat{G})$, so that G has Schur multiplier of even order.

In fact, one has a similar result by replacing Σ_n by $\mathrm{O}(n,\mathbb{R})$ and the hypothesis on letters moved by the requirement that t have 4 (mod 8) eigenvalues -1. R. Steinberg explained this to me; it is implicit in Schur [32]. See the paper of Garrison and Gagola [17] for an interesting discussion of these ideas and related ones.

(II) ('The extraspecial trick', 1973 [20]). Let $G\leq \mathrm{O}^{\varepsilon}(2n,2)$, an orthogonal group on $V\cong \mathbb{F}_2^{2n}$. Suppose that there are $t\in G$, $|t|=2$ and a 2-dimensional subspace W such that

(a) t fixes $w\in W$, $w\neq 0$ nonsingular;

(b) W is nonsingular and t interchanges the two vectors in $W-\langle w\rangle$;

(c) if $H=\{g\in G \mid g \text{ fixes } w\}$, then t lies in every subgroup of index 2 in H.

Then $H^2(G,V)$ is nonzero. In fact, the natural extension of G on V given by $\mathrm{Aut}(2_{\varepsilon}^{1+2n})$ is nonsplit.

(III) ('The Chevalley group trick', 1979 [18]). Suppose that $p\geq 5$, that $p\mid |G|$, where $G\leq G(K)$, where K is a field of characteristic p and G is a Chevalley group functor. Let M be the adjoint module for $G(K)$. Then $H^2(G,M)\neq 0$.

To prove this, we may assume $|G|=p$ and $G(K)$ is untwisted. Then consider the extension of $G(K)$ by M obtained by constructing $G(R)$ where R is a local ring with $J=\mathrm{rad}(R)$, $J^2=0\neq J$, $R/J\cong K$ and $J=pR$. The result follows by an easy induction argument. The analogous statements for $p=2$ and 3 are false for $A_2(2)$ and $A_1(3)$, respectively.

The smallest case (III) applies to give $H^2(G,M_3)\neq 0$ where $G=A_1(5)$ is the simple group of order 60 and where we write M_k for an irreducible module of dimension $k=1,3$ and 5; these are all the $\mathbb{F}_5G$-irreducibles. Since M_5 is the Steinberg module and the Schur multiplier of G has order prime to 5, $H^2(G,M_k)=0$ for $k\neq 3$. On the other hand, Shapiro's lemma implies that if the prime q divides the order of the finite group H, there exists an irreducible N in characteristic q such that $H^2(H,N)\neq 0$. For $H=G$ and $q=5$, we have found that $N=M_3$.

(IV) Let G be a subgroup of $\mathrm{Aut}(V)$ where V is a doubly even binary code. Assume the existence of t and W as in (II) and replace 'nonsingular' by 'odd code word'. Then $H^2(G,V)\neq 0$. In fact the extension of G given by $\mathrm{Aut}(\hat{V})$, where $\hat{V}$ is the code loop afforded by V, is nonsplit.

The proof of (II) with little change carries over to a proof of (IV). This criterion gives a different proof of Theorem 4.2 and, with the following argument, it proves that $\mathrm{Aut}(\mathscr{G}) \cong 2^{12}M_{24}$ and $C_{\mathrm{Aut}(\mathscr{G})}(Z(\mathscr{G})) \cong 2^{11}M_{24}$ are nonsplit; here $\mathscr{G}$ is the Golay code. An 'odd vector' in $\mathscr{G}$ is a dodecad and a doecad stabilizer in $\mathrm{Aut}(\mathscr{G}) \cong M_{24}$ is the simple group M_{12}. Let D be a dodecad and write $D = \mathscr{O}_1 + \mathscr{O}_2$, $\mathscr{O}_i$ octads, $i = 1, 2$. Let $T = \mathscr{O}_1 \cap \mathscr{O}_2$, a 2-set and $S_i = \mathscr{O}_i - T$, six-sets, $i = 1, 2$. In M_{24}, $\mathrm{Stab}(D) \cong M_{12}$, $\mathrm{Stab}(D) \cap \mathrm{Stab}(T) \cong \Sigma_6 \cdot 2$ and $\mathrm{Stab}(S_1) \cap \mathrm{Stab}(S_2) \cap \mathrm{Stab}(T) \cong \Sigma_6$. Letting $W = \{\phi, \mathscr{O}_1, \mathscr{O}_2, D\}$ and t an involution in $\mathrm{Stab}(T) \cap \mathrm{Stab}(D) - \mathrm{Stab}(S_1)$, we may apply (IV).

6. A theorem of Alperin

In the late 1960's and early 1970's, work on simple groups of low 2-rank was of great importance in the classification of finite simple groups. Extensions of GL(3, 2) by faithful modules $\mathbb{Z}_{2^n}^3$ were of special interest here since 2-locals in several finite simple groups are of this shape. A basic result about such extension was announced by Alperin [1], but he did not publish details. We do so here. Note that O'Nan requires them in his paper [28] on the simple group of order $2^9 3^4 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$. Some results in this section may be covered in the recent work [38].

Lemma 6.1. *Let G be a group, V a G-module and $f: G \to V$ a 1-cocycle, i.e., a function which satisfies $f(xy) = f(x)^y + f(y)$. Then*

(i) $f(1) = 0$,

(ii) $f(x^{-1}) = -f(x)^{x^{-1}}$,

(iii) $f(x^n) = \sum_{k=0}^{n-1} f(x)^{x^k} = f(x)^{E(n)}$, *where $n > 0$ and $E(n) = \sum_{k=0}^{n-1} x^k$.*

Proof. Trivial.

Proposition 6.2. $H^k(\mathrm{GL}(3,2), \mathbb{F}_2^3) \cong \mathbb{F}_2$, $k = 1, 2$.

Proof. This is a well-known result. Probably the easiest way to do this from scratch is to write out the projective indecomposables for $\mathbb{F}_2\mathrm{GL}(3,2)$ and the beginning of a projective resolution of $\mathbb{F}_2$, then compute cohomology with it. For a description of these projectives, see [3, p. 216].

Lemma 6.3. *Let $U \neq V$ be a unipotent subgroups of* PSL(2, *q*).

(a) *The set of elements of UV which are unipotent is $U \cup V$.*

(b) *Suppose $u_1, u_2, u_3, u_4 \in U$, $v_1, v_2 \in V$ and $u_1 v_1 u_2 = u_3 v_2 u_4$. Then $v_1 = v_2$ and, if $v_1 \neq 1$, $u_1 = u_3$ and $u_2 = u_4$.*

Proof. (a) Without loss we may take

$$U = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \middle| t \in \mathbb{F}_q \right\} \quad \text{and} \quad V = \left\{ \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \middle| t \in \mathbb{F}_q \right\}.$$

Then

$$\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ u & 1\end{pmatrix}=\begin{pmatrix}1+tu & t\\ u & 1\end{pmatrix}$$

is unipotent only if its trace is 2, i.e., $tu=0$.

(b) The equation implies that

$$u_3^{-1}u_1v_1=v_2u_4u_2^{-1} \quad\text{and}\quad u_2u_4^{-1}u_3^{-1}u_1v_1=(u_4u_2^{-1})^{-1}v_2(u_4u_2^{-1}).$$

Since the right side is unipotent, (a) implies that $v_1=1$ or $u_2u_4^{-1}u_3^{-1}u_1=1$. If $v_1=1$, $v_2\in U\cap V=1$. If $v_1\neq 1$, $v_1\in V\cap V^{u_4u_2^{-1}}$ implies that $u_4u_2^{-1}\in N_U(V)=1$ or $u_2=u_4$. At once, $v_1=v_2$ and $u_1=u_3$ follow.

