Invent. math. 69, 1-102 (1982)

Inventiones mathematicae
© Springer-Verlag 1982

The Friendly Giant

Robert L. Griess, Jr.

Department of Mathematics, University of Michigan, Ann Arbor, Mi 48109, USA

Table of Contents

1. Introduction

In this paper, we demonstrate the existence of the *Friendly Giant*, a finite simple group of order

$$2^{46}3^{20}5^9 7^6 11^2 13^3 . 17 . 19 . 23 . 29 . 31 . 41 . 47 . 59 . 71$$
$$=808{,}017{,}424{,}794{,}512{,}875{,}886{,}459{,}904{,}961{,}710{,}757{,}005{,}754{,}368{,}000{,}000{,}000.$$

Evidence for the existence of this group was produced independently in November, 1973, by Bernd Fischer in Bielefeld and by this author in Ann

Dedicated to the memory of Richard D. Brauer, February 10, 1901-April 17, 1977

Research supported in part by NSF grants MCS-78-02463 and MCS-80-03027

0020-9910/82/0069/0001/$20.40

Arbor. Serious work on this group - mainly a study of subgroups and conjugacy classes - began the first weekend of that month in both locations. Additional details of this early work are discussed in Sect. 15. For now, we add only that such a simple group appeared likely to have a complex irreducible character of degree 196883; in 1974, this number was established as a lower bound for the degree of a nonprincipal irreducible character [13, 37]. While this evidence for the existence was very persuasive, it did not constitute a proof. Our existence proof was announced on January 14, 1980 and more formally in [29].

Our method is to take a 196884-dimensional module B for a particular group C of shape $(2^{1+24})(\cdot 1)$, define on B the structure of a commutative nonassociative algebra with a symmetric nondegenerate associative bilinear form, then define an automorphism σ of this algebra. The group $G=\langle C, \sigma\rangle$ is the simple group of the title (the usual symbol for this group is F_1). The extra rigidity required by expecting our linear group to preserve an algebra structure enables us to make precise definitions of the relevant linear transformations and verify their required properties. The reason we thought of this approach is the following. Simon Norton had computed the values of a hypothetical character χ of degree 196883 and computed that $(S^2\chi, 1)=1$, $(S^3\chi, 1)=1$, $(S^3\chi, \chi)=1$ and χ is rational-valued. It follows that if M is a module affording χ, M has the structure of a commutative (but not necessarily associative) algebra with a nondegenerate associative symmetric bilinear form. This finding of Norton was the inspiration for this paper. See Sect. 15 for additional comments on algebras associated to finite simple groups.

We comment on some over-all aspects of the construction. In some sense, the algebra B is described using only basic linear algebra. The group theory used is descriptive in nature. Thus, one could say that the construction of $G=\langle C, \sigma\rangle$ is elementary. That is, starting from scratch, one may construct M_{24}, then $\cdot 0$ and finally G, with each stage depending on the previous one. See two paragraphs ahead and look at Table 1.1. However, the identification of G as a finite simple group with the right properties requires deep results from the classification of finite groups. It is possible that this dependence can be eliminated, for instance, by counting configuration of vectors in B permuted by G. An enumeration of any such configurations may be long and difficult, however.

Section 2 contains various preliminary results, mainly about group representations, the Leech lattice, Conway groups and the classification of finite simple groups. Sections 3 and 4 set up basic notation. In Sect. 5, we compute the C-invariant algebra structures on the module B, and in Sect. 6 we select the one we work with in the rest of the paper (modulo a choice of F made in Sect 7). Sections 7, 8 and 9 discuss various technicalities needed both in the definition of σ (Sect. 10) and in the proof of the "main result," Proposition 11.2, that σ is an algebra automorphism. Section 7 is concerned with a choice of complement F which will cause the function β to behave well, while Sects. 8 and 9 develop techniques for analyzing the action of certain elements of C on basis elements, mainly for the purpose of being able to analyze β. Nearly all of Sect. 11 is concerned with a proof of the main result, which in turn amounts to verifying a list of identities involving configurations of vectors in the Leech lattice; this is where the correctness of the plus and minus signs in the definition of σ is so critical.

In Sects. 12, 13, and 14, the mathematics departs from that of preceding sections in that we require results from the classification theory, and, in Sect. 14, we refer to work of others on the group F_1, only some of which has appeared. In Sect. 12, we identify $G=\langle C, \sigma\rangle$ as a finite simple group of order $2^{46}3^{20}5^{9}7^{6}11^{2}13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$. It is not obvious that G is finite, and if G is finite, it is not obvious that the containment $C\leqq C_G(z)$, $\langle z\rangle=Z(C)$, is equality, a necessary step in the identification of G. This problem is handled by a "reduction modulo p" procedure. In Sect. 13, we derive existence of a number of sporadic groups (besides G). These other groups had been constructed earlier; in some of these cases, existence proofs required computer work. All we need to do is name appropriate subquotients of G (although we use results from the classification theory to *identify* these subquotients), using little more than notation already established earlier in the paper. Also in Sect. 13, we derive existence of a number of nonsplit group extensions; hence we get nonvanishing of certain degree 2 cohomology groups.

In Sect. 14, we determine that the simple groups LyS, J_3, J_4, $O'S$ and Ru are not involved in the Friendly Giant. The sporadic groups which are involved in the Friendly Giant constitute the *Happy Family* and those which are not are called the *Pariahs*. The membership of every sporadic group in one of those two categories is settled, except for J_1. The twenty sporadics M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_2, Held, HiS, McL, Suz, $\cdot 1$, $\cdot 2$, $\cdot 3$, F_{22}, F_{23}, F_{24}', F_1, F_2, F_3, F_5 are involved in the Friendly Giant in a "visible" manner. A glance at the group orders shows that LyS and J_4 must be Pariahs, but it is certainly not obvious for J_3, Ru and $O'S$. The group J_1 has order "only" 175,560 and one might easily imagine a copy of J_1 floating as a tiny speck within F_1. We point which that J_1 is a subgroup of $O'S$ (the fixed points of an outer automorphism), which is not involved in F_1. In any case, suitable information is available (using outside sources) to carry out the arguments of Sect. 14.

In Sect. 15, we conclude with some comments on background and the proof. A list of notations and definitions and a list of tables to assist the reader has been placed before the references.

We make it clear that our construction of G (Sect. 2 through 11) is direct, explicit and is carried out entirely by hand. The identification of G, however, requires hard theorems from the classification of finite simple groups. A few of our arguments in Sect. 14 require computer calculations, but this is the only place in the paper where we make explicit reference to computer work. Some work in the theory of finite simple groups does involve computing machines and a few of the references we use do have some ultimate dependence on such work (e.g., in determining conjugacy classes and character tables). With these exceptions, the results of this paper are free of machine calculations.

This work was carried out mainly at the Institute for Advanced Study during the academic year 1979–80. We thank the Institute for Advanced Study for the privileges of membership during this time (and during Winter term, 1981), the National Sciences Foundation for partial financial support and the University of Michigan for partial financial support during that sabbatical year.

Special thanks go to my wife, Pamela Schwarzmann, for her support and patience with me during the year at the Institute for Advanced Study and to Enrico Bombieri for many words of encouragement. We acknowledge helpful remarks from Allan Adler, George Glauberman, Melvin Hochster, Michael O'Nan, Steven Smith and Ronald Solomon which led to clarifications and we acknowledge the computer work by Charles Sims and Steven Smith which settled a few points in Sect. 14. We thank the referee for investing an enormous amount of work in reading this paper and providing thoughtful and detailed commentary. In particular the referee caught some mistakes in the preprint version. Most were slips or small errors, but others were not. These exceptions are noted in the text.

Table 1.1. Construction of the happy family[a]

$$\begin{tikzcd}
\text{Construct...} & \text{then derive existence of...} \\
M_{24} \arrow[r] & M_{11}, M_{12}, M_{22}, M_{23}, M_{24} \arrow[dl] \\
\cdot 0 \arrow[r] & \cdot 1, \cdot 2, \cdot 3, \text{HiS, McL, Suz, HJ} \arrow[dl] \\
F_1 \arrow[r] & F_2, F_3, F_5, F_{22}, F_{23}, F'_{24}, \text{Held.}
\end{tikzcd}$$

[a] except possibly for J_1

§2. Preliminary Results

We begin by reviewing properties of the Leech lattice and by establishing some notation which will be used throughout the paper.

The Leech lattice, denoted Λ, is a free abelian group of rank 24 with a certain positive definite symmetric bilinear form $\langle\ ,\ \rangle$ which makes Λ unimodular, i.e. $\det\Lambda=1$, and be even, i.e. satisfy $\langle\lambda,\mu\rangle\in\mathbb{Z}$, $\langle\lambda,\lambda\rangle\in 2Z$ for all $\lambda,\mu\in\Lambda$.

All even integral unimodular lattices of rank 24 have been classified by Niemeyer; see [11] and [55]. There are 24 such lattices. Among these, Λ is the only one which contains no vector with squared length 2.

The lattice is of special interest to group theorists since $\mathrm{Aut}(\Lambda)=\{g\in O(\mathbb{R}\underset{\mathbb{Z}}{\otimes}\Lambda)\mid\Lambda^g=\Lambda\}$, the "group of units" of Λ, is a perfect group called .0 ("dot zero") of order $2^{22}\,3^9\,5^4\,7^2\,11.13.23$ whose central quotient is a simple group $\cdot 1=\cdot 0/\{\pm 1\}$ (*dot one*). These groups and several others closely associated to them ($\cdot 2$ and $\cdot 3$) are called *Conway groups* because John Conway was the first to investigate the group theoretic properties of the Leech lattice [10, 49, 50]. We refer to Conway's more detailed discussion of Λ and $\cdot 0$ found in [11]. In particular, we expect the reader to be familiar with [11], although we shall review some of the main definitions (in condensed form) and borrow some tables.

We let $\Omega=\mathbb{F}_{23}\cup\{\infty\}$, as in [11] and let $\{x_i\mid i\in\Omega\}$ be an orthonormal basis for $\mathbb{Q}^\Omega=\mathbb{Q}^{24}$. Let $\mathscr{S}=\mathscr{S}$ (5, 8, 24) be a Steiner system based on Ω. That is, $\mathscr{S}$ consists of a family of eight-element subsets of Ω such that, given five distinct points of Ω, there is a unique member of the family containing the five points.

Members of this family are called *octads*. The group preserving $\mathcal{S}$, i.e. $\{g\in\sum_\Omega | \mathcal{O}^g\in\mathcal{S}$ whenever $\mathcal{O}\in\mathcal{S}\}$, is the *Mathieu group* M_{24}, a simple group of order $2^{10}3^3 5.7.11.23$.

The power set $P(\Omega)$ of Ω may be regarded as a vector space over $\mathbb{F}_2$ via the operation of symmetric difference: $A, B\in P(\Omega)$, $A+B=A\cup B-A\cap B=(A-B)\cup(B-A)$. The subspace $\mathscr{C}$ of $P(\Omega)$ spanned by the 759 octads is, remarkably, only 12-dimensional. The subspace is called the *$\mathscr{C}$-sets*. In $\mathscr{C}$, there are 759 octads, 759 *special* 16-*sets* (=complements of octads). 2576 *special dodecads* (certain 12-sets), $\emptyset$ and Ω; we have $759+759+2576+1+1=4096$. The stabilizer of a dodecad in M_{24} is M_{12}, and the stabilizer of a pair of complementary dodecads is $M_{12}\cdot 2$. We shall also use the vector space $\bar{\mathscr{C}}=\mathscr{C}/\langle\Omega\rangle$, $\dim\bar{\mathscr{C}}=11$. Occasionally we shall blur the distinction between members of $\mathscr{C}$ and $\bar{\mathscr{C}}$.

We recall a useful result from [11].

Lemma 2.1. *Let* $\{a_1, \ldots, a_8\}$ *be an octad.* (i) *The number of octads intersecting* $\{a_1, \ldots, a_i\}$ *in* $\{a_1, \ldots, a_j\}$ *exactly is the* $(j+1)$-th *entry in the* $(i+1)$-th *line of Table* 2.1.1. (ii) *The number of dodecads intersecting* $\{a_1, \ldots, a_i\}$ *in* $\{a_1, \ldots, a_j\}$ *exactly is the* $(j+1)$-th *entry in the* $(i+1)$-th *line of Table* 2.1.2.

Table 2.1.1. How many octads?

759								
506	253							
330	176	77						
210	120	56	21					
130	80	40	16	5				
78	52	28	12	4	1			
46	32	20	8	4	0	1		
30	16	16	4	4	0	0	1	
30	0	16	0	4	0	0	0	1

Table 2.1.2. How many dodecads?

2576								
1288	1288							
616	672	616						
280	336	336	280					
120	160	176	160	120				
48	72	88	88	72	48			
16	32	40	48	40	32	16		
0	16	16	24	24	16	16	0	
0	0	16	0	24	0	16	0	0

On $P(\Omega)$, there is a natural bilinear form $(A, B)\mapsto|A\cap B|\,(\mathrm{mod}\,2)$. On $P(\Omega)_{\text{even}}$, the subspace of sets of even cardinality, we have a quadratic form $A\mapsto\frac{1}{2}|A|\,(\mathrm{mod}\,2)$; see [18, 31] for a discussion of quadratic forms in characteristic

2. Its associated bilinear form is the one above. The $\mathscr{C}$-sets form a subspace which is totally singular with respect to the quadratic form. Note that $\langle\Omega\rangle$ is the radical of the form on $P(\Omega)_{\text{even}}$. Thus, we have an induced form on $P(\Omega)_{\text{even}}/\langle\Omega\rangle$. When $\{i,j,\dots\}\subseteq\Omega$ and $S\subseteq\Omega$ we write $i,j,\dots$ in $S \pmod 2$ for $|\{i,j,\dots\}\cap S| \pmod 2$. When $\{i,j,\dots\}$ and S are even sets, we may replace either or both by their complements when computing $i,j,\dots$ in $S \pmod 2$. We shall enclose "$i,j,\dots$ in S" in brackets if clarity seems to require it.

We describe the Leech lattice, Λ, as follows. Let $(\ ,\ )$ be the usual dot product on $\mathbb{Q}^{\Omega}$, based on $(x_i,x_j)=\delta_{ij}$ and let $\langle\ ,\ \rangle=\frac{1}{8}(\ ,\ )$. The Leech lattice is defined as the span of all vectors of the shape

(i) (80^{23}) (i.e. $\pm 8x_i$ for all $i\in\Omega$)

(ii) $(2^8 0^{16})$ (i.e. the support is an octad, $\mathcal{O}$, each coordinate over $\mathcal{O}$ is ± 2 and the number of minus signs is even)

(iii) (31^{23}) (i.e. for each $i\in\Omega$, form $-3x_i+\sum_{j\neq i} x_j$, then change signs at every $\mathscr{C}$-set).

A subgroup of $\cdot 0$ of special interest is a group called N_{24}, a maximal subgroup of $\cdot 0$. It contains M_{24} as a group of coordinate permutations. Furthermore, $N_{24}=O_2(N_{24})\cdot M_{24}$, where $O_2(N_{24})\cong\mathscr{C}\cong 2^{12}$ and where the element ε_S of $O_2(N_{24})$, $S\in\mathscr{C}$, sends x_i to $-x_i$ if $i\in S$ and x_i to x_i if $i\notin S$. The set of generators for Λ described above is invariant under N_{24} (since the intersection of any two $\mathscr{C}$-sets has even cardinality). In [10], Conway describes an automorphism of Λ not in N_{24}, thereby proving that $\cdot 0 > N_{24}$.

For each integer $n\geq 0$ we define $\Lambda_n=\{\lambda\in\Lambda \mid \langle\lambda,\lambda\rangle=2n\}$, the *vectors of type* n in Λ. Clearly, the Λ_n partition Λ, and, as mentioned before, Λ_1 is empty. A *triangle of type abc* shall mean a triple of lattice vectors with sum zero whose three members have types a, b and c, respectively.

We shall be especially interested in Λ_2. From [11], we get $\Lambda_2 =\Lambda_2^4\cup\Lambda_2^2\cup\Lambda_2^3$, where

$$\Lambda_2^4=\text{all vectors of shape } (4^2 0^{22}) \text{ (i.e. all } \pm 4i\pm 4j,\ i-j \text{ in } \Omega);$$

$$\Lambda_2^2=\text{all vectors of shape } (2^8 0^{16});$$

$$\Lambda_2^3=\text{all vectors of shape } (31^{23}).$$

We have $|\Lambda_2^4|=\binom{24}{2}.2^2=1104$, $|\Lambda_2^2|=759.2^7=97152$, $|\Lambda_2^3|=24.2^{12}=98304$ and $|\Lambda_2|=196560=1104+97152+98304$.

We let $\tilde{L}=L/\{\pm 1\}$, for L a subset of Λ closed under $\lambda\mapsto-\lambda$. For $\lambda\in L$, let $\tilde{\lambda}$ denote the image of λ in $\tilde{L}$. Sometimes, we shall blur the distinction between elements of L and $\tilde{L}$. For instance, we may refer to the triangle of type 222 spanned by $\tilde{\lambda}, \tilde{\mu}\in\tilde{\Lambda}_2$.

Notation. For $i\in\Omega$, $\lambda_i := -3x_i+\sum_{j\neq i} x_j\in\Lambda$. When S is a $\mathscr{C}$-set, let

$$\lambda_{i,S} := \lambda_i^{\varepsilon_S} = \begin{cases} -3x_i+\sum\limits_{\substack{j\neq i\\ j\notin S}} x_j-\sum\limits_{\substack{j\neq i\\ j\in S}} x_j & \text{if } i\notin S,\\ 3x_i+\sum\limits_{\substack{j\neq i\\ j\notin S}} x_j-\sum\limits_{\substack{j\neq i\\ j\in S}} x_j & \text{if } i\in S.\end{cases}$$

For $i \neq j$, $\lambda_{ij} := 4x_i + 4x_j$, $\lambda_{ij'} := 4x_i - 4x_j$. For S a $\mathscr{C}$-set, $\lambda_S := \sum_{i \in S} 2x_i$. For $\lambda \varepsilon \Lambda$, let $\mathrm{supp}(\lambda) = \{i \in \Omega \mid \text{the } i^{\text{th}} \text{ coordinate of } \lambda \text{ is nonzero}\}$, $\mathrm{Pos}(\lambda) = \{i \in \Omega \mid \text{the } i^{\text{th}} \text{ coordinate of } \lambda \text{ is positive}\}$, $\mathrm{Neg}(\lambda) = \{i \in \Omega \mid \text{the } i^{\text{th}} \text{ coordinate of } \lambda \text{ is negative}\}$. Let $\mathcal{O}_\lambda = \mathrm{supp}(\lambda)$, for $\lambda \in \Lambda_2^2$, $i(\lambda) = j$ if $\lambda = \lambda_{i,S}$.

Later, in Sect. 7, an isomorphism $F(2) \cong \bar{\mathscr{C}} := \mathscr{C}/\langle \Omega \rangle$ will be described, where $F(2)$ is a certain 2-group of order 2^{11}. To $x \in F(2)$ we associate a pair $\{S_x, S_x + \Omega\}$ of $\mathscr{C}$-sets. We set $\lambda_{i,x} := \lambda_{i,S_x}$. This is not well defined, but does give a well-defined equivalence class in $\tilde{\Lambda}_2 = \Lambda_2/\{\pm 1\}$. The inverse operation assigns to $S \in \mathscr{C}$ or $\bar{\mathscr{C}}$ the element $x_S \in F(2)$.

Lemma 2.2. (i) *Let Ω be a finite set, $P(\Omega)$ the Boolean algebra of subsets of Ω, $E \leqq P(\Omega)_{\text{even}}$, the subspace of sets of even cardinality. The map $P(\Omega) \times P(\Omega) \to F_2$, $(A, B) \mapsto |A \cap B| \pmod 2$, is bilinear. The map $E \to \mathbb{F}_2$, $A \mapsto \frac{1}{2}|A| \pmod 2$ is a quadratic form on E with associated bilinear form $(A, B) \mapsto |A \cap B| \pmod 2$. The radical of the form is contained in $\langle \Omega \rangle$ and is $\langle \Omega \rangle$ if $|\Omega|$ is even.*

(ii) *Let E_1 be a subspace of $E = P(\Omega)_{\text{even}}$ such that if $A \in E_1$, then $|A| \equiv 0 \pmod 4$. If $A, B \in E_1$, Then $\frac{1}{4}|A+B| \equiv \frac{1}{2}|A-B| + \frac{1}{4}|B| + \frac{1}{4}|A| \pmod 2$. Also, $\frac{1}{2}|A-B| \equiv \frac{1}{2}|A \cap B| \pmod 2$ for $A, B \in E_1$.*

Proof. (i) For $A, B, C \in P(\Omega)$ one must check that $|(A+B) \cap C| = |A \cap C| + |B \cap C| \pmod 2$ and, when $A, B, C \in E$, $\frac{1}{2}|A+B| + \frac{1}{2}|A| + \frac{1}{2}|B| \equiv |A \cap B| \pmod 2$. The last statement essentially amounts to the observation that if $A \in E$, $A \neq \emptyset, \Omega$ and $i \in A$, $j \notin A$, then $|\{i, j\} \cap A| \equiv 1 \pmod 2$.

(ii) The condition $|A| \equiv 0 \pmod 4$ for $A \in E_1$ implies that $|\mathrm{A} \cap B| \equiv 0 \pmod 2$ for $A, B \in E_1$; see Lemma 2.1. In particular, all the $|A - B|$ are in $2\mathbb{Z}$. Write $\delta = |A \cap B|$, $|A| = \alpha + \delta$, $|B| = \beta + \delta$, $|A+B| = \alpha + \beta$. Our hypotheses imply that α, δ and β are all in either $4\mathbb{Z}$ or $2 + 4\mathbb{Z}$.

We have $\frac{1}{4}\{\alpha + \delta + \alpha + \beta\} \equiv \frac{1}{2}|A - B| + \frac{1}{4}|B|$. Also, $\frac{1}{4}\{\alpha + \delta + \alpha + \beta\} \equiv \frac{1}{4}|A + B| + \frac{1}{4}|A| \pmod 2$. Rearranging, we get the first statement.

The second statement needs only $|A| \equiv 0 \pmod 4$ and $|A \cap B|$ even, for all $A, B \in E_1$.

The next lemma will be used repeatedly.

Lemma 2.3. *Suppose that $\lambda = \lambda_{i,x} \pm \lambda_{j,y} \in \Lambda_2^2$. Then either*

(i) *$i = j$ and $S_x + S_y = \mathcal{O}$ or $\mathcal{O} + \Omega$, where $\mathcal{O}$ is an octad, $i \notin \mathcal{O}$; or*

(ii) *$i \neq j$ and $S_x + S_y = \mathcal{O}$ or $\mathcal{O} + \Omega$, where $\mathcal{O}$ is an octad and $i, j \in \mathcal{O}$; also, $\frac{1}{2}\langle \lambda_{ij}, \lambda \rangle \equiv 1 + \frac{1}{2}\langle \lambda_{ij'}, \lambda \rangle \equiv ij$ in $S_x + 1 \equiv ij$ in $S_y + 1 \pmod 2$ and $\{ij\} + S_x$ meets $\mathcal{O}$ in $\mathrm{Pos}(\lambda)$ or $\mathrm{Neg}(\lambda)$.*

Proof. (i) Suppose $i = j$. Then, arranging $i \notin S_x \cup S_y$, we must have

$$\begin{array}{lllll}
\lambda_{i,x} = (-3 & 1 \dots 1 & -1 \dots -1 & 1 \dots \ 1 & -1 \dots -1) \\
\lambda_{i,y} = (-3 & 1 \dots 1 & -1 \dots -1 & -1 \dots -1 & 1 \dots \ 1) \\
\lambda \quad = (\ \ \underset{i}{0} & 0 \dots 0 & \underbrace{0 \dots}_{S_x \cap S_y} 0 & \underbrace{2 \dots \ 2}_{S_y - S_x} & \underbrace{-2 \dots -2}_{S_x - S_y})
\end{array}$$

and the statement is obvious.

(ii) Suppose $i \neq j$. We may arrange $i \notin S_x$, and $j \notin S_y$. Since the coordinates of λ at i and j must be ± 2, we are forced to have either $i \notin S_y$, $j \notin S_x$ and the picture

$$\begin{array}{lcccccc}
\lambda_{i,x}=(& -3 & 1 & 1\ldots1 & 1\ldots\;1 & \multicolumn{2}{c}{\overbrace{-1\ldots-1 \quad -1\ldots-1}^{S_x})} \\
\lambda_{j,y}=(& 1 & -3 & 1\ldots1 & -1\ldots-1 & -1\ldots-1 & 1\ldots\;1) \\
\lambda\;\;=(& \underset{i}{-2} & \underset{j}{-2} & 2\ldots2 & \multicolumn{2}{c}{\underbrace{0\ldots\;0 \quad -2\ldots-2}_{S_y}} & 0\ldots\;0)
\end{array}$$

or $i \in S_y$, $j \in S_x$ and the picture

$$\begin{array}{lcccccc}
\lambda_{i,x}=(& -3 & 1\ldots\;1 & \multicolumn{3}{c}{\overbrace{-1\ldots-1 \quad -1 \quad -1\ldots-1}^{S_x}} & 1\ldots1) \\
\lambda_{j,y}=(& -1 & -1\ldots-1 & -1\ldots-1 & -3 & 1\ldots\;1 & 1\ldots1) \\
\lambda\;\;=(& \multicolumn{3}{c}{\underbrace{\underset{i}{-2} \quad 2\ldots\;2 \quad 0\ldots\;0}_{S_y}} & \underset{j}{2} & -2\ldots-2 & 0\ldots0).
\end{array}$$

In the former case, $S_x + S_y = \mathcal{O} + \Omega$ and in the latter case, $S_x + S_y = \mathcal{O}$. By inspection, $\{ij\} + S_x$ meets $\mathcal{O}$ in $\mathrm{Pos}(\lambda)$ or $\mathrm{Neg}(\lambda)$ in either case. Also, $S_x \cap S_y = S_x \cap \mathcal{O}$ when ij in $S_x \equiv 0 \pmod 2$ and $S_x + (S_x \cap S_y) \equiv S_x \cap (\Omega - S_y) = S_x \cap \mathcal{O}$ when ij in $S_x \equiv 1 \pmod 2$ (in the latter case, $S_x = S_x \cap \Omega = S_x \cap (\Omega - S_y + S_y) = S_x \cap (\Omega - S_y) + S_x \cap S_y$, so that $S_x \cap S_y = S_x + (S_x \cap \mathcal{O})$). Note also that $\frac{1}{2}\langle \lambda_{ij'}, \lambda \rangle + 1 \equiv \frac{1}{2}\langle \lambda_{ij}, \lambda \rangle \equiv ij$ in $S_x + 1 \equiv ij$ in $S_y + 1 \pmod 2$ in either case.

Definition. For an integer n, define $\Lambda(n) = \{\lambda \in \Lambda \mid$ every coordinate of λ is in $n\mathbb{Z}\} = \Lambda \cap \sum_{i \in \Omega} n\mathbb{Z} x_i$.

Lemma 2.4. *Let* $\lambda \in \Lambda_2^2$, $S \in \mathcal{C}$ *and* $\xi = \sum_{i \in S \cap \mathcal{O}_\lambda} 2x_i \pmod{\Lambda(4)}$. *If* $S \cap \mathcal{O} \neq \mathcal{O}, \emptyset$, *then* $\sum_{\substack{\mathrm{supp}(\zeta) = \mathcal{O} \\ \tilde{\zeta} \in \tilde{\Lambda}_2}} (-1)^{\langle \zeta, \xi \rangle} = 0$. (*Note that* ξ *lies in* Λ *if and only if* $S \cap \mathcal{O} = \mathcal{O}$ *or* $\emptyset$.)

Proof. Suppose $\xi = \sum_{i \in S \cap \mathcal{O}_\lambda} 2x_i + \eta$, where η is an integral vector, $\mathrm{supp}\,\eta \cap \mathcal{O}_\lambda = \emptyset$. Let $|S \cap \mathcal{O}_\lambda| = 2a$, $1 \leqq a \leqq 3$. Choose some index $k \in \mathcal{O}_\lambda - S$ and normalize our choices of $\zeta \in \tilde{\zeta}$ with $\mathrm{supp}\,\zeta = \mathcal{O}_\lambda$ to have positive coordinate at k. Given $b \in \{0, 1, \ldots, 2a\}$, the number of ζ with positive kth coordinate and with exactly b positive coordinates over $S \cap \mathcal{O}_\lambda$ is $\binom{2\mathrm{a}}{\mathrm{b}} 2^{6-2a}$. For such a ζ, $\langle \zeta, \xi \rangle = \frac{1}{8}[4b - 4(2a - b)] = b - a$. Therefore,

$$\sum_{\zeta} (-1)^{\langle \zeta, \xi \rangle} = \sum_{b=0}^{2a} (-1)^{b-a} \binom{2a}{b} 2^{6-2a} = 0,$$

as required.

Now for the general case: $\xi = \sum_{i \in S \cap \mathcal{O}_\lambda} 2x_i + \mu + \eta$, where η is an integral vector, $\mathrm{supp}\,\eta \cap \mathcal{O}_\lambda = \emptyset$, $\mu \in \Lambda(4)$. If μ has exactly c coordinates in $4 + 8\mathbb{Z}$ over $\mathcal{O}_\lambda$, then $(-1)^{\langle \zeta, \xi \rangle} = (-1)^{c + \langle \zeta, \delta - \mu)}$. The previous case may now be applied.

Lemma 2.5. *Let R be a commutative ring, G a finite group, H a subgroup and $M = R[G/H]$ the permutation for RG based on the right cosets of H. Then, regarding R as a trivial module,*

(i) $H^n(G, M) \cong H^n(H, R)$ *for all* $n \geqq 0$; *and*

(ii) *if* $\mathrm{Hom}(H/H', R) = 0$, $H^1(G, M) = 0$.

Proof. (i) Since $M = R \underset{RM}{\otimes} RG$ is an induced ($=$coinduced) module for the finite group G, (i) is a special case of Shapiro's lemma; see [39].

(ii) This follows from (i) since $H^1(H, R) \cong \mathrm{Hom}(H/H', R)$; see [39].

Lemma 2.6. *Let G be a finite group and M a vector space affording a real orthogonal representation of G. Let $\{x_i\}$ be an orthonormal basis. Invariant positive definite inner products for G on $M \otimes M$, $S^2 M$ and $\bigwedge^2 M$ are given by*

(i) $(x_i \otimes x_j, x_k \otimes x_l) = \delta_{ik}\,\delta_{jl}$,

(ii) $(x_i x_j, x_k x_l) = \delta_{ik}\,\delta_{jl} + \delta_{il}\,\delta_{jk}$,

(iii) $(x_i \wedge x_j, x_k \wedge x_l) = 2\delta_{\{i,j\},\{k,l\}}(-1)^{\delta_{ik}}$.

Proof. (i) is easy to check. Write $M \otimes M = S^2 M \otimes \bigwedge^2 M$. Then $S^2 M$ is spanned by all $x_i x_j = x_i \otimes x_j + x_j \otimes x_i$ and $\bigwedge^2 M$ is spanned by all $x_i \wedge x_j = x_i \otimes x_j - x_j \otimes x_i$. Thus the direct sum is orthogonal, and it is easy to deduce (ii) and (iii). Since the form on $M \otimes M$ is positive definite, the same is true for the forms on $S^2 M$ and $\bigwedge^2 M$.

Lemma 2.7. *Let G_0 be a finite group and A, B and C be self-dual $\mathbb{Q}G_0$-modules, all with G_0-invariant bilinear forms, written $(\ ,\ )$. There is an isomorphism $\mathrm{Hom}_{\mathbb{Q}G_0}(A \otimes B, C) \cong \mathrm{Hom}_{\mathbb{Q}G_0}(A, B \otimes C)$ such that if f and g are corresponding maps, then $(f(a \otimes b), c) = (g(a), b \otimes c)$. Furthermore, if A, B and C are absolutely irreducible, the multiplicity of C in $A \otimes B$ equals that of A in $B \otimes C$.*

Proof. This is a variant of the adjointness property of Hom and $\otimes$. Let $f \in \mathrm{Hom}_{\mathbb{Q}G_0}(A \otimes B, C)$. Define $\vec{f} \in \mathrm{Hom}_{\mathbb{Q}G_0}(A, B \otimes C)$ by $(\vec{f}(a), (b \otimes c)) = (f(a \otimes b), c)$. For $g \in \mathrm{Hom}_{\mathbb{Q}G_0}(A, B \otimes C)$, define $\overleftarrow{g} \in \mathrm{Hom}_{\mathbb{Q}G_0}(A \otimes B, C)$ by $(\overleftarrow{g}(a \otimes b), c) = (g(a), b \otimes c)$. The rest is an exercise.

Lemma 2.8. *Let χ be a complex character of the group G afforded by the module M. Then $S^3 M$ affords the character*

$$g \mapsto \tfrac{1}{6}\{\chi(g)^3 + 3\chi(g^2)\,\chi(g) + 2\chi(g^3)\}.$$

Proof. We may assume that $G = \langle g \rangle$. If $x_1, \dots, x_n$ is a basis of eigenvectors for the action of g on M, then all distinct $x_i x_j x_k$ form a basis for $S^3 M$. The result follows by studying the eigenvalues which occur.

Lemma 2.9. *Let R be a subring of $\mathbb{C}$. If the RG-module M has an R-valued invariant symmetric bilinear form $(\ ,\ )$, then a G-invariant map $S^2 M \to M$ satisfies the associative law $(ab, c) = (a, bc)$ for a, b, $c \in M$, if and only if there is a G-invariant map $f\colon S^3 M \to R$ which satisfies $f(a, b, c) = (ab, c)$.*

Proof. Exercise.

Lemma 2.10. *Let $\bar{G}\cong Suz$ and let $1\to\mathbb{Z}_2\to G\xrightarrow{\pi}\bar{G}\to 1$ be nonsplit. In the notation of* [4], (16.5), *an element of $e^{\pi^{-1}}$ has order* 4 (*e is an involution inducing a graph-field automorphism on a standard component of type $L_3(4)$ in $\bar{G}$*).

Proof. Since $|e|=2$, there are two possible conjugacy classes of $\bar{G}$ which might contain e. If the Lemma is false, then $C_G(e)$ looks like $2_-^{1+6}\cdot U_4(2)$. In the notation of [4], (16.5), $L\cong L_3(4)$ and $C_L(e)\cong PSU(3,2)=\mathbb{Z}_3^2\cdot Q_8$. The group $C_L(e)$ cannot be embedded in $C_G(e)$ since the smallest faithful $\mathbb{F}_2$-representation of $C_L(e)$ has dimension 8, a contradiction. The Lemma follows.

Lemma 2.11. (i) $H^1(\cdot 1,\mathbb{F}_2)=0$ (ii) $H^1(\cdot 1,\Lambda/2\Lambda)=0$; *in fact any module extension of $\Lambda/2\Lambda$ by $\mathbb{F}_2$ is split.*

Proof. (i) is obvious since $\cdot 1$ is perfect. (ii) may be proved by using the vanishing theorem of Alperin and Gorenstein [1]. Their hypotheses require a collection of subgroups $\mathscr{L}$ of $\cdot 1$ which satisfies (a) $H^0(L,\Lambda/2\Lambda)=0$ and $H^1(L,\Lambda/2\Lambda)=0$ for $L\in\mathscr{L}$; (b) $\cdot 1$ is generated by the subgroups of $\mathscr{S}$ (c) given $L_1,L_2\in\mathscr{S}$, there is $L\in\mathscr{L}$ with $L\leqq L_1\cap L_2$. We let $\mathscr{L}=\{A_1\times A_2,\ C(A_1),\ C(A_2)\}$, where $A_1\cong A_2\cong\mathbb{Z}_3$, $H^0(A_i,\Lambda/2\Lambda)=0$ for $i=1,2$, and $C(A_1\times A_2)=3.3.U_4(3)$ (see [11], p. 242 and 247). The groups $C(A_i)$ are perfect central extensions, 3. Suz. We get (a) for $\mathscr{L}$ from [14] or [58], (c) is obvious, and (b) may be proved in the following way. Let Y be the group generated by the elements of $\mathscr{L}$. We claim that Y and $\cdot 1$ both have involutions with centralizers of the shape $2_+^{1+8}\cdot D_4(2)$. Then [56] may be quoted to get $Y=\cdot 1$. Let $z\in\cdot 1$ be an involution with centralizer C of shape $2_+^{1+8}\cdot D_4(2)$. Without loss, we may arrange $A_1\times A_2\leqq C$ and $C_C(A_i)\cong 2_-^{1+6}\cdot U_4(2)$. An easy calculation in the group $D_4(2)$ shows that $C=\langle C_C(A_1), C_C(A_2)\rangle$, and we are done.

Lemma 2.12. (i) $|\Lambda:\Lambda(2)|=2$,

(ii) $|\Lambda:\Lambda(4)|=2^{13}$,

(iii) $|\Lambda:\Lambda(4)+2\Lambda|=2^{12}$,

(iv) $|\Lambda:\Lambda(8)|=2^{36}$,

(v) $|\Lambda:\Lambda(8)+2\Lambda|=2^{23}$.

Proof. (i) is clear. If $\{v_i|i\in\Omega\}$ is a basis for Λ, $\{2v_i|i\in\Omega\}$ is a basis for 2Λ. Let us take such a basis with $\{v_i|i\in\Omega, i\neq\infty\}$ in $\Lambda(2)$. Then $\Lambda(4)\cap 2\Lambda=\operatorname{span}\{4v_\infty, 2v_i|i\in\Omega\}$. It is clear that $\Lambda(4)$ is spanned by all $4x_i\pm 4x_j$, $i,j\in\Omega$. Since $8x_i\equiv 8x_j(\operatorname{mod}2\Lambda)$ for $i\neq j$ and $8x_i\notin 2\Lambda$, (v) is clear. The only linear dependence relations among the $4x_i+4x_j$ modulo $2\Lambda+\Lambda(8)$ have the form $\sum_{\{i,j\}}4x_i+4x_j\equiv 0(\operatorname{mod}2\Lambda+\Lambda(8))$, where $\sum_{\{i,j\}}\{i,j\}=S\in\mathscr{C}$ in $P(\Omega)$. Therefore, $\dim\Lambda(4)/2\Lambda+\Lambda(8)=23-12=11$, which, with (v), proves (ii) and (iii). For $x\in\Lambda(8)$, let $I(x)=\{i\in\Omega|\text{the } i^{\text{th}} \text{ coordinate of } x \text{ is in } 8+16\mathbb{Z}\}$. Easily, $M=\{x\in\Lambda(8)|I(x)\text{ is even}\}=2\Lambda(4)$ and $|\Lambda(8):M|=2$, proving (iv).

Lemma 2.13. *Let $G\cong M_{12}$, V the $\mathbb{F}_2G$-permutation module on the right cosets of $G_0<G$, $G_0\cong M_{11}$. Then $H^1(G,V)=0$, $H^1(G,[V,G])\cong\mathbb{Z}_2$ and $H^1(G,V/C_V(G))\cong\mathbb{Z}_2$.*

Proof. By Lemma 2.5, $H^1(G, V) \cong H^1(G_0, \mathbb{Z}_2) = 0$. Also, from $0 \to [V, G] \to V \to \mathbb{Z}_2 \to 0$ and the long exact cohomology sequence, we get $0 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \to H^1(G, [V, G]) \to 0$, whence $H^1(G, [V, G]) \cong \mathbb{Z}_2$. Likewise, from $0 \to \mathbb{Z}_2 \to V \to V/C_V(G) \to 0$, we get an exact sequence

$$0 = H^1(G, V) \to H^1(G, V/C_V(G)) \to H^2(G, \mathbb{Z}_2) \to H^2(G, V).$$

By [7], $H^2(G, \mathbb{Z}_2) \cong \mathbb{Z}_2$ and, by Lemma 2.5, $H^2(G, V) \cong H^2(G_0, \mathbb{Z}_2)$, which is 0, by [7]. So $H^1(G, V/C_V(G)) \cong \mathbb{Z}_2$.

Lemma 2.14 (Goldschmidt [26]). *Let Hypothesis* (*) *consist of the following assumptions:*

(a) *$T \in Syl_2(G)$, G a finite group,*
(b) *W is a weakly closed subgroup of T with respect to G,*
(c) *A is an abelian normal subgroup of $N_G(W)$ and $A \leqq C_T(W)$,*
(d) $\mathscr{S} = \{B \leqq T \mid B \underset{G}{\leqq} A, B \nleqq A\}$,
(e) $r = \max\{m(B/C_B(W)) \mid B \in \mathscr{S}\}$.

Assume (*). Then the following hold: (i) If $B \leqq T$ and $B \underset{G}{\leqq} A$, then $C_B(W) = B \cap A$ and there is $g \in G$ such that $B^g \leqq A$ and $N_T(B)^g \leqq T$.

(ii) Either $\Omega_1(A)$ is a strongly closed abelian subgroup (whence the normal closure of $\Omega_1(A)$ in G is a described in Theorem A of [26]) or (ii.1) there is $B \in \mathscr{S}$ with $m(B) + r \geqq m(A)$; and (ii.2) if t is an involution of T with $t \underset{G}{\in} A$, then $m([A, t]) \leqq 2r$, and if $B/C_B(W)$ is elementary abelian for all $B \in \mathscr{S}$ which satisfy (ii.1), then $m([A, t]) \leqq r$.

Lemma 2.15 (N.J. Patterson [56]). *Let $T \in Syl_2 \bar{N}_{24}$ where $\bar{N}_{24} \leqq \cdot 1$ and $\bar{N}_{24}$ is the image of N_{24} in $\cdot 1$. Then (i) the 2-rank of T is* 11; (ii) *$O_2(\overline{N_{24}})$ is the unique subgroup of T isomorphic to $\mathbb{Z}_2^{11}$.*

Lemma 2.16 (Steve Smith [63]). *If G_0 is a finite group containing an involution z such that $O_2(C_{G_0}(z)) \cong 2_+^{1+24}$, $C_G(O_2(C_{G_0}(z))) = \langle z \rangle$ and $C_{G_0}(z)/O_2(C_G(z)) \cong \cdot 1$, then either (i) there is an involution $t \in O_2(C_{G_0}(t))$ such that $C_{G_0}(t) \cong \hat{F}_2$ and $|G_0| = 2^{46} 3^{20} 5^9 7^6 11^2 13^3 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$; or* (ii) *$G_0 = 0(G_0)\, C_{G_0}(z)$.*

Lemma 2.17. *Let V be any faithful $\mathbb{F}_2 M_{23}$-module of dimension* 11. *Then $H^1(M_{23}, V) = 0$.*

Proof. Imitate the proof of Lemma 9.1 from [33].

Lemma 2.18. *Let H be a finite group with the following properties*

(i) $H/O_2(H) \cong M_{23}$,
(ii) $Z(O_2(H)) \cong \mathbb{Z}_2$,

(iii) *the set of chief factors of H within $O_2(H)$ consists of one trivial module, one factor isomorphic to $\mathscr{C}$ and one to $\mathscr{C}^* \cong P(\Omega)_{\text{even}}/\mathscr{C}$.*

(iv) $H = H'$.

Then H has trivial multiplier.

Proof. Since M_{23} has trivial multiplier [7], the only prime to examine here is 2. Let $\tilde{H}$ be a covering group of H. By Lemma 2.17 and $H^2(M_{23}, \mathbb{Q}/\mathbb{Z})=0$, the only trivial chief factors within $O_2(\tilde{H})$ occur within $O_2(\tilde{H})'$. Since $\mathscr{C}$ and $\mathscr{C}^*$ are absolutely irreducible and not selfdual, $|O_2(\tilde{H})' \cap Z(O_2(\tilde{H}))| \leqq 2$. This proves the Lemma.

Lemma 2.19. *Suppose that F is a field and that $G=NL$ is a finite group, $N \lhd G, L \leqq G$ and $N \cap L \leqq Z(L)$. Suppose that M is a finite dimensional FG-module, faithful for G, such that the restriction to FL is absolutely irreducible. Suppose that $n=\dim_F M, N \lhd G$ and that L has no proper subgroup of index $\leqq n$. Assume that $L_1=L/Z(L)$ is simple,* $\min\{\dim M_1 \mid M_1$ *is a finite dimensional E-vector space and L_1 is involved in* $\mathrm{Aut}_E(M_1)\} \geqq n$ *for all algebraically closed fields E, and, whenever P is a p-subgroup of N with L_1 involved in* $\mathrm{Aut}\, PM_1)\} \geqq n$ *for all algebraically closed fields E, and, whenever P is a p-subgroup of N with L_1 involved in* $\mathrm{Aut}\, P$, *P is abelian.*

Then N is scalar on M.

Proof. We may assume N is not scalar on M and that F is algebraically closed. Let $p \in \pi(N)$, $S \in \mathrm{Syl}_p(N)$, $S \nleqq Z(G)$. Then $N_G(S)$ covers G/N. If S is nonabelian, $C_G(S)$ is nonsolvable and involves L_1. One of our hypotheses on L_1 forces $C_G(S)$ to act irreducibly on M, whence S is scalar, a contradiction. If S is abelian but not scalar on M, the above argument shows that the action of $N_G(S)$ on S involves L_1. Then Clifford Theory applied to $1 \neq S \lhd N_G(S)$ plus the fact that L_1 has no proper subgroup of index n or less gives us the required contradiction.

Lemma 2.20. (i) *A proper subgroup of $D_4(2)$ has index at least* 28.

(ii) *Let $G=\cdot 0$ and let H be a proper subgroup. Then $|G:H| \geqq 832$.*

(iii) *In the notation of Lemma* 2.19. $\min_E \min \dim\{M_1 \mid \ldots\}$ *is* 8 *for* $D_4(2)$ *and* 24 *for* $\cdot 1$. *Also, $(L_1, n) \neq (D_4(2), 8)$, $(\cdot 1, 24)$ whenever a P arises with $P' \neq 1$ and L_1 involved in* $\mathrm{Aut}(P)$.

Proof. (i) Since $D_4(2)$ is simple, any proper subgroup of $D_4(2)$ fails to contain some $U_4(2)$-subgroup. Since the minimal index of a proper subgroup of $U_4(2)$ is 27 ([45], [17], p. 307), we get that if $H<G=D_4(2)$, then $|G:H| \geqq 27$. If $|G:H|$ is odd, H lies in a maximal parabolic, each of which has index 135. Thus $|G:H| \geqq 28$, as required.

(ii) If L is any subgroup of G such that $|L:L \cap H| \geqq 832$, we are done. We may suppose that $|G:H|<832$. Without loss, $Z(G) \leqq H$. Let bars denote images modulo $Z(G)$.

Take $L_1 \leqq L \leqq G$, $L_1=U_3(4)$, $L \cong 2G_2(4)$. Suppose $L_1 \nleqq H$. Since $|L_1| = 2^6.3.5^2.13$ and $|L_1|/832=75$, $H \cap L_1$ can not have odd order (an easy exercise). So, whether L_1 lies in H or not, H contains an elementary abelian 2-group $F \neq 1$ of L_1. Note that $\bar{F}$ lies in a root group in $\bar{L} \cong G_2(4)$, for a long root.

We now set $H_0 := \langle\{F^g \mid F^g \leqq H, g \in L\}\rangle$. If $O_2(\overline{H \cap L}) \neq 1$, $H \cap L_1$ lies in a maximal parabolic of L, whence $|L:L \cap H| \geqq 1365$, a contradiction. So, $O_2(\overline{H \cap L})=1$. Since $(\bigcup_{g \in L} F^g)^\#$ is a class of $\{4, \mathrm{odd}\}^+$-transpositions, of a theorem of Timmesfeld [72] identifies $\bar{H}_0 \leqq \overline{H \cap L}$, as $SL(2,4)$, $SL(3,4)$, $U_3(4)$ or $G_2(4)$. Since $|G_2(4)|/2|U_3(4)| = 2016 > 832$ and $|G_2(4)|/2|SL(3,4)| = 2080 > 832$, it is easy to deduce $L \leqq H$ from this.

This argument shows that H must contain every conjugate of L, whence $H = G$ is not proper. This contradiction proves the result.

(iii) Define $m_1(p) = \min\{\dim M_1 \mid M_1$ is a finite dimensional $\bar{\mathbb{F}}_p$-vector space and L_1 is involved in $\mathrm{Aut}_{\bar{\mathbb{F}}_p}(M_1)\}$, and let M_1 be such a module with $\dim_{\bar{\mathbb{F}}_p} M_1 = m_1(p)$. Then M_1 is irreducible.