Proposition 6.4. *Let R be the 2-adic integers, I an ideal of R, $G\cong L_3(2)$ and let M be a 3-dimensional irreducible $\mathbb{F}_2G$-module.*

(i) *There is a unique module U for $\bar{R}G$, free over $\bar{R}=R/I$, of rank 3, whose reduction modulo $2R$ is isomorphic to M.*

(ii) *If V is a four group in G, the (complex) character of V on U (for $I=0$) is $\varrho-1$, where ϱ is the character of the regular representation.*

(iii) *If S is a Σ_3 subgroup of G, S/S' inverts $C_U(S')\cong R$.*

(iv) *On $U/2^nU$, the fixed point set of V is isomorphic to $\mathbb{Z}_2$ or $\mathbb{Z}_2\times\mathbb{Z}_2$.*

Proof. (i) For $I=0$, this is part of the well known general theory of correspondence between representations of RG and $(R/2)G$. See [13, 14] for instance. For $I\neq 0$, we argue by induction on n, where $I=2^nR$. Without loss, $n>1$. Write $\bar{R}=R/2^nR$, $\bar{\bar{R}}=R/2^{n-1}R$. Let $\bar{U}$ be the unique $\bar{\bar{R}}G$-module which lifts M. Let $\phi: G\to \mathrm{GL}(\bar{U})$ be the associated representation. Choose a free $\bar{R}$-module $\bar{V}$ such that $V/2^nV\cong\bar{U}$ as $\bar{R}$-modules, and let G_1 be the inverse image of G^{ϕ} in $\mathrm{GL}(\bar{U})$. The kernel K of $\pi: G_1\to G^{\phi}$ is abelian and is isomorphic to $\mathrm{Hom}(M,M)$ as an $\mathbb{F}_2G$-module. This module is isomorphic to $\mathbb{F}_2\oplus S$, where S is the Steinberg module. Thus, π is a split epimorphism, and the splitting is unique up to conjugacy. The induction is now complete.

(ii) This follows from (i) and the complex character table of G.

(iii) Let $\langle h\rangle=S'$, $t\in S-S'$, $I=0$. Then $[U,h]$ is a free $R\langle t\rangle$-module of rank 2 over R. So, t has eigenvalues 1 and -1 on $[U,h]$. Now use (ii) and the t-stable decomposition $U=[U,h]\times C_U(h)$.

(iv) In G there are two conjugacy classes of four-groups, represented by V_1, V_2, say, where $C_M(V_1)\cong Z_2$ and $C_M(V_2)\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Let $\bar{U}=U/2^nU$. If the statement is false for V_i, $C_{\bar{U}}(V_i)\cong\mathbb{Z}_{2^r}$ for some $r>2$, if $i=1$ and $C_{\bar{U}}(V_i)\cong\mathbb{Z}_2\times\mathbb{Z}_{2^r}$ for some $r\geq 2$ if $i=2$. Without loss, $n=r$. Define $\langle u_0\rangle=C_{\bar{U}}(V_i)\cap C_{\bar{U}}(h)$, where $h\in N_G(V_i)$, $|h|=3$. Then $|u_0|=2^n$. Say $i=1$. Let $x\in V_1^{\#}$. There is $u\in 2U$ such that x inverts uu_0. Without loss, x inverts $\langle k\rangle\cong\mathbb{Z}_3$ and $u\in[2U,k]$; see (iii). Thus $(uu_0)^{-1}(uu_0)^x=u^xu$ forces $u^{-1}=u^x$ and $u_0^{-1}=u_0^x$, a contradiction to $n=r\geq 2$. Say $i=2$. Then, taking h as above, we see that $h=r\geq 2$ implies that h acts trivially on $C_{\bar{U}}(V_i)$, a contradiction.

Theorem 6.5. (a) *Let* $G=\mathrm{GL}(3,2)$ *and let* V_n *be the G-module of Proposition* 6.4(i) (*so that* $V_n \cong \mathbb{Z}_{2^n}^3$ *as abelian groups*). *Then* $H^k(G, V_n) \cong \mathbb{Z}_2$, $k=1,2$ *and all* $n \geq 1$.
Furthermore

(b) *the natural epimorphism of G-modules* $V_n \to V_{n-1}$ *induces the* 0-*map* $H^1(G, V_n) \to H^1(G, V_{n-1})$ *and an isomorphism* $H^2(G, V_n) \to H^2(G, V_{n-1})$;

(c) *the natural inclusion* $V_{n-1} \to V_n$ *of G-modules induces an isomorphism* $H^1(G, V_{n-1}) \to H^1(G, V_n)$ *and the* 0-*map* $H^2(G, V_{n-1}) \to H^2(G, V_n)$.

(d) *Let* A_n, B_n *represent the split and nonsplit extensions of G by* V_n, *for all* $n \geq 1$. *There are natural inclusions* $i_n : A_n \to A_{n+1}$ *extending the natural inclusions* $V_n \to V_{n+1}$ *and natural epimorphisms* $q_n : A_n \to A_{n-1}$ *extending* $V_n \to V_{n-1}$. *Furthermore, there exist embeddings* $j_n : B_n \to A_{n+1}$ *which extend* $i_n|_{V_n}$. *They satisfy* $\mathrm{Im}(i_n)\mathrm{Im}(j_n) = A_{n+1}$ *and* $B_{n-1}q_n \cong B_{n-2}$, *for* $n \geq 3$. *If* $m \neq n$, *there is no inclusion of* B_m *in* B_n. *For* $m<n$, *there is an embedding* $B_m \to A_n$.

Proof of (a), the case $k=1$. We use induction on n. For $n=1$, use Proposition 6.2. We henceforth assume that $n>1$. We have a natural epimorphism $p: V_n \to V_{n-1}$ of modules and we get $H^1 V_n \xrightarrow{p_*} H^1 V_{n-1}$.

We argue that $p_*=0$. Let B be a subgroup of order 21 in G. Let f be a 1-cocycle, $f: G \to V_n$. We may assume that $f|_B \equiv 0$ since $(|B|, |V_n|)=1$. Since $f(xy)=f(x)^y+f(y)$, f is constant on right cosets of B. Take $g \in G-B$, $|g|=7$, and set $v=f(g)$. For $n \geq 1$ define $E(n)=\sum_{k=0}^{n-1} g^k$. Lemma 6.1(iii) implies that $f(g^n)=v^{E(n)}$. If $v=0$, $f=0$ since $G=\langle B, g\rangle$.

Assume $|v|=2^r$, $r \geq 2$. We shall derive a contradiction, proving that if $v \neq 0$, $|v|=2$. Then $p_*=0$ follows.

So, we assume $r \leq 2$. Define $S:=\{v^{E(k)} \mid k=1,\dots,7\}$; then $\mathrm{Im}(f)=S \cup \{0\}$. We shall prove several properties of S.

We claim that $SB=S$. This is clear from the equation $f(xb)=f(x)^b+f(b)=f(x)^b$. Let $\langle u\rangle$ be a Sylow 7-group of B. Then $\langle u\rangle$ is transitive on S since $|S|=7$ and u fixes no nonzero vector of V_n. Thus, the stabilizer in B of an element of S has order 3.

Take an integer $m \in \{1,\dots,6\}$. Lemma 6.1(ii) implies that $f(g^{-m})=-f(g^m)^{g^{-m}}$. There are unique integers $p, q \in \{0,\dots,6\}$ so that $f(g^{-m})=v^{u^p}$ and $f(g^m)=v^{u^q}$ whence $v^{u^p g^m u^{-q}}=-v$. Set $x_m=u^p g^m u^{-q}$. Then $x_{m_1}=x_{m_2}$ implies $m_1=m_2$ by Lemma 6.3(b). Thus we have produced six distinct elements in $H:=\{y \in G \mid \langle v\rangle^y=\langle v\rangle\}$. By considering $V_n/\Omega_{r-1}(V_n)$, we see that H is contained in a Σ_4 subgroup of G and since $3 \mid |H|$ and we have six distinct elements which invert $\langle v\rangle$, we get $H \cong \Sigma_4$. Since H' is generated by elements of order 3 and $\mathrm{Aut}\langle v\rangle$ is a 2-group, $v^H=\{\pm v\}$, $\pm S=v^G$ and $H' \leq C(v)$. This contradicts Proposition 6.4(ii).

Since $p_*=0$, the long exact cohomology sequence applies to $0 \to V_1 \to V_n \to V_{n-1} \to 0$ gives $0 \to H^1 V_1 \to H^1 V_n \xrightarrow{p_*=0} H^1 V_{n-1}$, or $H^1 V_n \cong H^1 V_1 \cong \mathbb{Z}_2$, proving (a) for $k=1$.

Proof of (a), the case $k=2$. We may assume $n \geq 2$, by Proposition 6.2. The long exact sequence for $0 \to V_1 \xrightarrow{i} V_n \xrightarrow{p} V_{n-1} \to 0$ gives

$$0 \to H^1 V_1 \xrightarrow{i^1} H^1 V_n \xrightarrow{p^1} H^1 V_{n-1} \xrightarrow{\delta^1} H^2 V_1 \xrightarrow{i^2} H^2 V_n \xrightarrow{p^2} H^2 V_{n-1}.$$

From the above, $p^1 = 0$ and by Proposition 6.2, δ^1 is an isomorphism $\mathbb{Z}_2 \to \mathbb{Z}_2$. Therefore, $i^2 = 0$. By induction, $H^2 V_n \neq 0$.