Say $L_1 = D_4(2)$, $m_1 = m_1(p) \leqq 7$ for some $p > 0$. Then there is $A \leqq GL(m_1, \bar{\mathbb{F}}_p)$, and $B < A$ with $A/B \cong L_1$. Let A be of least order. Then, by a Frattini argument, B is a nilpotent p'-group. If $B \nleqq Z(A)$, (i) and the fact that $\bar{\mathbb{F}}_p$ is algebraically closed imply that every characteristic abelian subgroup of B is cyclic, whence B is as described by P. Hall's theorem ([27], p. 198). The bound $m_1 \leqq 7$ implies that the only nonsolvable composition factors of $\mathrm{Aut}(B)$ are various $PSL(2,r)$. Thus, $C_A(B)$ involves L_1, i.e., $B \leqq Z(A)$, whence $A \cong D_4(2)$ or $2D_4(2)$. If $p \neq 2$, a restriction of the representation to a $2.2^6.A_8$ subgroup gives a contradiction to $m_1 \leqq 7$. So, $p = 2$, and consideration of a $(3 \times U_4(2))2$ subgroup of $D_4(2)$ shows that $U_4(2)2$ or $2U_4(2)2$ must act faithfully in dimension 5, or $U_4(2)$ must act faithfully in dimension 3. These situations are eliminated by looking at the subgroups $3^{1+2}.GL(2,3)$ and a Frobenius group of order 20 in $\Sigma_6 \leqq \mathrm{U}_4(2)$.

Say $L_1 = \cdot 1$, $m_1 = m_1(p) \leqq 23$. As above, we get A quasisimple with $A/Z(A) \cong L_1$ in $GL(m_1, \bar{\mathbb{F}}_p)$. If $p \neq 2$, we see that neither N_{24} or $N_{24}/Z(N_{24})$ may be embedded in $GL(m_1, \bar{\mathbb{F}}_p)$ since the noncentral abelian normal subgroup of either group does not have an N_{24}-conjugacy class of fewer than m_1 hyperplanes. So, $p = 2$, and we get a similar contradiction by considering the subgroup $(3^6.2M_{12}) \times \langle -1 \rangle$ in .0.

Suppose that a nonabelian p-group P arises as in Lemma 2.15. By (i) and P. Hall's theorem ([27], p. 198), $P = \Omega_1(P)$ may be assumed extraspecial or of shape $2_\varepsilon^{1+2k} \circ \mathbb{Z}_4$. Since L is absolutely irreducible on M, p divides $n = \dim M$ and $p \neq \mathrm{char}\, F$ (M is our F-vector space). If $(L_1, n) = (D_4(2), 8)$, then $p = 2$. The structure of $\mathrm{Aut}\, P$ [31] forces $k \geqq 4$, whence $p^k = 16$ divides n, contradiction. If $(L_1, n) = (\cdot 1, 24)$, $p = 2$ or 3. If $p = 3$, $P \cong 3^{1+2}$ and $\mathrm{Aut}\, P$ is solvable, a contradiction. If $p = 2$, $P \cong 2_\varepsilon^{1+2k}$ or $2_\varepsilon^{1+2k} \circ \mathbb{Z}_4$, then $k \leqq 4$, a contradiction to an earlier part of (iii).

Proposition 2.21. *Let p be a prime, $p \geqq 5$, and let $\psi\colon \cdot 0 \to O(24,2)$ be the homomorphism associated with the natural action of $\cdot 0$ on $\Lambda/2\Lambda$. Then $\mathscr{X} := \{X \leqq O(24,2) \mid X$ contains $(\cdot 0)\psi$ and X has a projective representation on $\bar{\mathbb{F}}_p^{24}$ which is nontrivial on $(\cdot 0)\psi\}$ is just $\{(\cdot 0)\psi\}$.*

Proof. Let $\tilde{H} := (\cdot 0)^\psi < \tilde{G} \leqq \Omega(24,2)$, $\tilde{G} \in \mathscr{X}$ and G a central extension of $\tilde{G}$ with the relevant faithful representation on $\bar{\mathbb{F}}_p^{24}$. Let H be the subgroup of G isomorphic to $\cdot 0$ and mapping onto $\tilde{H}$ and let M be the relevant $\bar{\mathbb{F}}_p G$-module. Let $z \in H$ be an involution with eigenvalues $\{-1^{16}, 1^8\}$ and set $Q_0 := O_2(C_H(z)) \cong 2_+^{1+8} \times 2$; $\langle z \rangle = Q_0'$.

Let us set $C_1 := C_G(Q_0)$. Let C_1^ε be the group of linear transformations induced by C_1 on the ε eigenspace M_ε for z, $\varepsilon = +, -$; we have $\dim M_- = 16$,

$\dim M_+ = 8$. Then C_1^- must induce scalars since Q_0 is absolutely irreducible on M_-. By applying Clifford theory to C_1^+, normalized by the image $C_H(z)^+$ of $C_H(z)$ in $GL(M_+)$, we get that C_1^+ is scalar on M_+ (see Lemmas 2.19 and 2.20) or else $C_1^+ \cap C_H(z)^+ \geqq (C_H(z)^+)'$. Thus, C_1 is abelian of rank 2 and induces scalars on M_+ and M_-, or else C_1^+ contains a linear group $2D_4(2)$ on M_+. We eliminate the second alternative by looking at the action of G on V, a 24-dimensional $\mathbb{F}_2$-space on which H and G act as subgroups of the orthogonal group. Each term of the series $V > [V, Q_0] > [V, Q_0, Q_0] > 0$ has codimension 8 in the previous one [36]. Since $[Q_0, C_1] = 1$, the $P \times Q$ lemma ([27], p. 179) implies that $O^2(C_1)$ are nontrivially on $C_V(Q)$, which must be absolutely irreducible for $O^2(C_1)$, by Lemma 2.20(iii). Similarly, $O^2(C_1)$ is nontrivial on each factor of the above series since $[Q_0, C_1] = 1$. However, by absolute irreducibility, the subgroup of Q_0 commutating trivially, one factor to the one k steps lower must have index at most 2^k in Q_0. Consequently, a subgroup of index 2^3 in Q_0 acts trivially on V, which is absurd.

We conclude that C_1 is abelian of rank 2 and induces scalars on M_+ and M_-.

Let $Q := C_{Q_0}(M_+)$, $R := O_2(QC_1)$; $QC_1 = O(QC_1) \times R$. We set $H_1 := N_G(R)$. Possibly, $Q \lhd H_1 \leqq N_G(Q)$ although $Q \lhd H$ and $R \cong Q \circ \mathbb{Z}_4$, among other things, might be the case. We want to prove that $Q \lhd H_1$. Suppose $Q \ntriangleleft H_1$. Since $R' = Q' = \langle z \rangle$, H_1 acts on both M_+ and M_- and so $Q \leqq R_+ := C_R(M_+) < H_1$. The normal closure of Q in H_1 is $R_0 := QR_1$, $R_1 := Z(R_0)$ is cyclic, $|R_1| = 4$ and $R_0 = \Omega_1(R_+) \cong (2_+^{1+8}) \circ \mathbb{Z}_4$. Let $A := N_G(R_0)/R_0 C_G(R_0)$. Then A contains a natural copy of $D_4(2)$ (fixing Q) and A is embedded (by φ, say) into $\mathrm{Out}(R_0)' \cong Sp(8,2)$. Let $\mathcal{Y}$ be the set of 256 maximal subgroups of R_0 not containing R_1. Every member of $\mathcal{Y}$ is an extraspecial group of order 2^9. Let $\mathcal{Y}^\varepsilon$ be the set of elements of $\mathcal{Y}$ of ε type ($\varepsilon = +$ or $-$). The action of $\mathrm{Out}(R_0)' \cong Sp(8,2)$ is transitive on each set $\mathcal{Y}^+, \mathcal{Y}^-$ with point-stabilizers $G_X, X \in \mathcal{Y}$, natural $D_4(2).2$, ${}^2D_4(2).2$ subgroups, respectively (this follows from the definition of $\mathrm{Aut}(R_0)$; see [31] for more details), and a calculation ([27], p. 491) shows that $|\mathcal{Y}^+| = 136$, $|\mathcal{Y}^-| = 120$.

Furthermore, if $X \in \mathcal{Y}$, the stabilizer of X has two orbits on $\mathcal{Y} - \{X\}$ (reason: the orthogonal group G_X stabilizing X is transitive on the set of nonidentity cosets of $Z(X)$ which contain involutions and on the set of cosets which do not, and the mapping $Y \in \mathcal{Y} - \{X\}$, $Y \mapsto Z(X \cap Y)$, sets up a G_X-equivariant bijection between $\mathcal{Y} - \{X\}$ and $(X/Z(X))^\#$).

So, G_Q has orbits of length $1, 135$ on $\mathcal{Y}^+$, whence $Q \ntriangleleft H_1$ gives $|A^\varphi| \geqq (2^{12}.3^5.5^2.7)(2^3.17) \geqq \frac{1}{2}|Sp(8,2)|$ and so $A \doteq Sp(8,2)$, as $Sp(8,2)$ is simple.

Now let H_1^ε be the linear group induced by H_1 on M_ε, $\varepsilon = +, -$. At once, $H_1^+/Z(H_1^+) \cong Sp(8,2)$. Since the Schur multiplier of $Sp(8,2)$ is trivial [64], $(H_1^+)' \cong Sp(8,2)$. But then, the perfect group $2D_4(2)$ cannot be embedded in $(H_1^+)'$, a contradiction. So, $Q \lhd H_1 = N_G(Q)$, as desired.

The next step in the argument is to show that $H_1 = C_G(z)$. Let $H_2 := C_G(z)$, $H_3 = C_{H_2}(M_+)$. Our results prove $R \cap H_3 \in \mathrm{Syl}_2(H_3)$. Since $H_3/Z(H_3)$ has abelian Sylow 2-subgroups, the action of H_1 on Q and the classification of such groups [75] imply that H_3 is solvable of 2-length 1. We are done if $Q \lhd H_3$, so assume otherwise. Then $[O(H_3), Q] \neq 1$. Since $O(H_3)\, N_G(Q)$ acts absolutely irreducibly on the 16-dimensional space M_-, Clifford theory implies that $O_p(H_3) = 1$ and $O(H_3)$ is abelian. Then Lemma 2.20(i) and the fact that $Q/Z(Q)$ is an irreducible module of order 2^8 for $N_G(Q)$ imply that $O(H_3)$ is scalar on M_-, a contradiction.

We argue that $C_1 = \langle C_0, z\rangle$, where C_0 consists of scalar transformations on M. Choose $T \leqq H_1$, $T \cong \mathbb{Z}_2^{12}$ such that $N_1 := N_H(T)$ is the group N_{24}, i.e., $N_1 = TN_0$, $N_0 \cong M_{24}$. Then $C_1 \leqq C(T)$, an abelian group, since T operates on M with 24 distinct linear characters. Since $H_1 \neq C_G(z)$, $C_G(T) = C_{H_1}(T) = TC_1$. The action of N_0 on TC_1, and the fact that C_1 has rank 2 implies that $O(C_1)$ is scalar and that $\mho^1(O_2(C_1)) \cap T$ is scalar on M. By [33], 9.3, $O_2(C_1) = TT_1$ as a $\mathbb{Z}N_0$-module, where T_1 is scalar. So, $C_0 = O(C_1)\, T_1$ has the requisite property.

It follows from the above that $H_1 = N_G(Q) = N_G(R) = C_G(z)$ and $H_1/QC_0 \cong D_4(2)$ or $D_4(2).2$. We shall prove that if $H_1/QC_0 \cong D_4(2)2$, G has a normal subgroup of index 2. We have that $H_1' \cong (2 + 2_+^{1+8})\, D_4(2)$.

Suppose $H_1/QC_0 \cong D_4(2).2$. Let $S \in \mathrm{Syl}_2(H_1) \subseteq \mathrm{Syl}_2(G)$ (because $\Omega_1(Z(S)) = Z(Q_0)$) and set $S_0 := S \cap H_1' C_0$, a maximal subgroup of S. Define $2^a = \min\{|g| \mid g \in S - S_0\}$. An easy variation of the Thompson transfer lemma ([70], 5.38) says that if $g \in S - S_0$, $|g| = 2^a$ and $G = O^2(G)$, then g fuses in G to an element of S_0.

Let us suppose that $G = O^2(G)$ and produce a contradiction. Let $t \in S - S_0$ be an element which induces a transvection on $Q/Z(Q)$ and, among all such elements, has least possible order, say $2^b \geqq 2$. Choose a conjugate t_1 of t in $N_G(Q)$ such that $\langle t, t_1\rangle$ induces a natural $O^-(2,2) \cong \Sigma_3$ on $Q/Z(Q)$. Let $P \in \mathrm{Syl}_3(\langle t, t_1\rangle)$, $|P| = 3$. Then $\langle Q, P\rangle = [Q, P]\, P \times C_Q(P)$ and $[Q, P] \cong Q_8$. Recall that $p \neq 3$. Each eigenvalue for a generator h of P on M_- occurs with multiplicity 8 (since $C_Q(P)$ effects the linear group 2_-^{1+6} on M_-), and h is conjugate to h^{-1} in H_1'; so ω and ω^{-1} are these eigenvalues, where $\omega^3 = 1 \neq \omega \in \mathbb{F}_p$. Thus t has trace 0 on M_-. List the eigenvalues of t: $\{a_1, a_2, \ldots\}$ with multiplicities $m_1, m_2, \ldots$, indexed so that $a_{2i+1} = -a_{2i+2}$, $i = 0, 1, \ldots$. We have $m_{2i+1} = m_{2i+2}$ for $i = 0, 1, \ldots$. On M_+, H_1 induces a linear group $2D_4(2)$ and, on it, t centralizes an $Sp(6,2) \times \mathbb{Z}_2$ subgroup. So, on M_+, t has eigenvalues $\{c, c, c, c, c, c, c, c'\}$, $c \neq c'$. Let I, J be the set of i for which m_i is even, odd, respectively.

We argue that (1) t has an eigenvalue with odd multiplicity, and (2) we may assume $b = a = 1$ or t^2 generates $O_2(C_0)$. If c or c' does not occur in $\{a_1, a_2, \ldots\}$, (1) holds, and if c or c' does occur, as a_i, say, and $i \in I$, this is so. We may assume that $c = a_j$, $c' = a_{j'}$, $\{j, j'\} = J$. Then $m_j = m_{j'}$ and $\sum_{i \in I}' m_i = 2 \pmod 4$, whence at least one partial sum $m_{2i+1} + m_{2i+2}$ is in $2 + 4\mathbb{Z}$. Since $m_{2i+1} = m_{2i+2}$, this is a contradiction proving (1). As for (2), if we let $O(C_1) \leqq K \leqq N_G(Q)$ be a group of odd order commuting modulo C_1 with $\langle t, P\rangle$ and satisfying $[Q, K] \cong 2_-^{1+6}$, a Frattini argument with $K \leqq \langle R, K, t\rangle$ shows that we may arrange for $t^2 \in C_R(K) = [Q, P]\, C_0$ and even $t^2 \in \langle z, C_0\rangle$. If $t^2 \in C_0$, (2) follows, so assume $t^2 \in zC_0$ and $b > a$. Then take $x \in C_Q(\langle P, t\rangle)$, $x^2 = z$ and replace t by tx^{-1}. Note that this adjustment does not affect (1).

Since (2) holds, we get that t is conjugate in G to $u \in S_0$ because $b = a$ holds or because the image of t in $G/Z(G)$ is an involution in case $\langle t^2\rangle = O_2(C_0)$.

Write $u = u_1 u_2$, $u_1 \in H'_1 = N_H(Q)$, $u_2 \in C_0$. The above discussion of eigenvalues for t shows that t has at least two eigenvalues with odd multiplicity. However, every 2-element of $H'_1 C_1 = H'_1 C_0$ has every eigenvalue with even multiplicity: this is so for $u_1 \in H'_1$, by [12], and is also true for $u \in H'_1 C_0$ as C_0 consists of scalar matrices. This contradiction proves that $G \neq O^2(G)$ if $H_1/QC_0 \cong D_4(2).2$.

In view of the last two paragraphs and the fact that $\mathrm{Out}(\cdot 1) = 1$, we may assume that G has no normal subgroup of index 2 and that $H_1/QC_0 \cong D_4(2)$. Then [56] may be quoted to obtain $G/Z(G) \cong \cdot 1$. This contradiction proves the Lemma.

Lemma 2.22. *The* 2-rank *of* $GL(n, 2)$ *is precisely* $\left[\frac{n}{2}\right]\left(n - \left[\frac{n}{2}\right]\right)$ *for* $n \geqq 2$.

Proof. This is easily checked for $n = 2$ and 3. Set $g(n) := \left[\frac{n}{2}\right]\left(n - \left[\frac{n}{2}\right]\right)$. Suppose $n \geqq 2$ and take $A \leqq GL(n+2, 2)$, $A \cong \mathbb{Z}_2^r$, r maximal. By Sylow's theorem, we may assume A lies in a subgroup QL of $GL(n+2, 2)$, $Q \cong 2^{1+2n}$, $L \cong GL(n, 2)$. Then $|A \cap Q| \leqq 2^{n+1}$ and, by induction, $|A/A \cap Q| \leqq g(n)$. So

$$r \leqq k := n + 1 + \left[\frac{n}{2}\right]\left(n - \left[\frac{n}{2}\right]\right).$$

Since

$$g(n+2) = \left(\left[\frac{n}{2}\right] + 1\right)\left(n + 2 - \left\{\left[\frac{n}{2}\right] + 1\right\}\right) = \left(\left[\frac{n}{2}\right] + 1\right)\left(n + 1 - \left[\frac{n}{2}\right]\right) = k,$$

we get $r \leqq g(n+2)$. The opposite inequality is needed to finish. To prove that $g(n)$ is the 2-rank of $GL(n, 2)$, we exhibit an appropriate subgroup. If V is the underlying vector space and W is a subspace of dimension $\left[\frac{n}{2}\right]$, the stability group of the chain $0 < W < V$ is elementary of order $2^{g(n)}$.

These results are contained in the Cambridge thesis of P.E. Smith in which the p-ranks of all groups of Lie type in characteristic p are determined.

Corollary 2.23. *The* 2-rank *of* M_{24} *is precisely* 6.

Proof. M_{24} and $GL(5, 2)$ have isomorphic Sylow 2-subgroups [41].

Lemma 2.24. *The* 2-rank *of* $\cdot 3$ *is at least* 4 *and at most* 6.

Proof. We shall show that $\cdot 3$ contains a subgroup H of odd index where $O_2(H) \cong \mathbb{Z}_2^4$, H is 2-constrained, $H/O_2(H) \cong GL(4, 2)$.

Let us assume the above and deduce the Lemma. Let $E \leqq H$, $E \cong \mathbb{Z}_2^r$, r maximal. Then $r \geqq 4$. Since the 2-rank of $GL(4, 2)$ *is* 4, (see Lemma 2.22), achieved by, say, all matrices of the shape

$$\left\{ \begin{pmatrix} 1 & 0 & a & b \\ & 1 & c & d \\ & & 1 & 0 \\ & & & 1 \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{F}_2 \right\},$$

the fact that $H/O_2(H)$ acts faithfully on $O_2(H)$ implies that $r \leqq 6$, as required.

Now to exhibit the subgroup H.

Let

$$\xi=4x_k-2x_i+\sum_{\substack{j\in\mathcal{O}\\ j\neq i}}2x_j$$

be our vector of type 3; here, $\mathcal{O}$ is an octad containing i and avoiding k. Let A be the subgroup of $M_{24}\leqq N_{24}$ stabilizing $\mathcal{O}$ and fixing k. Thus, $A\cong A_8$ and $A_i^*:=\{g\in A\mid x_i^g=x_i\}\cong A_7$. Clearly, $Y:=\{g\in N_{24}\mid\xi^g=\xi\}\leqq O_2(N_{24})A$ and $Y_1:=Y\cap O_2(N_{24})=\{\varepsilon_S\mid S\in\mathcal{C},\ S\cap\mathcal{O}=\emptyset$ and $k\notin S\}\cong\mathbb{Z}_2^4$. So, $Y_1A_i^*\leqq Y$ and $Y/Y_1\cong A_7$ or A_8. We prove that $Y/Y_1\cong A_8$. For $g\in A$, we obtain $y_g\in Y$ as follows. If $i^g=j\in\mathcal{O}$, take any $\mathcal{C}$-set $S=S_g$ such that $S\cap(\mathcal{O}\cup\{k\})=\{i,j\}$; easily, such an S exists, and if T is another candidate, ε_{S+T} is in Y_1. We set $y_g:=\varepsilon_S g\in Y$. At once, $Y/Y_1\cong A_8$.

Since Y_1 is a nontrivial module for A, the group Y serves as our H, and we are done.

Lemma 2.25. *Let $\Xi=\{T_1,\ldots,T_6\}$ be a sextet. The only $\mathcal{C}$-sets disjoint from $T_1+T_2+T_3$ are the octads T_i+T_j, $i,j\in\{4,5,6\}$, $i\neq j$, and ϕ.*

Proof. Clearly, all such nonempty $\mathcal{C}$-sets are octads. There are 30 octads disjoint from the octad T_1+T_2 and any two distinct such octads are disjoint or meet in a 4-set; see Table 2.1.1. Let $\mathcal{O}$ be an octad disjoint from $T_1+T_2+T_3$. Take any index $i\in\{4,5,6\}$ such that $\mathcal{O}\cap T_i\neq\emptyset$. Then $\mathcal{O}\cap T_i=\mathcal{O}\cap(T_3+T_i)$ must be a nonempty even set since T_3+T_i is an octad. If there is $k\in\{4,5,6\}$ such that $T_k\cap\mathcal{O}=\emptyset$, $\mathcal{O}=T_i+T_j$, as required. If there is no such k, $|T_j\cap\mathcal{O}|$ must be 2 for $j\in\{4,5,6\}$, by the basic property of sextets. This means $|\mathcal{O}|=6$, a contradiction.

Lemma 2.26. (i) *Let V be a linear subspace of $\mathcal{C}$ such that V contains no dodecad. Then* $\dim V\leqq 6$. *If V does not contain a pair of disjoint octads,* $\dim V\leqq 5$. *In any case, V lies in a subspace of one of the following shapes: $\langle\mathcal{O}_1\mid\mathcal{O}_1$ is an octad, $\mathcal{O}_1=\mathcal{O}$ or $\mathcal{O}_1\cap\mathcal{O}=\emptyset\rangle$, for some octad $\mathcal{O}$ (dimension* 6); *$\langle\mathcal{O}\mid\mathcal{O}$ is the sum of two tetrads in $\Xi\rangle$, for some sextet Ξ (dimension* 5).

(ii) *Let V and $\mathcal{O}$ be as above,* $\dim V=6$, *W the subspace of $O_2(N_{24})$ corresponding to V and $\bar{\Lambda}=\Lambda/2\Lambda$. Then $C_{\bar{\Lambda}}(W)=\langle\lambda_{ij},\lambda_{ij'},\lambda_{\mathcal{O}}\mid i,j\in\mathcal{O}\rangle+2\Lambda/2\Lambda$ has dimension* 8.

Proof. (i) Without loss, $\Omega\in V$. If $\mathcal{O}_1$ and $\mathcal{O}_2$ are distinct octads in V, $\mathcal{O}_1\cap\mathcal{O}_2$ is $\emptyset$ or a 4-set.

Suppose V contains no pair of disjoint octads. Take $\mathcal{O}_0\in V$, $\mathcal{O}_0$ an octad. Let X be the set of octads in V distinct from $\mathcal{O}_0$. For $\mathcal{O}\in X$ we have the 4-set $T_{\mathcal{O}}:=\mathcal{O}\cap\mathcal{O}_0$. Since no pairs of disjoint octads are present, the map $\mathcal{O}\mapsto T_{\mathcal{O}}$ is one-to-one. Let $T_i:=T_{\mathcal{O}_i}$, $i=1,2$ be two such distinct 4-sets. Suppose that they have odd intersection. Then $|\mathcal{O}_1+\mathcal{O}_2|\leqq 15$, whence $\mathcal{O}_1+\mathcal{O}_2$ is an octad in V. But then the cardinality of $(\mathcal{O}_1+\mathcal{O}_2)\cap\mathcal{O}_0=(\mathcal{O}_1\cap\mathcal{O}_0)+(\mathcal{O}_2\cap\mathcal{O}_0)$ is $2\pmod 4$, hence can not be 0, 4 or 8, a contradiction. If $T_1\cap T_2=\emptyset$, $\mathcal{O}_1+\mathcal{O}_2=\mathcal{O}_0$. The remaining possibility is that $T_1\cap T_2$ is a 2-set in T_1, of which there are $\binom{4}{2}=6$. It follows that the map $T_2 \mapsto T_1 \cap T_2$ is at most two-to-one, since $|T_{\mathcal{O}} \cap T_{\mathcal{O}'}|$ is even for all octads $\mathcal{O}$, $\mathcal{O} \in X$. So, $|X| \leqq 1+1+6.2=14$, whence $\dim V \leqq 5$.

We show that there exists an octad disjoint from every octad of V. To $\mathcal{O}_1$ and $\mathcal{O}_2$ there is associated a sextet $\Xi=\{T_1, \ldots, T_6\}$ with $T_1=\mathcal{O}_1-\mathcal{O}_2$, $T_2=\mathcal{O}_2-\mathcal{O}_1$, $T_3=\mathcal{O}_1 \cap \mathcal{O}_2$.

Suppose that every octad in V is a union of tetrads. Since V does not contain a pair of disjoint octads, at most 4 tetrads are involved, and we can produce our octad from 2 tetrads which remain.

We may assume that some $\tilde{\mathcal{O}} \in V$ is not a union of these tetrads. Then $\tilde{\mathcal{O}}$ contains no tetrad and so meets each of T_i, $i=1,2,3$, in a proper subset of T_i. Since $\tilde{\mathcal{O}}$ meets each of $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_1+\mathcal{O}_2$ in a 4-set, $|\tilde{\mathcal{O}} \cap T_i|=2$, $i=1,2,3$. Two points of $\tilde{\mathcal{O}}$ are unaccounted for. Take $k \in \{4,5,6\}$ such that $\tilde{\mathcal{O}} \cap T_k=\emptyset$. Since the intersection of any two $\mathscr{C}$-sets is an even set, each $|\tilde{\mathcal{O}} \cap (T_k+T_j)|$ is even, $j \in \{1, \ldots, 6\}$. So, there is $j \in \{4,5,6\}-\{k\}$ with $|\tilde{\mathcal{O}} \cap T_j|=2$. Define $\mathcal{O}^* := T_i+T_{i'}$, where $\{i, i', j\}=\{4,5,6\}$. Reindex so that $j=4$, $i=5$, $i'=6$.

We claim that if $\mathcal{O} \in V$, $\mathcal{O}$ an octad, $\mathcal{O} \neq \mathcal{O}^*$, then $\mathcal{O} \cap \mathcal{O}^*=\emptyset$. Suppose false for $\mathcal{O} \in V$. Define $I=\{i \mid i \leqq 4 \text{ and } T_i \cap \mathcal{O} \neq \emptyset\}$. Since $\mathcal{O} \cap \mathcal{O}^* \neq \emptyset$, $\mathcal{O} \cap (\mathcal{O}^*+\Omega)$ is a 4-set.

If there is some T_l, $T_l \subseteq \mathcal{O}$, then $\mathcal{O}=T_l+T_5$ or T_l+T_6; but then $\mathcal{O} \cap \tilde{\mathcal{O}}$ is a 2-set, contradiction. If there is $i \in I$ such that $|T_i \cap \mathcal{O}|$ is odd, all $|T_i \cap \mathcal{O}|$ are odd, hence equal 1, forcing $\mathcal{O} \cap (T_1+T_2)$ to be a 2-set, another contradiction. So, if $i \in I$, $\mathcal{O} \cap T_i$ is a 2-set, whence $|I|=2$. Take $i, j \leqq 3$, $i \in I$, $j \notin I$. Then $T_i+T_j \in V$ and $|\mathcal{O} \cap (T_i+T_j)|=2$, contradiction. So, $\mathcal{O}^*$ has the requisite properties.

Now to analyze the other situation. Let $\mathcal{O}_1$, $\mathcal{O}_2$ be a pair of disjoint octads in V. Since $\Omega \in V$, $\mathcal{O}_3 := \mathcal{O}_1+\mathcal{O}_2+\Omega$ is an octad in V. Say $\mathcal{O}_4 \in X := \{S \in V \mid S \text{ is an octad distinct from } \mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3\}$. There is $i \in \{1,2,3\}$ such that $\mathcal{O}_4 \subseteq \mathcal{O}_i+\Omega$. Reindex so that $i=1$. If every octad in X is disjoint from $\mathcal{O}_1$, $\dim V \leqq 6$; see Lemma 2.1. Let us suppose otherwise. Take $\mathcal{O} \in X$, $\mathcal{O} \cap \mathcal{O}_1 \neq \emptyset$. Set $\mathcal{O}_5 := \mathcal{O}_4+\mathcal{O}_1+\Omega$, $T_{kl} := \mathcal{O}_k \cap \mathcal{O}_l$, $k=2,3$, $l=4,5$; the four T_{kl} partition $\mathcal{O}_1+\Omega$, and are part of a sextet Ξ. Let us say that $\mathcal{O}$ contains none of the T_{kl}. For some $j \in \{2,3\}$, $\mathcal{O} \cap \mathcal{O}_j \neq \emptyset$, whence $T_{jl} \cap \mathcal{O} \neq \emptyset$, $l=4,5$ (see Lemma 2.25). Thus, $\mathcal{O}$ meets $\mathcal{O}_4$ and $\mathcal{O}_5$ and so $|\mathcal{O} \cap \mathcal{O}_l| \geqq 4$, $l=4,5$, whence $\mathcal{O} \subseteq \mathcal{O}_4+\mathcal{O}_5$, a contradiction to $\mathcal{O} \cap \mathcal{O}_1 \neq \emptyset$. Thus, $\mathcal{O}$ contains some T_{kl}, hence must be one of the 15 octads associated to $\Xi(\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{O}_3$ are counted among these). We conclude that $\dim V \leqq 5$.

(ii) Let $\varepsilon_S \in W^{\#}$. If $\lambda \in \Lambda-\Lambda(2)$, then $\lambda(1-\varepsilon_S) \equiv \lambda_S \pmod{\Lambda(4)+2\Lambda}$, whence $C_{\bar{\Lambda}}(W) \leqq \overline{\Lambda(2)}$.

Suppose $U \in \mathscr{C}$ and $\lambda \equiv \lambda_U (\operatorname{mod}(\Lambda(4)+2\Lambda))$. Then $\lambda(1-\varepsilon_S) \equiv \sum_{i \in S \cap U} 4x_i$ $(\operatorname{mod} \mathbb{Z}8x_\infty+2\Lambda)$. So, $\bar{\lambda}$ is fixed by W only if $S \cap U \in \mathscr{C}$ for all ε_S in W. Easily, $U=\mathcal{O}$ or $\mathcal{O}+\Omega$. On the other hand, $\bar{\lambda}_{\mathcal{O}}$ is fixed by W.

It remains to determine $C_{\overline{\Lambda(4)}}(W)$. If $\lambda=\sum_{i \in U} \pm 4x_i$, for some $U \in P_{\text{even}}(\Omega)$, we get $\bar{\lambda}$ fixed by W if and only if $|U \cap S|$ is even, for all ε_S in W. This is equivalent to saying to saying that there is an even set $E \subseteq \mathcal{O}$ such that $\mathscr{C}+U=\mathscr{C}+E$ (reason: the set of such U correspond to the 6-dimensional annihilator in $P(\Omega)_{\text{even}}/\mathscr{C}$ of $V/\langle\Omega\rangle \leqq \bar{\mathscr{C}}$, and the image of $P(\mathcal{O})_{\text{even}}$ in $P_{\text{even}}(\Omega)/\mathscr{C}$ is a 6-dimensional subspace of the annihilator). Thus, $C_{\bar{\Lambda}}(W)$ is as described in (ii).

Definition 2.27. Let V be as in Lemma 2.26. If there exists a unique octad, $\mathcal{O}$, such that $V \leqq \langle \mathcal{O}_1 \mid \mathcal{O}_1$ is an octad, $\mathcal{O}_1 \cap \mathcal{O} = \emptyset$ or $\mathcal{O}_1 = \mathcal{O} \rangle$, call V a *space of octad type, based on the octad* $\mathcal{O}$. Suppose that there is more than one such octad, say $\mathcal{O}$ and $\mathcal{O}'$; if $\mathcal{O} \cap \mathcal{O}' = \emptyset$. $V \leqq \langle \Omega, \mathcal{O}, \mathcal{O}' \rangle$ and if $\mathcal{O} \cap \mathcal{O}'$ is a 4-set, Lemmas 2.25 and 2.26 apply. So, if V is not of octad type, there is (at least) one associated sextet, and so we call V a *space of sextet type.* The sextet is unique unless $V = \langle \mathcal{O}, \mathcal{O}', \Omega \rangle$, with $\mathcal{O}, \mathcal{O}'$ disjoint octads.

Lemma 2.28. *Let* $\langle \Omega \rangle < V$ *be as in Lemma* 2.26, *and* W *the corresponding subgroup of* $O_2(N_{24})$. *Then*

(i) $\dim C_{\Lambda(4)+2\Lambda/2\Lambda}(W) = 13 - \dim V$;

(ii) *the image of* $C_{\Lambda/2\Lambda}(W)$ *in* $\Lambda/\Lambda(4)+2\Lambda$ *lies in* $\Lambda(2)/2\Lambda \cong \bar{\mathcal{C}}$ *and corresponds to the image in* $\bar{\mathcal{C}}$ *of the set of all* $\mathcal{C}$*-sets which meet or avoid every* $\mathcal{C}$*-set in* V;

(iii) *let* $d = \dim [C_{\Lambda/2\Lambda}(W) + (\Lambda(4)+2\Lambda)/(\Lambda(4)+2\Lambda)]$; *we have*
$d=5$ *if* $\dim V = 2$,
$d=2$ *if* $\dim V = 3$,
$d=1$ *if* $\dim V \geqq 4$, *and* V *has octad type,*
$d=0$ *if* $\dim V \geqq 4$, *and* V *has sextet type.*

Proof. Since $V > \langle \Omega \rangle$, no vector in $\Lambda - \Lambda(2)$ with odd coordinates may be fixed modulo 2Λ (or even modulo $\Lambda(4)+2\Lambda$) by an element of $W - \{\pm 1\}$. So, $C_{\Lambda/2\Lambda}(W) \leqq \Lambda(2)/2\Lambda \cong \bar{\mathcal{C}}$. Since $\Lambda(4)+2\Lambda/\langle 8x_\infty, 2\Lambda \rangle \cong P(\Omega)_{\text{even}}/\mathcal{C}$ and the pairing of it with $W/\{\pm 1\}$ into $\langle 8x_\infty, 2\Lambda \rangle / 2\Lambda$ is the natural one, $\dim C_{\Lambda(4)+2\Lambda/2\Lambda}(W) = 13 - \dim V$.

For $\lambda \in \Lambda(2)$, let $S(\lambda) = \{ i \in \Omega \mid i^{\text{th}}$ coordinate of λ is in $2 + 4\mathbb{Z}\}$, and let $\bar{\bar{\lambda}}$ be $\lambda + \langle 2\Lambda, 8x_\infty \rangle / \langle 2\Lambda, 8x_\infty \rangle$. For $\bar{\bar{\lambda}}$ to be fixed by ε_S in W, $S(\lambda) \cap S$ must be a $\mathcal{C}$-set. So, for $\bar{\bar{\lambda}}$ to be fixed by every element of W, $S(\lambda)$ must lie in or avoid every $\mathcal{C}$-set associated to W. Conversely, if U is such a $\mathcal{C}$-set, $\lambda = \sum_{i \in U} 2x_i$ is fixed modulo 2Λ by W.

We get d by analyzing the "solution set", the $\mathcal{C}$-sets which satisfy our condition with respect to V, then taking the dimension of the image of this solution set in $\bar{\mathcal{C}}$.

For $\dim V = 2$, $d = 5$ by Table 2.1.2. Say $\dim V = 3$, $V = \langle \Omega, \mathcal{O}_1, \mathcal{O}_2 \rangle$, $\mathcal{O}_1$, $\mathcal{O}_2$ octads. If $\mathcal{O}_1 \cap \mathcal{O}_2 = \emptyset$, the solution set is just V. If $\mathcal{O}_1 \cap \mathcal{O}_2$ is a 4-set, let $T_1 = \mathcal{O}_1 \cap \mathcal{O}_2$, $T_2 = \mathcal{O}_1 - \mathcal{O}_2$, $T_3 = \mathcal{O}_2 - \mathcal{O}_1$ and $\Xi = \{T_1, \ldots, T_6\}$ the associated sextet. Let $U \neq \emptyset$, Ω be in the solution set. If $U \subseteq \mathcal{O}_i$, $i = 1$ or 2, $U = \mathcal{O}_i$; but $\mathcal{O}_1 \cap \mathcal{O}_2 \notin \mathcal{C}$. So $U \cap \mathcal{O}_i = \emptyset$, $i = 1, 2$. Now use 2.25.

Let us say $\dim V \geqq 4$. Suppose V has octad type, based on the octad $\mathcal{O}_0$. Then V has octads $\mathcal{O}_1$, $\mathcal{O}_2$ in $\mathcal{O}_0 + \Omega$ which meet in a 4-set. The only possible solutions, not ϕ, Ω, are $\mathcal{O}_0$, $\mathcal{O}_0 + \Omega$ and we have $d = 1$. Suppose V has sextet type. Take an octad $\mathcal{O}_3 \in V - \langle \Omega, \mathcal{O}_1, \mathcal{O}_2 \rangle$. Using the discussion of the last paragraph, if $\mathcal{O}_3 \cap (\mathcal{O}_1 \cup \mathcal{O}_2) = \emptyset$, the only possible solutions, not ϕ, Ω, are $\mathcal{O}_3$ or $\mathcal{O}_3 + \Omega$, and if $\mathcal{O}_3 \cap (\mathcal{O}_1 \cup \mathcal{O}_2)$ is a 4-set, the only possible solutions, not ϕ, Ω, are $\mathcal{O}_4 := \Omega + (\mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_3)$ or $\mathcal{O}_4 + \Omega$. But since, by definition, V is not of octad type, some member of V meets $\mathcal{O}_3$, $\mathcal{O}_4$, in these respective cases, in a 4-set; so $d = 0$.

Lemma 2.29. *Let $t \in N_{24}$ be an involution mapping to a non-2-central involution of $M_{24} \cong N_{24}/O_2(N_{24})$, i.e., one of cycle-shape 2^{12}. Then every involution in $O_2(N_{24})t$ is conjugate in $\cdot 0$ to t and every element of $O_2(N_{24})t$ with square -1 is in the class with a $2G_2(4)$-component in its centralizer. In any case, an involution $y \in O_2(N_{24})t/\{\pm 1\} \subseteq \cdot 1$ satisfies* $\dim(\Lambda/2\Lambda)(y-1)=12$.

Proof. To prove the first statement, it suffices to prove that $O_2(N_{24})$ is a free $\mathbb{F}_2\langle t\rangle$-module, then refer to the class list for $\cdot 0$ [12]. Let h be an element of order 11 in M_{24} inverted modulo $O_2(N_{24})$ by t; see [74]. The $\mathscr{C}$-sets fixed by h consist of ϕ, Ω, $\mathscr{D}$, $\mathscr{D}+\Omega$, where $\mathscr{D}$ is a dodecad. Thus, t stabilizes $\{\mathscr{D}, \mathscr{D}+\Omega\}$, and since $O_2(N_{24})=[O_2(N_{24}), h] \times C_{O_2(N_{24})}(h)$, it suffices to show that t interchanges $\mathscr{D}$ and $\mathscr{D}+\Omega$. This is clear, because the stabilizer of $\mathscr{D}$ in M_{24} is a copy of M_{12}, and elements of order 11 in M_{12} are not conjugate to their inverse (because permutations in M_{12} are even on the usual 12 points).

Now to prove the second statement. If $y \in O_2(N_{24})$ has order 4 and $y^2=-1$, this is obvious, since $C(y)$ contains a copy of $2G_2(4)$, of order divisible by 13, and so cannot act nontrivially on an $\mathbb{F}_2$-module of dimension less than 12. Replace t by a conjugate $u \in O_2(N_{24})$. Then $u=\varepsilon_{\mathscr{D}}$, $\mathscr{D}$ a dodecad. Clearly, $\Lambda(1-u)$ consists of vectors with support in $\mathscr{D}$. Say $\xi \in \Lambda$ and $\xi(1-u) \in \Lambda(4)+2\mathbb{Z}$. Then $\xi \in \Lambda(2)$ and $S:=\{i \mid i^{\text{th}}$ coordinate of ξ is in $2+4\mathbb{Z}\} \in \mathscr{C}$. We thus have a map $\bar{\mathscr{C}} \cong \Lambda(2)/2\Lambda \to \langle \Lambda(4), 8x_\infty, 2\Lambda\rangle/2\Lambda \cong P(\Omega)_{\text{even}}/\mathscr{C}$, based on $\xi \mapsto \xi(1-u)$, whose kernel is $\{\{S, S+\Omega\} \in \bar{\mathscr{C}} \mid S \subseteq \mathscr{D}$ or $S \subseteq \mathscr{D}+\Omega\} = \{\{\mathscr{D}, \mathscr{D}+\Omega\}, \{\phi, \Omega\}\}$; the image therefore has dimension 10. So, $\Lambda(1-u) \cong L := \langle \sum_{i \in E} \pm 4x_i \mid E \subseteq \mathscr{D}, E = \mathscr{D} \cap S$ for some $S \in \mathscr{C}\rangle$ and $\dim L+2\Lambda/2\Lambda=11$. Now take $l \in \Omega+\mathscr{D}$, $v=-3x_l + \sum_{i \in \Omega-\{l\}} x_i$. Then $v(1-u)=\sum_{j \in \mathscr{D}} 2x_i \in \Lambda(1-u)-L$ and it is clear, since $\mathscr{D}$ is the support of $v(1-u)$ and $\mathscr{D}$ contains no $\mathscr{C}$-set except ϕ and $\mathscr{D}$, that $v(1-u) \notin L+2\Lambda$. Thus, $\dim[\Lambda/2\Lambda, u]=12$.

Corollary 2.30. *The group $\cdot 1$ has 3 classes of involutions: one 2-central class, with centralizer of shape $2_+^{1+8}.D_4(2)$; two non 2-central classes, with centralizers of shape $2^{11}M_{12}.2$ and $(2\times 2\times G_2(4))2$. Also, if t is an involution in $\cdot 1$,* $\dim[\Lambda/2\Lambda, t]$ *is 8 if t is 2-central and is 12 otherwise.*

Proof. Lemmas 2.28, 2.29 and the class list [12].

Lemma 2.31. *Let Ξ be a sextet of tetrads and let X be its stabilizer in M_{24}. Set $X_0=O_{2,3}(X)$, the kernel of the permutation representation for X on Ξ, $X_1=O_2(X)$, $\langle h\rangle \in \mathrm{Syl}_3(X_0)$. Then (i) h acts fixed point freely on X_1; (ii) there are 21 h-invariant fours-groups in X_1, distributed into two orbits Y_1, Y_2 for $X/X_0 \cong \Sigma_6$ of lengths 6 and 15; (iii) the involutions in Y_1 have cycle shape 2^{12} (non 2-central) and those in Y_2 have cycle shape $1^8 2^8$ (2-central); (iv) if $E \subseteq T \in \Xi$, $|E|=2$ and $X_E=\{g \in X_1 \mid E^g=E\}$, then X_E has orbits of lengths 2, 2, 4, 4, 4, 4, 4 on Ω.*

Proof. By reference to the character table of M_{24} [74], $|C(h)|=1080 \leqq |C_X(h)|$; so (i) follows. The first part of (ii) is immediate from (i). Since (i) implies that X_1 is an irreducible module for X, the orbits of X on the 21 fours-groups have lengths $d_1, d_2, \ldots, d_r$, where each integer is at least 2. Since $7 \nmid |X|$, $r \geqq 2$. If $d_i \leqq 10$ then $d_i=6$ or 10 (an easily checked property of Σ_6). Therefore, $r=2$ and

$\{d_1, d_2\}=\{6, 15\}$, as claimed. Let Y_1, Y_2 be the orbits of lengths 6, 15, respectively. Since $|Y_2|$ is odd, $Y_2^{\#}$ lies in the 2-central class, i.e., the involutions of cycle shape $1^8 2^8$. Let f be the number of fixed points for involutions in $Y_1^{\#}$ and let π be the permutation character on Ω. By the orthogonality relations and the fact that X_1 is transitive on each member of Ξ, $6.2^6=\sum_{g\in X_1}\pi(g)=24+45.8+18f$, implying $f=0$ and (iii).

Now to prove (iv). Clearly, $|X_1:X_E|=2$ and X_E fixes no points of Ω. Since h acts fixed point freely on X_1, $X_2:=\bigcap_{k\in\langle h\rangle} X_E^k$ has index precisely 4 in X_1 (to verify this, look in the dual module of X_1).

Let us say X_E has a orbits of length 2 and b orbits of length 4 on Ω. At once $a\geqq 2$, and we must show that $a=2$. Suppose $a\geqq 3$. Then $a\geqq 4$ and X_2 fixes at least $2a\geqq 8$ points. Since $|X_2|=16$, X_2 fixes 8 points, which form an octad, $\mathcal{O}$, and $X_2=O_2(H)$, where H is the global stabilizer of $\mathcal{O}$. But then X_2 is regular on $\Omega+\mathcal{O}$, hence cannot stabilize the four members of Ξ disjoint from $\mathcal{O}$, a contradiction. So, $a=2$ and (iv) holds.

Lemma 2.32. *Let $\psi: N_{24}/\{\pm 1\}\to M_{24}$ be the natural map. Say $B\leqq N_{24}/\{\pm 1\}$, B an elementary abelian 2-group, such that $B_0:=B\cap\ker\psi=\langle\varepsilon_{\mathcal{O}_0}\{\pm 1\}\rangle$, $\mathcal{O}_0$ an octad. Assume that $B^{\#}$ lies in the 2-central class of $\cdot 1$. Let $H_0\cong 2^4\cdot A_8$ be the stabilizer of $\mathcal{O}_0$ in M_{24}, $B_1:=O_2(H_0)^{\psi^{-1}}\cap B$. Define $m_1=m(B_1/B_0)$, $m_2=m(B/B_1)$, $\bar{\Lambda}=\Lambda/2\Lambda$, $c(\tilde{B})=\dim C_{\bar{\Lambda}}(\tilde{B})$ for $\tilde{B}\leqq B$. Then $m_1\leqq 4$, $m_2\leqq 4$, $m_1+m_2\leqq 6$ and*

$$c(B_1)\leqq\begin{cases}12 & m_1=1,\\ 12-m_1 & m_1\geqq 2,\end{cases}$$

$$c(B)\leqq\begin{cases}12 & m_1=0,\ m_2=1\\ 11 & m_2=2,3\\ 10 & m_2=4\\ 10 & m_1=1,\ m_2=1\\ 9 & m_2=2,3\\ 6 & m_2=4\\ 10-m_1 & m_1\geqq 2,\ m_2=1,2,3\\ 7-m_1 & m_2=4.\end{cases}$$

If $c_1(\tilde{B}):=\dim C_{\Lambda(4)+2\Lambda/2\Lambda}(\tilde{B})$, then $c_1(B_1)=11$ and

$$c_1(B)\leqq\begin{cases}8 & m_1=0,\ m_2=1\\ 7 & m_2=2,3\\ 4 & m_2=4\\ 6 & m_1=1,\ m_2=1,2,3\\ 3 & m_2=4\\ 5 & m_1\geqq 2,\ m_2=1,2,3\\ 2 & m_2=4.\end{cases}$$

Proof. We have $m_1\leqq m(O_2(H_0))\leqq 4$, $m_2\leqq 4$ by Lemma 2.23 and $m_1+m_2\leqq 6$ by Corollary 2.24.

While we have a precise formula for the action of B_0 on $\bar{\Lambda}$, we know the action of elements of $B-B_0$ only up to the action of some element of $O_2(N_{24})$. This ambiguity disappears, however, when we study the action of B on a section in $\bar{\Lambda}$ on which $O_2(N_{24})$ operates trivially. Indeed, our upper bounds on $c(\tilde{B})$ are achieved by studying the action of $\tilde{B}/\tilde{\tilde{B}}$ on sections within $\bar{\Lambda}$ where $\tilde{\tilde{B}}$ operates trivially, for an appropriate chain $\tilde{\tilde{B}} \leqq \tilde{B} \leqq B$.

We use bars to indicate images in $\bar{\Lambda}=\Lambda/2\Lambda$ and double bars to indicate images in $\bar{\bar{\Lambda}}=\Lambda/\langle 2\Lambda, 8x_\infty\rangle$.