Using (a) for $k=1$ and $0 \to V_1 \to V_{n+1} \to V_n \to 0$, we get

$$\mathbb{Z}_2 \cong H^1 V_{n+1} \xrightarrow{p^1 = 0} H^1 V_n = \mathbb{Z}_2.$$

Let L_1 and L_2 be nonconjugate complements to V_{n+1} in a split extension $V_{n+1} \rtimes L_1$. Since $p^1 = 0$, their images in $V_n \times L_1$ under the natural map become conjugate. On the other hand, $V_n \times L_1$ does have complements not conjugate to L_1. Consider one and then its preimage J in $V_{n+1} \times L_1$. Then $J \cap V_{n+1} = 2V_{n+1}$ and J does not split over $2V_{n+1}$ since $H^1(2V_{n+1}) \cong H^1 V_n \cong \mathbb{Z}_2$ and we have already accounted for the complements. Therefore, we have $H^2 V_n \neq 0$, proving (a) for $k=2$.

Statements (b) and (c) follow from points made in the proof of (a).

To prove (d), let $n \geq 1$ and define B_n as follows. Since the natural map $H'(G, V_{n+1}) \to H'(G, V_1)$ is 0, there is a complement C to V_1 in A_1 not conjugate to the image of A_{n+1} in V_1 under $q = q_{n+1} q_n \cdots q_2$. Define $B_n = C^{q^{-1}}$. The rest is an exercise.

It is well known that the two types of extension of $\mathbb{Z}_4^3$ by GL(3, 2) (nontrivial action) occur as maximal 2-locals in sporadic groups. The split one occurs in the Higman–Sims group and the nonsplit one occurs in the O'Nan group. It seems worthwhile to display this nonsplit extension as an explicit matrix group, in fact as a subgroup of GL(3, $\mathbb{Z}/8\mathbb{Z}$), and record some properties.

Proposition 6.6. *Let* $G = \mathrm{GL}(3,2)$.

(a) *The matrices*

$$x = \begin{pmatrix} 2 & 5 & 3 \\ 5 & 3 & 2 \\ 1 & 0 & 0 \end{pmatrix}, \qquad t = \begin{pmatrix} 7 & 4 & 4 \\ 4 & 4 & 7 \\ 4 & 7 & 4 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

in GL(3, $\mathbb{Z}/8\mathbb{Z}$) *have orders* 7, 2 *and* 3, *respectively.*

(b) $\langle t, y\rangle \cong \Sigma_3$ *and* $\langle x, y\rangle$ *is nonabelian of order* 21.

(c) x, y *and* t *satisfy* $x^7 = y^3 = y^{-1}xyx^{-2} = t^2 = 1 = (yt)^2 = (xt)^3$.

(d) $\langle x, y, t\rangle = \langle x, t\rangle \cong G$ *via the natural map* GL(3, $\mathbb{Z}/8\mathbb{Z}$) $\to$ GL(3, 2) *'reduction modulo* 2'.

(e) *Up to conjugacy in* GL(3, $\mathbb{Z}/2^n\mathbb{Z}$), *for any* $n \geq 1$, *there is a unique subgroup isomorphic to* G.

(f) *Define*

$$s = x^5 y t x = \begin{pmatrix} 0 & 0 & 7 \\ 3 & 0 & 4 \\ 5 & 5 & 1 \end{pmatrix} \in G.$$

Then $P_1 = \langle s^2, t\rangle$ and $P_2 = \langle s^2, st\rangle$ are four-groups.

Proof. It is straightforward to check (a), (b) and (c). From [9, p. 216], we get that (c) implies (d).

Define $G_n := \mathrm{GL}(3, \mathbb{Z}/2^n\mathbb{Z})$ and let $\phi_{m,n}$ be the natural map $G_m \to G_n$, for $m \geq n$. Set $K_{m,n} := \mathrm{Ker}\ \phi_{m,n}$. Then, as a module for G_1, $\overline{K_{m,n}} := K_{m,n}/K_{m,n+1}$ is isomorphic to the space of 3×3 matrices with G_1 acting by conjugation. This module is the direct sum of the trivial module and the Steinberg module, which is projective and injective. To get existence, we quote Proposition 6.4(i) or use induction on m. Namely, we observe that $H^2(G_1, \bar{K}_{m,n}) \cong H^2(G_1, \mathbb{F}_2) \cong \mathbb{F}_2$ but that the nontrivial extension of G_1 does not arise here. If it did, we would have a subgroup $H \cong \mathrm{SL}(2,7)$ of G_n, and, by induction, the involution $z \in Z(H)$ acts by a scalar $\alpha = 1 + 2^{n-1}$. Then $\det z = \alpha^3 = \alpha \neq 1$, whereas H is perfect. To get uniqueness up to conjugacy, we use $H'(G_1, \bar{K}_{m,n}) = 0$ for $n = 1, \ldots, m-1$.

The proof of (f) is straightforward.

Proposition 6.7. *Let $n \geq 1$ and let $G_1 = G_{1,n}$, $G_2 = G_{2,n}$ represent the two isomorphism types of extensions of* GL(3, 2) *over $V = \mathbb{Z}_{2^n}^3$, with G_1 split over V.*

(i) *$G_i/\Phi(V)$ is split if and only if $i = 1$.*

(ii) *In G_i, let T be a Sylow 3-group and let $S_n \in \mathrm{Syl}_2(N(T))$. Then $S_n \cong D_{2^{n+1}}$. In particular, $G_i - V$ contains involutions.*

(iii) *Let F be the inverse image in G_i of a $\mathbb{Z}_4$ subgroup of G_i/V. Then F splits over V if and only if $i = 1$. In the nonsplit case, if $x \in F$ maps to a generator of $F/V \cong \mathbb{Z}_4$, $x^4 \in V - \Phi(V)$. Thus, the exponent of G_1 is $4 \cdot 3 \cdot 7$ if $n = 1$ and $2^n \cdot 3 \cdot 7$ if $n \geq 2$ and the exponent of G_2 is $2^{n+2} \cdot 3 \cdot 7$ if $n \geq 1$.*

Remark. (i) contradicts a result in [2].

Proof. (i) We use the proof and notation of Theorem 6.5. Let $\phi_n : V_n \to V_{n-1}$ be the natural epiomorphism. Then $(\phi_n)_* : H^2V_n \to H^2V_{n-1}$ is an isomorphism. By taking composites, we get (i).

(ii) Set $\langle v_n\rangle = C_{V_n}(T)$. Then $|S_n : \langle v_n\rangle| = 2$. Let $s_n \in S_n - \langle v_n\rangle$. The groups $\{\langle v_n\rangle \mid n \geq 1\}$ form an inverse system. Let $c_n \in \mathbb{Z}/2^n\mathbb{Z}$ be defined by $v_n^{s_n} = c_n v_n$. Then the class of $(c_1, c_2, \ldots,)$ in the 2-adic integers is -1, so there is an integer $n_0 > 0$ such that $n_1 > n_0$ implies $c_n \equiv -1 \pmod{2^{n_1}}$.

Given our integer n, we take $n_1 > \max\{n, n_0\}$. Since $\langle v_n\rangle$, s_n is the image of $\langle v_n\rangle$, s_{n_1}, respectively, under natural maps $G_{i,n_1} \to G_{i,n}$, we get $c_n \equiv c_{n_1} \equiv -1 \pmod{2^n}$. To get (ii), all we need to do is show that S_n splits over $\langle v_n\rangle$. Let $m = \min\{n \mid S_n$ is nonsplit over $\langle v_n\rangle\}$ and assume $m < \infty$. For any k, $s_k^2 \in \Omega_1(\langle v_k\rangle)$. So, $s_{m+1}^4 = 1$ and, applying the natural map $G_{i,m+1} \to G_{i,m}$, we get $s_m^2 = 1$, a contradiction which proves (ii).