By Lemma 2.28, we have $C_{\bar{\Lambda}}(B_0)$. The action of B_1/B_0 on $C_{\bar{\Lambda}}(B_0)/C_{\overline{\Lambda(4)}}(B_0)$ (isomorphic to the 5-dimensional subspace of $\mathscr{C}$ spanned by $\mathcal{O}_0$ and all octads disjoint from it; see Lemma 2.28) is faithful and stabilizes the chain

$$C_{\bar{\Lambda}}(B_0)/C_{\overline{\Lambda(4)}}(B_0) \geqq \langle C_{\overline{\Lambda(4)}}(B_0), \bar{\lambda}_{\mathcal{O}_0}\rangle / C_{\overline{\Lambda(4)}}(B_0) \geqq 0,$$

hence fixes precisely a subspace of dimension $5-m_1$; this is so, for otherwise, irreducibility of $H_0/O_2(H_0)$ on the 1 and 4 dimensional constituents would force $O_2(H_0)$ to stabilize all these octads, hence all their intersections, contradicting the fact that $O_2(H_0)$ is regular on $\Omega+\mathcal{O}_0$. Take $\lambda\in\Lambda(4)$, $\lambda=\sum_{i\in E} \pm 4x_i$, $E\in P_{\text{even}}(\Omega)$, $|E|\leqq 4$. Clearly, $\bar{\bar{\lambda}}$ is fixed by B_1 if $E\subseteq\mathcal{O}_0$. For $\bar{\lambda}$ to be fixed by B_0, $|E\cap\mathcal{O}_0|$ must be even.

Let $L\geqq\langle\overline{8x_\infty}\rangle$ be the subspace of $\overline{\Lambda(4)}$ corresponding to $P_{\text{even}}(\mathcal{O}_0)$, given by all λ, in above notation, with $E\subseteq\mathcal{O}_0$. Then $\dim L=7$. We claim that H_0 acts faithfully on $\Lambda(4)/L$, a reducible module with socle M/L, corresponding to $\{E\in P(\Omega)_{\text{even}} \,|\, |E\cap\mathcal{O}_0|\equiv 0 \pmod 2\}$. Clearly, M is H_0-irreducible of codimension 1. Let $i\in\mathcal{O}$, $j\in\Omega+\mathcal{O}$. Then, for $t\in O_2(H_0)$, $\{i,j\}+\{i,j\}^t=\{j,j^t\}$, a 2-element set in $\mathcal{O}_0+\Omega$. Thus, $\bar{\lambda}_{ij}$ is not fixed by t modulo M, whence the claim. In particular, $O_2(H_0)$ and M/L are isomorphic modules for $H_0/O_2(H_0)\cong A_8$. A similar argument shows that $O_2(H_0)$ is nontrivial on $M/\langle 8x_\infty\rangle$: take $\{i,j\}\subseteq\Omega+\mathcal{O}$, $i\neq j$ such that i and j are in different orbits for some $t\in O_2(H_0)$; then $\bar{\bar{\lambda}}_{ij}\in M$ and $\bar{\bar{\lambda}}{}^t_{ij}\neq\bar{\bar{\lambda}}_{ij}$. Since H_0 operates on $L/\langle 8x_\infty\rangle$ as it acts on $P(\mathcal{O}_0)_{\text{even}}/\langle\mathcal{O}_0\rangle$ (the kernel of the action is $O_2(H_0)$) we see that there is a morphism of $H_0/O_2(H_0)$-modules $O_2(H_0)\otimes M/L\to L/\langle\overline{8x_\infty}\rangle$, which may be identified with the natural map $M/L\otimes M/L\to\Lambda^2(M/L)$; see [30], p. 274. This latter depiction has the advantage that we can see the following: given $x, y\in M/L$, x, y independent, the annihilator of x, i.e., $\{u\in M/L \,|\, x\otimes u$ goes to 0 in $\Lambda^2(M/L)\}$, is 1-dimensional (namely, $\langle x\rangle$), and the annihilator of $\langle x, y\rangle$ is 0.

The preceding paragraphs imply the upper bounds on $c(B_1)$.

To prove the bounds on $c(B)$, we must investigate how elements of B act on $C_{\bar{\Lambda}}(B_1)$. We need to establish two points. Let M_1, M_2 be irreducible 4, 6-dimensional modules, respectively, for $\mathbb{F}_2 A_8$. If t is a 2-central involution of A_8, it operates as a transvection on M_1 and satisfies $\dim C_{M_2}(t)=4$. If t is an involution of A_8, not 2-central, $\dim C_{M_1}(t)=2$ and $\dim C_{M_2}(t)=4$. In addition, we claim that if E_n denotes a subgroup of A_8, $E_n\cong\mathbb{Z}_2^n$, then

(1) $\dim C_{M_2}(E_n)\leqq 3$ for $n=2, 3$ or E_n contains non 2-central involutions;

(2) $\dim C_{M_1}(E_4)=2$ and $\dim C_{M_2}(E_4)=1$.

Suppose $n=2$ and that $\dim C_{M_2}(E_2)\geqq 4$. Let P be the 8-dimensional $\mathbb{F}_2 A_8$-permutation module and P_0 the submodule of codimension 1; P has M_2 as a composition factor. If E_2 has two orbits, P is a free $\mathbb{F}_2 E_2$-module, and $\dim C_{M_2}(E_2) \leqq 3$. So, E_2 has at least 3 orbits. Since E_2 does not act semiregularly on the 8 points, E_2 has non-2-central involutions, proving (1). Since E_4 is uniquely determined up to conjugacy in A_8, it is easy to check $\dim C_{M_1}(E_4) = 2$ directly. We may write $E_4 = T_1 \times T_2$ where T_1 is regular on $\{1,2,3,4\}$ and trivial on $\{5,6,7,8\}$ and T_2 is trivial on $\{1,2,3,4\}$ and regular on $\{5,6,7,8\}$. Let $e_1, \ldots, e_8$ be the standard basis for P and let $I \subseteq \{1, \ldots, 8\}$ such that $e_I := \sum_{i \in I} e_i$ is a fixed point modulo $\mathbb{F}_2 \left(\sum_{i=1}^{8} e_i \right)$, but $I \neq \emptyset$, $\{1, 2, \ldots, 8\}$. Set $I_1 = \{1,2,3,4\} \cap I$, $I_2 = I - I_1$, $e_{(j)} = \sum_{i \in I_j} e_j$, $j = 1, 2$. Say $I_j \neq \emptyset$ for $j \in \{1, 2\}$. Using the action of T_j on $e_{(j)}$, we see that $|I_j| = 4$, proving (2).

We now complete the proof of the Lemma, using the preceeding discussion, by analyzing cases. The bounds on $c(B)$ are discussed and those for $c_1(B)$ are obtained from a similar discussion which is omitted.

Suppose $m_1 = 0$. If all involutions in the image of $B \to H_0/O_2(H_0)$ are 2-central, we have $c(B) \leqq \begin{cases} 12 & m_2 = 1, \\ 11 & m_2 = 2, 3. \end{cases}$ If some non-2-central involutions occur, we have $c(B) \leqq 10$, for all $m_2 \geqq 1$. In particular, $c(B) \leqq 10$ when $m_2 = 4$.

Suppose $m_1 = 1$. If all involutions in the image of $B \to H_0/O_2(H_0)$ are 2-central, we have $c(B) \leqq \begin{cases} 10 & m_2 = 1, \\ 9 & m_2 = 2, 3. \end{cases}$ If some non-2-central involutions occur, we have $c(B) \leqq \begin{cases} 9 & \text{for } m_2 \geqq 1 \\ 6 & \text{if } m_2 = 4. \end{cases}$

Suppose $m_1 \geqq 2$. If all involutions in the image of $B \to H_0/O_2(H_0)$ are 2-central, we have $c(B) \leqq \begin{cases} 10 - m_1, & m_2 = 1, \\ 9 - m_1, & m_2 = 2, 3. \end{cases}$ If some non-2-central involutions are present, we have

$$c(B) \leqq \begin{cases} 10 - m_1 & m_1 \geqq 2, \quad m_2 \geqq 1, \\ 7 - m_1 & m_1 \geqq 2, \quad m_2 = 4. \end{cases}$$

Some remarks of Allan Adler and Melvin Hochster led to a shortening of the original proof of Proposition 12.6 via the following elementary lemma (formulated by Melvin Hochster).

Lemma 2.33. *Let R be a unique factorization domain and S a subset of the free R-module $M \cong R^m$, $m \geqq 0$. Let $\mathfrak{p}$ be an infinite set of primes in R. Suppose that there is an integer n so that the image of S in M/pM has cardinality n, for all $p \in \mathfrak{p}$. Then $|S| = n$.*

Proof. Obviously, $|S| \geqq n$. Suppose that $y_1, \ldots, y_{n+1}$ are distinct elements of S. Consider the set Z of $z_{ij} := y_i - y_j$, $i \neq j$. Only finitely many primes divide any member of Z, whence $\mathfrak{p}^* := \{p \in \mathfrak{p} \mid p$ divides no element of $Z\}$ is infinite, hence nonempty. If $q \in \mathfrak{p}^*$, the images of all the z_{ij} in M/qM are nonzero, whence the image of S in M/qM has cardinality at least $n+1$, a contradiction.

Lemma 2.34. *In ${}^2F_4(2)'$, ${}^2F_4(2)$, $F_4(2)$ and ${}^2E_6(2)$, a Sylow 5-groups is elementary abelian of order 25 and all of its nonidentity elements are conjugate in the normalizer.*

Proof. Consider $G={}^2F_4(2)$. By [32], page 419, $P\in\mathrm{Syl}_5(G)$ is elementary abelian of order 25 and $N(P)/C(P)$ contains a group of order 2^5. Elementary Sylow theory and (B,N)-type arguments for G show that $C(P)=P$ and that 3 divides $|N(P)/C(P)|$. Therefore, $N(P)/P\cong SL(2,3).4$, a Hall $5'$-subgroup of $\mathrm{Aut}(P)\cong GL(2,5)$. The statement about conjugacy in G is now evident and the corresponding statements about the other groups in the hypothesis follow from the natural embedding of each group in the next.

Corollary 2.35. *On a 27-dimensional nontrivial module for* $\mathbb{F}_4[3\cdot{}^2E_6(2)]$, *an element of order* 5 *has trace* 2.

Proof. By Lemma 2.34, if P is a Sylow 5-group, the action of $N(P)$ on P forces $M|_P$ to be the direct sum of its regular representation and a 2-dimensional trivial module.

The referee found a gap in the original version of Lemma 2.36 and suggested the substitute argument which appears here.

Lemma 2.36. $Sz(8)$ *is not contained in* ${}^2E_6(2)$.

Proof. Suppose otherwise, and let M be a 27-dimensional $\mathbb{F}_4$-module for $3\cdot{}^2E_6(2)$. Then $G=Sz(8)$ acts on M. By a theorem of Steinberg [66], if V denotes the standard 4-dimensional module for $Sz(8)$ and V_i are the Galois conjugates, $i=1,2,3$, then every irreducible for $\overline{\mathbb{F}}_2\,Sz(8)$ has shape $V_{i_1}\otimes\ldots\otimes V_{i_r}$ where $\{i_1,\ldots,i_r\}\subseteq\{1,2,3\}$. A primitive 13-th root of unity in $\overline{\mathbb{F}}_2$ has degree 12 over $\mathbb{F}_2$ and degree 6 over $\mathbb{F}_4$. Let M_i be the $\overline{\mathbb{F}}_2\,G$-irreducibles which occur in $\overline{\mathbb{F}}_2\otimes M$. When M_i occurs, all Galois conjugates of M_i associated to elements of $\mathrm{Gal}(\overline{\mathbb{F}}_2/\mathbb{F}_4)$ must occur too. So $\dim M=27$ implies that $\dim M_i=1$ or 4 are the only possibilities. Thus $\{M_i\}$ consists of 3 or 6 4-dimensional modules, and the rest 1-dimensional. An element of order 5 in $Sz(8)$ has trace -1 on the standard 4-dimensional module [68], hence has trace $3(-1)+15=12$ or $6(-1)+3=-3$ on M. This contradicts Corollary 2.35.

Lemma 2.37 (Paul Fong [23]). *The principal 2-block for* J_1 *contains exactly* 5 *modular irreducibles, of degrees* 1, 20, 56, 56, 76.

Lemma 2.38. *Suppose that A is an algebra with an associative bilinear form* (,) *and that B is a subspace of A. Let $\pi\colon A\to B$ be an "orthogonal projection", i.e.* $(\ker\pi, B)=0$. *Define a product on B by* $x\cdot y=\pi(xy)$, $x,y\in B$. *Then the form on B is associative for this product.*

Proof. We have $(x\cdot y,z)=(\pi(xy),z)=(xy,z)$ for $x,y,z\in B$ since π is an orthogonal projection. Similarly, $(x,y\cdot z)=(x,yz)$. Now the result is obvious.

George Glauberman pointed out to us that the structure of a commutative nonassociative algebra may be given to S^2V, V a vector space with a symmetric bilinear form, by a simple formula (see (ii) in the lemma below). We were able to generalize this idea to the following result. Since the argument is elementary, it would not be surprising to find that this result has appeared elsewhere.

Lemma 2.39. *Let M be a module for FG, F a field, G a group and* $M^*=\mathrm{Hom}_F(M,F)$ *the dual module. Set* $A=M\otimes M^*$ *and let* (,) *be the natural*

pairing of $M \times M^*$ into F. In case $M \cong M^*$, we identify M with M^* and, if $\operatorname{char} F \neq 2$, *we let A^ε be the span of all $x \otimes y + \epsilon y \otimes x$, for $x, y \in M$, $\varepsilon = +, -$*
(i) *The following maps of $A \otimes A$ to A give G-invariant algebra structures on A:*

(i.1) $(x \otimes y) \otimes (x' \otimes y') \mapsto (x', y)\, x \otimes y'$,

(i.2) $(x \otimes y) \otimes (x' \otimes y') \mapsto (x, y')\, x' \otimes y$.

The map (i.1) *gives an associative algebra, making $A \cong \operatorname{End}(M)$, via the action $(x \otimes y)\, x' = (x', y)\, x$ and* (i.2) *gives an associative algebra making $A \cong \operatorname{End}(M^*)$, via the action $(x \otimes y)\, y' = (x, y')\, y$.*

Also, the form $(\ ,\ )$ on A given by $(x \otimes y,\ x' \otimes y') = (x, y')(x', y)$ is nondegenerate and symmetric.

(ii) *The product on A^ε given by*

$$\begin{aligned}(x \otimes y + \varepsilon y \otimes x)&(x' \otimes y' + \varepsilon y' \otimes x') \\ &= \{(x', y)\, x \otimes y' + \varepsilon (y, y')\, x \otimes x' + \varepsilon (x, x')\, y \otimes y' + (x, y')\, y \otimes x' \\ &\quad + \varepsilon (x', y)\, y' \otimes x + (y, y')\, x' \otimes x + (x, x')\, y' \otimes y + \varepsilon (x, y')\, x' \otimes y\}\end{aligned}$$

makes A^ε a Jordan or a Lie algebra as $\varepsilon = +, -$, respectively. The form $(\ ,\ )$ on A remains nondegenerate when restricted to each A^ε. Also, the form is associative for A and each A^ε.

(iii) *In A^+, let $\underline{\underline{d}} = \sum_{i=1}^{n} (x_i \otimes y_i + y_i \otimes x_i)$, where $x_1, \ldots, x_n$ is a basis for M and $y_1, \ldots, y_n$ is the dual basis and let*

$$A_0 = \underline{\underline{d}}^{\perp} = \left\{ \sum_{i,j=1}^{n} a_{ij} x_i \otimes y_i \mid a_{ij} = a_{ji} \text{ for all } i, j \text{ and } \sum_{i=1}^{n} a_{ii} = 0 \right\}.$$

Let $\pi\colon A^+ \to A_0$ be the orthogonal projection. For $a, b \in A_0$ define $a \circ b := \pi(a\,.\,b)$, where $a\,.\,b$ denotes the product of (ii). *Then A_0 becomes an algebra with $A_0^2 = 0$ if $n = 2$, $A_0^2 = A_0$ if $n \geqq 3$ and G acts as algebra automorphisms. Also, the form restricted to A_0 is nondegenerate and associative.*

Proof (i). The first assertion is obvious. Let $x, x', x'' \in M$, $y, y', y'' \in M^*$. Assume that the product on A is given by (i.1). Then

$$((x \otimes y)(x' \otimes y'))(x'' \otimes y'') = (x', y)((x \otimes y')(x'' \otimes y'')) = (x', y)(x'', y')\, x \otimes y''$$

and

$$(x \otimes y)((x' \otimes y')(x'' \otimes y'')) = (x'', y')(x \otimes y)(x' \otimes y'') = (x'', y')(x', y)\, x \otimes y'',$$

whence associativity. The identification of A with $\operatorname{End}(M)$ is given by $(x \otimes y)\, x' := (x', y)\, x$. This is an action because

$$((x \otimes y)(x' \otimes y'))\, x'' = ((x', y)\, x \otimes y')\, x'' = (x', y)(x'', y')\, x$$

equals

$$(x \otimes y)((x' \otimes y')\, x'') = (x'', y')((x \otimes y)\, x') = (x'', y')(x', y)\, x.$$

So we have a map $\alpha\colon A \to \operatorname{End}(M)$ of associative algebras. If $x_1, \ldots, x_n$ is a basis for M and $y_1, \ldots, y_n$ the dual basis, the elements $\{x_i \otimes y_j \mid i, j = 1, \ldots, n\}$ act on

M like elementary matrix units of $\mathrm{End}(M)$. Thus, α is onto and, by dimension considerations, is an isomorphism.

Using the map (i.2), we compute

$$((x\otimes y)(x'\otimes y'))(x''\otimes y'')=(x,y')(x'\otimes y)(x''\otimes y'')=(x,y')(x',y'')\,x''\otimes y$$

and

$$(x\otimes y)((x'\otimes y')(x''\otimes y''))=(x',y'')(x\otimes y)(x''\otimes y')=(x',y'')(x,y')\,x''\otimes y,$$

whence associativity. An argument as in the preceeding paragraph gives $A \cong \mathrm{End}(M^*)$ via the action $(x\otimes y)\,y'=(x,y')\,y$.

Concerning the inner product on A, if $x_1,\dots,x_n$ is a basis and $y_1,\dots,y_n$ is the dual basis, the Gram matrix relative to $\{x_i\otimes y_j\}$ is the identity, whence the form is nondegenerate.

(ii) A direct calculation will prove the first assertion. We give a more conceptual proof. Let $t\colon A\to A$ be given by $x\otimes y\mapsto y\otimes x$. Thinking of A as $\mathrm{End}(M)$, we may view A^+ as the set of symmetric matrices and A^- is the set of skew symmetric matrices, for if we identify $x_i\otimes y_j$ with the elementary matrix units, t becomes the transpose operation. If $\alpha,\beta\in A$ and juxtaposition indicates the natural product in $\mathrm{End}(M)$, the product we have defined on A^ε is merely $\alpha\otimes\beta\mapsto\alpha\beta+\varepsilon\beta\alpha$, $\alpha,\beta\in A$. This suffices to prove (ii), the only special comment to make being that the usual Jordan product on A^+ is $\alpha\otimes\beta\mapsto\frac{1}{2}(\alpha\beta+\beta\alpha)$, and if one map $A^+\otimes A^+\to A^+$ makes A^+ a Jordan algebra, any scalar multiple of that map does (and gives an isomorphic algebra if both maps are nonzero).

Since A^+, A^- is the 1, -1 eigenspace, respectively, for t on A, the form restricted to each A^ε is nondegenerate.

To check associativity of the form on A, we need $((x\otimes y)(x'\otimes y'),(x''\otimes y''))=(x',y)(x\otimes y',x''\otimes y'')=(x',y)(x,y'')(x'',y')$ to equal $(x\otimes y,(x'\otimes y')(x''\otimes y''))=(x'',y')(x,y'')(x',y)$, which it does equal. Say $a,b,c\in A^+$. Write $\circ$ for the product on A^+. Then $(a\circ b,c)=(ab+ba,c)=(ab,c)+(ba,c)=(a,bc)+(b,ac)=(a,bc)+(ac,b)=(a,bc)+(a,cb)=(a,bc+cb)=(a,b\circ c)$, as required. A similar argument proves associativity for A^-. Alternatively, Lemma 2.38 may be used since each A^ε is a nonsingular subspace of A.

(iii) Note that $\underline{\underline{d}}$ is left fixed by G since it corresponds to the invariant bilinear form on M $((\underline{\underline{d}},x\otimes y)=2(x,y))$ and the G-invariant form on A is nonsingular. Thus, A_0 and π are G-invariant. Without loss, $n>1$. Without loss, the field is algebraically closed and the basis $\{x_i\}$ of M is orthonormal. The elements $r_{ij}=x_i\otimes x_j+x_j\otimes x_i$ and $s_{ij}=x_i\otimes x_i-x_j\otimes x_j$, $i\neq j$, span A_0. We have $r_{ij}\cdot r_{ij}=2r_{ij}^2=s_{ij}\cdot s_{ij}=2s_{ij}^2=2[x_i\otimes x_i+x_j\otimes x_j]$, $r_{ij}s_{ij}=-x_i\otimes x_j+x_j\otimes x_i$, $s_{ij}r_{ij}=x_i\otimes x_j-x_j\otimes x_i$ and $r_{ij}\cdot s_{ij}=r_{ij}s_{ij}+s_{ij}r_{ij}=0$ so that $A_0^2=0$ if $n=2$. Let i,j,k be distinct. Then $s_{ij}^2-s_{jk}^2=s_{ik}=\pi(s_{ik})$, $r_{ij}s_{jk}=x_i\otimes x_j$ and $r_{ij}\cdot s_{jk}=x_i\otimes x_j+x_j\otimes x_i=r_{ij}=\pi(r_{ij})$ so that $A_0^2=A_0$ if $n\geqq 3$. Associativity of the form on A_0 follows from Lemma 2.38.

Lemma 2.40 (Bernd Fischer [21]). *Let G be a finite simple group generated by a class D of $\{3,4\}$ - transpositions such that if $d\in D$, $C_G(d)\cong 2.{}^2E_6(2).2$. Then*

(a) $|G|=2^{41}3^{13}5^{6}7^{2}11.13.17.19.23.31.47$.

(b) *G has exactly four classes of involutions with centralizers of the forms*

$$2.{}^2E_6(2).2, \quad (2^{1+22})(.2),$$
$$(2\times 2\times F_4(2))2, \quad (2\times 2^8)2^{16}.D_4(2).2,$$

(c) *If K is the last centralizer in* (b), $N_G(Z(O_2(K)))\cong 2^8.2.2^{16}.Sp(8.2)$.

(d) *G has exactly two classes of elements of order* 3; *they have centralizers of shapes* $3\times F_{22}.2$ *and* $3^{1+8}.2_-^{1+6}.U_4(2)$.

(e) *G has exactly* 2 *classes of elements of order* 5; *they have centralizers of the form* $5\times HiS.2$ *and* $5^{1+4}.2_-^{1+4}.A_5$.

(*f*) *G has exactly one class of elements of order* 7; *they have centralizer of shape* $7\times 2.L_3(4).2$.

(g) *The centralizers of the Sylow* 11- *and* 13-*groups have shape* $11\times\Sigma_5$ *and* $13\times\Sigma_4$.

Lemma 2.41. *Let* $G\cong\cdot 1$, $G\leqq GL(24,2)$, *V the natural* 24-*dimensional* $\mathbb{F}_2$-*module. Then V is absolutely irreducible and G preserves at most one nonzero quadratic form on V.*

Proof. Let $\alpha\in\mathrm{End}_G(V)$. We show that α is scalar. Take $PM\leqq G$, $P\cong 3^6$, $M\cong 2M_{12}$; see [11]. By Clifford theory and the structure of PM, $\bar V=\bar{\mathbb{F}}_2\underset{\mathbb{F}_2}{\otimes} V|_P$ is a direct sum of 24 distinct irreducible linear representations V_i, $i=1,\ldots,24$ and M is transitive on these. Thus PM is absolutely irreducible, whence α is scalar, as required for showing absolute irreducibility. Now let $Q\colon V\to\mathbb{F}_2$ be an invariant quadratic form and let $\bar Q$ be its extension to $\bar V$.

Choose a basis vector x_i for V_i, and let V_{2i-1}, V_{2i} be dual PM-modules. Then, by applying elements of P, we see that $Q(x_i)=0$ for all i, $V_{2i-1}+V_{2i}$ is orthogonal to $V_{2j-1}+V_{2j}$ for $i\neq j$. Thus Q is determined by the 6 scalars $c_i=(x_{2i-1},x_{2i})$, where (,) is the associated symmetric bilinear form. Let $\{g_i\}$ be any choice of elements of PM which carry V_1+V_2 to $V_{2i-1}+V_{2i}$. Require $x_{2i-1}=x_1^{g_i}$, $x_{2i}=x_2^{g_i}$. We argue that the scalar c_i then does not depend on the choice of the g_i. Suppose $\{g_i'\}$ is another choice. Since $c_i=(x_{2i-1},x_{2i})=(x_1,x_2)=(x_1^{g_1'},x_2^{g_1'})$, we have independence. In fact, this proves that the c_i are all equal. Thus, $\bar Q$ depends solely on the scalar c_1, whence the Lemma.

3. Faithful Modules for Extraspecial Groups

If p is a prime and P an extraspecial p-group of order p^{2n+1} (see [27]), n a natural number, then P has precisely p^{2n} linear characters and $(p-1)$ faithful irreducible characters of degree p^n, one for each primitive p^{th} root of unity. The faithful ones may be obtained as follows. Suppose we are given a nontrivial linear character ζ of $Z(P)$. Take any maximal abelian subgroup A of P, so that $|A|=p^{n+1}$, and take any extension α of ζ to A. Then the induced character α^P is irreducible and $\alpha^P|_{Z(P)}=p^n\zeta$. See [27] Sect. 5.5 for details. Note that if $p=2$ and A is elementary abelian, then ζ, α and α^P are all rational representations and that a nonzero invariant bilinear form is definite, hence may be chosen to be positive definite.

We use the notation p^{1+2n} to denote an extraspecial p-group of order p^{1+2n}. In case $p=2$, we may add a subscript $\varepsilon=+, -$ to indicate the Witt index of the quadratic form $xZ(P)\mapsto x^2\in Z(P)$ on $P/Z(P)$ ($\varepsilon=+$ if and only if the Witt index is maximal).

Now take $p=2$ and the faithful, irreducible module T for the group $Q \cong 2_+^{1+24}$. Let $E\leqq Q$, $E\cong \mathbb{Z}_2^{13}$ (since Q has plus type, there exist maximal abelian subgroups which are elementary abelian). Take any complement F to E in Q. Then $F\cong \mathbb{Z}_2^{12}$. Let $\varphi_1, \dots, \varphi_{2^{12}}$ be all the distinct linear characters of E not having $\langle z\rangle$ in their kernels. Then $T|_E$ affords $\varphi_1+\varphi_2+\dots+\varphi_{2^{12}}$. Since conjugation by F on E transitively permutes the 2^{12} hyperplanes of E which complement $\langle z\rangle$, the given action of F on T transitively permutes the 2^{12} eigenspaces for E affording the φ_i. By arbitrarily choosing one eigenspace to be associated to the element $1\in F$ and by choosing in it an eigenvector $e(1)$ of unit length (adjusting the form if necessary), the definition $e(x):=e(1)^x$, $x\in F$, picks out an orthonormal basis of eigenvectors for E which form a regular orbit under the action of F. Let φ_x denote the character of E afforded by $\mathbb{Q}\, e(x)$. Writing $g=yu$, $y\in F$, $u\in E$ for a typical element g of Q, we have $e(x)^g = e(x)^{yu} = e(xy)^u = \varphi_{xy}(u)\, e(xy)$. For completeness, we remark that if φ is a character of F occurring in $T|_F$, then φ has multiplicity 1 and is afforded by an eigenvector $\sum\limits_{x\in F} \varphi(x)\, e(x)$. Furthermore, every irreducible character of F does occur this way.

We now consider tensor products. As usual, a group acts on the tensor product of its modules by letting elements act on both variables of the tensors. We claim that $T\otimes T$ affords all the linear characters, each with multiplicity 1. First, some notation. If φ is such a character, then $|E\colon \ker(\varphi|_E)|=1$ or 2 and there is a unique $x\in F$ such that $C_E(x)=\ker(\varphi|_E)$; call it x_φ. Now set $A_\varphi = \frac{1}{2^6} \sum\limits_{x\in F} \varphi(x)\, e(x)\otimes e(xx_\varphi)$; the factor $\frac{1}{2^6}$ is simply to make A_φ have unit length. We argue that $A_\phi^g=\phi(g)\, A_\phi$, for $g\in E\cup F$. For $g\in F$, this is clear since $e(x)^g = e(xg)$. Now, say $g\in E$, x, $y\in F$. We have $\phi_x(g)=\phi_1^x(g)=\phi_1(g^x)$ and $\phi_x(g)\,\phi_y(g) = \phi_1(g^x g^y)=\phi_1((g g^{yx})^x)=\phi_1([g, yx]^x)=\phi_1([g, yx])$, since $[g, yx]$ is central in Q. Also, $\phi(g)=\phi_1([g, x_\phi])$, by definition of x_ϕ and the fact that $\phi|_{\langle z\rangle}$ is the nontrivial linear character. Since $\phi_1([g, x_\phi])=\phi_1([g, xx_\phi x])=\phi_x(g)\,\phi_{xx_\phi}(g)$, from above, we get $A_\phi^g=\frac{1}{2^6} \sum\limits_{x\in F} \phi(x)\,\phi_x(g)\,\phi_{xx_\phi}(g)\, e(x)\otimes e(xx_\phi)=\phi_1([g, x_\phi])\, A_\phi = \phi(g)\, A_\phi$, as required. Easily, $A_\phi^g=\phi(g)\, A_\phi$ for $g\in E\cup F$ implies the same for $g\in Q=EF$ since ϕ is a linear character. Consequently, ϕ occurs with multiplicity at least 1 in $T\otimes T$. Since $\dim T\otimes T=2^{24}=|Q/Q'|$, each ϕ occurs with multiplicity exactly 1, as we require.

4. The Groups $\hat{C}$, C_∞ and C and the Vector Space B

If the group F_1 exists, it has an involution z such that $C:=C_{F_1}(z)$ satisfies (i) $Q:=O_2(C)\cong 2_+^{1+24}$; (ii) C is 2-constrained, i.e. $C_C(Q)\leqq Q$, which means that $C_C(Q)=\langle z\rangle := Z(Q)$; (iii) $C/Q\cong \cdot 1$ operates faithfully on $Q/Q'\cong 2^{24}$.

It is proven in [36] that the above group-theoretic conditions on C restrict C to exactly two isomorphism types and that only one of these may live as the centralizer of an involution in a finite simple group; see [37]. In either case, there is an isomorphism of $\cdot 1$-modules $Q/Q' \cong \Lambda/2\Lambda$.

For later use, we shall need a set map $q\colon \Lambda \to Q$ which is constant on cosets of 2Λ, satisfies $q(0)=1$, and induces an isomorphism $\Lambda/2\Lambda \cong Q/Q'$ of $\cdot 1$-modules.

The main purpose of this paper is to build a simple group with C as the centralizer of an involution. So, our first step is to construct C very carefully. We do not make use of the first two paragraphs of this section.

We analyze some subgroups of $GL(2^n, \mathbb{Q})$. Let $\mathbb{Q}[Q]$ be the rational group algebra of $Q \cong 2_+^{1+2n}$, $n \geqq 2$. There is a unique, indecomposable 2-sided ideal, $I \cong \mathrm{End}_{\mathbb{Q}}(T)$, where T is the module discussed in Sect. 3. Let $A = \mathrm{Aut}(Q)$ act in the natural way on $\mathbb{Q}[Q]$. Since every indecomposable 2-sided ideal of $\mathbb{Q}[Q]$ has dimension 1 except for I, I is stable under A and A acts as a group of algebra automorphisms of I. By the Skolem-Noether theorem ([42], p. 24) there is a function $m\colon A \to I$ so that $m(A)$ consists of invertible matrices and $m(a)^{-1} u m(a) = u^a$ for all $u \in I$, $a \in A$.

Since the field $\mathbb{Q}$ is not algebraically closed, we are not quite able to assert that there is a covering group $\hat{A}$ of A and a homomorphism $\hat{m}\colon \hat{A} \to I^\times$ (the group of units of $\mathrm{End}_{\mathbb{Q}}(T)$) so that $m(a)^{-1} u m(a) = \hat{m}(\hat{a})^{-1} u \hat{m}(\hat{a})$ for all $u \in I$ whenever $\hat{a} \mapsto a$ under $\hat{A} \to A$. We may substitute the following argument. Let $A_1 = \langle m(A) \rangle \leqq I^\times$. Possibly A_1 is infinite, but at least we know that $|A_1 : Z(A_1)| = |A| < \infty$. Therefore, A_1' is finite, by an old result of Schur. Since the action of Q on T is absolutely irreducible, $Z(A_1')$ consists of scalar matrices, hence has order 1 or 2, as the field is $\mathbb{Q}$ and A_1' is finite. Since $\langle m(\mathrm{Inn}(Q)) \rangle' \neq 1$ is scalar, $Z(A_1') = \{\pm 1\}$. In particular, $O_2(A_1') \cong Q$ because there is an exact sequence $1 \to Z(A_1') \to O_2(A_1') \to Q/Q' \to 1$, the middle term is nonabelian (since $\langle m(\mathrm{Inn}(Q)) \rangle' \neq 1$), and Q/Q' is the natural $2n$-dimensional module for $\mathrm{Out}(Q)'$. It follows that A_1' is an extension of $\mathrm{Out}(Q)'$ by Q and A_1' induces $\mathrm{Aut}(Q)'$ on $O_2(A_1') \cong Q$.

Let A_0 be the subgroup $A_1' \leqq GL(2^n, \mathbb{Q})$ constructed above. We identify Q with $O_2(A_0)$, and we consider the case $2n = 24$. Since $\det \Lambda = 1$ the quadratic form on $\Lambda/2\Lambda$ given by $\lambda + 2\Lambda \mapsto (-1)^{\frac{1}{2}\langle \lambda, \lambda \rangle}$ is nondegenerate. Since $\cdot 0$ contains an element of order 3 which acts fixed point freely on Λ, the quadratic form on $\Lambda/2\Lambda$ has maximal Witt index since $n \equiv 0 \pmod 2$. Therefore, we get a map $\cdot 0 \to \Omega^+(24, 2)$ whose image is isomorphic to $\cdot 1$. Since any subgroup of $GL(24, 2)$ isomorphic to $\cdot 1$ preserves at most one nonzero quadratic form (Lemma 2.41), all embeddings of $\cdot 1$ in $\Omega^+(24, 2)$ are conjugate via elements of $\Omega^+(24, 2)$. Take any subgroup $C_\infty \leqq A_0$ with the property that $C_\infty/Q \cong \cdot 1$. We have an exact sequence $1 \to 2_+^{1+24} \to C_\infty \to \cdot 1 \to 1$. The group C which we seek to construct is the middle term of such a short exact sequence, but $C \not\cong C_\infty$.

Let $\hat{C}$ be the covering group for C_∞, $Z = Z(\hat{C})$. We claim that $|Z| \leqq 4$. Define $U := O_2(\hat{C})$, $Z_1 := \ker[\hat{C} \twoheadrightarrow C_\infty]$. Then $U/Z_1 \cong Q$. We argue that $Z(U)/Z_1$ maps onto $Z(Q)$, for if $Z_1 \leqq Z_1^* \leqq U$ and Z_1^*/Z_1 corresponds to $Z(Q)$, we have $[Z_1^*, \hat{C}, \hat{C}] \leqq [Z_1, \hat{C}] = 1$ so that $Z_1^* \leqq Z(\hat{C})$ by the three subgroups lemma and the fact that $\hat{C}$ is perfect. So, $Z_1^* \leqq Z(U)$ and we have $Z(U) = Z_1^*$.

Let $L = L_1 \oplus L_2$ be the Lie ring of U([27], 5.6) and let $\bar{L} = \bar{L}_1 \oplus \bar{L}_2$, where bars indicate taking images modulo $Z(U)/U'$, an ideal of L which lies in L_1. Then, as modules for $\hat{C}$, $\bar{L}_1 \cong Q/Q'$. Since $\bar{L}_1$ is elementary abelian and generates $\bar{L}$ as a Lie ring, $\bar{L}_2 \cong L_2$ is elementary abelian. As modules for $\hat{C}$, L_2 is a quotient of the exterior square of $\bar{L}_1$, whose maximal trivial quotient is one-dimensional because Q/Q' supports exactly one nontrivial $\cdot 1$-invariant bilinear form (see Lemma 2.41). Thus, $\dim L_2 = 1$ and so $|U'| = 2$. By Lemma 2.11, $\mathrm{Ext}^1_{\mathbb{F}_2(\cdot 1)}(\Lambda/2\Lambda, \mathbb{F}_2) \cong \mathrm{Ext}^1_{\mathbb{F}_2(\cdot 1)}(\mathbb{F}_2, \Lambda/2\Lambda) \cong H^1(\cdot 1, \Lambda/2\Lambda) = 0$, whence $O_2(\hat{C})/O_2(\hat{C})' \cong \Lambda/2\Lambda \oplus R$, where R is a trivial module. Since $H^2(\cdot 1, \mathbb{Q}/\mathbb{Z}) \cong Z_2$ [33], we get $|R| \leqq 2$ since $\hat{C}$ is perfect. Thus, $|Z| \leqq 4$ as claimed. Next, we claim that $Z \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let K be the kernel of the epimorphism $\hat{C} \to C_\infty$. Then $K \cap O_2(\hat{C})' = 1$, whence $|K| = 1$ or 2. We show that $K \neq 1$, which suffices, since $Z = O_2(\hat{C})' \times K$. Letting C^* be the pullback of the diagram

$$\begin{tikzcd}
C^* \arrow[r] \arrow[d, dashed] & C_\infty \arrow[d, "\psi"] & (\varphi, \psi \text{ onto}) \\
\cdot 0 \arrow[r, "\varphi"] & \cdot 1 &
\end{tikzcd}$$

i.e. $C^* \cong \{(g, h) \in \cdot 0 \times C_\infty \mid g^\varphi = h^\psi\}$, we find that C^* is a perfect central extension, and so is a homomorphic image of $\hat{C}$. Therefore, $K \neq 1$ since C^* maps onto $\cdot 0$ but C_∞ does not. We also have $\hat{C} \cong C^*$.

We summarize as follows. The quotients of $\hat{C}$ by the three subgroups of order 2 in Z are $C_\infty \cong 2^{1+24}.(\cdot 1)$, $C \cong 2^{1+24}.(\cdot 1)$ and $2^{24}.(\cdot 0) \cong 2^{25}.(\cdot 1)$. We shall see shortly that $C \not\cong C_\infty$. From the last paragraph, we see that $O_2(\hat{C}) = \hat{Q} \times \langle z_\infty \rangle$, where $|z_\infty| = 2$, $\langle z_\infty \rangle = K$, $\hat{Q} \lhd \hat{C}$, $\hat{Q} \cong Q$. Let $\langle \hat{z} \rangle = Z(\hat{Q})$.

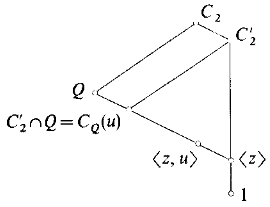
If ρ is the representation of $\hat{C}$ on T via $\hat{C} \to C_\infty$, it is easy to see that $\rho \otimes \rho'$ runs over all the irreducible representations for $\hat{C}$ which are faithful on $\hat{Q}$, as ρ' runs over all the irreducibles of $\hat{C}/\hat{Q} \cong \cdot 0$. We have

$$\ker(\rho \otimes \rho') = \begin{cases} \langle z_\infty \rangle & \text{if } \rho' \text{ is not faithful,} \\ \langle \hat{z} z_\infty \rangle & \text{if } \rho' \text{ is faithful.} \end{cases}$$

In particular, $C \not\cong C_\infty$, since C does not have a faithful character of degree 2^{12}.

We identify Q with the image of $\hat{Q}$ in C.

We are ready to define the C-module $B = U \oplus V \oplus W$. As $\hat{C}$-modules, $W = T \underset{\mathbb{Z}}{\otimes} \Lambda$ and $U \cong S^2(\mathbb{Q} \underset{\mathbb{Z}}{\otimes} \Lambda)$. The module V is an induced module, described as follows. Let C_2/Q be the subgroup of $C/Q \cong \cdot 1$ corresponding to the image of a natural $\cdot 2$ subgroup of $\cdot 0$ in $\cdot 1$. We claim that the lattice of normal subgroups of C_2 is the following:



Here, $u \in Q$ corresponds to a vector of type 2 under $Q/Q' \cong \Lambda/2\Lambda$. The validity of the picture follows from the structure of the extraspecial group Q together with the observations (a) C_2' must centralize the four group $\langle z, u\rangle$; (b) $C_2/Q \cong \cdot 2$ is simple; (c) $C_Q(u)/\langle u, z\rangle$ is a 22-dimensional $\mathbb{F}_2$ irreducible module for $\cdot 2$ (irreducibility is easy to prove, since a natural M_{23} subgroup of $M_{24} \leqq N_{24}$ fixing $-3x_i + \sum_{j \neq i} x_j$, has constituents of dimensions 1, 1, 11, 11 on $\Lambda/2\Lambda$, and a subgroup 3^{1+4} of $\cdot 2$ has constituents of dimensions 1, 1, 1, 1, 1, 1, 18, as may be deduced from the character table [12]). Given the above picture, we take the unique nontrivial linear character φ of C_2, let $V(\varphi)$ be a module affording it, then let $V := V(\varphi)^C$ be the induced module. Note that $\varphi|_Q = \varphi_\lambda$, where $\lambda \in \Lambda_2$ corresponds to u under our isomorphism $\Lambda/2\Lambda \cong Q/Q'$. Thus, $V|_Q$ affords the character $\sum_\lambda \varphi_\lambda$ where λ runs over representatives of the classes in $\tilde{\Lambda}_2$.

We may give another description of the module V. The above discussion indicates that V is characterized by the properties: (a) V is absolutely irreducible; (b) $C_C(V) = \langle z\rangle$; (c) $\dim V = 98280$. From the discussion in Sect. 3, we see that the $\hat{C}$-module $T \otimes T$ restricted to Q contains each linear character with multiplicity 1. Note that Z acts trivially on $T \otimes T$, so that $T \otimes T$ may be regarded as a C-module. Since $\cdot 1$ operates transitively on $\tilde{\Lambda}_2$ and $|\tilde{\Lambda}_2| = 98280$, the subspace $T(2)$ of $T \otimes T$ corresponding to the character φ_λ, $\lambda \in \Lambda_2$, is a C-submodule of dimension 98280, hence is isomorphic to V.

In the notation of Sect. 3, the character φ is afforded by the unit eigenvector $A_\varphi = \frac{1}{2^6} \sum_{x \in F} \varphi(x)\, e(x) \otimes e(x x_\varphi)$. In case $\lambda \in \Lambda$ and φ correspond as above, write A_λ for A_φ. Then $T(2)$ has basis $\{A_\lambda\}$ where λ runs over the classes of $\tilde{\Lambda}_2$. We write $v(\lambda) := A_\lambda$, $\lambda \in \tilde{\Lambda}_2$.

Table 4.1. The module structure of B

Action of ... on module	U	V	W
z	1	1	-1
Q	1	linear characters	$\bigoplus_1^{24} T$
C	$\cdot 1$	monomial group	$T \otimes_{\mathbb{Z}} \Lambda$
Dimensions:	300	98280	98304
Decomposition into irreducibles:	$1+299$	98280	98304

Irreducibility of W follows from our earlier discussion and irreducibility of V follows from Clifford theory. Finally, taking $\{x_i \mid i \in \Omega\}$ as an orthonormal basis for $\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$, the subspace $\mathbb{Q}(\sum_{i \in \Omega} x_i^2)$ and its orthogonal complement in $S^2(\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda)$ are invariant under the action of $\cdot 1$. The 299-dimensional complement must remain irreducible for $\cdot 1$, since the only irreducible degrees for $\cdot 1$

less than 300 are 299 and 276 [12], and the principal character may occur only once in U since $\mathbb{Q}\underset{\mathbb{Z}}{\otimes}\Lambda$ is absolutely irreducible.

We close this section with some notation. We fix group epimorphisms

$$\begin{aligned}\pi_1&: \hat{C}\to C\\ \pi_\infty&: \hat{C}\to C_\infty\\ \pi_0&: \hat{C}\to C_0:=2^{24}.(\cdot 0)\\ \pi&: \hat{C}\to\cdot 0\\ \bar{\pi}&: C\to\cdot 1\\ {}^{-}&: \cdot 0\to\cdot 1.\end{aligned}$$

We also choose a function $\hat{\pi}$: $C\to\cdot 0$ which is not a group homomorphism, but whose composite with the quotient map $\cdot 0\to\cdot 1$ does give the group homomorphism $\bar{\pi}$: $C\to\cdot 1$ onto $\cdot 1$. For $g\in C$, we require $g^{\hat{\pi}}\in(g^{\pi_1^{-1}})^{\pi}$ and we write $\hat{g}$ for $g^{\hat{\pi}}$. We abuse notation and write $\bar{g}$ for $g^{\bar{\pi}}=\bar{\hat{g}}$. When S is a subgroup of C, we write $\hat{S}$ or $S^{\hat{\pi}}$ for the group $(S^{\pi_1^{-1}})^{\pi}$ and $\bar{S}$ for $S^{\bar{\pi}}$ and $\hat{S}$. We do not use special notation for the quotient map $C\to C/\langle z\rangle$.

This notation is depicted as follows:

$$\begin{tikzcd}
 & C_\infty \arrow[r] & C_\infty/Z(C_\infty) \arrow[dr] & \\
\hat{C} \arrow[ur, "\pi_\infty"] \arrow[r, "\pi_0"] \arrow[rr, bend left, "\pi"] \arrow[dr, "\pi_1"'] & C_0 \arrow[r] & \cdot 0 \arrow[r] & \cdot 1 \\
 & C \arrow[r] \arrow[ur, dashed, "\hat{\pi}"] \arrow[urr, "\bar{\pi}"] & C/\langle z\rangle \arrow[ur] \arrow[d, phantom, "\Vert\wr"] & \\
 & & C_\infty/Z(C_\infty) &
\end{tikzcd}$$

In Sect. 3, we considered a factorization $Q=EF$ where $E\cong\mathbb{Z}_2^{13}$ and $F\cong\mathbb{Z}_2^{12}$, but no other requirements were imposed. From now on, we require $q(\Lambda(4))=E_0$, where $E_0:=C_E(e(1))$. (See Sect. 2 for the definition of $\Lambda(n)$ and Sect. 3 for the definition of $e(1)$). Thus, $E=E_0\times\langle z\rangle$.

The facts that N_{24} (see Sect. 2) operates monomially with respect to $\{x_i\,|\,i\in\Omega\}$ and is maximal in $\cdot 0$ imply that N_{24} is the stabilizer in $\cdot 0$ of $\Lambda(4)$. By Lemma 2.12, $|E|=2^{13}$. Without loss, we may alter q so that $E_0:=q(\Lambda(4))$ is a subgroup of E (therefore of index 2). Finally, one more piece of notation: for $x\in Q$, we let $\lambda_x\in\Lambda$ satisfy $q(\lambda_x)\in x\langle z\rangle$ with $\langle\lambda_x,\lambda_x\rangle$ as small as possible.

We write $u_{ij}=u(x_ix_j)\in U$, $\underline{\underline{d}}=\sum_{i\in\Omega}x_i^2$, $U_0=\underline{\underline{d}}$, the orthogonal complement in U, u_0: $U\to U_0$ the orthogonal projection; we also write $u_0(x)$ for $u_0(u(x))$, $x\in S^2(\mathbb{Q}\underset{\mathbb{Z}}{\otimes}\Lambda)$. Note that U has a basis $\{u_{ii}\,|\,i\in\Omega\}\cup\left\{u_{ij}\,\middle|\,ij\in\binom{\Omega}{2}\right\}$, where $\binom{\Omega}{2}$ is the set of unordered pairs of distinct elements from Ω.

5. Tensor Products of Irreducibles of $\hat{C}$

This published version of Sect. 5 differs significantly from the preprint version in a number of ways, due mainly to the use of Lemma 2.38. The referee found a number of problems with the original version, but these are circumvented by this new approach.

For two modules A_1 and A_2 of a finite group G_0, we let $\langle A_1, A_2\rangle$ or $\langle A_1, A_2\rangle_{G_0}$ be $\dim \mathrm{Hom}_{G_0}(A_1, A_2)$. We assume that the field has characteristic 0. When A_i is absolutely irreducible, this is just the multiplicity of A_i in A_j, for $\{i,j\}=\{1,2\}$.

Whenever we have such self-dual modules A_1, A_2, A_3, we have an adjointness relation $\mathrm{Hom}_{G_0}(A_1 \otimes A_2, A_3) \cong \mathrm{Hom}_{G_0}(A_1, A_2 \otimes A_3)$ (see Lemma 2.7) which implies that $\langle A_1 \otimes A_2, A_3\rangle = \langle A_1, A_2 \otimes A_3\rangle$.

We regard the faithful module T for Q as a $\hat{C}$-module (see Sect. 4). In this section all C-modules shall be regarded as $\hat{C}$ modules, and for course $\hat{C}$-modules on which $\langle \hat{z} z_\infty\rangle$ acts trivially may be regarded as C-modules.

For the modules U and W, C-invariant symmetric bilinear forms may be obtained from ones on T and Λ, by Lemma 2.6. The orthogonal projections $U \to \mathbb{Q}\underline{\underline{d}}$ and $U \to U_0 = \underline{\underline{d}}^\perp$ give forms on $\mathbb{Q}\underline{\underline{d}}$ and U_0. Finally, we get an invariant symmetric bilinear form on V by viewing V as an induced module $V = V(\phi)_{C_2}|^C$ (see Sect. 4), taking a basis element v for $V(\phi)$, and making $(v, v^g)=0$ whenever $v^g \neq \pm v$, and $(v^g, v^g)=1$ for $g \in C$. Given $g, h \in C$, either v^g and v^h are linearly independent or $v^g = \pm v^h$. Later, we shall adjust these forms by scalars.

Note that all of $\mathbb{Q}$, $T, \mathbb{Q} \otimes \Lambda, U_0, V$ and W are self-dual and absolutely irreducible.

Definition 5.1. For $\tilde{\lambda} \in \tilde{\Lambda}_2$, let ϕ_λ be the character of Q given by $q(\mu) \mapsto (-1)^{\langle \lambda, \mu\rangle}$ (it follows that $zq(\mu) \mapsto (-1)^{\langle \lambda, \mu\rangle}$ since $z \in Q'$). Write x_λ for the element x_{ϕ_λ} of F and A_λ for $A_{\phi\lambda}$.

Lemma 5.2. *Let $V \otimes V \to V$ be a nonzero $\hat{C}$-map. Then, up to a scalar multiple, the map is $v(\lambda) \otimes v(\mu) \mapsto$*

$$\begin{cases} \phi_{\lambda+\mu}(x_\lambda) v(\lambda+\mu) = \phi_\mu(x_\lambda) v(\lambda+\mu) & \text{if } \lambda, \mu, \lambda+\mu \in \Lambda_2, \\ 0 & \text{if } \tilde{\lambda}, \tilde{\mu} \text{ do not span a triangle type of } 222. \end{cases}$$

Furthermore, this is a $\hat{C}$-map and the form is associative with respect to the associated algebra, which is commutative.

Proof. We first show that $\langle V \otimes V, V\rangle = 1$. Let $f, g\colon V \otimes V \to V$ be $\hat{C}$-maps. If $\lambda, \mu \in \Lambda_2$ and $\tilde{\lambda}, \tilde{\mu}$ do not span a triangle on type 222, $f(v(\lambda) \otimes v(\mu)) = 0$, since $v(\lambda) \otimes v(\mu)$ affords the character $\phi_{\lambda+\mu}$ of Q.

Suppose that, for some triple $\lambda, \mu, \lambda+\mu \in \Lambda_2$, $f(v(\lambda) \otimes v(\mu) = 0$. Transitivity of $\cdot 0$ on the set of triangles of type 222 implies that f is 0 on all such $v(\lambda) \otimes v(\mu)$, whence $f=0$. Consequently, f and g are linearly dependent, for if a, b are scalars with $f(v(\lambda) \otimes v(\mu)) = av(\lambda+\mu)$, $g(v(\lambda) \otimes v(\mu)) = bv(\lambda+\mu)$ for $\lambda, \mu, \lambda + \mu \in \Lambda_2$, then $(bf - ag)(v(\lambda) \otimes v(\mu)) = 0$. At once, $\langle V \otimes V, V\rangle \leqq 1$. We need the opposite inequality.

Recall from Sect. 4 that V may be regarded as the subspace of $T\otimes T$ spanned by all $A_\lambda, \lambda\in\Lambda_2$. From Lemma 2.39, there is a product on $T\otimes T$ making the relevant form associative. Since the form on $T\otimes T$ is positive definite, Lemma 2.38 applies to the subspace V. It remains to show that the product on V inherited from $T\otimes T$ is nonzero and commutative. We compute, in the notation of Sect. 4 and Lemma 2.39,

$$\begin{aligned}
A_\phi \,.\, A_\psi &= \frac{1}{2^{12}} \sum_{x,y\in F} \phi(x)\psi(y)\, e(x)\otimes e(x x_\phi)\,.\, e(y)\otimes e(y x_\psi)\\
&\frac{1}{2^{12}} \sum_{x\in F} \phi(x)\psi(x x_\phi)\, e(x)\otimes e(x x_\phi x_\psi)\\
&= \frac{1}{2^{12}}\, \psi(x_\phi) \sum_{x\in F} \phi(x)\psi(x)\, e(x)\otimes e(x x_\phi x_\psi)\\
&= \frac{1}{2^{12}}\, \psi(x_\phi) \sum_{x\in F} (\phi\psi)(x)\, e(x)\otimes e(x x_{\phi\psi}) = \frac{1}{2^6}\, \psi(x_\phi) A_{\phi\psi}.
\end{aligned}$$

For $\lambda, \mu\in\Lambda$ and $\phi=\phi_\lambda$, $\psi=\phi_\mu$, this reads $A_\lambda\cdot A_\mu = \frac{1}{2^6}\,\phi_\mu(x_\lambda) A_{\lambda+\mu}$. Note that if λ has type congruent to $\delta(\text{mod}\, 2)$, $\delta=0$ or 1, then $\phi_\lambda(x_\lambda)=(-1)^\delta$ (namely, $q(\lambda) = x_\lambda\cdot u_\lambda$, $u_\lambda\in E$ and $[x_\lambda, u_\lambda]=1$ if and only if $q(\lambda)^2=1$). So, if we restrict λ to vectors of type 2, $\phi_\mu(x_\lambda)=\phi_{\lambda+\mu}(x_\lambda)$. The first statement of the Lemma follows. As for commutativity, if $\lambda, \mu, \lambda+\mu\in\Lambda_2$, $1=\phi_{\lambda+\mu}(x_{\lambda+\mu})=\phi_{\lambda+\mu}(x_\lambda)\phi_{\lambda+\mu}(x_\mu)$ implies the result.

Lemma 5.3. *Let $U\times V\to U$ be a nontrivial $\cdot 1$-invariant symmetric product with image lying in U_0 and $\underline{\underline{d}}\cdot U=0$. Then, up to a scalar, the product is*

$$u_{ii}^2 = -253 u_{ii} + 11 \sum_{j\neq i} u_{jj}; \tag{1}$$

$$u_{ii}u_{jj} = 11(u_{ii}+u_{jj}) - \sum_{k\neq i,j} u_{kk}; \tag{2}$$

$$u_{ii}u_{ij} = -132 u_{ij}; \tag{3}$$

$$u_{ii}u_{jk} = 12 u_{jk}; \tag{4}$$

$$u_{ij}^2 = -66(u_{ii}+u_{jj}) + 6 \sum_{k= i,j} u_{kk}; \tag{5}$$

$$u_{ij}u_{jk} = -72 u_{ik}; \tag{6}$$

$$u_{ij}u_{kl} = 0; \tag{7}$$

here, distinct symbols i, j, k, l mean that the indices are really distinct. Also, a $\cdot 1$-invariant inner product is the following: $(u_{ii}, u_{jj})=4\delta_{ij}$, $(u_{ii}, u_{jk})=0$ for $j\neq k$, $(u_{ij}, u_{kl})=2\delta_{\{i,j\},\{k,l\}}$ for $i\neq j$, $k\neq l$.

Proof. First we investigate products invariant under N_{24}. Since the action of N_{24} on the basis elements is so easy to understand, one can write down the N_{24}-invariant products:

(8)
$$\begin{aligned}
u_{ii}^2 &= \gamma u_{ii} + \delta \sum_{j \neq i} u_{jj};\\
u_{ii}u_{jj} &= \alpha(u_{ii}+u_{jj}) + \beta \sum_{k \neq i,j} u_{kk}, \qquad \text{for } i \neq j;\\
u_{ii}u_{ij} &= \alpha_1 u_{ij}, \qquad \text{for } i \neq j;\\
u_{ii}u_{jk} &= \alpha_2 u_{jk}, \qquad \text{for distinct } i,j,k;\\
u_{ij}^2 &= \zeta(u_{ii}+u_{jj}) + \eta \sum_{k \neq i,j} u_{kk}, \qquad \text{for } i \neq j;\\
u_{ij}u_{jk} &= \lambda u_{ij}, \qquad \text{for distinct } i,j,k;\\
u_{ij}u_{kl} &= 0, \qquad \text{for distinct } i,j,k,l;
\end{aligned}$$

for scalars γ, δ, α, β, α_1, α_2, ζ, η, λ.

We have $\underline{\underline{d}} = \sum_{i \in \Omega} u_{ii} \in U$ and we want to have $\underline{\underline{d}} \cdot U = 0$. So, $u_{ii} \cdot \underline{\underline{d}} = 0$ gives

(9) $$\gamma + 23\alpha = 0 \quad \text{and}$$

(10) $$\delta + \alpha + 22\beta = 0.$$

Also, $u_{ij} \cdot \underline{\underline{d}} = 0$ for $i \neq j$ gives

(11) $$\alpha_1 + 11\alpha_2 = 0.$$

Since we require $U^2 = U_0$, by looking at $u_{ii}u_{jj}$, we get

(12) $$\gamma + 23\delta = 0 \quad \text{and}$$

(13) $$\alpha + 11\beta = 0.$$

We conclude that

(14) $$\alpha = \delta = -11\beta \quad \text{and} \quad \gamma = 253\beta.$$

Also $u_{ij}^2 \in U_0$ for $i \neq j$ gives

(15) $$\zeta + 11\eta = 0.$$

We use the fact that $\cdot 0$ is transitive on vectors of types 2 and 4. Write $x \sim y$ if x, y lie in a module for $\cdot 0$ and there is $g \in \cdot 0$ such that $x^g = y$.

Now, $2x_1 \sim x_1 + x_2 + x_3 + x_4$, whence $4u_{11} \sim \sum_{i=1}^{4} u_{ii} + 2 \sum_{1 \leq i < j \leq 4} u_{ij}$. Therefore

$$\begin{aligned}
(4u_{11})^2 &= 16\{\gamma u_{11} + \delta \sum_{i \neq 1} u_{ii}\} = 16\{\delta \cdot \underline{\underline{d}} + (\gamma - \delta) u_{11}\}\\
&= 16\delta \underline{\underline{d}} + 4(\gamma-\delta)(4u_{11}) \sim \left\{ \sum_{i=1}^{4} u_{ii} + 2 \sum_{1 \leq i < j \leq 4} u_{ij} \right\}^2\\
&= \Bigg\{ (\gamma + 3\delta + 6\alpha + 6\beta + 4(3\zeta + 3\eta)) \sum_{i=1}^{4} u_{ii} + (4\delta + 12\beta + 4(6\eta)) \sum_{k \neq 1,2,3,4} u_{kk}\\
&\qquad + (4(4\lambda) + 4(2\alpha_1 + 2\alpha_2)) \sum_{1 \leq i < j \leq 4} u_{ij} \Bigg\}\\
&= \Bigg\{ (160\beta + 12(\zeta + \eta)) \sum_{i=1}^{4} u_{ii} + (-32\beta + 24\eta) \sum_{k \neq 1,2,3,4} u_{kk}\\
&\qquad + (16\lambda + 8(\alpha_1 + \alpha_2)) \sum_{1 \leq i < j \leq 4} u_{ij} \Bigg\}.
\end{aligned}$$

It follows that

$$(16) \qquad 16\delta = -32\beta + 24\eta, \quad \text{or } \eta = -6\beta;$$

and so

$$(17) \qquad \zeta = -11\eta = 66\beta.$$

We also deduce from the above $\sim$ relation that

$$(18) \qquad 4(\gamma - \delta) = 8\lambda + 4(\alpha_1 + \alpha_2), \quad \text{or } 264\beta = 2\lambda + \alpha_1 + \alpha_2.$$

What we seek is a further condition on λ, α_1, α_2.

We observe that $\beta \neq 0$; if $\beta = 0$, then the only structure constants which might be nonzero are λ, α_1 and α_2, which implies that $U^2 \leqq \operatorname{span}\{u_{ij} | i \neq j \text{ in } \Omega\} < U_0$, a contradiction. Therefore we may assume that $\beta = -1$, whence

$$(19) \qquad \alpha = \delta = 11, \quad \beta = -1, \quad \gamma = -253, \quad \eta = 6, \quad \zeta = -66;$$

and

$$(20) \qquad \alpha_1 + 11\alpha_2 = 0, \quad 2\lambda + \alpha_1 + \alpha_2 = -264.$$

Let $x = x_1 + x_2$ so that $4x \in \Lambda_2$. Then $u(x^2) = u_{11} + u_{22} + 2u_{12}$. Also,

$$\begin{aligned} u(x^2)^2 &= (-253 + 11 + 2(11) + 4(-66))(u_{11} + u_{22}) \\ &\quad + [11 + 11 - 2 + 4 \cdot 6] \sum_{k \neq 1,2} u_{kk} + 8\alpha_1 u_{12} \\ &= -484(u_{11} + u_{22}) + 44 \sum_{k \neq 1,2} u_{kk} + 8\alpha_1 u_{12} \\ &= \{-528(u_{11} + u_{12}) + 8\alpha_1 u_{12}\} + 44\underline{\underline{d}}. \end{aligned}$$

Since $\cdot 2$, the centralizer in $\cdot 0$ of $\mathbb{Q}x$, has constituents of dimensions 1, 23, 275 on U_0 it follows that $u(x^2)^2 \in \mathbb{Q}(u(x^2) - \frac{1}{12}\underline{\underline{d}})$. Therefore, $u(x^2)^2 = -528(u(x^2) - \frac{1}{12}\underline{\underline{d}})$, and this forces $8\alpha_1 = -1056$, or $\alpha_1 = -132$. Consequently,

$$(21) \qquad \alpha_1 = -132, \quad \alpha_2 = 12, \quad \lambda = -72,$$

and the Lemma is proven.

Lemma 5.4. *Suppose that A_1, A_2 and A_3 are among the $\mathbb{Q}\hat{C}$-modules $\{\mathbb{Q}, U_0, V, W\}$ and that $\langle A_1 \otimes A_2, A_3 \rangle \neq 0$. The either two of $\{A_1, A_2, A_3\}$ are equal and the third is $\mathbb{Q}$, or else one of the following cases occurs:*

(i) $\langle U_0 \otimes V, V \rangle = \langle U_0, V \otimes V \rangle = \langle U_0, S^2 V \rangle = 1$;

(ii) $\langle U_0 \otimes W, W \rangle = \langle U_0, W \otimes W \rangle = \langle U_0, S^2 W \rangle = 1$;

(iii) $\langle V \otimes V, V \rangle = \langle S^2 V, V \rangle = 1$ *and* $\langle S^3 V, \mathbb{Q} \rangle = 1$;

(iv) $\langle V \otimes W, W \rangle = \langle V, W \otimes W \rangle = \langle V, S^2 W \rangle = 2$;

(v) $\langle U_0 \otimes U_0, U_0 \rangle = \langle S^2 U_0, U_0 \rangle = 1$ *and* $\langle S^3 U_0, \mathbb{Q} \rangle = 1$.

Proof. By considering these modules restricted to Q, it is clear that the only candidates for $\langle A_1 \otimes A_2, A_3 \rangle \neq 0$ are the ones listed.

(i) Let us consider $\langle V\otimes V, U_0\rangle = \langle V, V\otimes U_0\rangle$. Using the discussion of Sect. 4, recall that V has a basis $v(\tilde{\lambda})$, $\tilde{\lambda}\in\tilde{\Lambda}_2$, where $v(\tilde{\lambda})$ affords a linear character of Q. In $V\otimes V$, the $v(\tilde{\lambda})\otimes v(\tilde{\mu})$ afford all the linear characters of Q. Since U_0 is a trivial Q-module, the only basis elements in $V\otimes V$ which are relevant are those with $\tilde{\lambda}=\tilde{\mu}$. Let V_1 be the $\mathbb{Q}$-span of all $v(\lambda)\otimes v(\lambda)$. Then clearly V_1 is just the permutation module for C on the cosets of C_2, and may be regarded as the permutation module for $\cdot 1$ on the cosets of $\cdot 2$, or rather of its image under $\cdot 0\to\cdot 1$. Thus, $\langle V\otimes V, U_0\rangle = \langle V_1, U_0\rangle = \langle 1_{C_2}^{C}, U_0\rangle = \langle 1_{C_2}, U_0|_{C_2}\rangle$, by Frobenius reciprocity. We argue that $U_0|_{C_2}$ is a direct sum of irreducibles of dimensions 1, 23 and 275, from which the desired result follows. See [12] for the degrees of the irreducibles for .2. This becomes clear by taking a vector λ of type 2 and considering $S^2(\mathbb{Q}\otimes\Lambda) = S^2(\mathbb{Q}\lambda^{\perp}\oplus\mathbb{Q}\lambda^{\perp})\cong S^2(\mathbb{Q}\lambda)\oplus S^2(\mathbb{Q}\lambda^{\perp})\oplus(\mathbb{Q}\lambda\otimes\mathbb{Q}\lambda^{\perp})$. Finally, we get $\langle S^2 V, U_0\rangle = 1$ since $V\otimes V\to V_1$ factors through $S^2 V$.

(ii) We have $W\cong T\otimes\Lambda$ and so $W\underset{\mathbb{Q}}{\otimes} W\cong(T\underset{\mathbb{Q}}{\otimes} T)\underset{\mathbb{Z}}{\otimes}(\Lambda\underset{\mathbb{Z}}{\otimes}\Lambda)$. We are interested only in the $\hat{C}$-constituents of $W\otimes W$ which are trivial for Q. This amounts picking out the single occurrence of the principal character for Q in $T\otimes T$. Thus,

$$\langle U_0, W\otimes W\rangle = \langle U_0, \mathbb{Q}\underset{\mathbb{Z}}{\otimes}\Lambda\underset{\mathbb{Z}}{\otimes}\Lambda\rangle = \langle U_0, U_0\oplus\mathbb{Q}\rangle = 1+0=1.$$

We exhibit a nonzero invariant map $W\otimes W\to U_0$, viz.,

$$(e(x)\otimes x_i)\otimes(e(y)\otimes x_j)\mapsto\delta_{xy}\,u_0(u_{ij}).$$

Since the map is clearly symmetric, we get $\langle U_0, S^2 W\rangle = 1$.

(iii) See Lemma 5.2.

(iv) We have $\langle W\otimes W, V\rangle = \langle T\otimes T\otimes\Lambda\otimes\Lambda, V\rangle$. We may decompose $T\otimes T = T(0)\oplus T(2)\oplus T(3)\oplus T(4)$ as $\hat{C}$-modules, where $T(i)$ represents all the linear characters corresponding to an orbit of $\hat{C}$ on Q/Q', represented by $\overline{q(\lambda)}$, where $\lambda\in\Lambda_i$. We have $\dim T(0)=1$, $\dim T(2)=98{,}280$, $\dim T(3)=8{,}386{,}560$, $\dim T(4)=8{,}292{,}375$. By checking $\dim S^2 T=8{,}390{,}656$ and $\dim\bigwedge^2 T=8{,}386{,}560$ and noting that the linear characters of Q occuring in $S^2 T$ and $\bigwedge^2 T$ must form orbits, we see that $T(0)$, $T(2)$ and $T(4)$ occur in $S^2 T$ and $T(3)=\bigwedge^2 T$. Since $V|_Q\cong T(2)$,

$$\langle W\otimes W, V\rangle = \langle T(2)\otimes\Lambda\otimes\Lambda, V\rangle = \langle V\otimes\Lambda\otimes\Lambda, V\rangle = \langle\mathbb{Q}\otimes\Lambda\otimes\Lambda, V\otimes V\rangle.$$

Since Λ is a trivial Q-module, the only constituents in $V\otimes V$ which count are the ones affording the principal Q-character. Using the notation in (i), V_1 means the submodule of $V\otimes V$ spanned by all $v(\lambda)\otimes v(\lambda)$. So,

$$\langle\mathbb{Q}\otimes\Lambda\otimes\Lambda, V\otimes V\rangle = \langle\mathbb{Q}\otimes\Lambda\otimes\Lambda, V_1\rangle = \langle\Lambda\otimes\Lambda, 1_{C_2}^{C}\rangle = \langle\Lambda\otimes\Lambda\ {}_{C_2}, 1_{C_2}\rangle_{C_2} = 2,$$

as in (i). But now it is clear that $\langle S^2 W, V\rangle = 2$ once we exhibit the maps

$$(t_1\otimes\lambda_1)\otimes(t_2\otimes\lambda_2)\to c_1\langle\lambda_1,\lambda_2\rangle\, p(t_1\otimes t_2) + c_2\, p_0(u_0(\lambda_1\,\lambda_2), p(t_1\otimes t_2)),$$

where c_1 and c_2 are scalars, p is the projection $T\otimes T\to T(2)\cong V$ and p_0 is the pairing $U_0\otimes V\to V$ described in (i).

(v) This may be deduced directly from a calculation with the character table of $\cdot 1$ [12], using Lemma 2.8. An alternate proof goes as follows. Lemma 2.39 (iii) shows that $\langle U_0 \otimes U_0, U_0 \rangle \geqq \langle S^2 U_0, U_0 \rangle \geqq 1$ and $\langle S^3 U_0, \mathbb{Q} \rangle \geqq 1$. We get $\langle S^2 U_0, U_0 \rangle \leqq 1$ from Lemma 5.2, whence $\langle S^2 U_0, U_0 \rangle = \langle S^3 U_0, \mathbb{Q} \rangle = 1$, as required.

Definition 5.5. For $\tilde{\lambda} \in \tilde{\Lambda}_2$, write $v(\lambda)$ or $v(\tilde{\lambda})$ for the element A_λ, regarding V as a direct summand of $T \otimes T$ ($V = T(2)$ in the notation of Lemma 5.4(iv)).

The bilinear map p: $U \times \mathbb{Q} \otimes \Lambda \to \mathbb{Q} \otimes \Lambda$ is defined by

$$\begin{aligned} &p(u_{ii}, x_i) = -69 x_i, && \\ &p(u_{jj}, x_i) = 3 x_i && i \neq j, \\ &p(u_{ij}, x_i) = -36 x_j && i \neq j, \\ &p(u_{jk}, x_i) = 0 && i \neq j \neq k \neq i. \end{aligned}$$

By examining the proof of Lemma 5.4 we can get the maps explicitly.

Corollary 5.6. *In the notation of Lemma* 5.4 *the relevant spaces of bilinear maps are spanned, by respectively:*

(i) $u_0 \otimes v(\lambda) \mapsto (u_0, u(\lambda^2))\, v(\lambda)$;
$v(\lambda) \otimes v(\mu) \mapsto \delta_{\tilde{\lambda}, \tilde{\mu}}\, u_0(\lambda^2)$;

(ii) $u_0 \otimes (e(x) \otimes x_i) \mapsto e(x) \otimes p(u_0, x_i)$;
$(e(x) \otimes x_i) \otimes (e(y) \otimes x_j) \mapsto \delta_{xy}\, u_0(u_{ij})$;

(iii) $v(\lambda) \otimes v(\mu) \mapsto \begin{cases} \beta'(\lambda, \mu)\, v(\lambda + \mu) & \lambda, \mu, \lambda + \mu \in \Lambda_2, \\ 0 & \textit{otherwise}; \end{cases}$

(iv) $(e(x) \otimes x_i) \otimes (e(y) \otimes x_i) \mapsto \sum\limits_{\substack{\tilde{\lambda} \in \tilde{\Lambda}_2 \\ x_\lambda = xy}} [c\delta_{ij} + c'(u_0(u_{ij}), u(\lambda^2))]\, \phi_\lambda(x)\, v(\lambda)$,
c, c' *scalars*;
$v(\lambda) \otimes (e(x) \otimes x_i) \mapsto \sum\limits_{j \in \Omega} [c\delta_{ij} + c'(u_0(u_{ij}), u(\lambda^2))]\, \phi_\lambda(x)\, e(x x_\lambda) \otimes x_j$.

Remark: Here, B is assumed to have a C-invariant positive definite form (,) (any choice will do here, see Definitions 5.1 and 5.5 for additional notation); also $u_0 \in U_0$, $\lambda \in \Lambda_2$, $x \in F$, $i \in \Omega$. The sign $\beta'(\lambda, \mu) = \pm 1$ may be arranged to equal $\phi_{\lambda+\mu}(x_\lambda)$; see Lemma 5.1.

Proof. Whenever possible, we shall use the notation in the proof of Lemma 5.2.

(i) Since C_2, the stabilizer in C of $\tilde{\lambda}$, has one 1-dimensional submodule in V, namely $\mathbb{Q} v(\lambda)$, and just one in U_0, namely $\mathbb{Q} u_0(\lambda^2)$, the first formula in (i) may be assumed to hold for one particular λ. To see that it holds for arbitrary $\lambda \in \Lambda_2$, apply elements of C to both sides of the equation. Thus, the first formula of (i) follows. As for the second, the image of $v(\lambda) \otimes v(\mu)$ in U_0, if nonzero, affords the character $\phi_\lambda \phi_\mu$ of Q. Since any nontrivial image must afford the trivial character, the second formula may be assumed to hold for particular λ. The validity for all elements of $\tilde{\Lambda}_2$ follows by applying elements of C to both sides of the equation for λ.

(ii) The second formula clearly exhibits a nontrivial C-map when interpreted as $(T \otimes \Lambda) \otimes (T \otimes \Lambda) \cong (T \otimes T) \otimes (\Lambda \otimes \Lambda) \to \mathbb{Q} \otimes U \to U_0$. The first argument may be taken from the second by use of the adjointness relation. The first argument may be taken from U (not just U_0) as long as we require $p(\underline{\underline{d}}, -)$ to be the zero map. We use a $\cdot$ to denote the first pairing. We have $(u_{ij} \cdot e(x) \otimes x_k,\ e(y) \otimes x_l) = a\delta_{xy}(u_{ij}, u_0(u_{kl}))$, for some scalar $a \neq 0$ and all $i, j, k \in \Omega$, $x \in F$. Without loss, $a = 1$. Thus, $u_{ij} \cdot e(x) \otimes x_k = e(x) \otimes h(u_{ij}, x_k)$, for some bilinear function $h \neq 0$ which commutes with the action of $\hat{C}$.

We now use the group $N_{24} \leqq .1$ to get the values of h. Since $h(u_{ij}, x_i) \in \mathbb{Q} \underset{\mathbb{Z}}{\otimes} \Lambda$ affords the character of $O_2(N_{24})$ which $\mathbb{Q}x_i$ affords, we must have $h(u_{ii}, x_i) = \alpha_1 x_i$, for some $\alpha_1 \in \mathbb{Q}$ since this character occurs with multiplicity one. Note that α_1 is independent of i, by the action of N_{24}. Since all the u_{ij} and x_k are eigenvectors for $O_2(N_{24})$, similar arguments give α_2, $\alpha_3 \in \mathbb{Q}$ so that $h(u_{jj}, x_i) = \alpha_2 x_i$ and $h(u_{ij}, x_i) = \alpha_3 x_j$ for $i \neq j$. Note that $h(u_{ij}, x_k) = 0$ for distinct i, j, k.

Since $h(\underline{\underline{d}}, x_i)$ is zero, we get $\alpha_1 + 23\alpha_2 = 0$. The vectors $\lambda = 8x_1$ and $\mu = 4(x_1 + x_2 + x_3 + x_4)$ have type 4, and there is $g \in \hat{C}$ with $\lambda^g = \mu$. We have $h(u(\lambda^2), \lambda) = h(64u_{11}, 8x_1) = 512\alpha_1 x_1 = 64\alpha_1 \lambda$. Also

$$\begin{aligned} h(u(\mu^2), \mu) &= h\left(16\left(\sum_{i=1}^{4} u_{ii} + 2\sum_{1 \leq i < j \leq 4} u_{ij}\right), 4(x_1 + x_2 + x_3 + x_4)\right) \\ &= 64(\alpha_1 + 3\alpha_2 + 6\alpha_3)(x_1 + x_2 + x_3 + x_4) = 16(\alpha_1 + 3\alpha_2 + 6\alpha_3)\,\mu. \end{aligned}$$

Since $\lambda^g = \mu$, $\alpha_1 + 3\alpha_2 + 6\alpha_3 = 4\alpha_1$, or $-\alpha_1 + \alpha_2 + 2\alpha_3 = 0$. So, $\alpha_1 = -23\alpha_2$ and $\alpha_3 = -12\alpha_2$, and taking $\alpha_2 = 3$ gives $h = p$, as desired.

(iii) This follows from Lemma 5.1.

(iv) To get the first formula, we need to project $e(x) \otimes e(y)$ into the space $T(2)$, in the notation of Lemma 5.3. Since the A_λ, $\tilde{\lambda} \in \tilde{\Lambda}_2$, form an orthonormal basis for $T(2)$, one has

$$e(x) \otimes e(y) \mapsto \sum_{\tilde{\lambda} \in \tilde{\Lambda}_2} (e(x) \otimes e(y), A_\lambda)\, A_\lambda = \sum_{\substack{\tilde{\lambda} \in \tilde{\Lambda}_2 \\ x_\lambda = xy}} \frac{1}{2^6}\, \phi_\lambda(x)\, A_\lambda.$$

Tensoring this map with the inner product $(\mathbb{Q} \otimes \Lambda) \otimes (\mathbb{Q} \otimes \Lambda) \to \mathbb{Q}$ gives one map. Using the map $(\mathbb{Q} \otimes \Lambda) \otimes (\mathbb{Q} \otimes \Lambda) \to U_0$ and the pairing from (i), we get a second map, clearly independent of the first.

Adjointness and the first formula imply the second.

Corollary 5.7. *Any algebra structure on B with an associative form, satisfying $B^2 \leqq U_0 + V + W$, $\underline{\underline{d}}B = 0$ and having C as a group of automorphisms is described by choices for six independent parameters.*

Proof. Lemma 5.3 and the adjointness requirement.

6. The Algebra Product

From Corollary 5.7, we see that an arbitrary C-invariant commutative algebra product $B \otimes B \to B$ satisfying $B^2 \leqq U_0 + V + W$, $\underline{\underline{d}}B = 0$ and the associative law for a nondegenerate symmetric bilinear form involves a choice of six parameters. We make the choices as indicated in Table 6.1, where we also choose a C-invariant bilinear form. The (ξ, η) entry gives the product $\xi\eta$. The commutative law permits us to drop certain entries in the table.

As mentioned in Sect. 4, the choice of structure constants is motivated by group-theoretic considerations, translated into linear algebra. We shall say more about this in Sect. 10.

From Corollary 5.5, we get explicitly described maps involving the relevant $\hat{C}$-modules. The symmetric map $\beta(\lambda, \mu)$ takes the values 0 or ± 36. When $\tilde{\lambda}, \tilde{\mu}$ do not span a triangle of type 222, $\beta(\lambda, \mu)=0$ and when they do, $\beta(\lambda, \mu)=-36\phi_{\lambda+\mu}(x_\lambda)=-36\phi_\mu(x_\lambda)$. Note that $x_\lambda=1$ for $\lambda \in \Lambda_2^4$, whence $\beta(\lambda, \mu)=-36$ whenever λ or μ is in Λ_2^4. Also, note that $\beta(\lambda, \mu)=\beta(\mu, \lambda)$, for all $\lambda, \mu \in \Lambda$.

Table 6.1. The algebra product

	$u \in U$	$v(\lambda),\ \tilde{\lambda} \in \tilde{\Lambda}_2$	$e(x) \otimes x_i,\ x \in F,\ i \in \Omega$
$u \in U$	(*)	$-\frac{9}{4}(u, u_0(\lambda^2))\, v(\lambda)$	$e(x) \otimes p(u, x_i)$ (**)
$v(\lambda)$	–	$-\frac{9}{4}u_0(\lambda^2)$	$\sum_{j \in \Omega} [-3\delta_{ij}+\frac{9}{32}(u_0(u_{ij}), u(\lambda^2))]\ \varphi_\lambda(x) \cdot e(x x_\lambda) \otimes x_j$
$v(\mu),\ \tilde{\lambda} \neq \tilde{\mu}$	–	$\beta(\lambda, \mu)\, v(\lambda+\mu)$ (***)	
$e(y) \otimes x_j$	–	–	$-18\delta_{xy}u_0(u_{ij})$ $+\sum_{\substack{\tilde{\lambda} \in \tilde{\Lambda}_2 \\ x_\lambda = xy}} [-3\delta_{ij}+\frac{9}{32}(u_0(u_{ij}), u(\lambda^2))] \cdot \varphi_\lambda(x) v(\lambda)$

(*) *The product on U:*

$u_{ii}^2=-253u_{ii}+11\sum_{j \neq i} u_{jj}$ $\qquad$ $u_{ii}u_{ij}=-132u_{ij}$

$u_{ii}u_{jj}=11(u_{ii}+u_{jj})-\sum_{k \neq i,j} u_{kk}$ $\qquad$ $u_{ii}u_{jk}=12u_{jk}$

$u_{ij}u_{jk}=-72u_{ik}$ $\qquad$ $u_{ij}^2=-66(u_{ii}+u_{jj})+6\sum_{k \neq i,j} u_{kk}$

$u_{ij}u_{kl}=0$ for i,j,k,l distinct

(**) $p(u_{ii}, x_i)=-69x_i$ $\qquad$ $p(u_{ij}, x_i)=-36x_j \quad i \neq j$

$p(u_{jj}, x_i)=3x_i, \quad i \neq j$ $\qquad$ $p(u_{ij}, x_k)=0 \quad i \neq j \neq k \neq i$

(***) $\beta(\lambda, \mu)=-36\phi_{\lambda+\mu}(x_\lambda)$ or 0 according to whether $\tilde{\lambda}$, $\tilde{\mu}$ do or do not span a triangle of type 222; in the former case, if λ or μ is in Λ_2^4, $\beta(\lambda, \mu)=-36$.

The inner product: $(u_{ii}, u_{jj})=4\delta_{ij}$, $(u_{ii}, u_{jk})=0$ for $j \neq k$.
$(u_{ij}, u_{kl})=2\delta_{\{i,j\},\{k,l\}}$ for $i \neq j$, $k \neq l$. $0=(U, V)=(V, W)=(U, W)$.
$(v(\lambda), v(\mu))=\delta_{\tilde{\lambda},\tilde{\mu}} \cdot (e(x) \otimes x_i, e(y) \otimes x_j)=\delta_{xy}\delta_{ij}$.

7. The Groups *F* and *J*

In this section we describe a particular complement F to E in Q (up to now, the complement has been arbitrary).

Write $E=\langle z\rangle\times E_0$, $E_0=C_E(e(1))$; see Sects. 3 and 4. We define $E(2)=\langle q(4x_i-4x_j)\,|\,i,j\in\Omega\rangle$. By Lemma 2.13, $|E_0\colon E(2)|=2$ and $E_0\cong\mathbb{Z}_2^{12}$. The subgroup $X=(N_C(E_0)\cap N_C(E(2)))'$ satisfies $X=X'$, $O_2(X)=E(2)$ and $X/E(2)\cong M_{24}$. Then $E_0=E(2)\times\langle z_1\rangle$ as X-modules, where $z_1=q(8x_\infty)$. (We may see that the extension $1\rightarrow 2^{11}\rightarrow X\rightarrow M_{24}\rightarrow 1$ is nonsplit because X may be embedded in F_{24}' as the stabilizer of a maximal commuting set of 3-transpositions [in the notation of Sects. 7 and 13, we may take $x_{3*}=\theta$, an element described below]; however, we do not need to know the extension type of X).

Since $E_0=q(\Lambda(4))$, if F is any complement to E in Q, we may define $F(2)=F\cap\langle q(\Lambda(2))\rangle$. Since $|\Lambda\colon\Lambda(2)|=2$ and $|\Lambda(8)+2\Lambda\colon 2\Lambda|=2$ (see Lemma 2.12), $\langle q(\Lambda(2))\rangle\cong 2\times 2_+^{1+22}$ and $|F\colon F(2)|=2$. From the definition of Λ in [11] one sees that if $\lambda\in\Lambda(2)$, then $S_\lambda:=\{i\in\Omega\,|\,\text{the } i^{\text{th}} \text{ coordinate of } \lambda \text{ is in } 2+4\mathbb{Z}\}$ is a $\mathscr{C}$-set. This is an invariant of the coset $\lambda+\Lambda(4)$ but not of $\lambda+2\Lambda$. Consider $\mu\in\lambda+2\Lambda$, with $S_\mu\neq S_\lambda$. Then $\mu-\lambda=2v$, $v\in\Lambda-\Lambda(2)$. Since every coordinate of v is odd, $2v\equiv(2,2,\dots,2)\,(\operatorname{mod}4)$. Thus, $S_\lambda+S_\mu=\Omega$ and we see that the element $\{S_\lambda,S_\lambda+\Omega\}\in\bar{\mathscr{C}}$ is an invariant of $\lambda+2\Lambda$. So, we get an isomorphism $F(2)\cong\bar{\mathscr{C}}$ (referred to in Sect. 2). We write this $x\mapsto S_x$ (where S_x means a $\mathscr{C}$-set or its image in $\bar{\mathscr{C}}$) and $S\mapsto x_S$ (where S means an element of $\mathscr{C}$ or $\bar{\mathscr{C}}$).

Choose $h\in C$, $|h|=11$ so that $\hat{h}=h^{\hat{\pi}}$ is arranged to satisfy

(1) $\hat{h}=(0)(1,2,4,8,16,9,18,13,3,6,12)(\infty)(15,7,14,5,10,20,17,11,22,21,19)\in M_{24}\leqq N_{24}$.

Recall that

(2) $\mathscr{Q}=\{0,1,2,4,8,16,9,18,13,3,6,12\}$, the squares in $\mathbb{F}_{23}$, is a dodecad in $\mathscr{C}$ and that

$$\mathscr{N}=\mathscr{Q}+\Omega,\qquad \mathscr{Q}^\times=\mathscr{Q}-\{0\},\qquad \mathscr{N}^\times=\mathscr{N}-\{\infty\}.$$

We have $E(2)^h=E(2)$ and

(3)
$$E_1:=[E(2),h]=\langle q(4x_i-4x_j)\,|\,i,j\in\mathscr{Q}^\times\rangle\cong\mathbb{Z}_2^{10};$$
$$E_1 \text{ has a basis } \{q(4x_1-4x_j)\,|\,j\in\mathscr{Q}^\times-\{1\}\}.$$

We claim that

(4) $N_X(E_1)^{\hat{\pi}}=\langle -1_\Lambda\rangle\times M_{12}.2$, where the second direct factor is a subgroup of M_{24} stabilizing the complementary pair of dodecads, $\{\mathscr{Q},\mathscr{N}\}$; furthermore $N_P(E_1)^{\hat{\pi}}=(\langle -1_\Lambda\rangle\times\langle\varepsilon_{\mathscr{Q}}\rangle\times M_{12})2$, where $P:=N_C(E_0)$.

Namely, $E(2)\cong P(\Omega)_{\text{even}}/\mathscr{C}$ as $N_X(E_1)$-modules, and the stabilizer of E_1 in X corresponds to the stabilizer of a certain nonzero vector $A+\langle\Omega\rangle$ in the dual module $\bar{\mathscr{C}}$. Since $A+\langle\Omega\rangle$ is stable under h, order 11, A must be a dodecad. Since $\dim C_{\bar{\mathscr{C}}}(h)=1$, $A=\mathscr{Q}$ or $\mathscr{N}$ as required. The second assertion follows from the first.

From [12], we get that the centralizer of an element of order 11 in $\cdot 0$ looks like $\mathbb{Z}_2\times\mathbb{Z}_{11}\times\Sigma_3$, and the elements of order 3 in the centralizer act fixed point freely on Λ. Without loss, $\hat{h}\in N_{24}$. Let $\theta\in C_C(h)$, $|\theta|=3$ and let $s\in C_C(h)$ satisfy $\theta^s=\theta^{-1}$ and $\hat{s}\in N_{24}$. Then $s^2\in C_Q(\theta)=\langle z\rangle$. We define J by $\langle z\rangle\leqq J\leqq C$

and $J/\langle z\rangle = C_{C/\langle z\rangle}(\langle\theta, s\rangle)$. From [4] and [12], we get that $J/\langle z\rangle \cong \operatorname{Aut} M_{12}$. Then Lemma 2.10 and [36], give $J' = J'' \cong 2M_{12} = \hat{M}_{12}$. Since $s \in O_2(N_{24})$ and $\hat{s}$ has eigenvalues $\{-1^{12}, 1^{12}\}$, $J^{\hat{\pi}} \leqq N_{24}$ [12]. From [36], we get that $|s| = 2$.

We intend to let F be E_0^θ or $E_0^{\theta^{-1}}$. One of the nice properties we will have is that E_0 and F are J-invariant. First, however, we must develop further properties of J, θ and s.

Next, we claim that

(5) $N_J(E_1)/\langle z\rangle \cong PGL(2, 11)$; moreover, $N_J(E_1)^{\hat{\pi}} = L \times \langle -1_\Lambda\rangle$, where $L \leqq M_{24}$, $L \cong L_2(11)$ is the stabilizer of $\mathcal{Q}$ and $\{0, \infty\}$; also $N_J(E_1)' \cong L$.

A look at the basis $\{q(4x_0 - 4x_k) \mid k \in \mathcal{Q}^\times\}$ for $E(2)$ makes it clear that $E(2)$ is the $\mathbb{F}_2 L$-permutation module on the cosets of an A_5-subgroup of L (we may regard E_0 as a module for N_{24}). By Lemma 2.5, $H^1(L, E_1) = H^1(L, E(2)) = 0$. Note that $E(2)$ is a self-dual L-module. Now let L^* be the subgroup of J which maps isomorphically onto $LO_2(N_{24})/O_2(N_{24})$ under $N_{24} \to N_{24}/O_2(N_{24})$. (Any intransitive $L_2(11)$ subgroup of M_{12} splits over the center of $\hat{M}_{12} = 2M_{12}$.) Since $H^1(L, E(2)) = H^1(L, \mathbb{Z}_2) = 0$, L and $((L^*)^{\hat{\pi}})'$ are conjugate. Complete reducibility of L on E_0 implies that the unique conjugate L^{**} of L in N_{24} stabilizes $[E_0, h^{**}]$ and $C_{E_0}(h^{**})$ where h^{**} is an element of order 11 in L^{**}. This and the way E_1 was defined imply that $L = ((L^*)^{\hat{\pi}})'$. Clearly, $N_J(L^*)$ is in $N_J(E_1)$, and since $N_J(L^*)$ is maximal in J, (5) follows.

We define $Q_0 := C_Q(h) \cong 2_+^{1+4}$, $Q_1 := [Q, h] \cong 2^{1+20}$, $K := C_C(Q_0/Q_0') \leqq N_C(Q_1)$. Since K centralizes $z_1\langle z\rangle/\langle z\rangle$, $K^{\hat{\pi}} \leqq N_{24}$, whence K normalizes $Q_1 \cap E = \langle z, E_1\rangle$ and so $K^{\hat{\pi}} \leqq N_P(E_1)^{\hat{\pi}}$, which is given by (4). Since K fixes $q(\lambda_\infty)$ and $q(\lambda_0)$ modulo $\langle z\rangle$, $K^{\hat{\pi}} \leqq M_{22} \times \langle -1_\Lambda\rangle$ and from the preceeding sentence, we get $K^{\hat{\pi}} \leqq L \times \langle -1_\Lambda\rangle$ where L is the group discussed above. Since $Q_0 = \langle q(\{\lambda_\infty, \lambda_0, \lambda_{\infty,0}, 8x_\infty\})\rangle$, we easily get $K^{\hat{\pi}} = L \times \langle -1_\Lambda\rangle$. Since $L \leqq J^{\hat{\pi}}$, $[K, \theta] \leqq K \cap Q$ and so $C_K(\theta)/\langle z\rangle \cong L$ and $N_J(C_K(\theta))/\langle z\rangle \cong PGL(2, 11)$, the group of (5).

We describe the involutions of Q_0. There are nine non-trivial cosets of $\langle z\rangle$ in Q_0 consisting of involutions. They are represented by

(6)
$$q(8x_\infty), \quad q(2\sum_{i \in \mathcal{Q}^\times} x_i - 2x_0 - 4x_\infty),$$
$$q(2\sum_{i \in \mathcal{Q}^\times} x_i - 2x_0 + 4x_\infty), \quad \text{all in } q(\Lambda_4);$$
$$q(4x_\infty - 4x_0), \quad q(4x_\infty + 4x_0),$$
$$q(\lambda_\infty), \quad q(\lambda_0),$$
$$q(\lambda_{\infty,\mathcal{Q}}), \quad q(\lambda_{\infty,\mathcal{Q}} + 4x_\infty + 4x_0) = q(\lambda_{0,\mathcal{Q}}), \quad \text{all in } q(\Lambda_2).$$

Let us examine the action of θ more carefully. We may alter q so that $q(\Lambda) \cap E^{\theta^j} = E_0^{\theta^j}$, for $j = 0, 1, 2$ (the only special requirement on the set function q: $\Lambda \to Q$ made before this one was $q(\Lambda(4)) = E_0$; see Sect. 4). By replacing θ with θ^{-1} if necessary, we may assume that θ satisfies

(7)
$$q(8x_\infty) \overset{\theta}{\mapsto} q(y_1) \overset{\theta}{\mapsto} q(y_2)$$

where

$$y_1:=2\sum_{i\in\mathcal{Q}^\times} x_i-2x_0-4x_\infty \quad\text{and}\quad y_2:=y_1+8x_\infty.$$

Since θ preserves commutativity, (6) and (7) give

$$(8)\qquad \{q(4x_\infty-4x_0),\, q(4x_\infty+4x_0)\}\overset{\theta}{\mapsto}\{q(\lambda_\infty),\, q(\lambda_{0,\mathcal{Q}})\}$$
$$\overset{\theta}{\mapsto}\{q(\lambda_0),\, q(\lambda_{\infty,\mathcal{Q}})\}.$$

Since, for any involution $x\in Q$, $\langle x^{\langle\theta\rangle}\rangle\cong\mathbb{Z}_2\times\mathbb{Z}_2$, we get

$$(9)\qquad q(4x_\infty-4x_0)\overset{\theta}{\mapsto}q(\lambda_\infty)\overset{\theta}{\mapsto}q(\lambda_0),$$

and

$$q(4x_\infty+4x_0)\overset{\theta}{\mapsto}q(\lambda_{0,\mathcal{Q}})\overset{\theta}{\mapsto}q(\lambda_{\infty,\mathcal{Q}}).$$

We note that $E/\langle z\rangle$ is a uniserial J-module with composition factors of dimensions 1, 10 and 1 in that order; the radical is $\langle E_1,z_1,z\rangle/\langle z\rangle$ and the socle is $\langle z_1,z\rangle/\langle z\rangle$. Finally, note that $\lambda_{\infty,\mathcal{Q}}+4x_\infty+4x_0\equiv\lambda_{0,\mathcal{N}}\pmod{2\Lambda}$.

We define $F=E_0^\theta=E_0^{s\theta}=E_0^{s_0}$, where $s_0=s\theta=\theta s\theta^{-1}$. We have $N_{\langle J,\theta,s\rangle}(E_0)=\langle J,s\rangle$ and $N_{\langle J,\theta,s\rangle}(F)=\langle J,\theta s\theta^{-1}\rangle$.

We conclude this section with a few lemmas.