(iii) It suffices to assume $n = 1$. Let $G = G_{2,1}$ and let $0 \neq v \in V = \mathrm{O}_2(G)$, $Q = C_G(v)$. Then $|\mathrm{O}_2(Q)| = 2^5$ and $Q/\mathrm{O}_2(Q) \cong \Sigma_3$; if $h \in Q$, $|h| = 3$, $C_Q(h) = \langle v\rangle \times \langle h\rangle$. By (ii),

$G-V$ contains involutions, whence $O_2(Q/\langle v\rangle)$ is elementary abelian. Taken an involution $x\in Q-O_2(Q)$. Without loss, $h^x=h^{-1}$. Since $V/\langle v\rangle$ is an injective $\langle h,x\rangle$-module, there is a complement $W/\langle v\rangle$ to $V/\langle v\rangle$ in $O_2(Q)/\langle v\rangle$.

We claim that W is quaternion. If false, $[W,h]\langle h,x\rangle$ complements V in Q, making G split, a contradiction. Thus W is quaternion, whence $W\langle x\rangle$ is semidihedral of order 16 and so contains a unique $\mathbb{Z}_8$ subgroup, W_1. We may take F to satisfy $F/V=W_1V/V$. If F were split over V, F would contain no element of order 8, which is incompatible with $W_1\le F$.

A representation of the nonsplit Alperin extension by matrices

Denote by Alp, the unique nonsplit extension of GL(3, 2) by $\mathbb{Z}_4^3$. We give Alp as a subgroup of $GL(4,\mathbb{Z}/8\mathbb{Z})$ contained in the subgroup Q consisting of all matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ & & * & \end{pmatrix}.$$

Such a matrix has the form

$$\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline & & & \\ c & & M & \\ & & & \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline & & & \\ c & & I & \\ & & & \end{array}\right)\left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & & & \\ 0 & & M & \\ 0 & & & \end{array}\right),$$

where c is a column vector of height 3. We may denote such a matrix by $(c\,|\,M)$ or $(r\,|\,M)$ where $r={}^tc$. The rules for a product are

$$(c\,|\,M)(c'\,|\,M)=(c+Mc'\,|\,MM') \quad\text{and}\quad (r\,|\,M)(r'\,|\,M')=(r+r'\,{}^tM\,|\,MM').$$

We have $O_2(Q)=\{(r\,|\,I)\,|\,r\in\mathbb{Z}_8^3\}$ and we take $V:=\mathrm{Alp}\cap O_2(Q)=O_2(\mathrm{Alp})$ to be $\{(2r\,|\,I)\,|\,r\in\mathbb{Z}_8^3\}$. Write $[i,j,k]$ for $((i,j,k)\,|\,I)\in O_2(Q)$. Set

$$X=\begin{pmatrix} 2 & 5 & 3 \\ 5 & 3 & 2 \\ 1 & 0 & 0 \end{pmatrix},\quad Y=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\quad T=\begin{pmatrix} 7 & 4 & 4 \\ 4 & 4 & 7 \\ 4 & 7 & 4 \end{pmatrix}\in GL(3,\mathbb{Z}/8\mathbb{Z}).$$

We define $x=(0\,|\,X)$, $y=(0\,|\,Y)$ and $t=(r_0\,|\,T)$, where t is chosen to satisfy $y^t=y^{-1}$ (which requires r_0 to have the form $r_0=(k,k,k)$) and to make ytx have order 16 (which requires k to be odd); $r_0=(1,1,1)$ works.

The 168 *Alperin matrices* are listed in Table 2 in the following order: first, the 21 matrices x^iy^j for $i=0,\dots,6$ and $j=0,1,2$ in the order $(i,j)=(0,0),(0,1),\dots,(6,2)$; second, the 147 matrices $x^iy^jtx^k$ for $i,k=0,\dots,6$ and $j=0,1,2$ in the order $(i,j,k)=(0,0,0),(0,0,1),\dots,(0,1,0),(0,1,1),\dots,(6,2,6)$. The Alperin matrices are therefore a system of coset representatives for $O_2(\mathrm{Alp})$ in Alp, where Alp is a particular subgroup of $GL(4,\mathbb{Z}/8\mathbb{Z})$ isomorphic to the nonsplit extension $\mathbb{Z}_4^3\cdot GL(3,2)$. The fact that $\langle x,y,t\rangle$ is this extension follows from Theorem 6.5 (the proof of (a) for $k=2$),

Table 2. The Alperin transversal
Transversal element is below and to the right of its label (1 to 168)

1	**2**	**3**	**4**	**5**	**6**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
0 1 0 0	0 0 1 0	0 0 0 1	0 2 5 3	0 3 2 5	0 5 3 2
0 0 1 0	0 0 0 1	0 1 0 0	0 5 3 2	0 2 5 3	0 3 2 5
0 0 0 1	0 1 0 0	0 0 1 0	0 1 0 0	0 0 1 0	0 0 0 1
7	**8**	**9**	**10**	**11**	**12**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
0 0 1 0	0 0 0 1	0 1 0 0	0 5 3 2	0 2 5 3	0 3 2 5
0 3 2 5	0 5 3 2	0 2 5 3	0 5 5 5	0 5 5 5	0 5 5 5
0 2 5 3	0 3 2 5	0 5 3 2	0 0 1 0	0 0 0 1	0 1 0 0
13	**14**	**15**	**16**	**17**	**18**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
0 3 2 5	0 5 3 2	0 2 5 3	0 5 5 5	0 5 5 5	0 5 5 5
0 0 0 1	0 1 0 0	0 0 1 0	0 1 0 0	0 0 1 0	0 0 0 1
0 5 3 2	0 2 5 3	0 3 2 5	0 3 2 5	0 5 3 2	0 2 5 3
19	**20**	**21**	**22**	**23**	**24**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
0 0 0 1	0 1 0 0	0 0 1 0	1 7 4 4	1 6 7 5	1 4 3 0
0 2 5 3	0 3 2 5	0 5 3 2	1 4 4 7	1 3 0 4	1 2 7 1
0 5 5 5	0 5 5 5	0 5 5 5	1 4 7 4	1 7 1 2	1 5 6 7
25	**26**	**27**	**28**	**29**	**30**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 7 5 2	1 1 2 7	1 3 3 7	1 4 0 7	1 4 4 7	1 3 0 4
1 0 4 7	1 7 5 6	1 5 2 7	1 3 7 3	1 4 7 4	1 7 1 2
1 7 3 3	1 0 4 3	1 7 4 0	1 2 7 5	1 7 4 4	1 6 7 5
31	**32**	**33**	**34**	**35**	**36**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 2 7 1	1 0 7 4	1 7 5 6	1 5 2 7	1 3 7 3	1 4 7 4
1 5 6 7	1 7 3 3	1 0 4 3	1 7 4 0	1 2 7 5	1 7 4 4
1 4 3 0	1 7 5 2	1 1 2 7	1 3 3 7	1 4 0 7	1 4 4 7
37	**38**	**39**	**40**	**41**	**42**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 7 1 2	1 5 6 7	1 7 3 3	1 0 4 3	1 7 4 0	1 2 7 5
1 6 7 5	1 4 3 0	1 7 5 2	1 1 2 7	1 3 3 7	1 4 0 7
1 3 0 4	1 2 7 1	1 0 7 4	1 7 5 6	1 5 2 7	1 3 7 3
43	**44**	**45**	**46**	**47**	**48**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 6 1 7	2 0 1 4	2 1 3 2	2 3 6 1	2 5 1 5	2 4 4 1
2 7 6 1	2 5 5 1	2 4 0 1	2 1 4 4	2 2 1 3	2 4 5 0
1 7 4 4	1 6 7 5	1 4 3 0	1 7 5 2	1 1 2 7	1 3 3 7

49	**50**	**51**	**52**	**53**	**54**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 5 0 4	2 1 7 6	2 3 2 1	2 1 5 5	2 0 4 5	2 1 4 0
2 1 3 6	2 6 1 7	2 0 1 4	2 1 3 2	2 3 6 1	2 5 1 5
1 4 0 7	1 4 4 7	1 3 0 4	1 2 7 1	1 0 7 4	1 7 5 6

55	**56**	**57**	**58**	**59**	**60**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 6 1 3	2 4 1 4	2 7 6 1	2 5 5 1	2 4 0 1	2 1 4 4
2 4 4 1	2 5 0 4	2 1 7 6	2 3 2 1	2 1 5 5	2 0 4 5
1 5 2 7	1 3 7 3	1 4 7 4	1 7 1 2	1 5 6 7	1 7 3 3