Lemma 7.1. (i) *In E_0, there are $2\binom{24}{2}=552$ members of $q(\Lambda_2)$.* (ii) *Under $\langle J,s\rangle$ the orbits are $\Gamma_k=\{q(4x_i\pm4x_j)\,|\,ij$ in $\mathcal{Q}\equiv k\pmod 2\}$ for $k=1,2$. We have $|\Gamma_1|=24\cdot12=288$, $|\Gamma_2|=24\cdot11=264$, and the stabilizers are J_1 and J_2 where $J_1/\langle z\rangle\cong PGL(2,11)$ and $J_2/\langle z\rangle\cong\mathbb{Z}_2\times\Sigma_6$, respectively.*

(iii) *Under J, the orbits are the same, and $J\cap J_1/\langle z\rangle\cong PSL(2,11)$, $J\cap J_2/\langle z\rangle\cong\Sigma_6$.*

Proof. (i) is clear. If ij in $\mathcal{Q}\equiv1\pmod 2$, then $(4x_i-4x_j)^s\equiv(4x_i+4x_j)\pmod{2\Lambda}$. Thus, it is clear that Γ_1 is an orbit for $\langle J,s\rangle$. Since $\langle J,s\rangle=J\times\langle s\rangle$, $|J_1/\langle z\rangle|=|PGL(2,11)|$, and the discussion of (5) shows that $J_1/\langle z\rangle\cong PGL(2,11)$. Now say ij in $\mathcal{Q}\equiv0\pmod 2$. Then s fixes both $4x_i-4x_j$ and $4x_i+4x_j\pmod{2\Lambda}$. It is not clear that Γ_2 is an orbit (it is possibly 2 orbits). We have $|J_2|=4.6!$ or $8.6!$ To settle this point and to determine J_2, we look at $\Gamma_2^\theta\subset q(\Lambda_2^2)$. Let $a=\pm1$ and say J_2 is the stabilizer of $q(u)$, where $u=4x_i+a4x_j$. Then J_2^θ is the stabilizer of $x=q(u^\theta)$. Since $x\in q(\Lambda_2^2)$, $\mathcal{O}=\operatorname{supp}(\lambda_x)$ is an octad. Since $J\cap J_2$ fixes $\{i,j\}$, $|\mathcal{O}\cap\mathcal{Q}|=2$ or 6 and so $J\cap J_2$ fixes both $\mathcal{Q}$ and $\mathcal{N}$. Let $\mathcal{D}_1\in\{\mathcal{Q},\mathcal{N}\}$ satisfy $|\mathcal{O}\cap\mathcal{D}_1|=6$. Then $J\cap J_2$ acts on $\mathcal{O}\cap\mathcal{D}_1$, and so we have a homomorphism $J\cap J_2\to\Sigma_6$. Since $J\cap J_2/\langle z\rangle\hookrightarrow\operatorname{Aut}(A_6)$, we get $J\cap J_2/\langle z\rangle\cong\Sigma_6$, proving (ii).

Since s fixes $4x_i-4x_j$ when ij in $\mathcal{Q}\equiv0\pmod 2$, clearly J is transitive on Γ_2 and $J\cap J_2/\langle z\rangle\cong\Sigma_6$. Let us consider Γ_1. If we arrange for $J\cap J_1$ to fix $\tilde\lambda_{\infty0'}$, it also fixes $\tilde\lambda_\infty=(\tilde\lambda_{\infty0'})^\theta$, hence fixes both ∞ and 0. Therefore, $J\cap J_1/\langle z\rangle$ has index 2 in $J_1/\langle z\rangle$, as required to complete the proof of (iii).

Lemma 7.2. *In the notation of Lemma 7.1, J_2 operates with orbits of length 2 and 6 on $\mathcal{O}$, where J_2 stabilizes $q(4x_i+a4x_j)$, $ij\equiv0\pmod 2$, $a=\pm1$, $\mathcal{O}=\operatorname{supp}q((4x_i+a4x_j)^\theta)$ and where J_2 acts via the action of N_{24} on Ω. Furthermore, the two orbits are $\mathcal{O}\cap\mathcal{Q}$ and $\mathcal{O}\cap\mathcal{N}$.*

Proof. In the natural action of $M_{12}\cdot 2$ on Ω, J_2 permutes $\{\mathcal{O}\cap\mathcal{Q},\ \mathcal{O}\cap\mathcal{N}\}$. Since the cardinalities of these sets are $\{2,6\}$ (see the proof of Lemma 7.1) J_2 fixes both and so fixes $\mathcal{Q}$ and $\mathcal{N}$. Easily, J_2 acts as Σ_6 on the one of size 6. Since the kernel of the action of J_2 on the one of size 2 must be embeddable in M_{10}, J_2 acts nontrivially there.

Lemma 7.3. *Let $\Delta(2,2)$, $\Delta(2,3)$ be the set of triangles in Λ_2 of type 222 whose vertices all lie in Λ_2^2 for $\Delta(2,2)$ and two of whose vertices lie in Λ_2^3 and one of whose vertices lie in Λ_2^2 for $\Delta(2,3)$. Let $H_\infty \leqq N_{24}$ satisfy $H_\infty \geqq O_2(N_{24})$, $H_\infty/O_2(N_{24})\cong M_{23}$, the subgroup fixing $\infty\in\Omega$. Then the orbits of H_∞ on $\Delta(2,2)$ and $\Delta(2,3)$ are as follows:*

$\Delta(2,2)$: *two orbits, according to whether ∞ lies in the support of one of the vectors or not.*

$\Delta(2,3)$: *six orbits according to whether*

$$\left.\begin{array}{lll} i=j & \infty\notin\mathcal{O}, & \infty=i,\\ i=j & \infty\notin\mathcal{O}, & \infty\neq i,\\ i=j & \infty\in\mathcal{O}, & \end{array}\right\} i\notin\mathcal{O}.$$

$$\left.\begin{array}{ll} i\neq j & \infty\notin\mathcal{O}\\ i\neq j & \infty\in\mathcal{O}-\{i,j\},\\ i\neq j & \infty\in\{i,j\} \end{array}\right\} i,j\in\mathcal{O}.$$

Remark. We extend the notation $\Delta(2,3)$, $\Delta(2,2)$ to triples of elements in $\tilde{\Lambda}_2$ in the obvious way. We may refer to a triple of elements of Q as a triangle in $\Delta(2,2)$ or $\Delta(2,3)$ if, modulo $\langle z\rangle$, it is the image of a triangle in $\Delta(2,2)$ or $\Delta(2,3)$ under q.

Proof. Consider $\Delta(2,2)$. Let $\lambda,\mu,\lambda+\mu$ be a triangle in $\Delta(2,2)$, $\mathcal{O}_1=\operatorname{supp}\lambda$, $\mathcal{O}_2=\operatorname{supp}\mu$, $\mathcal{O}_1+\mathcal{O}_2=\mathcal{O}_3=\operatorname{supp}\lambda+\mu$. The action of $O_2(H_\infty)$ enables us to assume λ has all positive coordinates and μ has all negative coordinates. If suffices to consider two cases.

If $\infty\in\mathcal{O}_1\cup\mathcal{O}_2\cup\mathcal{O}_3$, we may assume at the outset that $\infty\in\mathcal{O}_1\cap\mathcal{O}_2$. Given $\mathcal{O}_1$ and the four-element subset $\mathcal{O}_1\cap\mathcal{O}_2$ of $\mathcal{O}_1$, there are exactly four octads meeting $\mathcal{O}_1$ in this subset. These octads give a sextet of tetrads, and it is pretty easy to see that the subgroup of the sextet stabilizer in M_{23} stabilizing $\mathcal{O}_1\cap\mathcal{O}_2$ and $\mathcal{O}_1$ is transitive on the above four octads.

If $\infty\notin\mathcal{O}_1\cup\mathcal{O}_2\cup\mathcal{O}_3$ a similar argument works. All one needs is that a sextet stabilizer induces Σ_6 on the set of six tetrads and the kernel of the action induces A_4 on each tetrad.

Consider $\Delta(2,3)$. We may assume $\lambda=\lambda_{i,S}$, $\mu=\lambda_{j,T}$. Clearly, there are two cases: $\infty\in\{i,j\}$ and $\infty\notin\{i,j\}$. By using the action of $O_2(H)$, we may assume $S=\emptyset$. Then, we may arrange that either $i=j$ and T is an octad avoiding i or $i\neq j$ and T is a 16-set avoiding i and j (see Lemma 2.3). Assume $i=j$. Then $\lambda+\mu$ looks like $(2^8 0^{16})$ (all coordinates positive) and we have the required transitivity in all cases $i=\infty$, $i\neq\infty$, and $\infty\in T$, $\infty\notin T$. Assume $i\neq j$. If $\infty\in\mathcal{O}=\Omega+T$, the stabilizer of $\mathcal{O}$ in M_{23}, is $2^4.\ A_7$, doubly transitive on $\mathcal{O}-\{\infty\}$. If $\infty\in T$, the stabilizer of $\mathcal{O}$ in M_{23} is A_8, doubly transitive on $\mathcal{O}$. The lemma follows.

Lemma 7.4. $|q(\Delta(2,3))\cap F| = 2^7.3^2.11 = 24.12.22.2$ *and* $|q(\Delta(2,2))\cap F| = 2\binom{12}{2}2.10.2.\frac{1}{3} = 2^4.5.11$.

Proof. Since $E_0^\theta = F$, we need to compute only $|q(\Delta(2,3)^{\theta^{-1}})\cap E|$ and $|q(\Delta(2,2)^{\theta^{-1}})\cap E|$.

The number of ways to complete $4x_\infty - 4x_0$ to a triangle with sides in $\Lambda_2 \cap \Lambda(4)$ is $22\cdot 2 = 44$. Since Γ_1 is an orbit under $\langle J, s\rangle$, we get $|\Delta(2,3)\cap E| = \frac{1}{2}\cdot 24\cdot 12\cdot 2\cdot 44 = 2^7 3^2\cdot 11$. A similar calculation verifies the second statement.

Lemma 7.5. *Let* $\{\mathscr{D}_1, \mathscr{D}_2\} = \{\mathscr{Q}, \mathscr{N}\}$, $i\in\mathscr{D}_1$, $S\in\mathscr{C}$ *so that* $q(\lambda_{i,S})\in F$. *Let* $J(i,S) = C_J(\tilde{\lambda}_{i,S})$. *Then, there exists a unique* $j := \gamma(i,S)\in\mathscr{D}_2$ *such that* $\{k\in\Omega \mid J(i,S)$ *fixes* $k\} = \{i,j\}$. *Also, given* i, $\gamma(i,S)$ *ranges over the* 12 *values of* $\mathscr{D}_2$.

Proof. Let $u = q(\lambda_{i,S})^{\theta^{-1}} = q(\eta)$, for $\eta\in\Lambda_2^4$. Then $J(i,s)$ leaves invariant $\operatorname{supp}(\eta) = \{k,l\}$, say. Without loss, $\tilde{\lambda}_{i,S} = \tilde{\lambda}_\infty$, $\tilde{\eta} = \tilde{\lambda}_{\infty,0'}$. Then $J(i,S)^{\hat{\pi}} = L\times\{\pm 1\}$, which fixes precisely $\{\infty, 0\}$ in Ω. The first statement follows. Since an M_{11}-subgroup of J containing L and fixing ∞ has $\{\lambda_{\infty,S} \mid S\in\mathscr{C},\ q(\lambda_{\infty,S})\in F\}$ as an orbit of length 12 (see Lemma 7.1(iii)), the second statement follows since this M_{11}-subgroup is transitive on $\mathscr{D}_2$ [11].

Lemma 7.6. *Every member,* x, *of* $q(\Lambda_2^2)\cap F$ *lies in a triple of elements of* F *forming a triangle in* $\Delta(2,3)$. *In fact, it lies in* 24 *such triples. Also,* $C(x)\cap N_{\langle J,s,\theta\rangle}(F)$ *acts with two orbits on this set of triples. There are two* J-*orbits on* $q(\Delta(2,3))\cap F$.

Proof. Using θ, the first statement is equivalent to the following: given distinct $i,j\in\Omega$ and $a = \pm 1$ with ij in $\mathscr{Q}\equiv 0 \pmod 2$, there is $k\in\Omega$ with ik in $\mathscr{Q}\equiv 1 \pmod 2$ (for then $\{4x_i + a4x_j,\ -4x_i \pm 4x_k,\ \mp 4x_k - a4x_j\}$ is a triangle with two generators and one nongenerator for the J-module $\Lambda(4) + 2\Lambda/2\Lambda$). The latter statement is clearly true. The second statement is easily deduced from this discussion: for each ordered triple (i,j,a), there are 12 choices of k and two choices of coefficient ± 1. Lemma 7.1 and its proof imply that $C_{\langle J,s\rangle^{\hat{\pi}}}(4x_i + a4x_j)$ has two orbits on this set of triangles, corresponding to its two orbits on $\mathscr{N}$. The third and fourth statements follow.

Lemma 7.7. (i) *The triples in* $q(\Lambda_2)\cap F$ *represent every* H_∞ *orbit in* $\Delta(2,3)$ *and* $\Delta(2,2)$ *except for those orbits in* $\Delta(2,3)$ *with* $i = j$ *(in the notation of Lemma* 7.3).

(ii) *If* $\lambda = \lambda_{i,S}$, $q(\lambda)\in F$, *then the triangles in* $\Delta(2,3)\cap F^{p^{-1}}$ *which contain* λ *are spanned by* λ *and* μ, *where* $i\in\mathscr{D}_1\in\{\mathscr{Q},\mathscr{N}\}$, $\mu = \pm\lambda_{j,T}$, $j\neq i$ *and one of the following cases holds* ($\mathcal{O} = \operatorname{supp}(\lambda+\mu)$, $\lambda+\mu\in\Lambda_2^2$, $\mathscr{D}_2\in\{\mathscr{Q},\mathscr{N}\} - \{\mathscr{D}_1\}$):

(ii. a) $j\in\mathscr{D}_1$, $\{i,j\} = \mathcal{O}\cap\mathscr{D}_1$, $\gamma(i,S)\in\mathcal{O}\cap\mathscr{D}_2$;
(ii. b) $j = \gamma(i,S)\in\mathscr{D}_2$, $|\mathcal{O}\cap\mathscr{D}_1| = 2$;
(iii. c) $j = \gamma(i,S)\in\mathscr{D}_2$, $|\mathcal{O}\cap\mathscr{D}_1| = 6$,
(iv. d) $j\in\mathscr{D}_2 - \{\gamma(i,S)\}$, $\mathcal{O}\cap\mathscr{D}_2 = \{j, \gamma(i,S)\}$.

Furthermore, each case arises and characterizes an orbit of $J(i,S)$ *on the set of triangles in* $\Delta(2,3)$ *which contain* λ.

(iii) *In* (ii), *the pointwise stabilizer in* J *of* $\{\lambda, \mu, \lambda+\mu\}$ *is, modulo* $\langle z\rangle$, *isomorphic to* A_5, *and it fixes three points and has an orbit of length* 5 *on the octad* $\mathcal{O}$.

Proof. (i) We consider $\Delta(2,2)$. There are such triangles in $q(\Lambda_2)\cap F$, for instance, $\{4x_0-4x_1,\ 4x_0-4x_2,\ 4x_1-4x_2\}^{\hat{\theta}}$. If $\mathcal{O}, \mathcal{O}', \mathcal{O}''=\mathcal{O}+\mathcal{O}'$ are the octads which support the three vectors, its easy to arrange $\infty\in(\mathcal{O}\cup\mathcal{O}')^g$ or $\infty\notin(\mathcal{O}\cup\mathcal{O}')^g$ for appropriate $g\in J$. The statement about H_∞-orbits on $\Delta(2,2)$ now follows easily from Lemma 7.3.

We now consider $\Delta(2,3)$. There are triangles in $\Delta(2,3)\cap F^{q^{-1}}$ (see Lemma 7.4). We prove that, if $\{\lambda,\mu,\lambda+\mu\}$ is such a triangle, $\lambda,\mu\in\Lambda_2^3$, then $i(\lambda)\neq i(\mu)$. Given $\tilde{\lambda}_{\infty,0'}$, the set of $\tilde{\lambda}_{rs}, \tilde{\lambda}_{rs'}$ which, with $\lambda_{\infty,0'}$, span a triangle of type 222 is the union of eight sets $E(r,\mathcal{D},\varepsilon)$ where $r=0,\infty$, $\mathcal{D}=\mathcal{Q},\mathcal{N}$, $\varepsilon=+,-$ and $E(r,\mathcal{D},+)=\{\tilde{\lambda}_{r,s}|s\in\mathcal{D}^\times\}$ and $E(r,\mathcal{D},-)=\{\tilde{\lambda}_{r,s'}|s\in\mathcal{D}^\times\}$. Also, each of these eight sets is an L-orbit of length 11, where $L=C_{J^{\hat{\pi}}}(\tilde{\lambda}_{\infty,0'})\cong L_\lambda(11)$. This action leaves invariant an equivalence relation $\sim$, where $E(\infty,\mathcal{D},\varepsilon)\sim E(0,\Omega+\mathcal{D},\varepsilon)$, for all $\mathcal{D},\varepsilon$ (we explain the relation as follows: given a triangle of type 222 as above, the two legs distinct from $\lambda_{\infty,0'}$ correspond to elements of the two sets in a $\sim$-class). Similarly, on F, $E(\lambda):=\{\tilde{\eta}\in\tilde{\Lambda}_2^3|q(\eta)\in F$ and λ,η span a triangle of type 222$\}$ is a union of four L-orbits. Since $|\{\tilde{\eta}\in E(\lambda)|i(\eta)=i(\lambda)\}|$ is at most 11 (see Lemma 7.1 (ii)), $E^*(\lambda):=\{\tilde{\eta}\in E(\lambda)|i(\eta)\neq i(\lambda)\}$ consists of three or four of these orbits, whence $|E^*(\lambda)|/|E(\lambda)|=\frac{3}{4}$ or 1. By Lemma 7.1 (ii), this ratio is independent of $\lambda\in\Lambda_2^3\cap F^{q-1}$. For $\eta\in\Lambda_2^2$ with $q(\eta)\in F$, we let Δ_η be the set of triangles in $\Delta(2,3)\cap F^{q^{-1}}$ which contain η. By Lemma 7.6, $|\tilde{\Delta}_\eta|=24$ and $i(\zeta)=i(\rho)$ for 0, 12 or 24 of the $\{\tilde{\eta},\tilde{\zeta},\tilde{\rho}\}\in\tilde{\Delta}_\eta$. Write $i(\Delta_\eta)=0$, $\frac{1}{2}$ or 1 for these three cases, respectively. By Lemma 7.1 (ii), $i(\Delta_\eta)$ is independent of $\eta\in\Lambda_2^2\cap F^{q^{-1}}$. So, $|i(\Delta_\eta)|=|E^*(\lambda)|/|E(\lambda)|\geqq\frac{3}{4}$ implies that $i(\Delta_\eta)=1$ and $E^*(\lambda)=E(\lambda)$, as required.

To prove that one of the four cases in (ii) applies, we may assume that $\lambda=\lambda_\infty$ (because of Lemma 7.1 (iii) and the fact that J preserves $\{\mathcal{Q},\mathcal{N}\}$). Since $E(\lambda)$ decomposes into four orbits, we must show that each orbit corresponds to exactly one case in (ii). Since $\tilde{\lambda}=\tilde{\lambda}^\theta_{\infty,0'}$, the four orbits are the images of E_* under θ, where E_* ranges over a set of representatives for the four $\sim$ classes described above, and where we always choose E_* to contain $\tilde{\lambda}_{rs}$ or $\tilde{\lambda}_{rs'}$ with rs in $\mathcal{Q}\equiv 1 \pmod 2$.

Say $\mu=\pm\lambda_{k,S}\in E^\theta_*$. We may assume that S is an octad. Then $\infty, k\in S$ (see Lemma 2.3). Let $L_\mu=C_L(\mu)$. By transforming $\{\lambda,\mu,\lambda+\mu\}$ with θ^{-1}, we see that L_μ fixes three points of Ω, whence $L_\mu\cong A_5$ (one obtains nonconjugate L_μ, according to whether the fixed point distinct from ∞ and 0 lies in $\mathcal{Q}$ or in $\mathcal{N}$). The action of L_μ on $\mathcal{Q}$ and on $\mathcal{N}$ decomposes, in some order, into orbits $1+1+10$ and $1+5+6$. Note that k and S are stable under L_μ. In particular, the three fixed points are $\{\infty, 0, k\}$.

We list possibilities. If $k=0$, there are two possibilities for S. Each possibility corresponds to orbits $1+1$ and $1+5$, and the two possibilities are distinguished by whether $|S\cap\mathcal{Q}|=2$ or 6. Suppose $k\neq 0$. If $k\in\mathcal{Q}$, the evenness of $|S\cap\mathcal{Q}|$ forces $S\cap\mathcal{Q}=\{0,k\}$ and $|S\cap\mathcal{N}|=6$; in particular, $S\cap\mathcal{N}$ decomposes as $1+5$ into orbits because $\infty\in S\cap\mathcal{N}$. If $k\in\mathcal{N}$, clearly $S\cap\mathcal{N}=\{\infty,k\}$. However, there are two possibilities for the 6-set $S\cap\mathcal{Q}$, corresponding to $1+5$ and 6. We claim that $S\cap\mathcal{Q}$ can not correspond to 6. Suppose this happens. In all other cases, when $|S\cap\mathcal{D}_1|=6$ for $\mathcal{D}_1\in\{\mathcal{Q},\mathcal{N}\}$, $S\cap\mathcal{D}_1$ breaks up as $1+5$ into

L_μ-orbits. We observe that the action of $s(s^{\hat{\pi}}=\varepsilon_{\mathscr{Q}})$ fuses the four L-orbits in pairs, each pair containing one $E(r, \mathscr{D}, \varepsilon)$ for $\varepsilon=-$. A corresponding phenomenon occurs for the action of an involution in $Z(N_{\langle J,\theta,s\rangle}(F))-\langle z\rangle$ say $s_1=s^\theta$, on the four E_*^θ's. Even though s does not fix $\tilde{\lambda}_{\infty,0'}$, the fact that $\tilde{\lambda}^s_{\infty,0'}=\tilde{\lambda}_{\infty,0}$ implies that $\langle s\rangle$ permutes the set of four E_*'s. Therefore, as $[\langle s, s_1\rangle^\pi, L]=1$, s_1 permutes the four L-orbits on $E(\lambda)$, (the E_*^θ's) hence permutes the four sets of octads associated to the orbits. It follows that L_μ has orbits $1+1+1+5$ on each of the two octads from this set of 44 fixed by L_μ, since they come from different L-orbits (which are fused by the action of $\langle s_1\rangle$). Therefore, $S\cap\mathscr{Q}$ corresponds to $1+5$, as claimed, and we have accounted for all the E_*^θ's. The occurrence of the four cases listed in (ii) may be deduced from the above discussion. The discussion easily implies (iii).

Example. *In Lemma* 7.7(ii), *take* $\lambda=\lambda_\infty$. *The relevant values for* μ *are* $\pm\lambda_{j,\mathscr{O}}$, *where one of the following cases holds:*

(ii. a) $\{\infty, j\}=\mathscr{O}\cap\mathscr{N}$,

(ii. b) $|\mathscr{O}\cap\mathscr{N}|=2$, $j=\gamma(\infty,\phi)=0\in\mathscr{Q}$;

(ii. c) $|\mathscr{O}\cap\mathscr{N}|=6$, $j=\gamma(\infty,\phi)=0\in\mathscr{Q}$;

(ii. d) $|\mathscr{O}\cap\mathscr{N}|=6$, $j\in\mathscr{Q}$, $j\neq\gamma(\infty,\phi)=0$.

The associated $\lambda+\mu\in\Lambda_2^2$ *look like* $\pm(-2x_\infty-2x_j+\sum_{\substack{l\neq\infty,j\\ l\in\mathscr{O}}}2x_l)$ *in every case.*

Definition. When $\lambda=\pm\lambda_{i,S'}$ define $i(\lambda):=i$, $S(\lambda):=S(\operatorname{mod}\langle\Omega\rangle)$.

For a triangle $\{\lambda,\mu,\nu\}\in\Delta(2,3)$ containing $\lambda_{i,S}$ and $\lambda_{j,T}\neq\lambda_{i,S}$, define $\delta(\lambda,\mu):=(-1)^{\infty i \text{ in } S+\infty j \text{ in } T}$.

Lemma 7.8. *Let* $\{\lambda,\mu,\nu\}\in\Delta(2,2)$ *and let* $\{\lambda,\lambda',\lambda''\}$, $\{\mu,\mu',\mu''\}$, $\{\nu,\nu',\nu''\}$ *be in* $\Delta(2,3)$. *Write* $\lambda'=\lambda_{i_1,S_1}$, $\lambda''=\lambda_{j_1,T_1}$, $\mu'=\lambda_{i_2},S_2$, $\mu''=\lambda_{j_2,T_2}$, $\nu'=\lambda_{i_3,S_3}$, $\nu''=\lambda_{j_3,T_3}$. *Assume* $i_k\neq j_k$ *for* $k=1,2,3$. *Then*

(i) $\delta(\lambda',\lambda'')=(-1)^{\frac{1}{2}\langle\lambda_{i_1,j'_1},\lambda\rangle+[\infty i_1 \text{ in } \mathscr{O}_\lambda]}$;

(ii) $\delta(\lambda',\lambda'')\,\delta(\mu',\mu'')\,\delta(\nu',\nu'')=(-1)^{1+\frac{1}{2}\langle\lambda_{i_1,j'_1},\lambda\rangle+\frac{1}{2}\langle\lambda_{i_2,j'_2},\mu\rangle+\frac{1}{2}\langle\lambda_{i_3,j'_3},\nu\rangle}$.

Proof. We have

$$\begin{aligned}\delta(\lambda',\lambda'')&=(-1)^{[\infty i_1 \text{ in} S_1]+[\infty j_1 \text{ in} T_1]}=(-1)^{[\infty i_1 \text{ in}(S_1+T_1)]+[i_1 j_1 \text{ in} T_1]}\\&=(-1)^{[\infty i_1 \text{ in}\mathscr{O}_\lambda]+[i_1 j_1 \text{ in} T_1]}=(-1)^{\infty i_1 \text{ in}\mathscr{O}_\lambda+\frac{1}{2}\langle\lambda_{i_1,j'_1},\lambda\rangle}\end{aligned}$$

see Lemma 2.3(ii). This proves (i). We have

$$\begin{aligned}&[\infty i_1 \text{ in } \mathscr{O}_\lambda]+[\infty i_2 \text{ in } \mathscr{O}_\mu]+[\infty i_3 \text{ in } \mathscr{O}_\nu]\\&\quad\equiv[\infty \text{ in } (\mathscr{O}_\lambda+\mathscr{O}_\mu+\mathscr{O}_\nu)]+[i_1 \text{ in } \mathscr{O}_\lambda]+[i_2 \text{ in } \mathscr{O}_\mu]+[i_3 \text{ in } \mathscr{O}_\nu]\\&\quad\equiv[\infty \text{ in } \phi]+1+1+1\equiv 1 \qquad (\operatorname{mod} 2).\end{aligned}$$

This, with (i), implies (ii).

8. The Action of Elements of P on the $v(\lambda)$ and the $e(x)\otimes x_i$

For later use, we require a careful discussion of plus and minus signs. We shall use the notation of Sect. 7 (and earlier sections) as well as the following notation and definitions.

Set $z_1:=q(8x_\infty)$, as in Sect. 7. Set $P:=N_C(E_0)$. Thus $P\cap Q=E$ and $P/E\cong 2^{11}.M_{24}$. As P-modules, $E=E_0\times\langle z\rangle$.

We claim that $\hat{P}=\hat{P}'\times\langle\hat{z}\rangle$, where $\hat{z}=z^{\hat{\pi}}$, and that $\hat{P}'=C_{\hat{P}}(e(1))$. To see this, look at the following diagram

$$\begin{tikzcd}
\hat{P} \arrow[r] \arrow[d, "\pi"'] & \hat{P}^{\pi_\infty} \arrow[d] \\
N_{24} \arrow[r] & \overline{N_{24}},
\end{tikzcd}$$

derived from the one in Sect. 4. Clearly, $\hat{P}'(\ker\pi|_{\hat{P}})=\hat{P}$ since N_{24} is perfect. We have $\hat{E}:=\ker\pi|_{\hat{P}}\cong\mathbb{Z}_2^{13}$. Also, $[E,P]\geqq[E,X]=E(2)\cong\mathbb{Z}_2^{11}$ (see Sect. 7), and $[E,O_2(P)]=\langle z_1\rangle$, so that $[E,P]=\langle E(2),z_1\rangle=E_0$. From Sect. 4, we have the isomorphism $\hat{Q}\to Q$ of $\hat{C}$-groups. Since $\hat{E}\leqq\hat{Q}=\ker\pi|_{O_2(\hat{C})}$, we get an isomorphism $\hat{E}\to E$, whence $|[\hat{E},\hat{P}]|=2^{12}$. At once, $|\hat{P}:\hat{P}'|\leqq 2$. Since $\hat{z}$ acts as -1 on $\mathbb{Q}e(1)$, $\hat{P}=\langle\hat{P}',\hat{z}\rangle$. Since $\hat{z}\in Z(\hat{P})$, $\hat{P}=\hat{P}'\times\langle\hat{z}\rangle$, proving the claim.

On the notation of Sect. 4, the element $\hat{z}z_\infty$ acts as -1 on $\mathbb{Q}e(1)$ and generates $\ker\pi_1$. So, we also have $\hat{P}=\hat{P}'\times\langle\hat{z}z_\infty\rangle$. It follows that $P\cong\hat{P}'\cong P'$ is perfect.

Elements of $N_C(E)$ permute the characters of E and hence the elements of F. For $g\in N_C(E)$ and $x\in F$ we write $x\circ g=y\in F$ if $\phi_x^g=\phi_y$ on E, where $\phi_x^g(u)=\phi_x(u^{g^{-1}})$ for $u\in E$. We have $x\circ g\equiv x^g\,(\mathrm{mod}\,E)$ when $x\in F$ and $g\in P$. Thus $e(x)^g=\pm e(x\circ g)$ for such x, g. Also $x\circ g=x$ for $x\in F(2)$, $g\in O_2(P)$. The unique nontrivial linear character of $\hat{P}$ is afforded by $\mathbb{Q}e(1)$. In case g normalizes F (i.e., $g\in J$), then $x\circ g=x^g$.

The reader is advised to understand the preceding paragraphs thoroughly before going on.

For $i\in\Omega$, $g\in N_{24}$, define i^g by $(Qx_i)^g=Qx_{i^g}$. Extend this notation to g in $N_{24}^{\pi^{-1}}$ and $N_{24}^{\pi^{-1}\pi_1}$.

Let $N_{23}:=\{g\in N_{24}\mid\infty^g=\infty\}$ and define $H:=(N_{23}^{\pi^{-1}\pi_1}\cap P)'$. Then $O_2(H)\cong 2_+^{1+22}$ and $H/O_2(H)\cong M_{23}$.

We set $\tau=q(\lambda_\infty)\in F$.

There are functions $a\colon F\times\Omega\times P\to\{\pm1\}$, $a_T\colon F\times\hat{P}\to\{\pm1\}$ and $a_\Lambda\colon\Omega\times\hat{P}\to\{\pm1\}$ which satisfy $e(x)^g=a_T(x,g)\,e(x\circ g)$, $x_i^g=a_\Lambda(i,g)\,x_{i^g}$ for $x\in F$, $i\in\Omega$, $g\in\hat{P}$ and $(e(x)\otimes x_i)^g=a(x,i,g)\,e(x\circ g)\otimes x_{i^g}$ for $x\in F$, $i\in\Omega$, $g\in P$. We have $a(x,i,g)=a_T(x,\hat{g})\,a_\Lambda(i,\hat{g})$, for any $\hat{g}\in g^{\pi_1^{-1}}$, $g\in P$. There is a function b: $\tilde{\Lambda}_2\times C\to\{\pm1\}$ which satisfies $v(\lambda)^g=b(\lambda,g)\,v(\lambda^g)$, $\tilde{\lambda}\in\tilde{\Lambda}_2$, $g\in C$ (we identify $b(\lambda,g)$ with $b(\tilde{\lambda},g)$).

Let us calculate some values of the functions introduced in the last paragraph. Say x, $y\in F$, $g\in P$. Then $y^{\hat{g}}=(y\circ g)\,u=u(y\circ g)$, where $u\in E$. We have

$$\begin{aligned}
e(x)^{\hat{g}}\,y^{\hat{g}}&=a_T(x,\hat{g})\,e(x\circ g)(y\circ g)\,u=a_T(x,\hat{g})\,e(x\circ g)\,u(y\circ g)\\
&=a_T(x,\hat{g})\,\varphi_{x\circ g}(u)\,e((x\circ\hat{g})(y\circ\hat{g}))=a_T(x,\hat{g})\,\varphi_{x\circ g}(u)\,e((x\,y)\circ\hat{g}).
\end{aligned}$$

Also, $(e(x)y)^{g}=e(xy)^{g}=a_T(xy,\hat{g})\,e((xy)\circ\hat{g})$. So $a_T(xy,\hat{g})=a_T(x,\hat{g})\,\varphi_{x\circ g}(u)$. Taking $x=1$, we note that $\mathbb{Q}e(1)$ affords the nontrivial linear character of $\hat{P}$ and obtain

$$(8.1)\qquad a_T(y,\hat{g})=\begin{cases}\varphi_1(u) & \text{if } \hat{g}\in P',\\ -\varphi_1(u) & \text{if } \hat{g}\notin P',\end{cases}$$

for $y\in F$, $\hat{g}\in\hat{P}$, $u=y^{g}(y\circ g)$; in particular

$$a_T(y,\hat{g})=\begin{cases}\varphi_1([y,g]) & \text{if } \hat{g}\in\hat{P}',\\ -\varphi_1([y,g]) & \text{if } \hat{g}\notin\hat{P}',\end{cases}$$

for $y\in F(2)$, $g\in O_2(P)$.

Next, we consider $a(x,i,g)=a_T(x,\hat{g})\,a_\Lambda(i,\hat{g})$. For $g\in O_2(P)$ we write $g=g_S$ if $g^{\pi\bar{\imath}^{1}\pi}=\varepsilon_S$ or $\varepsilon_{\Omega+S}$ (g_S is not well-defined, though the coset Eg_S is). From (8.2) we get the possibilities for $a_T(x,\hat{g})$ and we have $a_\Lambda(i,\hat{g})=\begin{cases}-1 & i\in S\\ 1 & i\notin S\end{cases}$, where $\hat{g}=\varepsilon_S$. To use (8.2), we arrange for $\hat{g}\in\hat{P}'$ by the following device. We take $g\in O_2(H)$. Then there is a unique choice $\hat{g}\in(H^{\pi\bar{\imath}^{1}})'$ since H has trivial Schur multiplier (see Lemma 2.18). For this choice, $\hat{g}^{\pi}=\varepsilon_S$, where $\infty\notin S$. Therefore $a_\Lambda(i,\hat{g})=(-1)^{\infty i\,\mathrm{in}\,S}$ and so

$$(8.2)\qquad a(x,i,g)=\varphi_1([x,g])(-1)^{\infty i\,\mathrm{in}\,S}\quad\text{for } x\in F(2),\ g=g_S\in O_2(P).$$

Note that (8.2) does not require $\infty\notin S$, i.e. (8.2) holds for $S+\Omega$ in place of S.

For $g\in O_2(P)$, write S_g for S or $S+\Omega$, whenever ε_S or $\varepsilon_{S+\Omega}$ equals $\hat{g}^{\pi}$. For $\lambda\in\Lambda_2^2$ let S_λ be the support of λ and for $\lambda\in\Lambda_2^4$, let $S_\lambda=\emptyset$.

Now, we turn to calculate the $b(\lambda,g)$'s. We use the notation and discussion of Sect. 5. Our C-map $W\otimes W\to V$ is based on

$$(e(x)\otimes x_i)\otimes(e(y)\otimes x_j)\mapsto\sum_{x_\lambda=xy}\left[-3\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}),u(\lambda^2))\right]\phi_\lambda(x)\,v(\lambda).$$

Fix $\lambda\in\Lambda_2$. We get, for $g\in P$ and for any pair x, $y\in F$ with $xy=x_\lambda$,

$$\begin{aligned}(8.3)\qquad b(\lambda,g)&=a(x,i,g)\,a(y,j,g)\left[-3\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}),u(\lambda^2))\right]\\ &\quad\cdot\left[-3\delta_{i^g j^g}+\tfrac{9}{32}(u_0(u_{i^g j^g}),u((\lambda^g)^2))\right]^{-1}\phi_\lambda(x)\,\phi_{\lambda^g}(x\circ g)\\ &=a(x,i,g)\,a(y,j,g)\,a_\Lambda(i,\hat{g})\,a_\Lambda(j,\hat{g})\,\phi_\lambda(x)\,\phi_{\lambda^g}(x\circ g)\\ &=a_T(x,\hat{g})\,a_T(y,\hat{g})\,\phi_\lambda(x)\,\phi_{\lambda^g}(x\circ g)\\ &=a_T(1,\hat{g})\,a_T(x_\lambda,\hat{g})\qquad(\text{taking } x=1),\end{aligned}$$

whenever the bracketed coefficients are nonzero.

We remark that there was an error in the above calculation noted by the referee. Consequently, it was necessary to make some changes in the calculations of this section.

(8.4) The bracketed coefficients in (8.3) vanish precisely when $i=j\in\mathrm{supp}(\lambda)$, an octad, or else $i\neq j$, $\{i,j\}\nsubseteq\mathrm{supp}(\lambda)$; otherwise, the formulas of (8.3) hold.

Let us check the statement. Say $i=j$. We have

$$\tfrac{9}{32}(u_0(u_{ii}), u(\lambda_{kl}^2)) = \tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{r\neq i} u_{rr}, 16(u_{kk}+u_{ll}))$$

$$= \tfrac{9}{32}\cdot\tfrac{1}{24}\cdot 16\cdot 4\cdot\begin{cases}22 & i\in\{k,l\}\\ -8 & i\notin\{k,l\}\end{cases} = \begin{cases}\frac{33}{2} & i\in\{k,l\}\\ -6 & i\notin\{k,l\}\end{cases},$$

whence the bracketed coefficients is nonzero. If $\operatorname{supp}\lambda = \mathcal{O}$ is an octad,

$$\tfrac{9}{32}(u_0(u_{ii}), u(\lambda^2)) = \tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{k\neq i} u_{rr}, 4\sum_{l\in\mathcal{O}} u_{ll})$$

$$= \tfrac{3}{16}\begin{cases}16 & i\in\mathcal{O}\\ -8 & i\notin\mathcal{O}\end{cases},$$

giving precisely the exception noted in (8.5). If $\lambda\in\Lambda_2^3$, $\lambda=\lambda_{k,S}$, say. Then

$$\tfrac{9}{32}(u_0(u_{ii}), u(\lambda^2)) = \tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{l\neq i} u_{ll}, 9u_{kk} + \sum_{r\neq k} u_{rr})$$

$$= \tfrac{3}{256}\cdot 4\cdot\begin{cases}23\cdot 9 - 23 = 23\cdot 8, & i=k,\\ 23-9-22=-8, & i\neq k,\end{cases} = \begin{cases}\frac{69}{8}, & i=k,\\ -\frac{3}{8}, & i\neq k,\end{cases}$$

giving (8.4) in this case. When $i\neq j$, (8.4) is pretty obvious.

(8.5) The formula $b(\lambda,g) = a_T(1,\hat{g})\,a_T(x_\lambda,\hat{g})$ holds for all $\lambda\in\Lambda_2$, $g\in P$; in particular, $b(\lambda,g) = a_T(x_\lambda,\hat{g})$ if $\hat{g}\in\hat{P}'$.

To verify this, given λ, we need to find a pair of indices i, j for which the bracketed coefficients of (8.3) are nonzero. This is easy if we examine the cases $\lambda\in\Lambda_2^k$, $k=2,3,4$.

(8.6) For $\lambda\in\Lambda_2^2\cup\Lambda_2^4$ and $g\in O_2(P)$, $b(\lambda,g)=\varphi_1([x_\lambda,g])$ (take $i\neq j$ in $\operatorname{supp}\lambda$ and use (8.2) and (8.4)).

(8.7) If $\lambda+\mu+\nu=0$, λ, μ, $\nu\in\Lambda_2^2\cup\Lambda_2^4$, $g\in O_2(P)$, then $x_\nu = x_\lambda x_\mu$ and

$$b(\lambda,g)\,b(\mu,g)\,b(\nu,g) = \varphi_1([x_\lambda,g][x_\mu,g][x_\nu,g])$$
$$= \varphi_1([x_\lambda x_\mu, g][x_\lambda,g,x_\mu][x_\nu,g]) = \varphi_1([x_\lambda,g,x_\mu]) = (-1)^{|S_\lambda\cap S_\mu\cap S_g|};$$

consequently, $\beta(\lambda^g,\mu^g) = \beta(\lambda,\mu)(-1)^{|S_\lambda\cap S_\mu\cap S_g|}$.

Using (8.5) we get

(8.8) P permutes the $v(\lambda)$, $\lambda\in\Lambda_2^4$.

9. The Betas

We have a function $\beta(\lambda,\mu)$ which takes the value $-36\phi_{\lambda+\mu}(x_\lambda)$ when $\tilde{\lambda}$, $\tilde{\mu}$, $\widetilde{\lambda+\mu}\in\tilde{\Lambda}_2$ and which satisfies $v(\lambda)\,v(\mu) = \beta(\lambda,\mu)\,v(\lambda+\mu)$. For our work in Sect. 11, we need some precise results on the signs of certain $\beta(\lambda,\mu)$.

The function β has been rather troublesome. In the first version of this paper, the formulas of Lemmas 2.39 and 5.1 were not known to us. We had to deal with a function which took on the values 0, ± 36, but was not given by an explicit formula. The exact signs are very important and it took a considerable amount of work to evaluate them on particular triangles of type 222 and to measure the change in sign as the triangles change. At this point, it is comforting to have an explicit formula, but the work referred to has not diminished substantially. Perhaps we should not expect a great deal because of the following remarks. Our notations for Λ and $Q = EF$ are "independent", in some sense. This independence holds throughout the formulas of Table 6.1, except in the expressions $\phi_\mu(x_\lambda)$, where both the element x_λ of F as well as the character ϕ_μ depend on lattice elements. To appreciate the significance of this, one must become involved with the calculations of Sect. 11. Roughly speaking, in verifying certain equations, expressions like $\phi_\lambda(x)$ can be handled formally, but an expression like $\phi_\mu(x_\lambda)$ resists because one needs to know "how much" λ differs from the elements of $F^{q^{-1}}$ which map to x_λ under q. A direct measurement of these differences might be one way to solve our problems. Since Λ_2 and the set of triangles of type 222 are finite sets, a very large but finite number of measurements would have to be taken and coded in a sensible way to cope with the situation of Sect. 11. We did not see how to make this idea work. Instead, we chose less direct but shorter and more selective attempts to obtain values of beta.

Now to compute selected values of beta. We consider cases, according to how λ, μ, $\lambda + \mu$ are distributed among Λ_2^2, Λ_2^3 and Λ_2^4:

(A) λ, μ, $\lambda + \mu \in \Lambda_2^4$;

(B) one of λ, μ, $\lambda + \mu$ in Λ_2^4, the others in Λ_2^2;

(C) one of λ, μ, $\lambda + \mu$ in Λ_2^4, the others in Λ_2^3;

(D) all of λ, μ, $\lambda + \mu$ in Λ_2^2;

(E) one of λ, μ, $\lambda + \mu$ in Λ_2^2, the others in Λ_2^3.

Associativity of the form (,) implies that these cases are exhaustive.

First, some notation. For $x \in Q$, $g \in G$, write $x^g = u(x,g)\, v(x,g)$, where $u(x,g) \in E$ and $v(x,g) \in F$. Observe that $u(x,g)$ and $v(x,g)$ commute when x is an involution.

Lemma 9.1. *Suppose that* $\lambda \in \Lambda_2$ *and that* $q(\lambda) = x_\lambda \cdot u$, $x_\lambda \in F$, $u \in E$. *Then* $\varphi_\lambda(x_\lambda) = 1$.

Proof. Since $q(\lambda)$ is an involution and x_λ and u have order 1 or 2, they generate an abelian group. Therefore, $\varphi_\lambda(x_\lambda) = 1$.

Lemma 9.2. *Suppose that* $g \in C$ *and* $e(1)^{\hat{g}} = \sum_{x \in F} a_x e(x)$, *for scalars* a_x. *Let* $\lambda \in \Lambda_2$.

(i) $b(\lambda, g) = \sum_{x \in F} a_{v(x,g)}\, a_{v(x x_\lambda, g) x_\lambda g}\, \varphi_{x_\lambda g}(u(x x_\lambda, g))\, \varphi_\lambda(x)$.

(ii) *If* $x^g \in E$, $e(x)^{\hat{g}} = \sum_{y \in F} a_y \varphi_y(x^g) e(y)$ *and the coefficient of* $e(1) \otimes e(x_{\lambda^g})$ *in* $(e(x) \otimes e(x x_\lambda))^g$ *is* $a_1 a_{v(x x_\lambda, g) x_\lambda g}\, \varphi_{x_\lambda g}(u(x x_\lambda, g))$.

(iii) *If* $x^g \in E$ *and* $x_\lambda^g \in E$, *the coefficient of* $e(1) \otimes e(x_{\lambda^g})$ *in* $(e(x) \otimes e(x x_\lambda))^g$ *is* $a_1 a_{x_\lambda g}\, \phi_{x_\lambda g}((x x_\lambda)^g) = a_1 a_{x_\lambda g}\, \phi_{\lambda^g}((x x_\lambda)^g) = a_1 a_{x_\lambda g}\, \varphi_\lambda(x x_\lambda) = a_1 a_{x_\lambda g}\, \phi_\lambda(x)$.

(iv) *If* $F^g = E_0$ *and* $g^2 = 1$, $e(1)^{\hat{g}} = \pm\frac{1}{2^6}\sum_{x\in F} e(x)$ *so that* $a_x = \frac{1}{2^6}$ *for all* x *or* $a_x = -\frac{1}{2^6}$ *for all* x.

(v) *Finally, if* $F^g = E_0$, *and* $g^2 = 1$, *the coefficient of* $e(1)\otimes e(x_{\lambda^g})$ *in* A_λ^g *is*

$$\frac{1}{2^6}\sum_{x\in F} a_1 a_{x_{\lambda^g}}\cdot \varphi_\lambda(xx_\lambda)\varphi_\lambda(x) = a_1 a_{x_{\lambda^g}}\cdot\frac{1}{2^6}\sum_{x\in F}\varphi_\lambda(x_\lambda) = a_1 a_{x_{\lambda^g}}\cdot 2^6 = \frac{1}{2^6}.$$

In this case, $b(\lambda, g) = 1$ *and* $\beta(\lambda^g, \mu^g) = \beta(\lambda, \mu)$, *for all* μ *such that* λ, μ *span a triangle of type 222.*

(vi) *If* $g\in\hat{P}'$, *then* $e(1)^{\hat{g}} = e(1)$ *and* $b(\lambda, g) = \varphi_{x_{\lambda^g}}(u(x_\lambda, g)) = \varphi_{\lambda^g}(u(x_\lambda, g)) = \varphi_{x_{\lambda^g}}(x_\lambda^g)$. *In particular, if* $g\in\hat{P}'$ *and* $x_\lambda^g\in F$, *then* $b(\lambda, g) = 1$.

Proof. We have

$$e(x)^{\hat{g}} = e(1)^{x\hat{g}} = (e(1)^{\hat{g}})^{x^g} = \Big(\sum_{y\in F} a_y e(y)\Big)^{x^g} = \sum_{y\in F} a_y\varphi_y(u(x,g))\,e(y\,v(x,g)).$$

Therefore

$$\begin{aligned}&(e(x)\otimes e(xx_\lambda))^g\\ &\quad = \sum_{y_1, y_2\in F} a_{y_1} a_{y_2}\varphi_{y_1}(u(x,g))\,\varphi_{y_2}(u(xx_\lambda, g))\,e(y_1 v(x,g))\otimes e(y_2 v(xx_\lambda, g)).\end{aligned}$$

The coefficient of $e(1)\otimes e(x_{\lambda^g})$ in this expression is

$$a_{v(x,g)}\,a_{v(xx_\lambda, g)x_{\lambda^g}}\,\varphi_{v(x,g)}(u(x,g))\,\varphi_{v(xx_\lambda, g)x_{\lambda^g}}(u(xx_\lambda, g)),$$

which equals $a_{v(x,g)}a_{v(xx_\lambda,g)x_{\lambda^g}}\varphi_{x_{\lambda^g}}(u(xx_\lambda, g))$, because, for any $x\in F$ and any $g\in C$, $u(x,g)$ and $v(x,g)$ are commuting elements of order 1 or 2, whence $\varphi_{v(x,g)}(u(x,g)) = 1$.

Since $A_\lambda = \frac{1}{2^6}\sum_{x\in F}\varphi_\lambda(x)e(x)\otimes e(xx_\lambda)$, the coefficient of $e(1)\otimes e(x_{\lambda^g})$ in A_λ^g is

$$\frac{1}{2^6}\sum_{x\in F} a_{v(x,g)}\,a_{v(xx_\lambda, g)x_{\lambda^g}}\,\varphi_{x_{\lambda^g}}(u(xx_\lambda, g))\,\varphi_\lambda(x).$$

Since the coefficient in A_{λ^g} of $e(1)\otimes e(x_{\lambda^g})$ is $\frac{1}{2^6}$, (i) follows (see Sect. 5 for the relationship between A_λ and $v(\lambda)$).