61	**62**	**63**	**64**	**65**	**66**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 2 1 3	2 4 5 0	2 1 3 6	1 4 4 7	1 3 0 4	1 2 7 1
2 1 4 0	2 6 1 3	2 4 1 4	2 1 7 6	2 3 2 1	2 1 5 5
1 0 4 3	1 7 4 0	1 2 7 5	2 6 1 7	2 0 1 4	2 1 3 2

67	**68**	**69**	**70**	**71**	**72**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 0 7 4	1 7 5 6	1 5 2 7	1 3 7 3	1 4 7 4	1 7 1 2
2 0 4 5	2 1 4 0	2 6 1 3	2 4 1 4	2 7 6 1	2 5 5 1
2 3 6 1	2 5 1 5	2 4 4 1	2 5 0 4	2 1 7 6	2 3 2 1

73	**74**	**75**	**76**	**77**	**78**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 5 6 7	1 7 3 3	1 0 4 3	1 7 4 0	1 2 7 5	1 7 4 4
2 4 0 1	2 1 4 4	2 2 1 3	2 4 5 0	2 1 3 6	2 6 1 7
2 1 5 5	2 0 4 5	2 1 4 0	2 6 1 3	2 4 1 4	2 7 6 1

79	**80**	**81**	**82**	**83**	**84**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 6 7 5	1 4 3 0	1 7 5 2	1 1 2 7	1 3 3 7	1 4 0 7
2 0 1 4	2 1 3 2	2 3 6 1	2 5 1 5	2 4 4 1	2 5 0 4
2 5 5 1	2 4 0 1	2 1 4 4	2 2 1 3	2 4 5 0	2 1 3 6

85	**86**	**87**	**88**	**89**	**90**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 7 6 1	2 5 5 1	2 4 0 1	2 1 4 4	2 2 1 3	2 4 5 0
7 3 3 3	7 0 0 7	7 7 0 0	7 6 3 5	7 0 7 0	7 3 5 6
1 4 4 7	1 3 0 4	1 2 7 1	1 0 7 4	1 7 5 6	1 5 2 7

91	**92**	**93**	**94**	**95**	**96**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
2 1 3 6	2 6 1 7	2 0 1 4	2 1 3 2	2 3 6 1	2 5 1 5
7 5 6 3	7 3 3 3	7 0 0 7	7 7 0 0	7 6 3 5	7 0 7 0
1 3 7 3	1 4 7 4	1 7 1 2	1 5 6 7	1 7 3 3	1 0 4 3

97

1	0	0	0
2	4	4	1
7	3	5	6
1	7	4	0

98

1	0	0	0
2	5	0	4
7	5	6	3
1	2	7	5

99

1	0	0	0
2	1	7	6
7	3	3	3
1	7	4	4

100

1	0	0	0
2	3	2	1
7	0	0	7
1	6	7	5

101

1	0	0	0
2	1	5	5
7	7	0	0
1	4	3	0

102

1	0	0	0
2	0	4	5
7	6	3	5
1	7	5	2

103

1	0	0	0
2	1	4	0
7	0	7	0
1	1	2	7

104

1	0	0	0
2	6	1	3
7	3	5	6
1	3	3	7

105

1	0	0	0
2	4	1	4
7	5	6	3
1	4	0	7

106

1	0	0	0
2	1	7	6
1	4	7	4
2	7	6	1

107

1	0	0	0
2	3	2	1
1	7	1	2
2	5	5	1

108

1	0	0	0
2	1	5	5
1	5	6	7
2	4	0	1

109

1	0	0	0
2	0	4	5
1	7	3	3
2	1	4	4

110

1	0	0	0
2	1	4	0
1	0	4	3
2	2	1	3

111

1	0	0	0
2	6	1	3
1	7	4	0
2	4	5	0

112

1	0	0	0
2	4	1	4
1	2	7	5
2	1	3	6

113

1	0	0	0
2	7	6	1
1	7	4	4
2	6	1	7

114

1	0	0	0
2	5	5	1
1	6	7	5
2	0	1	4

115

1	0	0	0
2	4	0	1
1	4	3	0
2	1	3	2

116

1	0	0	0
2	1	4	4
1	7	5	2
2	3	6	1

117

1	0	0	0
2	2	1	3
1	1	2	7
2	5	1	5

118

1	0	0	0
2	4	5	0
1	3	3	7
2	4	4	1

119

1	0	0	0
2	1	3	6
1	4	0	7
2	5	0	4

120

1	0	0	0
2	6	1	7
1	4	4	7
2	1	7	6

121

1	0	0	0
2	0	1	4
1	3	0	4
2	3	2	1

122

1	0	0	0
2	1	3	2
1	2	7	1
2	1	5	5

123

1	0	0	0
2	3	6	1
1	0	7	4
2	0	4	5

124

1	0	0	0
2	5	1	5
1	7	5	6
2	1	4	0

125

1	0	0	0
2	4	4	1
1	5	2	7
2	6	1	3

126

1	0	0	0
2	5	0	4
1	3	7	3
2	4	1	4

127

1	0	0	0
7	3	3	3
1	7	4	4
2	1	7	6

128

1	0	0	0
7	0	0	7
1	6	7	5
2	3	2	1

129

1	0	0	0
7	7	0	0
1	4	3	0
2	1	5	5

130

1	0	0	0
7	6	5	3
1	7	5	2
2	0	4	5

131

1	0	0	0
7	0	7	0
1	1	2	7
2	1	4	0

132

1	0	0	0
7	3	5	6
1	3	3	7
2	6	1	3

133

1	0	0	0
7	5	6	3
1	4	0	7
2	4	1	4

134

1	0	0	0
7	3	3	3
1	4	4	7
2	7	6	1

135

1	0	0	0
7	0	0	7
1	3	0	4
2	5	5	1

136

1	0	0	0
7	7	0	0
1	2	7	1
2	4	0	1

137

1	0	0	0
7	6	3	5
1	0	7	4
2	1	4	4

138

1	0	0	0
7	0	7	0
1	7	5	6
2	2	1	3

139

1	0	0	0
7	3	5	6
1	5	2	7
2	4	5	0

140

1	0	0	0
7	5	6	3
1	3	7	3
2	1	3	6

141

1	0	0	0
7	3	3	3
1	4	7	4
2	6	1	7

142

1	0	0	0
7	0	0	7
1	7	1	2
2	0	1	4

143

1	0	0	0
7	7	0	0
1	5	6	7
2	1	3	2

144

1	0	0	0
7	6	3	5
1	7	3	3
2	3	6	1

145	**146**	**147**	**148**	**149**	**150**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
7 0 7 0	7 3 5 6	7 5 6 3	1 4 7 4	1 7 1 2	1 5 6 7
1 0 4 3	1 7 4 0	1 2 7 5	2 6 1 7	2 0 1 4	2 1 3 2
2 5 1 5	2 4 4 1	2 5 0 4	7 3 3 3	7 0 0 7	7 7 0 0

151	**152**	**153**	**154**	**155**	**156**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 7 3 3	1 0 4 3	1 7 4 0	1 2 7 5	1 7 4 4	1 6 7 5
2 3 6 1	2 5 1 5	2 4 4 1	2 5 0 4	2 1 7 6	2 3 2 1
7 6 3 5	7 0 7 0	7 3 5 6	7 5 6 3	7 3 3 3	7 0 0 7

157	**158**	**159**	**160**	**161**	**162**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 4 3 0	1 7 5 2	1 1 2 7	1 3 3 7	1 4 0 7	1 4 4 7
2 1 5 5	2 0 4 5	2 1 4 0	2 6 1 3	2 4 1 4	2 7 6 1
7 7 0 0	7 6 3 5	7 0 7 0	7 3 5 6	7 5 6 3	7 3 3 3

163	**164**	**165**	**166**	**167**	**168**
1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
1 3 0 4	1 2 7 1	1 0 7 4	1 7 5 6	1 5 2 7	1 3 7 3
2 5 5 1	2 4 0 1	2 1 4 4	2 2 1 3	2 4 5 0	2 1 3 6
7 0 0 7	7 7 0 0	7 6 3 5	7 0 7 0	7 3 5 6	7 5 6 3

Proposition 6.7(ii) and the facts that when $n=1$, two nonconjugate complements to $O_2(G_1)$ in the split extension G_1 meet in a group of odd order (of order 21, in fact) and that a pair of conjugate complements meet in a D_8-subgroup.

7. Descriptions of sporadic parabolics by loops

Our purpose here is to make a few loop-theoretic descriptions of certain sporadic 2-locals. We concentrate on a few nontrivial examples and do not attempt an exhaustive treatment. We use notation of Section 6.

The group $\mathrm{Aut}\,\mathbb{O}_{16}$. This occurs as a maximal 2-local in $G_2(K)$, where K is any field of characteristic not 2.

The group $2\cdot\mathrm{Aut}\,\mathbb{O}_{16}$. This occurs as a nonmaximal 2-local in *McL*. Its socle is $\mathbb{Z}_2\times V_1$ as a GL(3, 2)-module and the quotient

$$\mathrm{Aut}\,\mathbb{O}_{16}/[\mathrm{Aut}\,\mathbb{O}_{16}, O_2(\mathrm{Aut}\,\mathbb{O}_{16})]\cong \mathrm{SL}(2,7).$$

Parabolics of shape $\mathbb{Z}_4^3\mathrm{GL}(3,2)$ *in* HiS *and* O'Nan

We have already discussed the two isomorphism types of such 2-constrained groups; see Section 6. The split one occurs as a maximal 2-local in the Higman–Sims group and the nonsplit one as a maximal 2-local in the O'Nan group.

Write $V_n\cong\mathbb{Z}_{2^n}$ and let A_n, B_n be the split and nonsplit extensions of GL(3, 2) by

V_n; see Theorem 6.5. We show how to describe A_n and B_n with automorphisms of a loop. We have below two natural epimorphisms (solid arrows) and we let $\mathscr{L}_n$ be the pullback, i.e. $\{(a,b) \in U_n \times \mathbb{O}_{16} \mid a^\alpha = b^\beta\}$:

$$\begin{array}{ccc} \mathscr{L}_n & \dashrightarrow & \mathbb{O}_{16} \\ \downarrow & & \downarrow \beta \\ U_n = V_n \times Z_n & \xrightarrow{\ \alpha\ } & V_1 \\ (x,y) & \longrightarrow & x \,(\mathrm{mod}\ \Phi(V_n)). \end{array}$$

Here, $Z_n \cong \mathbb{Z}_{2^n}$. Define $A_n^* := \{\sigma \in \mathrm{Aut}(U_n) \times \mathrm{Aut}(\mathbb{O}_{16}) \mid \sigma$ fixes $\mathscr{L}_n$ and induces an element of our $\mathrm{GL}(3,2)$ on $U_n/Z_n \cong V_n\}$ and $R_n := \{\sigma \in A_n^* \mid \sigma$ induces 1 on $U_n/Z_n\}$. Then $R_n = V_n^* \times D$, where $V_n^* \cong \mathrm{Hom}(V_n, Z_n)$ and $D \cong \mathrm{Diag}(\mathbb{O}_{16})$; see Section 4. So, $R_n \cong \mathbb{Z}_{2^n}^3 \times \mathbb{Z}_2^3$. Certainly, A_n^* maps onto $\mathrm{Aut}(\mathbb{O}_{16})$ but, $A_n^*/D \cong A_n$. For $n \geq 2$, we get $B_{n-1}^* \leq A_n^*$ corresponding to $B_{n-1} \leq A_n$ as in Theorem 6.5(d). Let D_0 be the diagonal A_n^*-submodule of $\Omega_1(V_n^*) \times D$.

We claim that B_{n-1}^*/D_0 is nonsplit. If not, let $X \leq B_{n-1}^*$, $X \geq D_0$, complement $V_n^* \times D$ modulo D_0 in B_{n-1}^*. Using Theorem 6.5(d) on the inclusion of X into B_{n-1}^*/D, we see that X contains a subgroup $Y \cong \mathrm{GL}(3,2)$. However, since $\mathrm{Aut}(\mathbb{O}_{16})$ is nonsplit, Y acts trivially on the second factor, whence so does A_n^*, a contradiction.

The parabolic $2^{3+8}\mathrm{GL}(3,2)$ *in Rudvalis' group,* Ru

The subgroup P satisfies: $\mathrm{O}_2(P)$ has class 2, $Z = Z(\mathrm{O}_2(P))$ is a 3-dimensional irreducible for $\bar{P} := P/\mathrm{O}_2(P) \cong \mathrm{GL}(3,2)$, $\mathrm{O}_2(P)/Z$ is the Steinberg module for $\bar{P}$. If we go to the covering group $\widehat{\mathrm{Ru}}$ we find that $\mathrm{O}_2(\hat{P})$ has class 2 and that $\mathrm{O}_2(\hat{P})' = Z(\mathrm{O}_2(\hat{P}))$ is the direct sum of a 3- and a 1-dimensional module for $\mathrm{GL}(3,2)$. Furthermore, $\hat{P} = \mathrm{O}_2(\hat{P})\hat{L}$, $\hat{L} \cap \mathrm{O}_2(\hat{P}) = Z(\mathrm{O}_2(\hat{P}))$ and $\hat{L} \cong \mathbb{Z}_2 \times \mathrm{Aut}\,\mathbb{O}_{16}$. See [21], [7] for details.

Lemma 7.1. *Let* $G = \mathrm{GL}(3,2)$, *S the Steinberg module for* $\mathbb{F}_2G$. *Then* $S \otimes S \cong P_1 \oplus P_3 \oplus P_{3'} \oplus P_8 \oplus P_8 \oplus P_8$, *where* ($P_i$ *or* $P_{i'}$) *is the projective cover of an irreducible* V_i (*or* $V_{i'}$) *of dimension i and where* P_3 *and* $P_{3'}$ *are dual modules;* $S = P_8$.

Also, $d_k = \dim \mathrm{Hom}(\Lambda^2 S, V_k) = 1$ *for* $k = 1, 3, 3'$ *and* 8.

Proof. From the action of G on 3×3 matrices of trace 0, we get $d_1 > 0$ and $d_8 > 0$. Recall that $\dim P_k = 8, 16, 16, 8$ for $k = 1, 3, 3', 8$. Since $V_8 = P_8$ is absolutely irreducible, $d_1 \leq 1$. Since V_8 is self-dual, $d_3 = d_{3'}$. Since Rudvalis's group exists $d_3 = d_{3'} > 0$. Since S is projective, so is $S \otimes S$, whence $S \otimes S$ is a direct sum of various P_k's. Above comments and a dimension count, together with the isomorphisms $T_1 := S \otimes S \geq T_2 := \langle x \otimes x \mid x \in S \rangle \geq T_3 := \langle x \otimes y - y \otimes x \mid x, y \in S \rangle$, $T_1/T_2 \cong \Lambda^2 S \cong T_3$, $T_2/T_3 \cong S$, force the required answer.

Lemma 7.2. *There is a unique group P with the following properties:*

(i) $Q := O_2(P)$ *has class* 2 *and order* 2^{11}.

(ii) $P/Q \cong GL(3,2)$.

(iii) $Z(Q)$ *is the faithful* 3-*dimensional module* V_3 *for* P/Q *and* $Q/Z(Q)$ *is the Steinberg module.*

(iv) *If* $L \geq Z(Q)$ *complements* Q *modulo* $Z(Q)$ *in* P, *the isomorphism type of* L *is given* (*i.e. either split or nonsplit* $2^3 \cdot GL(3,2)$).

Proof. Let S be the Steinberg module for $\mathbb{F}_2G$, $G = GL(3,2)$. Let $1 \to R \to F \to S \to 1$ be a free presentation for the group S and let

$$R_1 = (F' \cap R)\langle x^2 \mid x \in R\rangle \quad \text{and} \quad R_2 = [R,F]\langle x^2 \mid x \in R\rangle.$$

Then $R \geq R_1 \geq R_2$, $R/R_1 \cong S$ and $R/R_2 \cong \Lambda^2 S \oplus S$.

We may lift the action of G on S to the action of a group G_1 on F/R_2, where $G_1/O_2(G_1) \cong G$ and $O_2(G_1) \cong \mathrm{Hom}(S, \Lambda^2 S \oplus S)$ as G-modules. Since S is projective and injective so is $\mathrm{Hom}(S, \Lambda^2 S \oplus S)$, which implies that G_1 contains a copy of G, unique up to conjugacy. The construction of a group Q as above is equivalent to choosing $R_2 \leq R_3 \leq R$ to satisfy

(a) R_3 is G-invariant and $R/R_3 \cong V_3$,

(b) $F'R_3 = R$.