The remaining statements are more-or-less obvious from the above discussion. To get (iv), we refer to Sect. 4. To get $\varphi_\lambda(x_\lambda) = 1$ for $\lambda\in\Lambda_2$, use Lemma 9.1. We get (vi) from (i) by studying the definitions. Namely, the only nonzero summands occur when (among other things) $v(x,g) = 1$, or $x^g\in E$. Since $g\in P$, this means $x = 1$. Consequently, $v(xx_\lambda, g) = v(x_\lambda, g) = x_{\lambda^g}$. Thus, $b(\lambda, g) = \varphi_{x_{\lambda^g}}(u(x_\lambda, g))$, and the rest of (vi) is easy.

Lemma 9.3. $\beta(\lambda,\mu) = -36$ *in cases* (A), (B) *and* (C).

Proof. Let $\lambda\in\Lambda_2^4$. Then $x_\lambda = 1$ so that, from Table 6.1, $\beta(\lambda,\mu) = -36\phi_{\lambda+\mu}(x_\lambda) = -36$.

Lemma 9.4. *Let $\{\lambda, \mu, \lambda+\mu\}$ be any triangle of type 222 and suppose $q(\lambda) \in F$. Then $\beta(\lambda, \mu) = -36$.*

Proof. Since $q(\lambda) \in F$, $q(\lambda^{s_0}) \in E_0$, whence $\beta(\lambda^{s_0}, \mu^{s_0}) = -36$ by Lemma 9.3. By Lemma 9.2(v), $-36 = \beta(\lambda^{s_0}, \mu^{s_0}) = \beta(\lambda, \mu)$.

Lemma 9.5. *Let $\{\lambda, \mu, \nu\} \in$ (2, 2) and suppose that $g = g_S \in O_2(H)$ satisfies $q(\lambda^g) \in F$. Then $\beta(\lambda, \mu) = (-1)^{1+|S \cap S_\lambda \cap S_\mu|} 36$.*

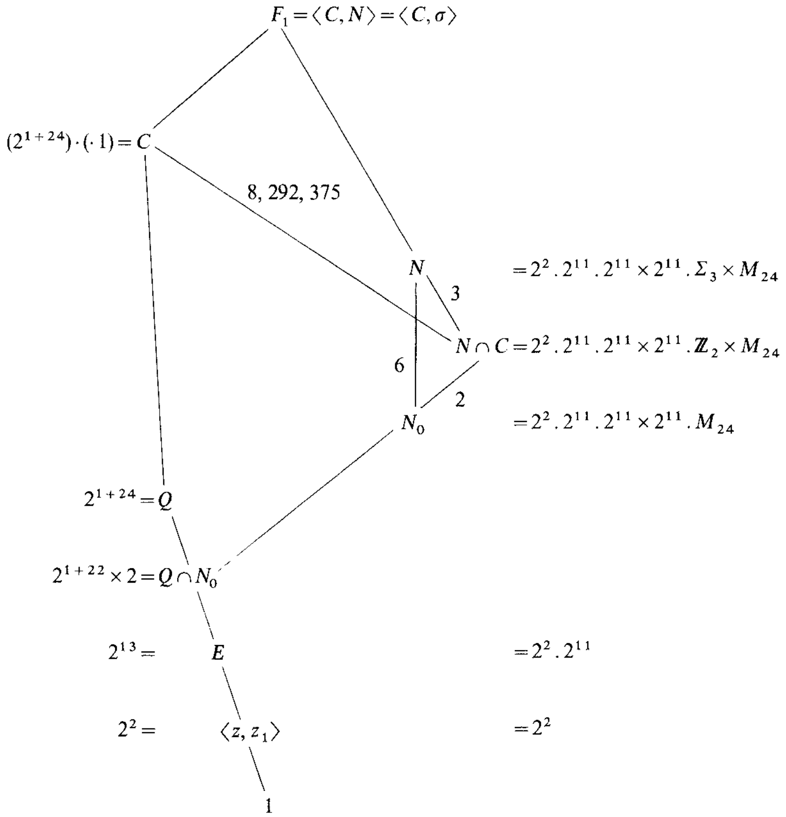
Proof. Lemma 9.4 and (8.7).

Remark. For the hypothesis to be satisfied, we need $|\mathcal{O}_\lambda \cap \mathcal{Q}| = 2$ or 6; see Lemmas 7.6 and 7.7.

10. The Definition of σ

We shall define a linear transformation σ of order 2 which commutes with a group H (defined below), fixes z_1, and interchanges z and zz_1 under con-

Table 10.1. The groups N and C


$F_1 = \langle C, N \rangle = \langle C, \sigma \rangle$
$(2^{1+24}) \cdot (\cdot 1) = C$
8, 292, 375
N
$= 2^2 . 2^{11} . 2^{11} \times 2^{11} . \Sigma_3 \times M_{24}$
3
$N \cap C = 2^2 . 2^{11} . 2^{11} \times 2^{11} . \mathbb{Z}_2 \times M_{24}$
6
2
N_0
$= 2^2 . 2^{11} . 2^{11} \times 2^{11} . M_{24}$
$2^{1+24} = Q$
$2^{1+22} \times 2 = Q \cap N_0$
$2^{13} =$
E
$= 2^2 . 2^{11}$
$2^2 =$
$\langle z, z_1 \rangle$
$= 2^2$
1

jugation. One should keep in mind that the definition of σ is motivated by the principle that if H_1 and H_2 are subgroups of $GL(B)$ and $H_1^\sigma = H_2$, then the set of irreducible constituents for H_1 are transformed by σ to the set of irreducible constituents for H_2.

We should comment that the algebra structure constants and the definition of σ were determined by a common strategy. Imagine that F_1 exists, is in $G(B)$ and contains C as the centralizer of an involution. In F_1, the four-group $\langle z, z_1 \rangle$ has normalizer N of the shape $2^2 . 2^{11} . (2^{11} \times 2^{11}) . (M_{24} \times \Sigma_3)$. If we let $N_0 = N''$, then $N = N_0 \langle \tau, \sigma \rangle$ (semi-direct product), where $\tau = q(\lambda_\infty)$ as before and σ is an involution which satisfies $\langle \tau, \sigma \rangle \cong \Sigma_3$. Some of the interaction of N and C is diagrammed in Table 10.1. The point is that most of N lies in C ($|C : N \cap C| = 3$) and $\langle \sigma \rangle$ must permute the subgroups of the group N_0. That is, N_0 is described already in our notation since $N_0 \leqq C$, and N_0 is big enough to yield information about B and C.

We concentrated mainly on the cases $H_1 = H_2 = \langle z, z_1 \rangle$, $O_2(N_0)'$, $O_2(N_0)$ and where H_1 and H_2 are normal subgroups of N_0 or order 2^{24}. Eventually, this line of analysis shows that there are particular bases $e_1, e_2, \ldots$ and $e'_1, e'_2, \ldots$ of B so that σ must behave like $e_i^\sigma = \pm e'_i$, for all i. Squaring gives exact relations. All this implies enough linear relations among the six independent parameters of Corollary 5.8 to make all six linearly dependent on one of them. Thus, B is forced to be essentially unique. As far as we can tell, an exact description of σ is not forced. Unfortunately, the signs required to describe σ took some guesswork to find. The results are summarized in Table 10.2.

We need a refinement of $B = U \oplus V \otimes W$. Define

$$\begin{array}{rll}
B_{24} = & \text{span of } u_{ii},\ i \in \Omega, & \text{dimension } 24; \\
B_{276} = & \text{span of } u_{ij},\ i, j \in \Omega,\ i \neq j, & \text{dimension } 276; \\
B_2^{4,+} = & \text{span of } v_{ij} + v_{ij'},\ i, j \in \Omega,\ i \neq j, & \text{dimension } 276; \\
B_2^{4,-} = & \text{span of } v_{ij} - v_{ij'},\ i, j \in \Omega,\ i \pm j, & \text{dimension } 276; \\
B_2^2 = & \text{span of } v(\lambda),\ \lambda \in \Lambda_2^2, & \text{dimension } 2^6 . 759; \\
B_2^3 = & \text{span of } v(\lambda),\ \lambda \in \Lambda_2^3, & \text{dimension } 2^{11} . 24; \\
B_{\text{even}} = & \text{span of } e(x) \otimes x_i,\ x \in F(2),\ i \in \Omega, & \text{dimension } 2^{11} . 24; \\
B_{\text{odd}} = & \text{span of } e(\tau x) \otimes x_i,\ x \in F(2),\ i \in \Omega, & \text{dimension } 2^{11} . 24;
\end{array}$$

where $v_{ij} = v(\lambda_{ij})$ and $v_{ij'} = v(\lambda_{ij'})$.

There is no problem giving our explicit description of σ on basis vectors in B_{24}, B_{276} and $B_2^{4,+}$ and $B_2^{4,-}$. See the beginning of Table 10.2. Defining σ on the remaining summands requires some discussion. We will start by considering the summands B_2^3, B_{even} and B_{odd}.

Let $R_0 = \langle q(\Lambda(2)) \rangle$. Then $N_0 := \langle R_0, P \rangle = R_0 P$ satisfies $O_2(N_0) = R_0 R$, where $R := O_2(P)$, and, as a module for $N_0 / O_2(N_0) \cong M_{24}$, $O_2(N_0) / \Phi(O_2(N_0))$ is completely reducible and is isomorphic to a direct sum $\mathscr{C} \oplus \mathscr{C}$. Therefore, there is a unique subgroup R_1 of index 2^{11} in $O_2(N_0)$, normal in N_0 and distinct from R_0 and R.

We want σ to satisfy $R^\sigma = R$, $R_0^\sigma = R_1$, $z^\sigma = zz_1$ and $[z_1, \sigma] = 1$, and for $C_R(\sigma)$ to be a group of index 2 in R, meeting $\langle z, z_1\rangle$ in $\langle z_1\rangle$. We have the eigenvalues

	B_2^3	B_{even}	B_{odd}
z:	1	-1	-1
z_1:	-1	1	-1
zz_1:	-1	-1	1,

and this implies that σ must switch B_2^3 with B_{odd} and leave B_{even} invariant.

The eigenspaces for R_0 on B_2^3 are the $\mathbb{Q}v(\lambda_{i,x})$, $i \in \Omega$, $x \in F(2)$, and the characters afforded are all distinct. Also $C_{R_0}(B_2^3) = \langle z\rangle$ and z_1 is -1 on B_2^3.

On B_{even}, z_1 is 1 and zz_1 is -1. Note that $R^\tau = R_1$. The eigenspaces for R on B_{even} are the $e(x) \otimes x_i$, $x \in F(2)$, $i \in \Omega$ (this is because $[E_0, R] \leqq \langle z_1\rangle$; see Sect. 8). We define σ on B_{even} by

$$(e(x) \otimes x_i)^\sigma = (-1)^{\langle \lambda_\infty, \lambda_{i,x}\rangle} e(x) \otimes x_i.$$

On B_{odd}, the kernel of the action of R is $\langle zz_1\rangle$ and $R/\langle zz_1\rangle \cong 2_+^{1+22}$. So, R does not have eigenspaces here. The eigenspaces for $R_1 = R^\tau$ on B_{odd} are the $e(\tau x) \otimes x_i$, the transforms of the $e(x) \otimes x_i$ under τ. Since we want σ to switch R_0 and R_1, we make σ switch $\mathbb{Q}e(\tau x) \otimes x_i$ and $\mathbb{Q}v(\lambda_{i,x})$. Thus, we must describe a function $d(\lambda_{i,x}) \in \{\pm 1\}$ which gives $v(\lambda_{i,x})^\sigma = d(\lambda_{i,x})\, e(\tau x) \otimes x_i$ and $(e(\tau x) \otimes x_i)^\sigma = d(\lambda_{i,x})\, v(\lambda_{i,x})$.

Although we will not get $[X, \sigma] = 1$ ($[X, \sigma] = O_2(X)$, actually), the actions of σ and X on $\sum_{i \in \Omega} \mathbb{Q}v(\lambda_i)$ and $\sum_{i \in \Omega} \mathbb{Q}e(\tau) \otimes x_i$ will turn out to commute. Here, X acts as $M_{24} \cong X/O_2(X)$. If σ is defined here and the actions do commute, then $d(\lambda_i)$ will be constant for $i \in \Omega$. Replacing σ by σz_1 if necessary, we may then arrange for $d(\lambda_i) = 1$, all $i \in \Omega$. Therefore, we *define* $d(\lambda_i) = 1$, for all i. Thus, σ is now defined on these two spaces.

For a $\mathscr{C}$-set S, we let $d(\lambda_{i,S}) = (-1)^{\infty i \text{in} S}$ (see Sect. 2). This is really a function on $\Omega \times \bar{\mathscr{C}}$. For $S = \emptyset$ or Ω, it agrees with the above definition of $d(\lambda_i)$.

Let $H_\infty \leqq X$, $H_\infty \geqq O_2(X)$, $H_\infty/O_2(X)$ be the M_{23} subgroup fixing $\infty \in \Omega$, and set $H := (RH_\infty)' \cong 2^{1+22} \cdot M_{23}$ (see Sect. 8 and Lemma 2.18).

We now verify that the actions of σ and H commute on $B_2^3 \oplus B_{\text{odd}}$. Let $g = g_S \in O_2(H)$ (recall that g_S is really a choice of element in a coset of E_0). Then

$$v(\lambda_i)^g = b(\lambda_i, g)\, v(\lambda_{i,S}) \quad \text{and} \quad (e(\tau) \otimes x_i)^g = a(\tau, i, g)\, e(\tau x_S) \otimes x_i.$$

We have

$$b(\lambda_i, g)\, v(\lambda_i)^{g\sigma} = v(\lambda_{i,S})^\sigma = d(\lambda_{i,S})\, e(\tau x_S) \otimes x_i$$

and

$$b(\lambda_i, g)\, v(\lambda_i)^{\sigma g} = b(\lambda_i, g)\, d(\lambda_i)(e(\tau) \otimes x_i)^g = b(\lambda_i, g) \cdot 1 \cdot a(\tau, i, g)\, e(\tau x_S) \otimes x_i.$$

These are equal since $a(\tau, i, g)\, b(\lambda_i, g) = (-1)^{\infty i \text{in} S} = d(\lambda_{i,S})$, by (8.1), (8.2) and (8.5). Thus, the actions of σ and $O_2(H)$ commute. Now let $g \in H$ so that $\hat{g}$ lies in the standard M_{23} in N_{24} fixing ∞, i.e. $g \in H_\infty$. Then each $a_\Lambda(i, g) = 1$ so that $a(\tau x, i, g) = a_T(\tau x, g)$. Write $x = x_S$ for $S \in \mathscr{C}$. Then

$$v(\lambda_{i,S})^{\sigma g} = d(\lambda_{i,S})(e(\tau x) \otimes x_i)^g = d(\lambda_{i,S})\, a_T(\tau x, g)\, e(\tau(x \circ g)) \otimes x_{i^g}$$

and, by (8.4),

$$v(\lambda_{i,S})^{g\sigma} = a_T(\tau x, g)\, v(\lambda_{i^g, S^g})^\sigma = a_T(\tau x, g)\, d(\lambda_{i^g, S^g})\, e(\tau(x \circ g)) \otimes x_{i^g}.$$

Since g fixes ∞, $d(\lambda_{i,S}) = d(\lambda_{i^g, S^g})$ as required. Thus, the actions H and σ do commute on $B_2^3 \oplus B_{\text{odd}}$.

Commutativity of the actions on B_{even} is verified as above - just check definitions and use the fact that H fixes ∞.

The definition of σ on B_2^2 requires the notion of an F-triple. Given $\lambda \in \Lambda_2^2$, we call $\{\lambda, \mu, \nu\} \in \Delta(2,3)$ an *F-triple* if there is $g \in H$ with $q(\{\lambda, \mu, \nu\}^g) \subset F$ and if μ and ν have the shape $\mu = \lambda_{i,S}$ and $\nu = \lambda_{j,T}$, with $\infty \notin \{i,j\}$. By Lemma 7.7(ii), $i \neq j$. By Lemma 7.7(i), every $\lambda \in \Lambda_2^2$ is part of an F-triple, even of one whose image under q lies in F when $q(\lambda) \in F$.

To define $v(\lambda)^\sigma$, we enlarge λ to an F-triple $\{\lambda, \mu, \nu\}$, $\mu = \lambda_{i,S}$, $\nu = \lambda_{j,T}$, then set

$$\begin{aligned} v(\lambda)^\sigma :&= \beta(\mu,\nu)^{-1}\, v(\mu)^\sigma\, v(\nu)^\sigma \\ &= \beta(\mu,\nu)^{-1}(-1)^{\infty i \,\text{in}\, S + \infty j \,\text{in}\, T}(e(x_\mu) \otimes x_i)(e(x_\nu) \otimes x_j) \\ &= \beta(\mu,\nu)^{-1}(-1)^{\infty i \,\text{in}\, S + \infty j \,\text{in}\, T} \sum_{x_\zeta = x_\lambda} \tfrac{9}{32}(u_{ij}, u(\zeta^2))\, \phi_\zeta(\tau x_S)\, v(\zeta) \\ &= \beta(\mu,\nu)^{-1}(-1)^{\infty i \,\text{in}\, S + \infty j \,\text{in}\, T}(\tfrac{9}{2}) \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta\rangle}\, \phi_\zeta(\tau x_S)\, v(\zeta). \end{aligned}$$

We must show that this is well defined. Note that there are 64 summands.

Suppose that $\{\lambda, \mu, \nu\}$ and $\{\lambda, \mu_1, \nu_1\}$ are two F-triples containing λ. Write $\mu = \lambda_{i,S}$, $\nu = \lambda_{j,T}$, $\mu_1 = \lambda_{i_1, S_1}$, $\nu_1 = \lambda_{j_1, T_1}$. By Lemmas 7.3, 7.7 and the definition of F-triple, there is $g \in H$, $\hat{g} \in \hat{P}'$ so that $\tilde{\lambda}^g = \tilde{\lambda}$, $\tilde{\mu}^g = \tilde{\mu}_1$, $\tilde{\nu}^g = \tilde{\nu}_1$. Let A, A_1 be the formula given for $v(\lambda)^\sigma$ using the first and second F-triples respectively. We want to show that $A = A_1$. We have

$$A = \beta(\mu,\nu)^{-1}(-1)^{\infty i \,\text{in}\, S + \infty j \,\text{in}\, T}(\tfrac{9}{2}) \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta\rangle}\, \phi_\zeta(x_\mu)\, v(\zeta), \tag{10.1}$$

$$A_1 = \beta(\mu_1,\nu_1)^{-1}(-1)^{\infty i_1 \,\text{in}\, S_1 + \infty j_1 \,\text{in}\, T_1}(\tfrac{9}{2}) \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{i_1 j_1'}, \zeta\rangle}\, \phi_\zeta(x_{\mu_1})\, v(\zeta).$$

Write $g = p g_U$, where $p^{\hat{\pi}} \in M_{24}$, $U \in \mathscr{C}$. We have $i_1 = i^g = i^p$, $j_1 = j^g = j^p$, $S_1 \equiv S^g + U$, $T_1 \equiv T^g + U$ (modulo $\langle \Omega \rangle$). Therefore, as $g \in H$,

$$\begin{aligned} &[\infty i^g \text{ in } S_1] + [\infty j_1 \text{ in } T_1] \\ &\quad \equiv [\infty i_g \text{ in } S^q] + [\infty i_1 \text{ in } U] + [\infty j_g \text{ in } T^g] + [\infty j_1 \text{ in } U] \\ &\quad \equiv [\infty i \text{ in } S] = [\infty j \text{ in } T] + [i_1 j_1 \text{ in } U] \quad (\text{mod}\, 2). \end{aligned} \tag{10.2}$$

Also, we have

$$\beta(\mu_1, \nu_1) = \beta(\mu,\nu)\, b(\mu, g)\, b(\nu, g)\, b(\lambda, g); \tag{10.3}$$

$$\begin{aligned} \langle \lambda_{i,j'}, \zeta \rangle = \langle \lambda_{i,j'}^g, \zeta^g \rangle = \langle \lambda_{i_1, j_1'}^{g_U}, \zeta^g \rangle = \\ \pm \begin{cases} \langle \lambda_{i_1 j_1}, \zeta^g \rangle & \text{if } i_1 j_1 \text{ in } U \equiv 0 \;(\text{mod}\, 2), \\ \langle \lambda_{i_1 j_1}, \zeta^g \rangle & \text{if } i_1 j_1 \text{ in } U \equiv 1 \;(\text{mod}\, 2), \end{cases} \end{aligned} \tag{10.4}$$

whence

$$(-1)^{\frac{1}{2}\langle\lambda_{i,j'},\zeta\rangle}=a_\Lambda(i,\hat{g})\,a_\Lambda(j,\hat{g})(-1)^{\frac{1}{2}\langle\lambda_{i_1,j_1'},\zeta^g\rangle};$$

$$a_\Lambda(i,\hat{g})\,a_\Lambda(j,\hat{g})=(-1)^{i_1j_1\,\mathrm{in}\,U}; \tag{10.5}$$

$$v(\zeta)^g=b(\zeta,g)\,v(\zeta^g)=b(\lambda,g)\,v(\zeta^g). \tag{10.6}$$

Since every $v(\zeta)$ in (10.1) satisfies $x_\zeta=x_\lambda$, we get $b(\zeta,g)=b(\lambda,g)$ for all such ζ, from (8.5). Since A is a linear combination of such $v(\zeta)$,

$$A^g=b(\lambda,g)A, \quad \text{or} \quad A=b(\lambda,g)A^g. \tag{10.6}$$

Using (10.1), (10.2), (10.3) and (10.4) and making ζ^g the variable of summation, we have

$$\begin{aligned} A_1 &= \beta(\mu,\nu)^{-1}\,b(\mu,g)\,b(\nu,g)\,b(\lambda,g)(-1)^{\infty i_1\,\mathrm{in}\,S_1+\infty j_1\,\mathrm{in}\,T_1}. \\ &\quad (\tfrac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{i_1,j_1'},\zeta^g\rangle}\,\phi_{\zeta^g}(x_{\mu_1})\,v(\zeta^g) \\ &= \beta(\mu,\nu)^{-1}\,b(\mu,g)\,b(\nu,g)\,b(\lambda,g)(-1)^{\infty i\,\mathrm{in}\,S+\infty j\,\mathrm{in}\,T+i_1j_1\,\mathrm{in}\,U}. \\ &\quad a_\Lambda(i,\hat{g})\,a_\Lambda(j,\hat{g})(\tfrac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{i,j'},\zeta\rangle}\,\phi_{\zeta^g}(x_{\mu_1})\,v(\zeta^g). \end{aligned} \tag{10.7}$$

To compute $b(\lambda,g)A^g$, one replaces $v(\zeta)$ by $v(\zeta^g)$ in the first line of (10.1); see (10.6). So upon cancelling (making use of (10.5)), we see that equality of A and A_1 amounts to equality of $\phi_\zeta(x_\mu)$ with $\phi_{\zeta^g}(x_{\mu_1})\,b(\mu,g)\,b(\nu,g)\,b(\lambda,g)$. From (8.3) and (8.5), using $\hat{g}\in\hat{P}'$.

$$\begin{aligned} b(\lambda,g) &= a_T(x_\mu,\hat{g})\,a_T(x_\nu,\hat{g})\,\phi_\lambda(x_\mu)\,\phi_{\lambda^g}(x_\mu\circ g) \\ &= a_T(x_\mu,\hat{g})\,a_T(x_\nu,\hat{g})\,\phi_\lambda(x_\mu)\cdot\phi_\lambda(x_{\mu_1}); \end{aligned} \tag{10.8}$$

$$b(\mu,g)=a_T(x_\mu,\hat{g}); \tag{10.9}$$

$$b(\nu,g)=a_T(x_\nu,\hat{g}). \tag{10.10}$$

Thus, we must verify the equality

$$\phi_{\lambda+\zeta}(x_\mu)=\phi_{\lambda+\zeta^g}(x_{\mu_1}), \qquad \text{for all } \zeta \text{ with } x_\zeta=x_\lambda. \tag{10.11}$$

Note that $\lambda+\zeta$, $\lambda+\zeta^g\in\Lambda(4)$, so that $x_\mu^g\equiv x_{\mu_1}$ (modulo E) and $\phi_{\lambda+\zeta}(x_\mu)=\phi_{(\lambda+\zeta)^g}(x_\mu^g)=\phi_{\lambda+\zeta^g}(x_{\mu_1})$, as required. Our proof of the well definedness of $v(\lambda)^\sigma$ is now complete.

We use notation $\delta(\mu,\nu):=(-1)^{\infty i\,\mathrm{in}\,S+\infty j\,\mathrm{in}\,T}$ whenever $\{\lambda,\mu,\nu\}\in\Delta(2,3)$ and the two vectors in Λ_2^3 have shape $\lambda_{i,S}$ and $\lambda_{j,T}$. When $\{\lambda,\mu,\nu\}$ is an F-triple, we have $i\neq j$ and $\infty\notin\{i,j\}$.

We now show that σ commutes with H on B_2^2, using the commutativity on $B_2^3\oplus B_{\mathrm{even}}\oplus B_{\mathrm{odd}}$. Let $v(\lambda)=\beta(\mu,\nu)^{-1}v(\mu)v(\nu)$, where $\{\lambda,\mu,\nu\}$ is an F-triple.

Table 10.2. The definition of σ

B_{24}	$u_{ii}^{\sigma}=u_{ii}$
B_{276}	$u_{ij}^{\sigma}=-v_{ij}+v_{ij'}$
$B_2^{4,+}$	$(v_{ij}+v_{ij'})^{\sigma}=v_{ij}+v_{ij'}$
$B_2^{4,-}$	$(-v_{ij}+v_{ij'})^{\sigma}=u_{ij}$
B_2^2	$v(\lambda)^{\sigma}=\delta(\mu,v)\,\beta(\mu,v)^{-1}(\frac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{ij'},\zeta\rangle}\varphi_\zeta(x_\mu)\,v(\zeta)$
B_2^3	$v(\lambda_{i,x})^{\sigma}=(-1)^{\infty i\,\mathrm{in}\,S_x}e(\tau x)\otimes x_i$
B_{even}	$(e(x)\otimes x_i)^{\sigma}=(-1)^{\langle\lambda_\infty,\lambda_{i,x}\rangle}e(x)\otimes x_i$
B_{odd}	$(e(\tau x)\otimes x_i)^{\sigma}=(-1)^{\infty i\,\mathrm{in}\,S_x}v(\lambda_{i,x})$

On B_2^2, $\{\lambda,\mu,v\}$ is required, by definition, to be an F-triple, although, once Proposition 11.2 is proved, we need require only that $\{\lambda,\mu,v\}\in\Delta(2,3)$; $i=i(\mu)$, $j=i(v)$.

Then $v(\lambda)^{\sigma}$ is, by definition $\beta(\mu,v)^{-1}v(\mu)^{\sigma}v(v)^{\sigma}$. Thus, for $g\in H$,

$$\begin{aligned}v(\lambda)^{\sigma g}&=\beta(\mu,v)^{-1}(v(\mu)^{\sigma}v(v)^{\sigma})^{g}\\&=\beta(\mu,v)^{-1}v(\mu)^{\sigma g}v(v)^{\sigma g}=\beta(\mu,v)^{-1}v(\mu)^{g\sigma}v(v)^{g\sigma}\\&=\beta(\mu,v)^{-1}b(\mu,g)\,b(v,g)\,v(\mu^{g})^{\sigma}v(v^{g})^{\sigma}\\&=\beta(\mu,v)^{-1}b(\mu,g)\,b(v,g)\,\beta(\mu^{g},v^{g})\,v(\lambda^{g})^{\sigma}\\&=\beta(\mu,v)^{-1}b(\mu,g)\,b(v,g)\,\beta(\mu^{g},v^{g})\,b(\lambda,g)\,v(\lambda)^{g\sigma}=v(\lambda)^{g\sigma},\end{aligned}$$

as required.

Since $b(\lambda_{ij},g)=b(\lambda_{ij'},g)=1$ for $i,j\in\Omega$, $g\in P$ (see (8.7)), the actions of σ and H clearly commute on the first four summands of B listed in Table 10.2.

We conclude that $[H,\sigma]=1$.

Two more basic results are needed.

Proposition 10.1. *σ preserves the inner product on B.*

Proof. It is obvious that $(e^{\sigma},f^{\sigma})=(e,f)$ for basis vectors e and f, except possibly when e, $f\in B_2^2$. Say $e=f=v(\lambda)$, $\lambda\in\Lambda_2^2$. Then

$$(v(\lambda)^{\sigma},v(\lambda^{\sigma}))=\tfrac{1}{64}\Big(\sum_{x_\zeta=x_\lambda}\varphi_\zeta(x_\mu)v(\zeta),\ \sum_{x_\zeta=x_\lambda}\varphi_\zeta(x_\mu)v(\zeta)\Big),$$

where $\{\lambda,\mu,v\}$ is an F-triple. Since there are 64 summands, we get $(v(\lambda)^{\sigma},v(\lambda)^{\sigma})=1$, as required. Now say $e=v(\lambda)\neq f=v(\mu)$, λ, $\mu\in\Lambda_2^2$. Let $\{\lambda,\lambda',\lambda''\}$ and $\{\mu,\mu',\mu''\}$ be F-triples. Then

$$(v(\lambda)^{\sigma},(\mu)^{\sigma})=\pm\tfrac{1}{64}\Big(\sum_{x_\zeta=x_\lambda}\varphi_\zeta(x_{\lambda'})v(\zeta),\ \sum_{x_\eta=x_\mu}\varphi_\eta(x_{\mu'})v(\eta)\Big)$$

which is clearly zero if $x_\lambda\neq x_\mu$. So, let us assume $x_\lambda=x_\mu$. Then the inner product is $\pm\frac{1}{64}\sum_{x_\zeta=x_\lambda}\varphi_\zeta(x_{\lambda'}x_{\mu'})$. Let $g=g_S\in O_2(H)$ satisfy $\tilde{\lambda}^{g}=\tilde{\mu}$. Without loss, $i\notin S$, $(\tilde{\lambda}')^{g}=\tilde{\mu}'$ and $(\tilde{\lambda}'')^{g}=\tilde{\mu}''$. Then $\varphi_\zeta(x_{\lambda'}x_{\mu'})=(-1)^{\langle\zeta,\xi\rangle}$ for all ζ with $x_\zeta=x_\lambda$, where

$$\operatorname{supp}\xi\subseteq\mathcal{O}_\lambda\quad\text{and}\quad\xi=(\underbrace{2\,2\ldots2}_{S\cap\mathcal{O}_\lambda}0\,0\ldots0)\quad(\operatorname{mod}\Lambda(4)).$$

Since $\tilde{\lambda}\neq\tilde{\mu}$, $S\cap\mathcal{O}_\lambda\neq\emptyset$ or $\mathcal{O}_\lambda$. Therefore $\sum_{x_\zeta=x_\lambda}(-1)^{\langle\zeta,\zeta\rangle}=0$; see Lemma 2.6. The proof is complete.

Corollary 10.2. $\sigma^2=1$.

Proof. It suffices to show that $e^{\sigma^2}=e$ for each basis element e. This is clear except possibly for $e=v(\lambda)$, $\lambda\in\Lambda_2^2$. The inner product $(v(\lambda)^{\sigma^2},v(\zeta)^\sigma)=(v(\lambda)^\sigma,v(\zeta))$ is nonzero if and only if $\zeta\in\Lambda_2$ and $x_\zeta=x_\lambda$. It suffices to show that this equals $(v(\lambda),v(\zeta)^\sigma)$, for all ζ with $x_\zeta=x_\lambda$ since $\{v(\tilde{\rho})^\sigma\,|\,\tilde{\rho}\in\tilde{\Lambda}_2\}$ is an orthonormal basis of V. Take $g=g_S\in O_2(H)$ such that $\tilde{\lambda}^g=\tilde{\zeta}$. Then

$$\begin{aligned}(v(\lambda),v(\zeta)^\sigma)^g&=(v(\lambda)^g,v(\zeta)^{\sigma g})=(v(\lambda)^g,v(\zeta)^{g\sigma})\\&=b(\lambda,g)\,b(\zeta,g)(v(\zeta),v(\lambda)^\sigma)=(v(\zeta),v(\lambda)^\sigma)\end{aligned}$$

because $b(\lambda',g)=b(\lambda'',g)$ whenever $x_{\lambda'}=x_{\lambda''}$ (see (8.5)). So, we are done.

§11. A Proof that σ is an Algebra Automorphism

The proof that σ preserves the algebra structure is, in some sense, the main result of the paper. It allows us to define a subgroup $G:=\langle C,\sigma\rangle$ of $G(B)$ which contains C properly. We show in Sect. 12 that G is a finite simple group of order $2^{46}3^{20}5^9 7^6 11^2 13^3 17.19.23.29.31.41.47.59.71$. The sign problem for σ, referred to in Sect. 10, is so important because we want $\sigma\in G(B)$, not just $\sigma\in\{g\in GL(B)\,|\,g$ preserves $(\ ,\ )\}$.

First, we prove a technical result. The phrase "$\tilde{\mu}\in\tilde{\Lambda}_2$" is meant to be understood when "$x_\mu=x_\lambda$" appears under a summation sign. Similar omissions appear throughout this section. We hope that no confusion results.

Lemma 11.1. *Let $\mathcal{O}$ be an octad, $\lambda=\lambda_{\mathcal{O}}$, $x\in F(2)$ and i, j, k, l distinct indices in $\mathcal{O}$. Then*

(i) $\displaystyle\sum_{x_\mu=x_\lambda}\varphi_{\mu+\lambda}(\tau x)=8(-1)^{\frac{1}{2}|S_x\cap\mathcal{O}|}$.

(ii) $\displaystyle\sum_{x_\mu=x_\lambda}\varphi_{\mu+\lambda}(\tau x)(-1)^{\frac{1}{2}\langle\lambda_{ij'},\mu\rangle}=8(-1)^{\frac{1}{2}|(S_x\cap\mathcal{O})+\{i,j\}|}$.

(iii) $\displaystyle\sum_{x_\mu=x_\lambda}\varphi_{\mu+\lambda}(\tau x)(-1)^{\frac{1}{2}\langle\lambda_{ij'}+\lambda_{kl'},\mu\rangle}=8(-1)^{\frac{1}{2}|(S_x\cap\mathcal{O})+\{i,j,k,l\}|}$.

More generally, if U is a subset of $\mathcal{O}$ of even cardinality, and $v=\sum_{i\in U}4x_i$, we have

$$\sum_{x_\mu=x_\lambda}\varphi_{\mu+\lambda}(\tau x)(-1)^{\frac{1}{2}\langle v,\mu\rangle+\frac{1}{2}|U|}=8(-1)^{\frac{1}{2}|(S_x\cap\mathcal{O})+U|}.$$

Proof. (i) Note that $\varphi_{\mu+\lambda}(\tau)$ is $(-1)^{\frac{1}{2}|\mathrm{supp}(\lambda+\mu)|}$, so the statement is clear for $|S_x\cap\mathcal{O}|=0$. Let $m(\lambda,x)=\sum_{x_\mu=x_\lambda}\varphi_{\lambda+\mu}(\tau x)$.

Suppose $|S_x\cap\mathcal{O}|=2$. We make a table, the (α,β) entry of which denotes the number of cosets $\lambda+\mu+2\Lambda$, as $\tilde{\mu}$ varies, containing a vector of shape $(\overbrace{4,4,\dots,4}^{2\alpha},0,\dots,0)$ whose support meets S_x in a set of cardinality $\beta(\mathrm{mod}\,2)$. Write $S(\lambda,\mu)$ for the support of this vector. It is a well defined element of $P(\mathcal{O})$ modulo $\langle\mathcal{O}\rangle$.

	$\beta=0$	$\beta=1$
$\alpha=0$	1	0
1	$1+15$	12
2	15	20

So, $m(\lambda, x)=-(0+1+15+20)+(1+12+15)=-8$, as required.

Suppose $|S_x \cap \mathcal{O}|=4$. We make a similar table

	$\beta=0$	$\beta=1$
$\alpha=0$	1	0
1	$\binom{4}{2}+\binom{4}{2}=12$	$4\cdot 4=16$
2	$1+3\binom{4}{2}=19$	16

So, $m(\lambda, x)=(1+16+19)-(0+12+16)=8$, as required.

Finally, if $s=|S_x \cap \mathcal{O}| \geqq 4$, we note that the associated table must be the same as that for the case $|S_x \cap \mathcal{O}|=8-s$, and quote a previous case to finish.

Now, let U, v be as in the Lemma. Let S be a $\mathscr{C}$-set which meets $\mathcal{O}$ in $(S_x \cap \mathcal{O})+U$. By (i), $8(-1)^{\frac{1}{2}|(S_x \cap \mathcal{O})+U|}=\sum_{x_\mu=x_\lambda} \varphi_{\mu+\lambda}(\tau x_S)$. It suffices to show that $\varphi_{\mu+\lambda}(x x_S)=(-1)^{\frac{1}{2}\langle v,\mu\rangle+\frac{1}{2}|U|}$, and, indeed, we have that

$$\begin{aligned}\varphi_{\mu+\lambda}(x x_S)&=(-1)^{|S(\lambda,\mu)\cap(S_x+S)|}=(-1)^{|S(\lambda,\mu)\cap((S_x+S)\cap\mathcal{O})|}\\&=(-1)^{|S(\lambda,\mu)\cap((S_x\cap\mathcal{O})+(S\cap\mathcal{O}))|}=(-1)^{|S(\lambda,\mu)\cap U|}\\&=(-1)^{\frac{1}{2}\langle v,\lambda+\mu\rangle}=(-1)^{\frac{1}{2}\langle v,\mu\rangle+\frac{1}{2}|U|},\end{aligned}$$

since $\lambda=\lambda_{\mathcal{O}}$ and $|U|$ is even. So, the last part of the Lemma holds.

We deduce (ii) by noting that for $U=\{i,j\}$, $\frac{1}{2}\langle\lambda_{ij},\mu\rangle+1 \equiv \frac{1}{2}\langle\lambda_{ij'},\mu\rangle \pmod 2$ and we deduce (iii) by noting that for $U=\{i,j,k,l\}$, $\frac{1}{2}\langle\lambda_{ij}+\lambda_{kl},\mu\rangle+0 \equiv \frac{1}{2}\langle\lambda_{ij'}+\lambda_{kl'},\mu\rangle+1+1 \pmod 2$.

We recommend that the reader become thoroughly familiar with Tables 6.1 and 10.2 before attempting Proposition 11.2.

Proposition 11.2. *σ preserves the algebra product on B.*

Proof. We study σ on products of basis vectors. Since we are using the decomposition $B=B_{24}\oplus B_{276}\oplus B_2^{4,+}\oplus B_2^{4,-}\oplus B_2^2\oplus B_2^3\oplus B_{\text{even}}\oplus B_{\text{odd}}$, evidently there are 36 cases. Some of the cases are equivalent by associativity of the form or by the action of σ. Thus, not every case needs to be treated in detail.

Here is how we make use of the property $[H,\sigma]=1$ (see Sect. 10). Suppose e and f are basis vectors and we wish to prove that $(ef)^\sigma=e^\sigma f^\sigma$. We take $h\in H$ so that $e_1=\varepsilon e^h$ and $f_1=\delta f^h$ where $\varepsilon=\pm 1$, $\delta=\pm 1$ and e_1, f_1 is a pair of basis vectors with more pleasant properties than e, f. It suffices to prove that $(e_1 f_1)^\sigma=e_1^\sigma f_1^\sigma$ because

$$(e_1 f_1)^\sigma=\varepsilon\delta(e^h f^h)^\sigma=\varepsilon\delta(ef)^{h\sigma}=\varepsilon\delta(ef)^{\sigma h}$$

and

$$e_1^\sigma f_1^\sigma=\varepsilon\delta\, e^{h\sigma} f^{h\sigma}=\varepsilon\delta\, e^{\sigma h} f^{\sigma h}=\varepsilon\delta(e^\sigma f^\sigma)^h.$$

Case 1. (B_{24}, B_{24}). Since σ acts trivially, there is nothing much to check.

Case 2. (B_{24}, B_{276}). We have, for $i \neq j$, $u_{ii}u_{ij} = -132u_{ij} \xmapsto{\sigma} -132(-v_{ij}+v_{ij'})$ and

$$\begin{aligned} u_{ii}^{\sigma}u_{ij}^{\sigma} &= u_{ii}(-v_{ij}+v_{ij'}) = -\tfrac{9}{4}(u_0(u_{ii}), u(\lambda_{ij}^2))(-v_{ij}+v_{ij'}) \\ &= -\tfrac{9}{4}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{k \neq i} u_{kk}, 16(u_{ii}+u_{jj}))(-v_{ij}+v_{ij'}) \\ &= -\tfrac{3}{2}\cdot 22.4(-v_{ij}+v_{ij'}) = -132(-v_{ij}+v_{ij'}), \end{aligned}$$

as required.

Let i, j, k be distinct indices. We have $u_{ii}u_{jk} = 12u_{jk} \xmapsto{\sigma} 12(-v_{jk}+v_{jk'})$ and

$$\begin{aligned} u_{ii}^{\sigma}u_{jk}^{\sigma} &= u_{ii}(-v_{jk}+v_{jk'}) = -\tfrac{9}{4}(u_0(u_{ii}), u(\lambda_{jk}^2))(-v_{jk}+v_{jk'}) \\ &= -\tfrac{9}{4}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{k=i} u_{kk}, 16(u_{jj}+u_{kk}))(-v_{jk}+v_{jk'}) \\ &= -\tfrac{3}{2}\cdot(-2)\cdot 4(-v_{jk}+v_{jk'}) = 12(-v_{jk}+v_{jk'}), \end{aligned}$$

as required.

Case 3. $(B_{24}, B_2^{4,+})$. Since σ acts trivially here, there is nothing much to check.

Case 4. $(B_{24}, B_2^{4,-})$. See Case 2.

Case 5. (B_{24}, B_2^2). We have

$$\begin{aligned} u_{ii}v(\lambda) = -\tfrac{9}{4}(u_0(u_{ii}), u(\lambda^2))\, v(\lambda) \xmapsto{\sigma} \tfrac{-81}{8}(u_0(u_{ii}), u(\lambda^2)) \\ \cdot\, \delta(\mu, v)\,\beta(\mu, v)^{-1} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{ik'}, \zeta\rangle} \varphi_\zeta(\tau x_S)\, v(\zeta), \end{aligned}$$

where $\{\lambda, \mu, v\}$ is an F-triple, $\mu = \lambda_{j,S}$, $v = \lambda_{k,T}$. Also

$$\begin{aligned} u_{ii}^{\sigma}v(\lambda)^{\sigma} &= \tfrac{9}{2}\beta(\mu, v)^{-1}\,\delta(\mu, v)\, u_{ii}\Big(\sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{jk'}, \zeta\rangle} \varphi_\zeta(\tau x_S)\, v(\zeta)\Big) \\ &= -\tfrac{81}{8}\beta(\mu, v)^{-1}\,\delta(\mu, v)(u_0(u_{ii}), u(\lambda^2))\cdot \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{jk'}, \zeta\rangle} \varphi_\zeta(\tau x_S), \end{aligned}$$

as required (we have used the fact that $u(\lambda^2)$ and $u(\zeta^2)$ have the same projection into B_{24} if $x_\zeta = x_\lambda$).

Case 6. (B_{24}, B_2^3). We have

$$\begin{aligned} u_{ii}v(\lambda_{j,x}) = -\tfrac{9}{4}(u_0(u_{ii}), u(\lambda_{j,x}^2))\, v(\lambda_{j,x}) &\xmapsto{\sigma} -\tfrac{9}{4}(u_0(u_{ii}), u(\lambda_{j,x}^2))(-1)^{\infty j \mathrm{in} S_x} e(\tau x) \otimes x_j \\ &= (-1)^{\infty j \mathrm{in} S_x}(\tfrac{-9}{4})(\tfrac{1}{24})(23u_{ii} - \sum_{k \neq i} u_{kk}, 9u_{jj} + \sum_{k \neq j} u_{kk})\, e(\tau x) \otimes x_j \\ &= (-1)^{\infty j \mathrm{in} S_x}(\tfrac{-3}{32})\cdot \begin{cases} 4\cdot 23\cdot 8 \\ 4\cdot(-8) \end{cases} e(\tau x) \otimes x_j \quad \begin{matrix} \text{if } i=j \\ \text{if } i \neq j \end{matrix} \\ &= (-1)^{\infty j \mathrm{in} S_x} \begin{cases} -69 \\ 3 \end{cases} e(\tau x) \otimes x_j \quad \begin{matrix} \text{if } i=j \\ \text{if } i \neq j \end{matrix}. \end{aligned}$$

Also,

$$\begin{aligned} u_{ii}^{\sigma} v(\lambda_{j,x})^{\sigma} &= u_{ii}[(-1)^{\infty j \mathrm{in} S_x} e(\tau x) \otimes x_j] \\ &= (-1)^{\infty j \mathrm{in} S_x} \begin{cases} -69 \\ 3 \end{cases} e(\tau x) \otimes x_j \quad \begin{matrix} \text{if } i=j \\ \text{if } i \neq j \end{matrix}, \end{aligned}$$

which agrees with the above.

Case 7. $(B_{24}, B_{\mathrm{even}})$. We have

$$u_{ii} \cdot e(x) \otimes x_j = e(x) \otimes p(u_{ii}, x_j) \xmapsto{\sigma} (-1)^{\langle \lambda_\infty, \lambda_{j,x} \rangle} e(x) \otimes p(u_{ii}, x_j)$$

because $p(u_{ii}, x_j) \in \mathbb{Q} x_j$. Also,

$$u_{ii}^{\sigma}(e(x) \otimes x_j)^{\sigma} = u_{ii}[(-1)^{\langle \lambda_\infty, \lambda_{j,x} \rangle} e(x) \otimes x_j] = (-1)^{\langle \lambda_\infty, \lambda_{j,x} \rangle} e(x) \otimes p(u_{ii}, x_j).$$

Case 8. $(B_{24}, B_{\mathrm{odd}})$. See Case 6.

Case 9. (B_{276}, B_{276}). By using associativity of the form, it suffices to treat the case $u_{ij} u_{kl}$, where $\{i,j\} \neq \{k,l\}$. It is easy to do the case $\{i,j\} \cap \{k,l\} = \emptyset$ (all relevant products are zero). We calculate

$$u_{ij} u_{jk} = -72 u_{ik} \xmapsto{\sigma} -72(-v_{ik} + v_{ik'})$$

and

$$u_{ij}^{\sigma} u_{jk}^{\sigma} = (-v_{ij} + v_{ij'})(-v_{jk} + v_{jk'}) = -72(-v_{ik} + v_{ik'}) = -72 u_{ik}^{\sigma},$$

as required.

Case 10. $(B_{276}, B_2^{4,+})$. We have $u_{ij}(v_{kl} + v_{kl'}) = 0$ if $\{i,j\} \neq \{k,l\}$ and

$$u_{ij}(v_{ij} + v_{ij'}) = 144(-v_{ij} + v_{ij'}) \xmapsto{\sigma} 144 u_{ij}$$

because

$$-\tfrac{9}{4}(u_{ij}, u(\lambda_{ij}^2)) = -144 \quad \text{and} \quad -\tfrac{9}{4}(u_{ij}, u(\lambda_{ij'}^2)) = 144.$$

Also $u_{ij}^{\sigma}(v_{kl} + v_{kl'})^{\sigma} = (-v_{ij} + v_{ij'})(v_{kl} + v_{kl'}) = 0$ if $\{i,j\} \neq \{k,l\}$ and if $\{i,j\} = \{k,l\}$ it equals $-\frac{9}{4}(-u_0(\lambda_{ij}^2) + u_0(\lambda_{ij'}^2)) = 144 u_{ij}$, as required.

Case 11. $(B_{276}, B_2^{4,-})$. This is equivalent to Case 10 by associativity of the form.

Case 12. (B_{276}, B_2^2). Here, $\operatorname{supp} \lambda = \mathcal{O}$ is an octad. Let $\{\lambda, \mu, \nu\}$ be an F-triple, $\mu = \lambda_{k,S}$, $\nu = \lambda_{l,T}$. We have

$$\begin{aligned} u_{ij} v(\lambda) = -\tfrac{9}{4}(u_{ij}, u(\lambda^2)) v(\lambda) \xmapsto{\sigma} & -\tfrac{81}{8}(u_{ij}, u(\lambda^2)) \\ & \cdot \delta(\mu, \nu) \beta(\mu, \nu)^{-1} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \zeta \rangle} \varphi_\zeta(x_\mu) v(\zeta). \end{aligned}$$

Also,

$$u_{ij}^{\sigma} v(\lambda)^{\sigma} = (-v_{ij} + v_{ij'})(\tfrac{9}{2}) \delta(\mu, \nu) \beta(\mu, \nu)^{-1} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \zeta \rangle} \varphi_\zeta(x_\mu) v(\zeta).$$

For a given $\tilde{\zeta}$, just one of $\lambda_{ij} \pm \zeta$, $\lambda_{ij'} \pm \zeta$ is in $\tilde{\Lambda}_2$; call it ζ'. The map $\tilde{\zeta} \mapsto \tilde{\zeta}'$ is a permutation of order 2 of $\{\tilde{\eta} \in \tilde{\Lambda}_2 \mid \operatorname{supp} \eta = \mathcal{O}\}$. After computing the product $(-v_{ij} + v_{ij'}) v(\zeta)$, let $-36 \gamma_{ij}(\zeta)$ be the coefficient of $v(\zeta')$. We must show that

$$(-1)^{\frac{1}{2}\langle \lambda_{ij'}, \lambda \rangle + \frac{1}{2}\langle \lambda_{kl'}, \zeta' \rangle} \varphi_{\zeta'}(x_\mu) = (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \zeta \rangle} \varphi_\zeta(x_\mu) \gamma_{ij}(\zeta),$$

for all ζ. It is easy to check that $\langle \zeta - \zeta', \mu \rangle \equiv ij$ in $S + ij$ in $\mathrm{Pos}(\zeta) + 1 \pmod 2$. Using Lemma 2.3(ii), ij in $S \equiv ij$ in $\mathrm{Pos}(\lambda) + ij$ in $\{k, l\} \pmod 2$. Since $\frac{1}{2}\langle \lambda_{kl'}, \zeta - \zeta' \rangle \equiv ij$ in $\{kl\} \pmod 2$, $\frac{1}{2}\langle \lambda_{ij'}, \lambda \rangle \equiv ij$ in $\mathrm{Pos}(\lambda)$ we are reduced to proving that $\gamma_{ij}(\zeta) = (-1)^{ij \mathrm{in} \mathrm{Pos}(\zeta) + 1}$. But this follows from the definition of $\gamma_{ij}(\zeta)$ and Corollary 9.3.

Case 13. (B_{276}, B_2^3). We have

$$\begin{aligned} u_{ij} v(\lambda_{k,x}) &= -\tfrac{9}{4}(u_{ij}, u(\lambda_{k,x}^2))\, v(\lambda_{k,x}) \\ &\xmapsto{\sigma} -\tfrac{9}{4}(u_{ij}, u(\lambda_{k,x}^2))(-1)^{\infty k \mathrm{in} S_x} e(\tau x) \otimes x_k. \end{aligned}$$

Also,

$$\begin{aligned} u_{ij}^{\sigma} v(\lambda_{k,x})^{\sigma} &= (-v_{ij} + v_{ij'})(-1)^{\infty k \mathrm{in} S_x} e(\tau x) \otimes x_k \\ &= -(-1)^{\infty k \mathrm{in} S_x} \sum_{l \in \Omega} [-6\delta_{kl} \varphi_{\lambda_{ij}}(\tau x) \\ &\qquad + \tfrac{9}{32}(u_0(u_{kl}), \varphi_{\lambda_{ij}}(\tau x) u(\lambda_{ij}^2) - \varphi_{\lambda_{ij'}}(\tau x) u(\lambda_{ij'}^2))]\, e(\tau x) \otimes x_l. \end{aligned}$$

For $k \neq l$ in the latter sum, we claim that the bracketed coefficient is zero. This is quite clear for $\{i, j\} \neq \{k, l\}$ and for $\{i, j\} = \{k, l\}$ it is almost as clear (we use $\varphi_{\lambda_{ij}}(\tau x) = -\varphi_{\lambda_{ij'}}(\tau x)$). Now take $k = l$. The bracketed term is

$$\begin{aligned} &-6\varphi_{\lambda_{ij}}(\tau x) + \tfrac{9}{32}(u_0(u_{kk}), \varphi_{\lambda_{ij}}(\tau x) u(\lambda_{ij}^2) - \varphi_{\lambda_{ij'}}(\tau x) u(\lambda_{ij'}^2)) \\ &\quad = [-6 + \tfrac{9}{32} \cdot \tfrac{1}{24}(23 u_{kk} - \sum_{r \neq k} u_{rr}, 32(u_{ii} + u_{jj}))]\, \varphi_{\lambda_{ij}}(\tau x) \\ &\quad = -6 + \tfrac{3}{2}\left\{ \begin{matrix} 22 & \text{if } k \in \{i, j\} \\ -2 & \text{if } k \notin \{i, j\} \end{matrix} \right] \varphi_{\lambda_{ij}}(\tau x) = \begin{cases} 27\varphi_{\lambda_{ij}}(\tau x) & \text{if } k \in \{i, j\} \\ -9\varphi_{\lambda_{ij}}(\tau x) & \text{if } k \notin \{i, j\} \end{cases}. \end{aligned}$$

Up to a factor of $-(-1)^{\infty k \mathrm{in} S_x}$, this agrees with

$$\begin{aligned} &(-1)^{\infty k \mathrm{in} S_x}(-\tfrac{9}{4})(u_{ij}, u(\lambda_{k,x}^2)) \\ &\quad = (-1)^{\infty k \mathrm{in} S_x + ij \mathrm{in} S_x}(-\tfrac{9}{4}) \begin{cases} -12 & \text{if } k \in \{i, j\} \\ 4 & \text{if } k \notin \{i, j\} \end{cases} \end{aligned}$$

because $\varphi_{\lambda_{ij}}(\tau x) = (-1)^{1 + ij \mathrm{in} S_x}$. So, σ preserves the product in this case.

Case 14. $(B_{276}, B_{\text{even}})$. We have $u_{ij} \cdot e(x) \otimes x_k = e(x) \otimes p(u_{ij}, x_k)$, which is zero unless $k \in \{i, j\}$ in which case it equals $-36 e(x) \otimes x_l$, where $\{k, l\} = \{i, j\}$. When nonzero, its image under σ is $-36(-1)^{\langle \lambda_\infty, \lambda_{l,x} \rangle} e(x) \otimes x_l$. In either case,

$$\begin{aligned} u_{ij}^{\sigma}(e(x) \otimes x_k)^{\sigma} &= (-v_{ij} + v_{ij'})(-1)^{\langle \lambda_\infty, \lambda_{k,x} \rangle} e(x) \otimes x_k \\ &= -(-1)^{\langle \lambda_\infty, \lambda_{k,x} \rangle} \sum_{r \in \Omega} [\tfrac{9}{32}(u_0(u_{kr}), u(\lambda_{ij}^2) - u(\lambda_{ij'}^2))]\, \varphi_{\lambda_{ij}}(x)\, e(x) \otimes x_r. \end{aligned}$$

When the product is zero ($k \notin \{i, j\}$), we observe that $u_{ij}^{\sigma}(e(x) \otimes x_k)^{\sigma} = 0$, as required. Now assume $k \in \{i, j\}$. For $r = k$, $(u_0(u_{kk}), u(\lambda_{ij}^2) - u(\lambda_{ij'}^2)) = 0$, as required. For $r \neq k$ and $\{r, k\} \neq \{i, j\}$, the bracketed coefficient is zero. If $\{r, k\} = \{i, j\}$, then $r = l$ and

$$\tfrac{9}{32}(u_{kl}, u(\lambda_{ij}^2) - u(\lambda_{ij'}^2)) = \tfrac{9}{32}(u_{ij}, 64 u_{ij}) = 36.$$

This gives the desired equality because

$$\begin{aligned}1+\langle\lambda_\infty,\lambda_{k,x}\rangle+ij \text{ in } S_x &\equiv 1+\tfrac{1}{4}|S_x|+\infty k \text{ in } S_x+ij \text{ in } S_x\\ &\equiv 1+\tfrac{1}{4}|S_x|+\infty l \text{ in } S_x\equiv 1+\langle\lambda_\infty,\lambda_{l,x}\rangle \pmod 2.\end{aligned}$$

Case 15. $(B_{276}, B_{\text{odd}})$. See Case 13.

Case 16. $(B_2^{4,+}, B_2^{4,+})$. We have $(v_{ij}+v_{ij'})(v_{kl}+v_{kl'})=0$ when $\{i,j\}\cap\{k,l\}=\emptyset$,

$$(v_{ij}+v_{ij'})^2=\tfrac{9}{4}(u_0(\lambda_{ij}^2)+u_0(\lambda_{ij'}^2))$$

and

$$(v_{ij}+v_{ij'})(v_{jk}+v_{jk'})=-72(v_{ik}+v_{ik'}).$$

Clearly, everything is fixed by σ, so there is no problem.

Case 17. $(B_2^{4,+}, B_2^{4,-})$. This is equivalent to Case 10.

Case 18. $(B_2^{4,+}, B_2^2)$. We have $(v_{ij}+v_{ij'})v(\lambda)=0$ if $\{i,j\}\nsubseteq\mathcal{O}=\operatorname{supp}\lambda$ and when $i, j\in\mathcal{O}$, $(v_{ij}+v_{ij'})v(\lambda)=-36v(\lambda')$ where $\lambda'=\lambda\pm\lambda_{ij}$ or $\lambda\pm\lambda_{ij'}$, whichever lies in Λ_2^2; see Case 12 and Corollary 9.3. If $\{i,j\}\nsubseteq\mathcal{O}$, it is clear that $(v_{ij}+v_{ij})^\sigma v(\lambda)^\sigma=0$. So, we assume $i, j\in\mathcal{O}$ from now on.

We have $-36v(\lambda')^\sigma=-162\delta(\mu',\nu')\beta(\mu',\nu')^{-1}\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\varphi_\zeta(x_{\mu'})v(\zeta)$, where $\{\lambda',\mu',\nu'\}$ is an F-triple with $k=i(\mu')$, $l=i(\nu')$. Also,

$$\begin{aligned}(v_{ij}+v_{ij'})^\sigma v(\lambda)\sigma&=(v_{ij}+v_{ij'})(\tfrac{9}{2})\delta(\mu,\nu)\beta(\mu,\nu)^{-1}\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\varphi_\zeta(x_\mu)v(\zeta)\\ &=(-162)\delta(\mu,\nu)\beta(\mu,\nu)^{-1}\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{k,l'},\zeta'\rangle}\varphi_{\zeta'}(x_\mu)v(\zeta),\end{aligned}$$

where $\{\lambda,\mu,\nu\}$ is an F-triple with $k=i(\mu)$, $l=i(\nu)$. (This is easy to arrange; for instance, let $g\in O_2(N_{24})$ satisfy $\lambda'^g=\lambda$, then take $\mu=\mu'^g$, $\nu=\nu'^g$.) Thus, we must prove, for all ζ, that

$$\begin{aligned}&\delta(\mu',\nu')\beta(\mu',\nu')\varphi_\zeta(x_{\mu'})(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\\ &\quad=\delta(\mu,\nu)\beta(\mu,\nu)\varphi_{\zeta'}(x_\mu)(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta'\rangle}.\end{aligned}$$

We now verify two claims. The first is

$$\delta(\mu,\nu)\beta(\mu,\nu)^{-1}\varphi_\zeta(x_\mu)(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\delta(\mu',\nu')\beta(\mu',\nu')^{-1}\varphi_{\zeta'}(x_{\mu'})(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta'\rangle}.$$

Take $g\in O_2(H)$ so that $\tilde{\lambda}^g=\tilde{\lambda}'$. Then

$$\begin{aligned}v(\lambda')^\sigma&=b(\lambda',g)v(\lambda)^{g\sigma}=b(\lambda',g)v(\lambda)^{\sigma g}\\ &=b(\lambda',g)\delta(\mu,\nu)\beta(\mu,\nu)^{-1}(\tfrac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\varphi_\zeta(x_\mu)v(\zeta)^g\\ &=\delta(\mu,\nu)\beta(\mu,\nu)^{-1}(\tfrac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle}\varphi_\zeta(x_\mu)v(\zeta')\end{aligned}$$

because $b(\xi, g)$ depends only on x_ξ (see (8.5)). Comparing this with the formula for $v(\lambda')^\sigma$, we get the claim. The second claim is that $\langle\lambda+\lambda', \mu+\mu'\rangle \equiv 0 \pmod 2$. Since $\lambda+\lambda' \equiv \zeta+\zeta' \pmod{2\Lambda+\Lambda(8)}$, this claim implies that

$$\begin{aligned}1 &= (-1)^{\langle\zeta+\zeta', \mu+\mu'\rangle} = \varphi_{\zeta+\zeta'}(\mu+\mu') = \varphi_{\zeta+\zeta'}(x_\mu x_{\mu'})\\ &= \varphi_\zeta(x_\mu)\,\varphi_{\zeta'}(x_{\mu'})\,\varphi_\zeta(x_{\mu'})\,\varphi_{\zeta'}(x_\mu),\end{aligned}$$

which, together with the first claim, proves the required equality stated at the end of the last paragraph. So, let us prove the second claim. We have $\mu=\lambda_{k,S}$, $v=\lambda_{l,T}$, $\mu'=\lambda_{k,S'}$, $v'=\lambda_{l,T'}$. Since $(\{k,l\}+S)\cap\mathcal{O} \equiv \operatorname{Pos}(\lambda) \pmod{\langle\Omega\rangle}$ and $(\{k,l\}+S')\cap\mathcal{O} \equiv \operatorname{Pos}(\lambda') \pmod{\langle\Omega\rangle}$ (see Lemma 2.3(ii)), we have $(S+S')\cap\mathcal{O} \equiv \operatorname{Pos}(\lambda) + \operatorname{Pos}(\lambda') \equiv \{ij\} \pmod{\langle\Omega\rangle}$. Therefore, the coordinates of $\mu-\mu'$ over $\mathcal{O}$ consist of ± 2 at i and j and 0 elsewhere, whence $\langle\lambda+\lambda', \mu+\mu'\rangle \equiv \frac{1}{8}(\pm 8 \pm 8) \equiv 0 \pmod 2$. The second claim follows, and we are done.

Case 19. $(B_2^{4,+}, B_2^3)$. We have $(v_{ij}+v_{ij'})\,v(\lambda_{k,x})=0$ unless $k\in\{i,j\}$ and if $\{k,l\}=\{i,j\}$ we have $(v_{ij}+v_{ij'})\,v(\lambda_{k,x}) = -36\,v(\lambda_{l,x}) \xrightarrow{\sigma} (-1)^{\infty l \text{ in } S_x+1}\, 36\, e(\tau x)\otimes x_l$. In either case,

$$\begin{aligned}(v_{ij}+v_{ij'})^\sigma\, v(\lambda_{k,x})^\sigma &= (-1)^{\infty k \text{ in } S_x}(v_{ij}+v_{ij'})\, e(\tau x)\otimes x_k\\ &= (-1)^{\infty k \text{ in } S_x} \sum_{l\in\Omega} \tfrac{9}{32}(u_0(u_{kl}), u(\lambda_{ij}^2)-u(\lambda_{ij'}^2))\, \varphi_{\lambda_{l,j}}(\tau x)\, e(\tau x)\otimes x_l.\end{aligned}$$

The coefficient is zero unless $\{k,l\}=\{i,j\}$ in which case $(u_{ij}, u(\lambda_{ij}^2)-u(\lambda_{ij'}^2)) = (u_{ij}, 64u_{ij}) = 128$. Thus, when $\{k,l\}=\{i,j\}$, we must prove that ∞l in $S_x + 1 \equiv \infty k \text{ in } S_x + \langle\lambda_{\infty,x}, \lambda_{ij}\rangle \pmod 2$. Since $\langle\lambda_{\infty,x}, \lambda_{ij}\rangle = \langle\lambda_\infty, \lambda_{ij}\rangle + \langle\lambda_{S_x}, \lambda_{ij}\rangle \equiv 1 + ij$ in $S_x \pmod 2$, the congruence is valid.

Case 20. $(B_2^{4,+}, B_{\text{even}})$. We have

$$\begin{aligned}&(v_{ij}+v_{ij'})\, e(x)\otimes x_k\\ &\quad= \sum_{l\in\Omega} [-6\delta_{kl} + \tfrac{9}{32}(u_0(u_{kl}), u(\lambda_{ij}^2)+u(\lambda_{ij'}^2))]\, \varphi_{\lambda_{l,j}}(x)\, e(x)\otimes x_l\\ &\quad= -6 + \tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{kk} - \sum_{r\neq k} u_{rr}, 32(u_{ii}+u_{jj}))\, \varphi_{\lambda_{l,j}}(x)\, e(x)\otimes x_k\\ &\quad= -6 + \tfrac{3}{2}\begin{cases} 22 & k\in\{i,j\}\\ -2 & k\notin\{i,j\}\end{cases}\Bigg] (-1)^{ij \text{ in } S_x}\, e(x)\otimes x_k\\ &\quad= (-1)^{ij \text{ in } S_x}\cdot \begin{cases} 27 & k\in\{i,j\}\\ -9 & k\notin\{i,j\}\end{cases} e(x)\otimes x_k \overset{\sigma}{\longmapsto} (-1)^{ij \text{ in } S_x + \langle\lambda_\infty, \lambda_{k,x}\rangle}\\ &\qquad\cdot \begin{cases} 27 & k\in\{i,j\}\\ -9 & k\notin\{i,j\}\end{cases} e(x)\otimes x_k.\end{aligned}$$

Also, $(v_{ij}+v_{ij'})^\sigma (e(x)\otimes x_k)^\sigma = (v_{ij}+v_{ij'})(-1)^{\langle\lambda_\infty, \lambda_{k,x}\rangle}\, e(x)\otimes x_k$, which is easily seen to equal the image of the product under σ by comparing the previous sentence.

Case 21. $(B_2^{4,+}, B_{\text{odd}})$. See Case 19.

Case 22. $(B_2^{4,-}, B_2^{4,-})$. See Case 9.

Case 23. $(B_2^{4,-}, B_2^2)$. See Case 12.

Case 24. $(B_2^{4,-}, B_2^3)$. See Case 15.

Case 25. $(B_2^{4,-}, B_{\text{even}})$. See Case 14.

Case 26. $(B_2^{4,-}, B_{\text{odd}})$. See Case 13.

Case 27. (B_2^2, B_2^2). We first consider $v(\lambda)v(\mu)$ where $\{\lambda, \mu, v\}$ forms a triangle of type 222. By quoting Cases 18 and 23, we need to treat only the case where $\{\lambda, \mu, v\} \in \Delta(2, 2)$. Later, we shall consider $v(\lambda)v(\mu)$ where $\lambda+\mu$, $\lambda-\mu \notin \Lambda_2$, i.e. the case $v(\lambda)v(\mu)=0$.

Since $[H, \sigma]=1$, we may assume $q(\{\lambda, \mu, \lambda+\mu\}) \subset F$ without loss; see Lemma 7.3. Expand λ, μ, v to F-triples $\{\lambda, \lambda', \lambda''\}$, $\{\mu, \mu', \mu''\}$ and $\{v, v', v''\}$ all of whose vectors map to elements of F under q. Write $\lambda'=\lambda_{i_1, S_1}$, $\lambda''=\lambda_{j_1, T_1}$, $\mu'=\lambda_{i_2, S_2}$, $\mu''=\lambda_{j_2, T_2}$, $v'=\lambda_{i_3, S_3}$, $v''=\lambda_{j_3, T_3}$.

We have

$$v(\lambda)v(\mu) = -36\,v(v) \xmapsto{\sigma}$$
$$-36\,\beta(v', v'')^{-1}\,\delta(v', v'')(\tfrac{9}{2}) \sum_{x_\rho = x_v} (-1)^{\frac{1}{2}\langle \lambda_{i_1 j_1}, \rho\rangle}\,\varphi_\rho(x_{v'})\,v(\rho).$$

Also,

$$v(\lambda)^\sigma v(\mu)^\sigma = \tfrac{81}{4}\,\beta(\lambda', \lambda'')^{-1}\,\beta(\mu', \mu'')^{-1}\,\delta(\lambda', \lambda'')\,\delta(\mu', \mu'').$$
$$\sum_{x_\rho = x_v} \Big\{ \sum_{\substack{x_\zeta = x_\lambda,\, x_\eta = x_\mu \\ \tilde{\zeta} + \tilde{\eta} = \tilde{\rho}}} (-1)^{\frac{1}{2}\langle \lambda_{i_2 j_2}, \zeta\rangle + \frac{1}{2}\langle \lambda_{i_3 j_3}, \eta\rangle}\,\varphi_\zeta(x_{\lambda'})\,\varphi_\eta(x_{\mu'})\,\beta(\zeta, \eta)\Big\}\,v(\rho).$$

We have $-36\beta(v', v'')^{-1}=1$ and $\frac{81}{4}\beta(\lambda', \lambda'')^{-1}\beta(\mu', \mu'')^{-1}=\frac{1}{64}$. Also,

$$\beta(\zeta, \eta) = (-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|}\,\beta(\lambda, \mu) = -36(-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|},$$

where $g=g_{\zeta,\eta} \in O_2(H)$ satisfies $\tilde{\lambda}^g=\tilde{\zeta}$, $\tilde{\mu}^g=\tilde{\eta}$ and $\tilde{v}^g=\tilde{\rho}$. Note that the image of g in $\cdot 1$ under $\bar{\pi}$ is not uniquely determined since the annihilator of $\mathcal{O}_\lambda \cup \mathcal{O}_\mu$ in $\mathscr{C}$ with respect to the natural bilinear form on $P(\Omega)$ is a four-group consisting of the images of $\emptyset$ and three octads disjoint from $\mathcal{O}_\lambda \cup \mathcal{O}_\mu$ (expand $\mathcal{O}_\lambda \cap \mathcal{O}_\mu$ to a sextet of tetrads to see this). So, we must prove that

$$\delta(v', v'')(-1)^{\frac{1}{2}\langle \lambda_{i_1 j_1'}, \rho\rangle}\,\varphi_\rho(x_{v'}) =$$
$$-\tfrac{1}{8}\,\delta(\lambda', \lambda'')\,\delta(\mu', \mu'') \sum_{\substack{x_\zeta = x_\lambda,\, x_\eta = x_\mu \\ \zeta + \eta = \rho}} (-1)^{\frac{1}{2}\langle \lambda_{i_2, j_2'}, \zeta\rangle + \frac{1}{2}\langle \lambda_{i_3 j_3'}, \eta\rangle}$$
$$\cdot\,\varphi_\zeta(x_{\lambda'})\,\varphi_\eta(x_\mu)(-1)^{|S_{g_{\zeta,\eta}} \cap \mathcal{O}_\lambda \cap \mathcal{O}_\mu|}.$$

Since there are eight summands, each ± 1, certainly one of the requirements is that the summands be constant. Writing this out, we find that we must prove that

$$(*) \qquad f(\rho, \zeta, \eta) = (-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|}, \qquad g = g_{\zeta,\eta},$$

where

$$f(\rho, \zeta, \eta) := \varphi_\rho(x_{\nu'})\,\varphi_\zeta(x_{\lambda'})\,\varphi_\eta(x_{\mu'})\,\delta(\nu', \nu'')\,\delta(\lambda', \lambda'')\,\delta(\mu', \mu'')$$
$$\cdot(-1)^{\frac{1}{2}\langle\lambda_{i_1 j_1'}, \rho\rangle + \frac{1}{2}\langle\lambda i_2 j_2', \zeta\rangle + \frac{1}{2}\langle\lambda_{i_3 j_3'}, \eta\rangle + 1}$$
$$= \varphi_\rho(x_{\nu'})\,\varphi_\zeta(x_{\lambda'})\,\varphi_\eta(x_{\mu'})(-1)^{\frac{1}{2}\langle\lambda_{i_1 j_1'}, \rho-\nu\rangle + \frac{1}{2}\langle\lambda_{i_2 j_2'}, \zeta-\lambda\rangle + \frac{1}{2}\langle\lambda_{i_3 j_3'}, \eta-\mu\rangle}$$

using Lemma 7.8(ii) to simplify. Strictly speaking, $g_{\zeta,\eta}$ is not a well defined element of $O_2(H)$. It suffices to check $(*)$ for any choice of $g_{\zeta,\eta}$ since $\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap \mathrm{S}_{g_{\zeta,\eta}}\,(\mathrm{mod}\,\langle\mathcal{O}_\lambda \cap \mathcal{O}_\mu\rangle)$ is all that matters here.

Define

$$\mathcal{I}^* = \{(\tilde{\rho}, \tilde{\zeta}, \tilde{\eta}) \in \Delta(2, 2) \mid x_\rho = x_\nu,\ x_\zeta = x_\lambda,\ x_\eta = x_\mu,\ \rho = \zeta + \eta\},$$

$$\mathcal{I} = \{(\tilde{\rho}, \tilde{\zeta}, \tilde{\eta}) \in \mathcal{I}^* \mid (*) \text{ holds for } (\rho, \zeta, \eta)\}.$$

Using $q(\{\lambda, \mu, \nu\}) \subset F$ we get $f(\nu, \lambda, \mu) = 1$. Since we may take $g = 1$, we see that $(\tilde{\nu}, \tilde{\lambda}, \tilde{\mu}) \in \mathcal{I} \neq \emptyset$.

In what follows, we shall assume that $\lambda + \mu = \nu$ and $\zeta + \eta = \rho$ in Λ, not just modulo 2Λ. Also, we shall drop the tilde notation for triples in $\mathcal{I}$.

Suppose $(\rho, \zeta, \eta) \in \mathcal{I}$. Keeping ρ fixed, we make the change $\zeta \mapsto \zeta'$, $\eta \mapsto \eta'$ by changing the signs of the coordinates for ζ and η at indicates r and s. Let $g_1 \in O_2(H)$ effect this change. We show that $(\rho, \zeta', \eta') \in \mathcal{I}$. We have $r, s \in \mathcal{O}_\lambda \cap \mathcal{O}_\mu$. Note that the right side of $(*)$ is not changed by the priming operation since $r, s \in \mathcal{O}_\lambda \cap \mathcal{O}_\mu$. We have $\langle\zeta - \zeta', \lambda'\rangle \equiv 1 + rs$ in $\mathrm{Pos}(\zeta) + rs$ in $S_1\,(\mathrm{mod}\,2)$ and $\langle\eta - \eta', \mu'\rangle \equiv 1 + rs$ in $\mathrm{Pos}(\eta) + rs$ in $S_2(\mathrm{mod}\,2)$. Therefore, $\langle\zeta - \zeta', \lambda'\rangle + \langle\eta - \eta', \mu'\rangle \equiv rs$ in $(S_1 + S_2)\,(\mathrm{mod}\,2)$ and so

$$f(\rho, \zeta', \eta')\,f(\rho, \zeta, \eta) = (-1)^{rs \text{ in } S_1 + S_2 + \frac{1}{2}\langle\lambda_{i_2 j_2'}, \zeta - \zeta'\rangle + \frac{1}{2}\langle\lambda_{i_3 j_3'}, \eta - \eta'\rangle}$$
$$= (-1)^{rs \text{ in } S_1 + S_2 + rs \text{ in } \{i_2 j_2\} + \{i_3, j_3\}}$$
$$= (-1)^{rs \text{ in } \mathrm{Pos}(\lambda) + \mathrm{Pos}(\mu)} = (-1)^{rs \text{ in } \emptyset} = 1,$$

(see Lemma 2.3(ii)). Since $S_{g_1} \cap \mathcal{O}_\lambda \cap \mathcal{O}_\mu \equiv \{r, s\}\,(\mathrm{mod}\,\mathcal{O}_\lambda \cap \mathcal{O}_\mu)$, the right sides of $(*)$ for (ρ, ζ, η) and (ρ, ζ', η') differ by a factor of $(-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_{g_1}|} = (-1)^{|\{r,s\}|} = 1$. Thus, $(\rho, \zeta', \eta') \in \mathcal{I}$.

Next, suppose that $(\rho, \zeta, \eta) \in \mathcal{I}$ and that we change ρ to ρ' at indices r, s in $\mathcal{O}_\nu$. We change ζ, η to ζ', η' by coordinate sign changes exactly at r, s in case $\{r, s\} \subseteq \mathcal{O}_\lambda - \mathcal{O}_\mu$ or $\mathcal{O}_\mu - \mathcal{O}_\lambda$, and otherwise we introduce a third index $t \in \mathcal{O}_\lambda \cap \mathcal{O}_\mu$ and change the signs of the coordinates of ζ and η exactly at $\{r, s, t\}$. We show that $(\rho', \zeta', \eta') \in \mathcal{I}$. Let $g' \in O_2(H)$ satisfy $\tilde{\nu}^{g'} = \tilde{\rho}'$ and let $g_1 \in O_2(H)$ satisfy $\rho^g = \rho'$, $\zeta^g = \zeta'$, $\eta^g = \eta'$.

Let us treat the case $\{r, s\} \subseteq \mathcal{O}_\lambda - \mathcal{O}_\mu$. We claim that $|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_{g'}| \equiv |\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|\,(\mathrm{mod}\,2)$. Namely, write $g_1 = g_T$, $T \in \mathcal{C}$. Then T is a $\mathcal{C}$-set which meets $\mathcal{O}_\nu$ in $\{r, s\}$ exactly. Since any two $\mathcal{C}$-sets intersect in a set of even cardinality, $|T \cap (\mathcal{O}_\lambda - \mathcal{O}_\mu)| \equiv 0\,(\mathrm{mod}\,2)$ implies that $|T \cap \mathcal{O}_\lambda \cap \mathcal{O}_\mu| \equiv 0\,(\mathrm{mod}\,2)$. The claim follows by using the natural bilinear form on $P(\Omega)$. Since η is unaffected by sign changes, we concentrate on the effect of $\zeta \mapsto \zeta'$ and $\rho \mapsto \rho'$. Given the claim, the analysis proceeds as in the case ρ fixed but ζ and η changed. Another way to finish off the argument is to observe that the left side of $(*)$ is symmetric in the pairs (ρ, ν), (ζ, λ) and (η, μ) so that we can invoke symmetry and quote the earlier case where ρ was fixed, using $|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g| \equiv |\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_{g'}| \pmod 2$. Either way, we obtain $f(\rho', \zeta', \eta) = f(\rho, \zeta, \eta)$, whence $(\rho', \zeta', \eta) \in \mathscr{I}$.

Let us now treat the case $r \in \mathcal{O}_\lambda - \mathcal{O}_\mu$, $s \in \mathcal{O}_\mu - \mathcal{O}_\lambda$, $t \in \mathcal{O}_\lambda \cap \mathcal{O}_\mu$. We argue as in the above paragraph to get $|S_\lambda \cap S_\mu \cap S_{g'}| \equiv 1 + |S_\lambda \cap S_\mu \cap S_g| \pmod 2$. So, we must show that the left side of $(*)$ changes sign as we move from (ρ, ζ, η) to (ρ', ζ', η').

We have

$$\langle \zeta - \zeta', \lambda' \rangle \equiv 1 + rt \text{ in } \mathrm{Pos}(\zeta) + rt \text{ in } S_1 \pmod 2,$$

$$\langle \eta - \eta', \mu' \rangle \equiv 1 + st \text{ in } \mathrm{Pos}(\eta) + st \text{ in } S_2 \pmod 2$$

and

$$\langle \rho - \rho', \nu' \rangle \equiv 1 + rs \text{ in } \mathrm{Pos}(\rho) + rs \text{ in } S_3 \pmod 2.$$

Also,

$$\tfrac{1}{2}\langle \lambda_{i_1 j_1'}, \zeta - \zeta' \rangle \equiv rt \text{ in } \{i_1 j_1\} \pmod 2,$$

$$\tfrac{1}{2}\langle \lambda_{i_2, j_2'}, \eta - \eta' \rangle \equiv st \text{ in } \{i_2 j_2\} \pmod 2$$

and

$$\tfrac{1}{2}\langle \lambda_{i_3, j_3'}, \rho - \rho' \rangle \equiv rs \text{ in } \{i_3 j_3\} \pmod 2.$$

The sum of these six terms is

$$\begin{aligned} &3 + rt \text{ in } (\{i_1 j_1\} + S_1) + st \text{ in } (\{i_2 j_2\} + S_2) + rs \text{ in } (\{i_3 j_3\} + S_3) \\ &\qquad + r \text{ in } (\mathrm{Pos}(\zeta) + \mathrm{Pos}(\rho)) + s \text{ in } (\mathrm{Pos}(\eta) + \mathrm{Pos}(\rho)) + t \text{ in } (\mathrm{Pos}(\zeta) + \mathrm{Pos}(\eta)) \\ &\quad \equiv 3 + rt \text{ in } \mathrm{Pos}(\lambda) + st \text{ in } \mathrm{Pos}(\mu) + rs \text{ in } \mathrm{Pos}(\nu) + 0 + 0 + 0 \\ &\quad \equiv 1 + r \text{ in } \mathrm{Pos}(\lambda) + \mathrm{Pos}(\nu) + t \text{ in } \mathrm{Pos}(\lambda) + \mathrm{Pos}(\mu) + s \text{ in } \mathrm{Pos}(\mu) + \mathrm{Pos}(\nu) \\ &\quad \equiv 1 + 0 + 0 + 0 \equiv 1 \pmod 2, \end{aligned}$$

which is exactly what we need to show that the left side of $(*)$ changes sign.

Since every member of $\mathscr{I}^*$ may be obtained from (ν, λ, μ) by a sequence of sign changes, two coordinates at a time, it follows that $\mathscr{I} = \mathscr{I}^*$. Thus σ preserves the product in this case.

Now we turn to the situation $v(\lambda) v(\mu) = 0$, $\lambda, \mu \in \Lambda_2^2$. We must prove that $v(\lambda)^\sigma v(\mu)^\sigma = 0$. If $v(\lambda)^\sigma v(\mu)^\sigma \neq 0$, we must have $v(\zeta) v(\eta) \neq 0$ for some $\zeta, \eta \in \Lambda_2$ with $x_\zeta = x_\lambda$ and $x_\eta = x_\mu$. Thus, $\mathcal{O}_\lambda = \mathcal{O}_\mu$ or $\mathcal{O}_\lambda + \mathcal{O}_\mu$ is an octad. In either case, we have

$$\begin{aligned} &v(\lambda)^\sigma v(\mu)^\sigma \\ &\quad = c\Big\{ \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta \rangle} \varphi_\zeta(x_{\lambda'}) v(\zeta) \Big\} \Big\{ \sum_{x_\eta = x_\mu} (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \eta \rangle} \varphi_\eta(x_{\mu'}) v(\eta) \Big\} \\ &\quad = c \sum_{\tilde{\rho} \in \tilde{\Lambda}_2} \Big\{ \sum_{\substack{x_\zeta = x_\lambda, x_\eta = x_\mu \\ \zeta + \eta = \rho}} (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta \rangle + \frac{1}{2}\langle \lambda_{kl'}, \eta \rangle} \varphi_\zeta(x_{\lambda'}) \varphi_\eta(x_{\mu'}) \beta(\zeta, \eta) \Big\} v(\rho), \end{aligned}$$

for some constant c and F-triples $\{\lambda, \lambda', \lambda''\}$ and $\{\mu, \mu', \mu''\}$ with $i = i(\lambda')$, $j = i(\lambda'')$. $k = i(\mu')$, $l = i(\mu'')$.

Subcase 1. $\mathcal{O}_\lambda = \mathcal{O}_\mu$. Then each $\beta(\zeta, \eta) = -36$ since $\rho \in \Lambda_2^4$; see Lemma 9.3. Fix $\rho = \lambda_{rs}$ or $\lambda_{rs'}$. When $x_\zeta = x_\lambda$ and there is an $\eta \in \Lambda_2$ with $x_\eta = x_\mu = x_\lambda$ such that $\zeta + \eta = \rho$, set

$$f(\zeta) = f_\rho(\zeta) = (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta \rangle + \frac{1}{2}\langle \lambda_{kl'}, \eta \rangle} \varphi_\zeta(x_{\lambda'}) \varphi_\eta(x_{\mu'}),$$

for $\eta \in \Lambda_2$ with $x_\eta = x_\mu$, $\zeta + \eta = \rho$. We must show that $\sum_{\zeta} f(\zeta) = 0$, where there are 32 summands, corresponding to those $\tilde{\zeta}$ whose coefficients over $\{r, s\}$ look like $\pm\frac{1}{2}\rho$. Since $x_\rho = 1$, $x_\lambda = x_\mu$. By taking $g = g_S \in O_2(H)$ with $\tilde{\lambda}^g = \tilde{\mu}$, we see that we may assume $\{\tilde{\lambda}, \tilde{\lambda}', \tilde{\lambda}''\}^g = \{\tilde{\mu}, \tilde{\mu}', \tilde{\mu}''\}$. Thus, $x_{\lambda'} = x_{\mu'} x_S$ and

$$\begin{aligned} f(\zeta) &= (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta+\eta \rangle} \varphi_\zeta(x_{\lambda'}) \varphi_\eta(x_{\mu'}) \\ &= (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \rho \rangle} \varphi_\rho(x_{\mu'}) \varphi_\zeta(x_S) = c_1 \varphi_\zeta(x_S), \end{aligned}$$

c_1 a constant. So, we must show that $\sum_{\tilde{\zeta}} \varphi_\zeta(x_S) = 0$. Let us fix one of these $\tilde{\zeta}$'s; call it $\tilde{\zeta}_0$. The other $\tilde{\zeta}$ which occur are obtained by changing coordinates at $A \in P^*(\mathcal{O}) = P(\mathcal{O})_{\text{even}}/\langle \mathcal{O} \rangle$, $A = \{A_1, A_1 + \Omega\}$, $A_1 \cap \{r, s\} = \emptyset$. The relevant A which arise range over a subspace, Y, of $P^*(\mathcal{O})$; with respect to the natural bilinear form on $P^*(\mathcal{O})$, Y is the annihilator of $\{r, s\} + \langle \mathcal{O} \rangle$. Thus, $\sum_{\tilde{\zeta}} \varphi_\zeta(x_S) = \varphi_{\zeta_0}(x_S) \sum_{A \in Y} \psi(A)$, where ψ is the character of Y obtained by pairing with $S \cap \mathcal{O}$ under the natural bilinear form. Since $|S| = 4$, $S \neq \{r, s\}$ or $\{r, s\} + \mathcal{O}$ and $\psi \neq 1$ so that $\sum_{A \in Y} \psi(A) = 0$ by the orthogonality relations, and we are done.

Subcase 2. $\mathcal{O}_\rho := \mathcal{O}_\lambda + \mathcal{O}_\mu$ is an octad. Fix ρ. Let

$$f(\zeta) = (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta \rangle + \frac{1}{2}\langle \lambda_{kl'}, \eta \rangle} \varphi_\zeta(x_{\lambda'}) \varphi_\eta(x_{\mu'}) \beta(\zeta, \eta),$$

for each $\tilde{\zeta}$ such that $x_\zeta = x_\lambda$ and there is $\eta \in \Lambda_2$ with $x_\eta = x_\mu$ and $\zeta + \eta = \rho$. We must show that $\sum_{\tilde{\zeta}} f(\zeta) = 0$. Note that there are eight summands. Let $Z(\rho)$ denote the set of $\tilde{\zeta}$ which occur.

Using the action of H, we may assume that one of the triangles of type 222 which occurs in the expression for $v(\lambda)^\sigma v(\mu)^\sigma$ is in $F^{q^{-1}}$. Let us call it $\{\zeta_0, \eta_0, \rho_0\}$, and let $\{\zeta_0, \zeta_0', \zeta_0''\}$, $\{\eta_0, \eta_0', \eta_0''\}$ and $\{\rho_0, \rho_0', \rho_0''\}$ be F-triples, with all vectors in $F^{q^{-1}}$. Let $r_1 = i(\zeta_0')$, $s_1 = i(\zeta_0'')$, $r_2 = i(\eta_0')$, $s_2 = i(\eta_0'')$, $m = i(\rho_0')$, $n = i(\rho_0'')$. Without loss, we may arrange $i = r_1$, $j = s_1$, $k = r_2$, $l = s_2$ and $\zeta_0 + \eta_0 = \rho_0$.

We have $\beta(\zeta, \eta) = \beta(\zeta_0, \eta_0)(-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|} = -36(-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|}$ where $g = g_{\zeta,\eta} \in O_2(H)$ satisfies $\tilde{\zeta}_0^g = \tilde{\zeta}$ and $\tilde{\eta}_0^g = \tilde{\eta}$. Then

$$\begin{aligned} f(\zeta) = (-1)^{\frac{1}{2}\langle \lambda_{ij'}, \zeta \rangle + \frac{1}{2}\langle \lambda_{kl'}, \eta \rangle + \frac{1}{2}\langle \lambda_{mn'}, \rho \rangle} & \varphi_\zeta(x_{\lambda'}) \varphi_\eta(x_{\mu'}) \\ \cdot \varphi_\rho(x_{\rho_0'}) (-1)^{|\mathcal{O}_\lambda \cap \mathcal{O}_\mu \cap S_g|} c_1, & \end{aligned}$$

where c_1 is constant as a function of ρ. Using the identity $(*)$, there are constants c_2 and c_3 so that

$$f(\zeta) = \varphi_\zeta(x_{\lambda'} x_{\zeta_0'}) \varphi_\eta(x_{\mu'} x_{\eta_0'}) c_2 = \varphi_\zeta(x_{\lambda'} x_{\mu'} x_{\zeta_0'} x_{\eta_0'}) c_3.$$

We claim that $f(\zeta)$ is not constant. It suffices to show that $f_1(\zeta)$ is not constant, where there exists some element ξ of $\Lambda(4)$ such that $f_1(\zeta) = f(\zeta)\varphi_\zeta(\xi)$. We take $f_1(\zeta) = \varphi_\zeta(\lambda' + \mu')\varphi_\zeta(\zeta' + \eta_0')$. Since $\zeta_0 + \eta_0 = \rho_0$, $\operatorname{Pos}(\zeta_0) + \operatorname{Pos}(\eta_0) \supseteq \mathcal{O}_\lambda \cap \mathcal{O}_\mu$. Since $\lambda + \mu$ and $\lambda - \mu$ are not in Λ_2, $\operatorname{Pos}(\lambda)$

$+\operatorname{Pos}(\mu)\cap\mathcal{C}_\lambda\cap\mathcal{C}_\mu \neq \emptyset$ or $\mathcal{C}_\lambda\cap\mathcal{C}_\mu$. Therefore, $\xi=\lambda'+\zeta_0'+\mu'+\eta_0'$ looks like $(\underbrace{2\dots2}_{k}\ \underbrace{0\dots0}_{4-k})$ (mod 4) over $\mathcal{C}_\lambda\cap\mathcal{C}_\mu$, where $0<k<4$. It follows that if $a, b\in\mathcal{C}_\lambda\cap\mathcal{C}_\mu$ and the coordinate of ξ at a, b is in $2+4\mathbb{Z}$, $4\mathbb{Z}$, respectively, then by changing the signs of the coordinates of ζ at $\{a, b\}$, we change the value of $f_1(\zeta)$. This proves our claim that f is not constant.

Take $\zeta_1\in Z(\rho)$ with $f(\zeta_1)=c_3$. Then $\sum f(\zeta)=c_3\sum\varphi_{\zeta-\zeta_1}(y)$, $y=x_{\lambda'}x_{\mu'}x_{\zeta_0'}x_{\eta_0'}$. The latter sum is $\sum\limits_{A\in P(\mathcal{C}_\lambda\cap\mathcal{C}_\mu)_{\text{even}}}\psi(A)$, where ζ and A correspond if and only if A is the support of $\zeta-\zeta_1$ (replacing ζ by $-\zeta$ if necessary). Then ψ is a character of $P(\mathcal{C}_\lambda\cap\mathcal{C}_\mu)_{\text{even}}$. Since f is not constant, $\psi\neq 1$. By orthogonality, the sum is zero.

This completes the arguments for Case 27.

Case 28. (B_2^2, B_2^3). When a nonzero product $v(\lambda)v(\mu)$ occurs here, it has the form $\beta(\lambda,\mu)v(\lambda+\mu)$, $\{\lambda,\mu,\lambda+\mu\}\in\Delta(2,3)$ and $\lambda+\mu\in\Lambda_2^3$. This situation is equivalent to one in Case 31, and we deal with it there.

When we have a zero product $v(\lambda)v(\mu)=0$, $\lambda\in\Lambda_2^2$, $\mu\in\Lambda_2^3$, we must show that $v(\lambda)^\sigma v(\mu)^\sigma=0$. It is clear from the definition of σ that

$$v(\lambda)^\sigma v(\mu)^\sigma\in\sum_{j\in\Omega}\mathbb{Q}\,e(x_{\lambda+\mu})\otimes x_j,$$

so, it suffices to prove that $(v(\lambda)^\sigma v(\mu)^\sigma,\ e(x_{\lambda+\mu})\otimes x_j)=0$, for $j\in\Omega$. Let $\mu=\lambda_{i,S}$. Take $j\in\Omega$. We compute

$$\begin{aligned}(v(\lambda)^\sigma v(\mu)^\sigma, e(x_{\lambda+\mu})\otimes x_j)&=(v(\lambda)^\sigma, v(\mu)^\sigma e(x_{\lambda+\mu})\otimes x_j)\\&=(-1)^{\infty i\text{ in }S}(v(\lambda)^\sigma,(e(x_\mu)\otimes x_i)(e(x_{\lambda+\mu})\otimes x_j))\\&=(-1)^{\infty i\text{ in }S}\beta(\lambda',\lambda'')^{-1}\delta(\lambda',\lambda'')(\tfrac{9}{2})\sum_{x_\zeta=x_\lambda}(-1)^{\frac12\langle\lambda_{kl'},\zeta\rangle}\\&\quad\cdot\varphi_\zeta(x_{\lambda'})[-3\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}),u(\zeta^2))]\varphi_\zeta(x_\mu)\\&=c^*\sum_{A\in P^*(\mathcal{C})}\chi(A),\end{aligned}$$

where c^* is a constant, $\{\lambda,\lambda',\lambda''\}$ is an F-triple, $\mathcal{C}=\mathcal{C}_\lambda$, $P^*(\mathcal{C}):=P(\mathcal{C})_{\text{even}}/\langle\mathcal{C}\rangle$ and χ is the irreducible character of the abelian group $P^*(\mathcal{C})$ defined as follows: set

$$\psi(\zeta):=(-1)^{\frac12\langle\lambda_{kl'},\zeta\rangle}\varphi_\zeta(x_{\lambda'})\varphi_\zeta(x_\mu)\qquad\text{if } i=j$$

and

$$\psi(\zeta):=(-1)^{\frac12\langle\lambda_{kl'},\lambda_{ij'},\zeta\rangle}\varphi_\zeta(x_{\lambda'})\varphi_\zeta(x_\mu)\qquad\text{if } i\neq j;$$

we shall find a $\zeta_0\in\Lambda_2^2$ with support $\mathcal{C}$ satisfying $\psi(\zeta_0)=1$; we then set $\chi(A):=\psi(\zeta)=\psi(\zeta)\psi(\zeta_0)=\psi(\zeta-\zeta_0)$, where ζ is obtained from ζ_0 by coordinate sign changes at A (more precisely, at $A_1\in P(\mathcal{C})_{\text{even}}$, where $A=\{A_1, A_1+\mathcal{C}\}$). Without loss, $q(\{\lambda,\lambda',\lambda''\})\subset F$. We let $\lambda^*:=\frac12\lambda_{kl'}+\lambda'+\lambda_{x_\mu}$ if $i=j$ and $\lambda^*:=\frac12(\lambda_{kl'}+\lambda_{ij'})+\lambda'+\lambda_{x_\mu}$ if $i\neq j$. Then $\psi(\zeta)=(-1)^{\langle\lambda^*,\zeta\rangle}$. Let ζ_A be obtained from ζ_0 by coordinate sign changes at A, $A\in P^*(\mathcal{C})$. Then, for any $A, B\in P^*(\mathcal{C})$,

$$\begin{aligned}\chi(A+B)=\psi(\zeta_{A+B})&=(-1)^{\langle\lambda^*,\zeta_{A+B}\rangle}=(-1)^{\langle\lambda^*,\zeta_{A+B}-\zeta_0\rangle}\\&=(-1)^{\langle\lambda^*,\zeta_A-\zeta_0+\zeta_B-\zeta_0+\zeta^*\rangle}\end{aligned}$$

where ζ^* is a vector with nonzero coordinates ± 8. Since λ^* has coordinates in $2\mathbb{Z}$, $(-1)^{\langle\lambda^*,\zeta^*\rangle}=1$ and so $\chi(A+B)=\chi(A)\chi(B)$, i.e. χ is a character of $P^*(\mathcal{O})$. Finally, we shall show $\chi\neq 1$. The orthogonality relations for irreducible characters of finite groups then imply $\sum\limits_{A\in P^*(\mathcal{O})}\chi(A)=0$, as required.