How unique is this choice? Certainly, $R_3 \cap R'$ is determined, by Lemma 7.1, so we need only study $R/R_3 \cap R'$, which looks like $2^{3+8+8} = (2^3 \times 2^8)2^8$ or $2^3\mathbb{Z}_4^8$. The group R_3 corresponds to a central G-chief factor of shape 2^8 in this and so R_3 is uniquely determined. We take $Q = F/R_3$.

Condition (iv) is easy to handle, given Q and $G \leq \mathrm{Aut}(Q)$.

Lemma 7.3. *Let* $G \cong GL(3,2)$ *and* V *an indecomposable* 6-*dimensional* $\mathbb{F}_2G$-*module with composition factors* V_3 *and* $V_{3'}$. *Then* $\dim H^2(G,V) = 1$ *and if* $f: \mathrm{soc}\, V \to V$ *is the inclusion, and* $g: V \to V/\mathrm{soc}\, V$ *the quotient,* $H^2(G,f)$ *is the* 0-*map and* $H^2(G,g)$ *is an isomorphism.*

Proof. Set $M = V \oplus \mathbb{F}_2$, a permutation module for G on the cosets of $H \leq G$, $H \cong \Sigma_4$. By Shapiro's Lemma $H^2(G,M) \cong H^2(H,\mathbb{F}_2) = \mathbb{F}_2^2$. Since $H^2(G,\mathbb{F}_2) \cong \mathbb{F}_2$, we get $H^2(G,V) \cong \mathbb{F}_2$. Similarly, $H^1(G,V) \cong \mathbb{F}_2$.

Using the long exact sequence for cohomology ($H^n \equiv H^n(G,-)$), applied to $0 \to 3 \to V \to 3' \to 0$ (representing $0 \to \mathrm{soc}\, V \xrightarrow{f} V \xrightarrow{g} V/\mathrm{soc}\, V \to 0$) we get

$$H^0 3' \to H^1 3 \to H^1 V \to H^1 3 \to H^2 3 \to H^2 V \to H^2 3'$$

$$\begin{array}{lccccccccccccc} \text{dimensions:} & 0 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \\ \text{maps:} & & 0 & & \cong & & 0 & & \cong & & 0 & & \cong & , \end{array}$$

proving the lemma.

We now propose a realization of P via loop maps. We use the notation and results of Section 2. Let H be the Hamming code on the index set $\Omega=\mathbb{F}_2^3-\{0\}$ and consider $F:=\{(a_k)\mid k\in\Omega,\ a_k\in\mathbb{O}_{16}\}$. The group $G=\mathrm{Aut}(\mathbb{O}_{16})$ acts on Ω and $\mathbb{O}_{16}$, hence on this set. Here, $\mathbb{O}_{16}$ is based on the 'code' H^* in which all nonzero vectors are declared 'odd'. We may identify Ω with $H^*-\{0\}$.

Define maps $x(i,d)$, $i\in H$, $d\in\mathbb{O}_{16}$, by $x(i,d):(a_k)\to(a_k')$ where $a_k'=a_kd$ if $\langle k,i\rangle=1$ and $a_k'=a_k$ if $\langle k,i\rangle=0$. Then $(a_k)^{x(i,d)x(j,e)}=(a_k')$ where

$$\begin{aligned} a_k' &= a_k d\cdot e && \text{if } \langle k,i\rangle=1, && \langle k,j\rangle=1,\\ &= a_k d && \qquad\quad =1, && \qquad\quad =0,\\ &= a_k e && \qquad\quad =0, && \qquad\quad =1,\\ &= a_k && \qquad\quad =0, && \qquad\quad =0. \end{aligned}$$

Therefore, $[x(i,d),x(j,e)]=z_{i\cap j}^{N(d,e)}$. We have $x(i,d)x(i,e)=x(i,de)y(i,d\cap e)$ and $x(i,d)x(j,d)=x(i+j,d)z_{i\cap j}^{Nd}$. In the notation of Section 2, $XYZ/YZ\cong H\otimes H^*$ as G-modules, where we make the additional restriction that $\lambda\in H$; see (2.8). We are interested in X_0YZ, where X_0 is generated by all products $\prod_r x(i_r,d_r)$ with $\sum_r\langle i_r,d_r\rangle=0$. Since $(XYZ)'=Z$, XYZ/Z is abelian and $X_0YZ/YZ\cong S$ is projective and injective as G-modules, we get a subgroup Q_0, $Z\le Q_0\le X_0YZ$ such that $Q_0Y=X_0YZ$. In fact, Q_0 is uniquely determined by these conditions since $YZ/Z\cong H\otimes H$, of shape $(3'\ 3\ 3')^{\mathrm{t}}$, involves only composition factors not isomorphic to S.

We argue that $Q_0'=Z$. Certainly, Q_0' is a G-submodule of $Z\cong PE(H)$, of shape $(3\ 3')^{\mathrm{t}}$. In the group $R=XYZ$ we define $R_0\ge Q_0$ by $R_0/Q_0=C_{R/Q_0}(G)\cong\mathbb{Z}_2$. By considering the G-action on the Lie rings associated to R_0 and Q_0, one sees that it suffices to prove $R_0'=Z$.

For i,d, let $\xi(i,d)\in R_0$ satisfy $\xi(i,d)=x(i,d)y$, for some $y\in YZ$. Take a basis $\{z_\alpha\}$ for Z. We claim that $[\xi(i,d),\xi(j,e)]=\prod_\alpha z_\alpha^{p_\alpha+q_\alpha}$, where there exist scalars a_α,b_α such that $p_\alpha=a_\alpha N(d,e)$ and $q_\alpha=b_\alpha N(d,e,f)$ for some $f\in\mathbb{O}_{16}$. The claim follows from the formulas of Section 2.

Observe that there is an α such that $a_\alpha=1$. For instance, $[x(i,d)x(j,e)]=z_{i\cap j}^{N(d,e)}$ implies that some $a_\alpha\ne0$. We now claim that, for any such α, $z_\alpha\in R_0'$. If false, $p_\alpha(d,e)+q_\alpha(d,e)=0$ for all d,e or that $N(d,e)$ is linear in d and e, which is false. We conclude that $z_{i\cap j}\in Q_0'$. High transitivity implies that $Z\le Q_0'$.

Let $A=\mathrm{Aut}(\mathbb{O}_{16})$ and let A act on L by $g\in A, g:(a_k)\to((a_{k^{g^{-1}}})^g)$. Then $g\in\mathrm{Diag}(\mathbb{O}_{16})=O_2(A)$ acts by $(a_k)\to(a_kz^{\langle k,S\rangle})$ for some $S\in H\le\mathrm{PE}(\Omega)$. The group $ZA\le\Sigma_L$ satisfies $Z\cap A=\mathrm{soc}(Z)$ and

$$1\to Z\to ZA\to\mathrm{GL}(3,2)\to1$$

is split, according to Lemma 7.3. We take $P_1:=Q_0A\le\Sigma_L$, proving the Lemma.

We give explicit generators for Q_0 modulo Z. Let $\{i_1,i_2,i_3\}$ be a basis of H and let $\{d_1,d_2,d_3\}$ be a basis of $\mathbb{O}_{16}$ modulo its center. We take them to express the duality of H and H^*. An element of XYZ/Z may be represented by a 3×6 matrix over $\mathbb{F}_2$, where the elementary matrix unit E_{jk} stands for the coset of $x(i_j,d_k)$ if $k\le3$ and for the coset of $y(i_j,i_k)$ if $4\le k\le6$. Let M_L, M_R, respectively, be the span of the E_{jk} for $j=1,2,3$ and for $k=1,2,3$ and $4,5,6$, respectively.

We may identify the action of G on this set of matrices by taking the natural action of G on $V_3 \otimes V_3$ to be the action on M_R. Since M_L is not a module direct summand, we need a factor set to modify the natural action of G on $V_3 \otimes V_{3'}$ to get the right action on $V_3 \otimes V$. The rule $x(i,d)x(i,e)=x(i,de)y(i,d \cap e)$ gives the factor set. Note that the subgroup of GL(3,2) preserving the direct sum is the group of permutation matrices Σ_3, taken with respect to the basis $\{i_1, i_2, i_3\}$ (or, equivalently, with respect to $\{d_1, d_2, d_3\}$).

Our generators for Q_0 modulo Z are all

$$\xi_{jk} := x(i_j, d_j)x(i_k, d_k)y(i_j, i_k i_l), \quad \text{for } \{j,k,l\}=\{1,2,3\},$$

$$\eta_{jk} := x(i_j, d_k)y(i_j, i_j i_l)y(i_l, i_j), \quad \text{for } \{j,k,l\}=\{1,2,3\}.$$

These generators correspond to the respective matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and those obtained from them by natural action of Σ_3 on the indices $\{1,2,3\}$ and $\{4,5,6\}$ via the bijection $k \leftrightarrow k+3$. To get a basis, remove one ξ_{jk}. The validity of this paragraph was established with a computer program.

For $X=L,R$, let p_X be the projection of $M=M_L \oplus M_R$ onto the summand M_X. Then p_X carries this 8-dimensional space of matrices isomorphically onto $M_L^0 = \{[A \mid 0] \mid \operatorname{tr} A = 0\}$ if $X=L$ and onto $M_R^0 = \{[0 \mid B] \mid$ the sum of the off-diagonal terms is $0\}$ if $X=R$. The Σ_3-module M_L^0 is a direct sum of the 2-dimensional faithful module M_L^1 and M_L^2, isomorphic to the group algebra $\mathbb{F}_2\Sigma_3$; in fact, $M_L^1 = \{[A \mid 0] \mid A$ is diagonal and $\operatorname{tr} A = 0\}$ and $M_L^2 = \{[A \mid 0] \mid$ the diagonal of A is $0\}$. The above isomorphism $M_L \cong M_R$ carries M_L^1 to $\{[0 \mid B] \mid B$ is diagonal and $\operatorname{tr} B = 0\}$ and M_L^2 to the span of all $E_{j,j+3}+E_{j,k+3}+E_{k,j+3}$, for $j \neq k$.

Proposition 7.4. $P \approx P_1/\operatorname{soc}(Z)$.

Proof. Lemma 7.2.

A slight variation of this idea ought to give $\hat{P}$, possibly something using the extended code for $H \times \langle \Omega \rangle$ in $\mathbb{F}_2^8$.

Remark 7.5. It is not always necessary to employ the loop concept to describe parabolics in sporadics. In the monster, the centralizer of a 2-central involution has shape $(2_+^{1+24})(.1)$ and is described with the theory of extraspecial groups and their automorphisms. Some 2-locals in sporadics are so small that no special theories are needed.

Remark 7.6. To study representations of certain sporadic parabolics P, it is useful to have a group $\hat{P}$ with a quotient isomorphic to P. The kernels of relevant $\hat{P}\to P$ are

$$\begin{array}{lll} \mathbb{Z}_2 & \text{for } P=(2_\varepsilon^{1+2n})(\Omega^\varepsilon(2n,2)) & \text{in } J_2, J_3, \mathrm{Suz}, .1; \\ \mathbb{Z}_2^2 & \quad\;\; =(2^{2+11+22})(\Sigma_3\times M_{24}) & \text{in } F_1; \\ \mathbb{Z}_2^3 & \quad\;\; =2^{3+8}\mathrm{GL}(3,2) & \text{in Ru.} \end{array}$$

References

[1] J. Alperin, Sylow 2-subgroups of 2-rank 3, in: Finite Groups '72 (Proc. Gainesville Conf., Univ. Florida, Gainesville, FL, 1972), North-Holland Mathematical Studies, Vol. 7 (North-Holland, Amsterdam, 1973) 1–12.

[2] G. Avrunin, The image of the restriction map on 2-cohomology, Arch. Math. (Basel) 34 (1980) 502–508.

[3] D. Benson, Modular Representation Theory via Representation Rings, Lecture Notes in Math. (Springer, Berlin, 1985).

[4] N. Blackburn, The extension theory of the symmetric and alternating groups, Math. Z. 117 (1970) 191–206.

[5] E. Cline, B. Parshall, L.L. Scott, Jr. and W. van der Kallen, Rational and generic cohomology, Invent. Math. 39 (1977) 143–163.

[6] E. Cline, B. Parshall, L.L. Scott, Jr., Cohomology of finite groups of Lie type, I, Inst. Hautes Etuds Sci. Publ. Math. 45 (1975) 169–191.

[7] J. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, Atlas of Finite Groups (Oxford University Press, 1985).

[8] J. Conway, A simple construction for the Fischer-Griess Monster group, Invent. Math.

[9] J. Conway, Three lectures on exceptional groups, in: G. Higman and M. Powell, eds., Finite Simple Groups, Oxford, 1969 (Academic Press, London, 1971).

[10] H.S.M. Coxeter, Integral Cayley numbers, Duke Math. J. 13 (1946) 561–578.

[11] U. Dempwolff, On the extensions of an elementary group of order 2^5 by GL(5,2), Rend. Sem. Mat. Padova 48 (1972) 359–364.

[12] U. Dempwolff, On the second cohomology of GL(n,2), J. Austral. Math. Soc. 16 (1973) 207–209.

[13] L. Dornhoff, Group Representation Theory, 2 volumes (Marcel Dekker, New York 1971, 1972).

[14] W. Feit, The Representation Theory of Finite Groups (North-Holland, Amsterdam, 1982).

[15] E.M. Friedlander, Homological stability for classical groups over finite fields, Algebraic K-Theory (Proc. of a conference at Northwestern University in Evanston, IL, 1976), Lecture Notes in Math. 551 (Springer, Berlin, 1976) 290–302.

[16] E.M. Friedlander and B. Parschall, On the cohomology of Chevalley groups, Bull. Amer. Math. Soc. 7 (1982) 247–250.

[17] S. Gagola and S. Garrison, Real characters, double covers and the multiplier, J. Algebra 74 (1982) 20–51.

[18] R.L. Griess, Jr., Lecture at the Santa Cruz conference, 1979.

[19] R.L. Griess, Jr., A sufficient condition for a finite group of even order to have nontrivial Schur multiplicator, Notices Amer. Math. Soc. (1970).

[20] R.L. Griess, Jr., Automorphisms of extraspecial groups and nonvanishing degree 2 cohomology, Pacific J. Math. 48 (1973) 403–422.

[21] R.L. Griess, Jr., Schur multipliers of the known finite simple groups, III, in: Proc. of the Rutgers Group Theory Year 1983–84 (Cambridge University Press, Cambridge, 1984) 69–80.

[22] R.L. Griess, Jr., Code loops, J. Algebra, to appear.

[23] R.L. Griess, Jr., The friendly giant, Invent. Math. 69 (1982) 1–102.

[24] R.L. Griess, Jr., The monster and its nonassociative algebra, Proc. Montreal Conference on Finite Groups, to appear.

[25] D.G. Higman, Flag transitive collineation groups of finite projective spaces, Illinois J. Math. 6 (1962) 434–446.

[26] B. Huppert, Endliche Gruppen I (Springer, Berlin, 1967).

[27] V. Landazuri, Thesis, University of Michigan, 1975.

[28] M. O'Nan, Some evidence for the existence of a new simple group, Proc. London Math. Soc. 32 (1976) 421–479.

[29] M. Ronan and S.D. Smith, 2-local geometries for finite groups, Proc. The Santa Cruz Conference on Finite Groups (Amer. Math. Soc., Providence, RI, 1980).

[30] I. Schur, Ueber die Darstellung der endliche Gruppen durch gebrochene lineare Substitutionen, Crelle J. Math. 127 (1904) 20–50.

[31] I. Schur, Untersuchungen ueber die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen, Crelle J. Math. 132 (1907) 85–137.

[32] I. Schur, Ueber die Darstellungen der symmetrischen und alternierenden Gruppen durch gebrochene lineare Substitutionen, Crelle J. Math. 139 (1911) 155–250.

[33] R. Steinberg, Générateurs, relations et revêtements de groupes algébriques, Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), Librairie Universitaire, Louvain (Gauthier-Villars, Paris, 1962) 113–127.

[34] R. Steinberg, Lectures on Chevalley groups, Yale Lecture Notes, 1967.

[35] J. Tits, Remarks on Griess' construction of the Griess–Fischer sporadic group I, II, III, IV, Preprints distributed 1982–1983.

[36] J. Tits, Théorie des groupes, Annuaire du Collège de France, 1982–1983.

[37] J. Tits, Le monstre, Séminaire Bourbaki, 620, November 1983.

[38] Peterfalvi, Le théorème de Bender–Suzuki, I, Preprint.