To summarize, we must (i) exhibit ζ_0 with $\psi(\zeta_0)=1$ and (ii) prove $\chi\neq 1$ (equivalently, find ζ_1 with $\psi(\zeta_1)=-1$). So, what we really have to do is to show that ψ is not constant as a function of $\{\tilde{\zeta}\in\tilde{\Lambda}_2 \mid x_{\tilde{\zeta}}=x_\lambda\}$. Without loss, the bracketed term is not identically zero, whence, by (8.4) either (a) $i=j\notin\mathcal{O}$ or (b) $i\neq j$, $i,j\in\mathcal{O}$.

We shall assume $\psi(\zeta)$ is constant, then seek a contradiction. Since $\psi(\zeta)$ has the form $(-1)^{\langle\lambda^*,\zeta\rangle}$, we may replace λ^* by anything in the coset $\lambda^*+\Lambda(4)$ since, for $\xi\in\Lambda(4)$, $(-1)^{\langle\xi,\zeta\rangle}$ is constant in ζ. In particular, we may replace λ_{x_μ} by μ.

Recall that, if $\xi\in\Lambda_2$, $\xi+\lambda\in\Lambda_2$ if and only if $\langle\xi,\lambda\rangle=-2$. Since $\lambda\pm\mu\notin\Lambda_2$, this means $\langle\lambda'\pm\mu,\lambda\rangle\neq 0$.

Suppose $i=j$. Since $\lambda\pm\mu$ are not in Λ_2, the part of the vector μ over $\mathcal{O}$ looks like $(\pm 1,\pm 1,\ldots,\pm 1)$ but does not have the shape

$$\pm(\underbrace{1,\ldots,1,}_{\mathrm{Pos}(\lambda)}\ \underbrace{-1,\ldots,-1}_{\mathrm{Neg}(\lambda)}).$$

By Lemma 2.3(ii), the part of λ' over $\mathcal{O}$ is

$$\pm(\underset{k}{-3},\ \underset{l}{1},\ \underbrace{1,\ldots,1,}_{\mathrm{Pos}(\lambda)}\ -1,\ldots,-1)\quad\text{or}\quad\pm(\underset{k}{-3}\ \underbrace{1\ldots 1}_{\mathrm{Pos}(\lambda)}\ \underset{l}{-1}\ -1\ldots-1).$$

Thus the part of $\lambda'+\mu$ over $\mathcal{O}$ may be assumed to have shape $(\pm 2, 2, a_1,\ldots,a_6)$, with $a_i\in\{0,\pm 2\}$ all i, and not all the a_i are zero. So, $\lambda^*\equiv(0,0,a_1,\ldots,a_6)\pmod 4$ over $\mathcal{O}$, and it is easy to see that ψ is not constant.

Suppose $i\neq j$. Then $i,j\in\mathcal{O}$. Proceeding as in the last paragraph, the part of μ over $\mathcal{O}$ does not have shape

$$\pm(\underset{i}{-3},\ \underset{j}{1},\ \underbrace{1,\ldots,1,}_{\mathrm{Pos}(\lambda)}\ -1,\ldots,-1)\quad\text{or}\quad\pm(\underset{i}{-3},\ \underbrace{1,\ldots,1,}_{\mathrm{Pos}(\lambda)}\ \underset{j}{-1},\ -1,\ldots,-1)$$

whereas the part of λ' over $\mathcal{O}$ has shape

$$\pm(\underset{k}{-3}\ \underset{l}{1}\ \underbrace{1\ldots 1}_{\mathrm{Pos}(\lambda)}\ -1\ldots-1)\quad\text{or}\quad\pm(\underset{\mathrm{k}}{-3}\ \underbrace{1\ldots 1}_{\mathrm{Pos}(\lambda)}\ \underset{l}{-1}\ -1\ldots-1).$$

We consider the subcases. Since $\lambda'+\lambda''\equiv\lambda\ (\mathrm{mod}\ 2\Lambda)$ and $\langle\lambda,\zeta\rangle\in 2\mathbb{Z}$ for $\zeta\in\Lambda_2^2$ with support $\mathcal{O}$, we may switch k and l without loss in the following arguments.

Subcase 1. $i\in\{k,l\}$, $j\in\{k\,l\}$. Then we may replace λ^* with $\lambda'+\mu$. Without loss, $i=k$, the k-entry of $\lambda'+\mu$ is 0, all the other coordinates over $\mathcal{O}$ are 0 or ± 2 and they are not all zeroes. It is trivial to see that ψ is not constant here.

Subcase 2. $\{i,j\}\cap\{k,l\}=\{i\}=\{k\}$. We may cancel out the -3's. Without loss, λ^* may be replaced by $\lambda'+\mu+\frac{1}{2}\lambda_{jl'}$. Since ψ is assumed constant, the part of λ^* over $\mathcal{O}$ looks like $(0\ldots 0)\pmod 4$. So, over $\mathcal{O}$,

$$\lambda+\mu\equiv\pm(0\ldots 0\ \underset{j}{2}\ 0\ldots 0\ \underset{l}{2}\ 0\ldots 0)\pmod 4.$$

Assume jl in $\mathrm{Pos}(\lambda)\equiv 1 \pmod 2$. We derive a contradiction. Suppose λ' has the first of the two possible shapes. Then jl in $\mathrm{Pos}(\lambda)\equiv 1 \pmod 2$ forces j to be in the interval marked $\mathrm{Pos}(\lambda)$. We obtain $\tilde{\mu}$ from $\tilde{\lambda}'$ by changing coordinate signs at a $\mathscr{C}$-set, say U. Since

$$\lambda'+\mu\equiv(0\ldots0\ \underset{j}{2}\ 0\ldots0\ \underset{l}{2}\ 0\ldots0) \pmod 4$$

over $\mathcal{O}$, we may assume $U\cap\mathcal{O}=\{j,l\}$. Then $\lambda'-(\lambda')^{\varepsilon_U}$ over $\mathcal{O}$ looks like

$$\pm(0\ \underset{j}{2}\ 0\ldots0\ \underset{l}{2}\ 0\ldots\ \ldots0)$$

a contradiction, as $\langle\lambda'+\mu,\lambda\rangle\neq 0$. If λ' has the second of the two possible shapes, the discussion is similar. We conclude that $\langle\lambda^{*},\zeta\rangle$ is not constant $\pmod 2$, as required. Assume jl in $\mathrm{Pos}(\lambda)\equiv 0 \pmod 2$. Whichever shape λ' has, a similar analysis shows that either possibility, $\{j,l\}\subseteq\mathrm{Pos}(\lambda)$ or $\{j,l\}\subseteq\mathrm{Neg}(\lambda)$, forces $\langle\lambda-\mu,\lambda\rangle=0$ or $\langle\lambda+\mu,\lambda\rangle=0$, a contradiction.

Subcase 3. $i\notin\{k,l\}$, $j\notin\{k,l\}$. As in Subcase 2, we have no problem unless

$$\lambda'+\mu\equiv(0\ldots0\ \underset{i}{2}\ 0\ldots0\ \underset{j}{2}\ 0\ldots0\ \underset{k}{2}\ 0\ldots0\ \underset{l}{2}\ 0\ldots0) \pmod 4.$$

We examine the possibilities to get a contradiction.

Suppose λ' has shape $\pm(\underset{k}{-3}\ \underset{l}{1}\ \underbrace{1\ldots1}_{\mathrm{Pos}(\lambda)}\ -1\ldots-1)$ over $\mathcal{O}$. If ij in $\mathrm{Pos}(\lambda)=1$, then we may arrange to have one of the following pictures:

$$\begin{array}{rl}
\lambda'=(\underset{k}{-3}\ \underset{l}{1}\ \overbrace{\underset{i}{1}\ \ldots\ 1}^{\mathrm{Pos}(\lambda)}\ \underset{j}{-1}\ \ldots\ -1) & \text{over } \mathcal{O},\\
\mu=(\ 1\ 1\ -3\ -1\ \ldots\ -1\ -1\ 1\ \ldots\ 1) & \text{over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ 2\ -2\ 0\ \ldots\ 0\ -2\ 0\ \ldots\ 0) & \text{over } \mathcal{O};\quad\text{or}
\end{array}$$

$$\begin{array}{rl}
\lambda'=(\underset{k}{-3}\ \underset{l}{1}\ \overbrace{\underset{j}{1}\ -1\ \ldots\ 1}^{\mathrm{Pos}(\lambda)}\ \underset{i}{-1}\ \ldots\ -1) & \text{over } \mathcal{O},\\
\mu=(\ 1\ 1\ 1\ -1\ \ldots\ -1\ 3\ 1\ \ldots\ 1) & \text{over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ 2\ 2\ 0\ \ldots\ 0\ 2\ 0\ \ldots\ 0) & \text{over } \mathcal{O}.
\end{array}$$

In both cases, $\langle\lambda'+\mu,\lambda\rangle=0$, a contradiction. If ij in $\mathrm{Pos}(\lambda)=0$, we have one of

$$\begin{array}{rl}
\lambda'=(\underset{k}{-3}\ \underset{l}{1}\ \overbrace{\underset{i}{1}\ \underset{j}{1}\ -1\ \ldots\ 1}^{\mathrm{Pos}(\lambda)}\ -1\ \ldots\ -1) & \text{over } \mathcal{O},\\
\mu=(\ 1\ 1\ -3\ 1\ -1\ \ldots\ -1\ 1\ \ldots\ 1) & \text{over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ 2\ -2\ 2\ 0\ \ldots\ 0\ 0\ \ldots\ 0) & \text{over } \mathcal{O};\quad\text{or}
\end{array}$$

$$\begin{array}{rl}
\lambda'=(\underset{k}{-3}\ \underset{l}{1}\ \overbrace{1\ 1\ \ldots\ 1}^{\mathrm{Pos}(\lambda)}\ \underset{i}{-1}\ \underset{j}{-1}\ \ldots\ -1) & \text{over } \mathcal{O},\\
\mu=(\ 1\ 1\ -1\ -1\ \ldots\ -1\ 3\ -1\ 1\ \ldots\ 1) & \text{over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ 2\ 0\ \ldots\ 0\ 2\ -2\ 0\ \ldots\ 0) & \text{over } \mathcal{O}.
\end{array}$$

Again, $\langle\lambda'+\mu, \lambda\rangle=0$ in both cases, a contradiction.

Suppose λ' has the shape $(\underset{k}{-3}\ \overbrace{1\ \dots\ 1\ -1}^{\mathrm{Pos}(\lambda)}\ -1\ \dots\ -1)$. If ij in $\mathrm{Pos}(\lambda)\equiv 1 \pmod 2$, then we may arrange for one of the following pictures to hold:

$$\begin{array}{l}
\lambda'=(\underset{k}{-3}\ \ \overbrace{\underset{i}{1}\ \ 1\ \dots\ \ 1\ \ \underset{l}{-1}}^{\mathrm{Pos}(\lambda)}\ \ \underset{j}{-1}\ \ -1\ \dots\ -1) \text{ over } \mathcal{O},\\
\mu=(\ 1\ \ -3\ \ -1\ \dots\ -1\ \ -1\ \ -1\ \ +1\ \dots\ +1) \text{ over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ \ -2\ \ \ 0\ \dots\ \ 0\ \ -2\ \ -2\ \ \ 0\ \dots\ \ 0) \text{ over } \mathcal{O};\quad \text{or}
\end{array}$$

$$\begin{array}{l}
\lambda'=(\underset{k}{-3}\ \overbrace{\underset{j}{1}\ \ 1\ \dots\ \ 1\ \ \underset{l}{-1}}^{\mathrm{Pos}(\lambda)}\ \ \underset{i}{-1}\ \ -1\ \dots\ -1) \text{ over } \mathcal{O},\\
\mu=(\ 1\ \ 1\ \ -1\ \dots\ -1\ \ -1\ \ \ 3\ \ -1\ \dots\ -1) \text{ over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ \ 2\ \ \ 0\ \dots\ \ 0\ \ -2\ \ \ 2\ \ \ 0\ \dots\ \ 0) \text{ over } \mathcal{O}.
\end{array}$$

In both cases, $\langle\lambda'+\mu, \lambda\rangle=0$, a contradiction.

Suppose that ij in $\mathrm{Pos}(\lambda)\equiv 0 \pmod 2$. Then one of the following pictures must hold:

$$\begin{array}{l}
\lambda'=(\underset{k}{-3}\ \ \overbrace{\underset{i}{1}\ \underset{j}{1}\ \ \dots\ \ 1\ \ \underset{l}{-1}}^{\mathrm{Pos}(\lambda)}\ \ -1\ \dots\ -1) \text{ over } \mathcal{O},\\
\mu=(\ 1\ \ -3\ \ 1\ \ -1\ \dots\ -1\ \ -1\ \ \ 1\ \dots\ \ 1) \text{ over } \mathcal{O},\\
\hline
\lambda'+\mu=(-2\ \ -2\ \ 2\ \ \ 0\ \dots\ \ 0\ \ -2\ \ \ 0\ \dots\ \ 0) \text{ over } \mathcal{O};\quad \text{or}
\end{array}$$

$$\begin{array}{l}
\lambda'=(\underset{k}{-3}\ \ \overbrace{1\ \ 1\ \dots\ \ 1\ \ -1}^{\mathrm{Pos}(\lambda)}\ \ \underset{i}{-1}\ \ \underset{j}{-1}\ \ \underset{l}{}\ \dots\ -1)\\
\mu=(\ 1\ \ -1\ \ -1\ \dots\ -1\ \ -1\ \ \ 3\ \ -1\ \ 1\ \dots\ \ 1)\\
\hline
\lambda'+\mu=(-2\ \ \ 0\ \ \ 0\ \dots\ \ 0\ \ -2\ \ \ 2\ \ -2\ \ 0\ \dots\ \ 0),
\end{array}$$

and in both cases, $\langle\lambda'+\mu, \lambda\rangle=0$, contradiction.

Subcase 4. $i\notin\{k, l\}$, $j\in\{k, l\}$. Say $j^*\in\{k, l\}-\{j\}$. Then, there is no problem unless possibly $\lambda'+\mu$ has shape

$$(0\ \dots\ 0\ \underset{i}{2}\ 0\ \dots\ 0\ \underset{j^*}{2}\ 0\ \dots\ 0) \pmod 4 \quad \text{over } \mathcal{O}.$$

In this event, we refer to Subcase 2.

We have completed the discussion of the zero product situation.

Case 29. $(B_2^2, B_{\mathrm{even}})$. We have

$$\begin{aligned}
v(\lambda)(e(x)\otimes x_i)&=\sum_{j\in\Omega}\left[-3\,\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}), u(\lambda^2))\right]\varphi_\lambda(x)\,e(x\,x_\lambda)\otimes x_j\\
\xmapsto{\sigma} a_1:&=\sum_{j\in\Omega}\left[-3\,\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}), u(\lambda^2))\right]\varphi_\lambda(x)(-1)^{\langle\lambda_\infty, \lambda_j, x x_\lambda\rangle}\,e(x\,x_\lambda)\otimes x_j.
\end{aligned}$$

Also,

$$a_2 := v(\lambda)^\sigma (e(x)\otimes x_i)^\sigma = \beta(\mu, v)^{-1}\,\delta(\mu, v)\,(\tfrac{9}{2})\,(-1)^{\langle\lambda_\infty, \lambda_{\iota,x}\rangle}.$$

$$\sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle}\,\varphi_\zeta(x_\mu)\,v(\zeta)\,(e(x)\otimes x_i) = \beta(\mu, v)^{-1}\,\delta(\mu, v)\,(\tfrac{9}{2})\,-1)^{\langle\lambda_\infty, \lambda_{\iota,x}\rangle}.$$

$$\sum_{j\in\Omega}\sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle}\,\varphi_\zeta(x_\mu x)\,[-3\delta_{ij} + \tfrac{9}{32}(u_0(u_{ij}), u(\zeta^2))]\,e(x x_\lambda)\otimes x_j,$$

where $\{\lambda, \mu, v\}$ is an F-triple with $\mu=\lambda_{k,S}$, $v=\lambda_{l,T}$ for indices k and l in $\mathcal{O}=\mathcal{O}_\lambda$ and $S, T\in\mathscr{C}$, $k\notin S$, $l\notin T$.

Let $a_{1,j}$, $a_{2,j}$ be the coefficient of $e(xx_\lambda)\otimes x_j$ in a_1, a_2, respectively.

Without loss, we may assume that $q(\{\lambda, \mu, v\})\subset F$.

For $j=i$ we have

$$\tfrac{9}{32}(u_0(u_{ii}), u(\zeta^2)) = \tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii} - \sum_{r\neq i} u_{rr}, 4\sum_{r\in\mathcal{O}} u_{rr})$$

$$= \tfrac{3}{16}\begin{cases} 16 & \text{if } i\in\mathcal{O} \\ -8 & \text{if } i\notin\mathcal{O} \end{cases} = \begin{cases} 3 & \text{if } i\in\mathcal{O} \\ -3/2 & \text{if } i\notin\mathcal{O} \end{cases}$$

Thus,

$$a_{1,i} = \begin{cases} 0 & \text{if } i\in\mathcal{O} \\ -\frac{9}{2}\varphi_\lambda(x)\,(-1)^{\langle\lambda_\infty, \lambda_{\iota,xx_\lambda}\rangle} & \text{if } i\notin\mathcal{O} \end{cases}$$

and

$$a_{2,i} = \begin{cases} 0 & \text{if } i\in\mathcal{O} \\ -\frac{81}{4}\beta(\mu, v)^{-1}\,\delta(\mu, v)\,(-1)^{\langle\lambda_\infty, \lambda_{\iota,x}\rangle}\displaystyle\sum_{x_\zeta = x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle}\,\varphi_\zeta(x_\mu x) & \text{if } i\notin\mathcal{O}. \end{cases}$$

Without loss, $i\notin\mathcal{O}$. Thus $a_{1,i}=a_{2,i}$ if and only if

$$(-1)^{\langle\lambda_\infty, \lambda_{\iota,x} - \lambda_{\iota,xx_\lambda}\rangle}\,\delta(\mu, v)\,\varphi_\lambda(x) = \tfrac{9}{2}\beta(\mu, v)^{-1}\sum_{x_\zeta = x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{k,l'}, \zeta\rangle}\,\varphi_\zeta(x_\mu x).$$

Since $q(\{\lambda, \mu, v\})\subset F$, $\varphi_\lambda(x_\mu)=1$, $\beta(\mu, v)=-36$, and the condition reads

$$(*)\qquad (-1)^{\langle\lambda_\infty, \lambda_{\iota,x} - \lambda_{\iota,xx_\lambda}\rangle}\,\delta(\mu, v) = -\tfrac{1}{8}\sum_{x_\zeta = x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle}\,\varphi_{\zeta+\lambda}(x_\mu x).$$

We have $\lambda - \lambda_\mathcal{O} \equiv (\underbrace{4, \ldots, 4,}_{\{k, l\}+(S\cap\mathcal{O})}\ 0, \ldots, 0) \pmod{2\Lambda}$, whence

$$\varphi_{\lambda+\lambda_\mathcal{O}}(x) = (-1)^{|S_x\cap(\{k, l\}+(S\cap\mathcal{O}))|} = (-1)^{kl \text{ in } S_x + |S_x\cap S\cap\mathcal{O}|}$$

(see Lemma 2.3). Also,

$$\varphi_{\lambda+\lambda_\mathcal{O}}(x_\mu) = \varphi_{\lambda_\mathcal{O}}(x_\mu) = (-1)^{\langle\lambda_\mathcal{O}, \lambda_{k,S}\rangle} = (-1)^{\langle\lambda_\mathcal{O}, \lambda_k\rangle + \langle\lambda_\mathcal{O}, \lambda_S\rangle} = (-1)^{1+\frac{1}{2}|S\cap\mathcal{O}|},$$

using $k\in\mathcal{O}$. Therefore, the right side of $(*)$ equals

$$\{-\tfrac{1}{8}\sum_{x_\zeta = x_\lambda}(-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle}\,\varphi_{\zeta+\lambda_\mathcal{O}}(x_\mu x)\}\cdot(-1)^{kl \text{ in } S_x + |S_x\cap S\cap\mathcal{O}| + 1 + \frac{1}{2}|S\cap\mathcal{O}|}$$

$$= (-1)^{1+\frac{1}{2}|((S+S_x)\cap\mathcal{O}) + \{k, l\}| + kl \text{ in } S_x + |S_x\cap S\cap\mathcal{O}| + 1 + \frac{1}{2}|S\cap\mathcal{O}|}.$$

We have

$$\begin{aligned}
&\langle\lambda_\infty, \lambda_{i,x}\rangle - \langle\lambda_\infty, \lambda_{i,xx_\lambda}\rangle\\
&\quad\equiv\langle\lambda_\infty, \lambda_{\infty,x}\rangle + \langle\lambda_\infty, \lambda_{\infty,xx_\lambda}\rangle + \infty i \text{ in } S_x + \infty i \text{ in } (S_x + \mathcal{O})\\
&\quad\equiv\langle\lambda_\infty, \lambda_{\infty,x}\rangle + \langle\lambda_\infty, \lambda_{\infty,xx_\lambda}\rangle + \infty i \text{ in } \mathcal{O} \equiv \tfrac{1}{4}|S_x| + \tfrac{1}{4}|S_x + \mathcal{O}| + \infty i \text{ in } \mathcal{O}\\
&\quad\equiv\tfrac{1}{2}|S_x - \mathcal{O}| + \infty i \text{ in } \mathcal{O} \equiv \tfrac{1}{2}|S_x \cap \mathcal{O}|S_x \cap \mathcal{O}| + \infty i \text{ in } \mathcal{O} (\text{mod } 2);
\end{aligned}$$

see Lemma 2.2. So, the left side of $(*)$ is $(-1)^{E_1}$, where $E_1 \equiv \frac{1}{2}|S_x \cap \mathcal{O}| + \infty i$ in $\mathcal{O}$ $+ \infty k$ in $S + \infty l$ in $T (\text{mod } 2)$. Since $i \notin \mathcal{O}$, $k \notin S$ and $l \notin T$, Lemma 2.3(ii) implies that ∞i in $\mathcal{O} + \infty k$ in $S + \infty l$ in $T \equiv \infty$ in $\mathcal{O} + S + T \equiv 1 + kl$ in S (mod 2). Therefore, $E_1 \equiv \frac{1}{2}|S_x \cap \mathcal{O}| + kl$ in $S + 1$ (mod 2).

Let $(-1)^{E_2}$ be the right side of $(*)$. Then,

$$\begin{aligned}
E_2 &\equiv \tfrac{1}{2}|((S + S_x) \cap \mathcal{O}) + \{k, l\}| + kl \text{ in } S_x + |S_x \cap S \cap \mathcal{O}| + \tfrac{1}{2}|S \cap \mathcal{O}|\\
&\equiv \tfrac{1}{2}|(S + S_x) \cap \mathcal{O}| + \tfrac{1}{2}|\{k, l\}| + |(S + S_x) \cap \{k, l\}| + kl \text{ in } S_x + |S_x \cap S \cap \mathcal{O}| + \tfrac{1}{2}|S \cap \mathcal{O}|\\
&\equiv \tfrac{1}{2}|S \cap \mathcal{O}| + \tfrac{1}{2}|S_x \cap \mathcal{O}| + |S \cap S_x \cap \mathcal{O}| + 1 + kl \text{ in } S + kl \text{ in } S_x\\
&\qquad + kl \text{ in } S_x + |S_x \cap S \cap \mathcal{O}| + \tfrac{1}{2}|S \cap \mathcal{O}|\\
&\equiv \tfrac{1}{2}|S_x \cap \mathcal{O}| + kl \text{ in } S + 1 \equiv E_1 (\text{mod } 2).
\end{aligned}$$

We conclude that $(*)$ holds, proving $a_{1,i} = a_{2,i}$.

Next, let $j \neq i$. Then $a_{1,j} = a_{2,j} = 0$ unless $i, j \in \mathcal{O}$ in which case

$$\tfrac{9}{32}(u_{ij}, u(\zeta^2)) = \tfrac{9}{2}(-1)^{\frac{1}{2}\langle\lambda_{ij'}, \zeta\rangle}, \qquad a_{1,j} = \tfrac{9}{2}(-1)^{\frac{1}{2}\langle\lambda_{ij'}, \lambda\rangle + \langle\lambda_\infty, \lambda_{j,xx_\lambda}\rangle}\varphi_\lambda(x)$$

and

$$a_{2,j} = \beta(\mu, \nu)^{-1}\,\delta(\mu, \nu)\,(\tfrac{9}{2})\,(-1)^{\langle\lambda_\infty, \lambda_{i,x}\rangle} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle + \frac{1}{2}\langle\lambda_{ij'}, \zeta\rangle}\varphi_\zeta(x_\mu x).$$

We assume $i, j \in \mathcal{O}$. Since $q(\{\lambda, \mu, \nu\}) \subset F$, $\varphi_\lambda(x) = 1$ and $\beta(\mu, \nu) = -36$. Writing $a_{r,j} = (-1)^{E_r}$, $r = 1, 2$, the condition we must verify is $E_1 \equiv E_2 (\text{mod } 2)$, or

$$(**)\quad \tfrac{1}{2}\langle\lambda_{ij'}, \lambda\rangle + \langle\lambda_\infty, \lambda_{j,xx_\lambda}\rangle \equiv 1 + \infty k \text{ in } S + \infty l \text{ in } T + \langle\lambda_\infty, \lambda_{i,x}\rangle + E_3 (\text{mod } 2),$$

where

$$(-1)^{E_3} = \tfrac{1}{8} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle + \frac{1}{2}\langle\lambda_{ij'}, \zeta\rangle}\varphi_\zeta(x_\mu x).$$

Now, $\varphi_{\lambda + \lambda_\mathcal{O}}(x_\mu x) = (-1)^{E_4}$, where $E_4 \equiv \frac{1}{2}|S \cap \mathcal{O}| + 1 + |S_x \cap (k, l\} + S \cap \mathcal{O})| (\text{mod } 2)$; see the lines following $(*)$. It follows that $(-1)^{E_3} = (-1)^{E_4 + E_5}$, where

$$(-1)^{E_5} = \tfrac{1}{8} \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle\lambda_{kl'}, \zeta\rangle + \frac{1}{2}\langle\lambda_{ij'}, \zeta\rangle}\varphi_{\zeta + \lambda_\mathcal{O}}(x_\mu x),$$

using $\varphi_\lambda(x_\mu x) = 0$. So, $(**)$ is equivalent to

$$\begin{aligned}
(***)\qquad 0 &\equiv \tfrac{1}{2}\langle\lambda_{ij'}, \lambda\rangle + \langle\lambda_\infty, \lambda_{j,xx_\lambda}\rangle + 1 + \infty k \text{ in } S + \infty l \text{ in } T\\
&\qquad + \langle\lambda_\infty, \lambda_{i,x}\rangle + E_4 + E_5 (\text{mod } 2).
\end{aligned}$$

We prove $(***)$ by analyzing subcases.

Subcase 1. $\{i, j\} = \{k, l\}$. Without loss, $k = i$ and $l = j$. Then $(***)$ becomes

$$\begin{aligned}0 &\equiv \tfrac{1}{2}\langle\lambda_{kl'},\lambda\rangle+\langle\lambda_{\infty,xx_\lambda}\rangle+\infty l \text{ in } (S_x+\mathcal{O})+1+\infty k \text{ in } S+\infty l \text{ in } T\\ &\quad+\langle\lambda_\infty,\lambda_{\infty,x}\rangle+\infty k \text{ in } S_x+E_4+E_5\\ &\equiv kl \text{ in } S+\tfrac{1}{4}|S_x+\mathcal{O}|+\tfrac{1}{4}|S_x|+kl \text{ in } S_x+\infty l \text{ in } \mathcal{O}+\infty k \text{ in } S+\infty l \text{ in } T\\ &\quad+1+E_4+E_5 (\operatorname{mod} 2),\end{aligned}$$

after applying Lemma 2.3(ii) to the first summand. We have $\frac{1}{4}|S_x+\mathcal{O}|+\frac{1}{4}|S_x|\equiv\frac{1}{2}|S_x\cap\mathcal{O}| (\operatorname{mod} 2)$, by Lemma 2.2, and we have ∞l in $\mathcal{O}+\infty k$ in $S+\infty l$ in $T\equiv 1+kl$ in $S+1+0+0=kl$ in S (mod 2), by Lemma 2.3(ii). So, the right side of (∗∗∗) becomes $\frac{1}{2}|S_x\cap\mathcal{O}|+kl$ in $S_x+1+E_4+E_5 (\operatorname{mod} 2)$. Since $i=k$ and $j=l$, Lemma 11.1(i) applies to give

$$E_5\equiv\tfrac{1}{2}|(S+S_x)\cap\mathcal{O}|\equiv\tfrac{1}{2}|S\cap\mathcal{O}|+\tfrac{1}{2}|S_x\cap\mathcal{O}|+|S\cap S_x\cap\mathcal{O}| (\operatorname{mod} 2).$$

Continuing, and substituting for E_4 and E_5, we see that the right side of (∗∗∗) equals

$$\begin{aligned}E_6 &:= kl \text{ in } S_x+|S_x\cap(\{kl\}+(S\cap\mathcal{O}))|+|S\cap S_x\cap\mathcal{O}|\\ &\equiv kl \text{ in } S_x+|S_x\cap(\{kl\}+(S\cap\mathcal{O})+(S\cap\mathcal{O}))|\equiv kl \text{ in } S_x\cap\{kl\}|\equiv 0 (\operatorname{mod} 2),\end{aligned}$$

as required.

Subcase 2. $|\{i,j\}\cap\{k,l\}|=1$. Suppose first that $j=k$ and $i\neq l$. Then $\frac{1}{2}\langle\lambda_{ij'},\zeta\rangle+\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle\equiv\frac{1}{2}\langle\lambda_{il'},\zeta\rangle (\operatorname{mod} 2)$, and $E_5\equiv\frac{1}{2}|((S+S_x)\cap\mathcal{O})+\{i,l\}| (\operatorname{mod} 2)$. Then (∗∗∗) becomes

$$\begin{aligned}0 &\equiv \tfrac{1}{2}\langle\lambda_{ik'},\lambda\rangle+\langle\lambda_\infty,\lambda_{\infty,xx_\lambda}\rangle+\infty k \text{ in } (S_x+\mathcal{O})+1+\infty k \text{ in } S+\infty l \text{ in } T\\ &\quad+\langle\lambda_\infty,\lambda_{\infty,x}\rangle+\infty i \text{ in } S_x+\tfrac{1}{2}|S\cap\mathcal{O}|+1+|S_x\cap(\{k,l\}+S\cap\mathcal{O})|\\ &\quad+\tfrac{1}{2}|((S+S_x)\cap\mathcal{O})+\{i,l\}|\equiv ik \text{ in } (S+\{k,l\})+\tfrac{1}{4}|S_x+\mathcal{O}|+ik \text{ in } S_x+\infty k \text{ in } \mathcal{O}\\ &\quad+1+\infty k \text{ in } S+\infty l \text{ in } T+\tfrac{1}{4}|S_x|+\tfrac{1}{2}|S\cap\mathcal{O}|+1+kl \text{ in } S_x\\ &\quad+|S_x\cap S\cap\mathcal{O}|+\tfrac{1}{2}|(S+S_x)\cap\mathcal{O}|+1+il \text{ in } (S+S_x)\equiv\infty l \text{ in } S\\ &\quad+\infty k \text{ in } \mathcal{O}+\infty l \text{ in } T\\ &\quad+4+\tfrac{1}{2}|S_x\cap\mathcal{O}|+\tfrac{1}{2}|S\cap\mathcal{O}|+|S_x\cap S\cap\mathcal{O}|+\tfrac{1}{2}|S\cap\mathcal{O}|\\ &\quad+\tfrac{1}{2}|S_x\cap\mathcal{O}|+|S\cap S_x\cap\mathcal{O}|\equiv kl \text{ in } \mathcal{O}+|S_x\cap S\cap\mathcal{O}|+|S_x\cap S\cap\mathcal{O}|\equiv 0 (\operatorname{mod} 2).\end{aligned}$$

Since (∗∗∗) is verified, we are done.

Suppose $i=k$ and $j\neq l$. Then

$$\begin{aligned}&\tfrac{1}{2}\langle\lambda_{ij'},\lambda\rangle+\langle\lambda_\infty,\lambda_{j,xx_\lambda}\rangle+1+\infty i \text{ in } S+\infty l \text{ in } T+\langle\lambda_\infty,\lambda_{i,x}\rangle\\ &\qquad+\tfrac{1}{2}|S\cap\mathcal{O}|+1+|S_x\cap(\{il\}+S\cap\mathcal{O}|+\tfrac{1}{2}((S+S_x)\cap\mathcal{O})+\{j,l\}|\\ &\quad\equiv ij \text{ in } (S+\{i,l\})+\infty j \text{ in } (\mathcal{O}+S_x)+\langle\lambda_\infty,\lambda_{\infty,xx_\lambda}\rangle\\ &\qquad+1+\infty i \text{ in } S+\infty l \text{ in } T+\infty i \text{ in } S_x+\langle\lambda_\infty,\lambda_{\infty,x}\rangle+\tfrac{1}{2}|S\cap\mathcal{O}|\\ &\qquad+1+il \text{ in } S_x+|S_x\cap S\cap\mathcal{O}|+\tfrac{1}{2}|(S+S_x)\cap\mathcal{O}|+1+jl \text{ in } (S+S_x)\\ &\quad\equiv 1+\infty j \text{ in } \mathcal{O}+\infty l \text{ in } S+\infty l \text{ in } T+\emptyset \text{ in } S_x+\tfrac{1}{4}|\mathcal{O}+S_x|+\tfrac{1}{4}|S_x|\\ &\qquad+\tfrac{1}{2}|S\cap\mathcal{O}|+|S_x\cap S\cap\mathcal{O}|+\tfrac{1}{2}|S\cap\mathcal{O}+S_x\cap\mathcal{O}|+1\\ &\quad\equiv\infty j \text{ in } \mathcal{O}+\infty l \text{ in } \mathcal{O}+\tfrac{1}{4}|\mathcal{O}|+\tfrac{1}{2}|S\cap S_x|+\tfrac{1}{2}|S\cap\mathcal{O}|+|S_x\cap S\cap\mathcal{O}|+\tfrac{1}{2}|S\cap\mathcal{O}|\\ &\qquad+\tfrac{1}{2}|S_x\cap\mathcal{O}|+|S\cap S_x\cap\mathcal{O}|\equiv jl \text{ in } \mathcal{O}\equiv 0 (\operatorname{mod} 2).\end{aligned}$$

Since the roles of k and l are symmetric here, as k and l were introduced via the F-triple containing λ, the above two paragraphs suffice to verify (***) in Subcase 2.

Subcase 3. $\{i, j\} \cap \{k, l\} = \emptyset$. Using Lemma 11.1(iii), we get $E_5 \equiv \frac{1}{2}|((S+S_x) \cap \mathcal{O}) + \{ijkl\}|(\mathrm{mod}\, 2)$. So, (***) becomes

$$\begin{aligned} 0 \equiv {} & \tfrac{1}{2}\langle \lambda_{ij'}, \lambda\rangle + \langle \lambda_\infty, \lambda_{\infty, xx_\lambda}\rangle + \infty j \text{ in } (S_x + \mathcal{O}) + 1 + \infty k \text{ in } S + \infty l \text{ in } T \\ & + \langle \lambda_\infty, \lambda_{\infty, x}\rangle + \infty i \text{ in } S_x + \tfrac{1}{2}|S \cap \mathcal{O}| + 1 + |S_x \cap (\{k, l\} + (S \cap \mathcal{O}))| \\ & + \tfrac{1}{2}|((S+S_x) \cap \mathcal{O}| + \{ijkl\}| \equiv ij \text{ in } (S + \{k, l\}) + \tfrac{1}{4}|S_x + \mathcal{O}| + \infty j \text{ in } (S_x + \mathcal{O}) \\ & + 1 + \infty k \text{ in } S + \infty l \text{ in } T + \tfrac{1}{4}|S_x| + \infty i \text{ in } S_x + \tfrac{1}{2}|S \cap \mathcal{O}| \\ & + 1 + kl \text{ in } S_x + |S_x \cap S \cap \mathcal{O}| + \tfrac{1}{2}|(S+S_x) \cap \mathcal{O}| + 2 + |(S+S_x) \cap \{ijkl\}| \\ \equiv {} & ij\infty k \text{ in } S + \infty l \text{ in } T + \infty j \text{ in } \mathcal{O} + ijkl \text{ in } S_x + \tfrac{1}{2}|S_x \cap \mathcal{O}| + \tfrac{1}{2}|S \cap \mathcal{O}| \\ & + |S_x \cap S \cap \mathcal{O}| + \tfrac{1}{2}|S \cap \mathcal{O}| + \tfrac{1}{2}|S_x \cap \mathcal{O}| + |S \cap \mathcal{C} \cap S_x| \\ & + ijkl \text{ in } S + ijkl \text{ in } S_x \equiv \infty l \text{ in } (S + T) + \infty j \text{ in } \mathcal{C} + lj \text{ in } \mathcal{O} \equiv 0 (\mathrm{mod}\, 2). \end{aligned}$$

Thus (***) is valid here too, completing the arguments for this subcase and Case 29.

Case 30. $(B_2^2, B_{\mathrm{odd}})$. This is equivalent to Case 28.

Case 31. (B_2^3, B_2^3). We have $v(\lambda_{i,x})\, v(\lambda_{j,y}) = 0$ or $-\frac{9}{4} u_0(\lambda_{i,x}^2)$ when $i=j$, $x=y$, or $\beta(\lambda_{i,x}, \lambda_{j,y})\, v(\lambda)$ for some $\lambda \in \Lambda_2^2$.

When the product is 0, one can get $v(\lambda_{i,x})^\sigma v(\lambda_{j,y})^\sigma = 0$ as follows. Say $x=y$. Then $i \neq j$, and if $v(\lambda_{i,x})^\sigma v(\lambda_{j,x})^\sigma \neq 0$, then $v(\lambda_{i,x})^\sigma\, v(\lambda_{j,x})^\sigma \in B_2^{4,+} \oplus B_2^{4,-}$ and we may use associativity of the form to quote Cases 21 and 26. Say $x \neq y$. Assuming that $v(\lambda_{i,x})^\sigma\, v(\lambda_{j,y})^\sigma \neq 0$, we get $\lambda \in \Lambda_2^2$ with $x_\lambda = x_y$. Choosing $a = \pm 1$ so that $\xi = \lambda_{i,x} + a\lambda_{j,y}$ satisfies $\langle \xi, \xi\rangle = 4 + 4 + 2a\langle \lambda_{i,x}, \lambda_{j,y}\rangle \leqq 8$, the facts that $x_\xi = x_\lambda$ and the type of ξ is 2, 3 or 4 imply that ξ has type 2. This contradicts $v(\lambda_{i,x})\, v(\lambda_{j,y}) = 0$ since $\{\lambda_{i,x}, \lambda_{j,y}, \xi\}$ is a triangle of type 222.

When $i=j$ and $x=y$, we may use Cases 6 and 13.

Now we turn to the third alternative.

We have $\lambda \in \Lambda_2^2$ and $\lambda_{i,x}, \lambda_{j,y} \in \Lambda_2^3$ such that $\lambda = \lambda_{i,x} - \lambda_{j,y}$. Set $\mathcal{O} = \mathcal{O}_\lambda$. We have ij in $\mathcal{O} \equiv 0$ (mod 2); see Lemma 2.3. By using the action of H, we may assume that $q(\lambda) \in F$. The $\beta(\lambda_{i,x}, \lambda_{j,y}) = -36$, by Lemma 9.4. Let $\{\lambda, \mu, \nu\} \in \Delta(2, 3)$ satisfy $\mu = \lambda_{k,S}$, $\nu = \lambda_{l,T}$ and $q(\{\lambda, \mu, \nu\}) \subset F$; see Lemma 7.6. Then $k \neq l$ and

$$v(\lambda_{i,x})\, v(\lambda_{j,y}) = -36\, v(\lambda) \overset{\sigma}{\longmapsto} \delta(\mu, \nu)\, (\tfrac{9}{2}) \sum_{x_\zeta = x_\lambda} (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \zeta\rangle} \varphi_\zeta(x_\mu)\, v(\zeta).$$

Also,

$$\begin{aligned} v(\lambda_{i,x})^\sigma\, v(\lambda_{j,y})^\sigma &= (-1)^{\infty i \,\mathrm{in}\, S_x + \infty j \,\mathrm{in}\, S_y} (e(\tau x) \otimes x_i)\, (e(\tau y) \otimes x_j) \\ &= (-1)^{\infty i \,\mathrm{in}\, S_x + \infty j \,\mathrm{in}\, S_y} \sum_{x_\zeta = x_\lambda} [-3\delta_{ij} + \tfrac{9}{32}(u_0(u_{ij}), u(\zeta^2))]\, \varphi_\zeta(\tau x)\, v(\zeta). \end{aligned}$$

Thus, we must show that

$$\delta(\mu, \nu)\, (-1)^{\frac{1}{2}\langle \lambda_{kl'}, \zeta\rangle} \varphi_\zeta(x_\mu) = (-1)^{\infty i \,\mathrm{in}\, S_x + \infty j \,\mathrm{in}\, S_y} \varphi_\zeta(\tau x) \cdot \gamma,$$

where

$$\gamma=\tfrac{2}{9}[-3\delta_{ij}+\tfrac{9}{32}(u_0(u_{ij}), u(\zeta^2))]$$
$$=\begin{cases}\tfrac{2}{9}[-3+\tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii}-\sum\limits_{r\neq i}u_{rr}, r\sum\limits_{r\in\mathcal{O}}u_{rr})]=\tfrac{2}{9}[-3-\tfrac{3}{2}]=-1 & \text{if } i=j\notin\mathcal{O}\\ \tfrac{2}{9}[\tfrac{9}{32}(u_{ij}, u(\zeta^2))]=(-1)^{\frac{1}{2}\langle\lambda_{ij'},\zeta\rangle} & \text{if } i\neq j, i, j\in\mathcal{O}\end{cases}.$$

Subcase 1. $i=j\notin\mathcal{O}$. Then $S_x+S_y=\mathcal{O}$ or $\mathcal{O}+\Omega$. We must show that

$$\begin{aligned}0&\equiv\infty k \text{ in } S+\infty l \text{ in } T+\tfrac{1}{2}\langle\lambda_{kl'},\zeta\rangle\\&\quad+\langle\mu,\zeta\rangle+\infty i \text{ in } S_x+\infty i \text{ in } S_y+\langle\zeta,\lambda_\infty+\lambda_x\rangle+1\\&\equiv\infty k \text{ in } S+\infty l \text{ in } T+\tfrac{1}{2}\langle\lambda_{kl'},\zeta\rangle\\&\quad+\langle\mu,\zeta\rangle+\infty i \text{ in } \mathcal{O}+\langle\zeta,\lambda_\infty\rangle+\langle\zeta,\lambda_x\rangle+1,\end{aligned}$$

which, we argue, is congruent to $f(\zeta):=\frac{1}{2}\langle\lambda_{kl'},\lambda+\zeta\rangle+\langle\mu,\zeta\rangle+\langle\zeta,\lambda_\infty\rangle+\langle\zeta,\lambda_x\rangle(\text{mod } 2)$. To see this, look at the proof of Lemma 2.3(ii). With those conventions in effect, we have either

$$\begin{aligned}&S+T=\mathcal{O},\ k\in S,\ l\in T,\ kl \text{ in } \mathrm{Pos}(\lambda)\equiv 1(\text{mod } 2),\\&\text{so that } \infty k \text{ in } S+\infty l \text{ in } T+\tfrac{1}{2}\langle\lambda_{kl'},\lambda\rangle\\&+\infty i \text{ in } \mathcal{O}+1\equiv\infty \text{ in } (S+T+\mathcal{O})+k \text{ in } S+l \text{ in } T\\&+i \text{ in } \mathcal{O}+\tfrac{1}{2}\langle\lambda_{kl'},\lambda\rangle+1\equiv 0+1+1+0+1+1\\&\equiv 0(\text{mod } 2);\end{aligned}$$

or

$$\begin{aligned}&S+T=\mathcal{O}+\Omega,\ k\notin S,\ l\notin T,\ kl \text{ in } \mathrm{Pos}(\lambda)\equiv 0(\text{mod } 2),\\&\text{so that } \infty k \text{ in } S+\infty l \text{ in } T+\tfrac{1}{2}\langle\lambda_{kl'},\lambda\rangle+\infty i \text{ in } \mathcal{O}+1\\&\equiv\infty \text{ in } (S+T+\mathcal{O})+k \text{ in } S+l \text{ in } T+i \text{ in } \mathcal{O}+\tfrac{1}{2}\langle\lambda_{kl'},\lambda\rangle+1\\&\equiv 1+0+0+0+0+1\equiv 0(\text{mod } 2),\end{aligned}$$

as required. Therefore, it sufficies to prove that $f(\zeta)\equiv 0(\text{mod } 2)$. Since $q(\lambda)\in F, f(\lambda)\equiv 0(\text{mod } 2)$. So, $\mathcal{S}=\{\zeta\in\Lambda_2|\mathcal{O}_\zeta=\mathcal{O}$ and $f(\zeta)\equiv 0(\text{mod } 2)\}$ is nonempty. Suppose that $\zeta\in\mathcal{S}$ and that ζ' is obtained from ζ by changing the signs of the coordinates at the two indices $r, s\in\mathcal{O}$. Then $\zeta-\zeta'\equiv\lambda_{rs}$ or $\lambda_{rs'}(\text{mod } 2)$. Suppose $\zeta-\zeta'\equiv\lambda_{r,s}(\text{mod } 2)$. Then $\frac{1}{2}\langle\lambda_{kl'},\zeta-\zeta'\rangle\equiv rs$ in $\{kl\}(\text{mod } 2)$, $\langle\mu,\zeta-\zeta'\rangle\equiv 1+rs$ in S $(\text{mod } 2)$, $\langle\lambda_\infty,\zeta-\zeta'\rangle\equiv 1(\text{mod } 2)$ and $\langle\lambda_x,\zeta-\zeta'\rangle\equiv rs$ in $S_x(\text{mod } 2)$. So, $f(\zeta)-f(\zeta')\equiv rs$ in $(\{k,l\}+S+S_x)\equiv rs$ in $\emptyset\equiv 0(\text{mod } 2)$; see Lemma 2.3. Finally, suppose $\zeta-\zeta'\equiv\lambda_{rs'}(\text{mod } 2)$. Then $\frac{1}{2}\langle\lambda_{kl'},\zeta-\zeta'\rangle\equiv rs$ in $\{k,l\}(\text{mod } 2)$, $\langle\mu,\zeta-\zeta'\rangle\equiv rs$ in $S(\text{mod } 2)$, $\langle\lambda_\infty,\zeta-\zeta'\rangle\equiv 0(\text{mod } 2)$ and $\langle\lambda_x,\zeta-\zeta'\rangle\equiv rs$ in $S_x(\text{mod } 2)$, and we get $f(\zeta')\equiv 0(\text{mod } 2)$, as above. Since every $\zeta\in\Lambda_2^2$ with $\mathcal{O}_\zeta=\mathcal{O}$ may be obtained from λ by a sequence of coordinate changes, two at a time, we get $\mathcal{S}=\{\zeta\in\Lambda_2^2|\mathcal{O}_\zeta=\mathcal{O}\}$, thus completing the analysis of this subcase.

Subcase 2. $i\neq j$, $i, j\in\mathcal{O}$. We must show that $0\equiv\infty k$ in $S+\infty l$ in $T+\frac{1}{2}\langle\lambda_{kl'},\zeta\rangle+\langle\mu,\zeta\rangle+\infty i$ in $S_x+\infty j$ in $S_y+\langle\lambda_\infty+\lambda_x,\zeta\rangle+\frac{1}{2}\langle\lambda_{ij'},\zeta\rangle(\text{mod } 2)$. Since $i\neq j$, Lemma 7.7 tells us that we may assume that $q(\{\lambda,\lambda_{i,x},\lambda_{j,y}\})\subset F$. Thus, we may as well take $\mu=\lambda_{i,x}$, $\nu=\lambda_{j,y}$ so that $i=k$, $j=l$, $S_x=S$ and $S_y=T$. Thus, the right side of our congruence becomes $f(\zeta):=\langle\mu,\zeta\rangle+\langle\lambda_\infty+\lambda_x,\zeta\rangle(\mathrm{mod}\,2)$. Clearly, $f(\lambda)\equiv 0(\mathrm{mod}\,2)$ since $q(\lambda)\in F$. Note that $f(\zeta)\equiv\langle\lambda_{i,x}+\lambda_\infty+\lambda_x,\zeta\rangle(\mathrm{mod}\,2)$. So, if ζ' is obtained from ζ by changing the signs of coordinates at $r, s\in\mathcal{O}$, $r\neq s$, we get $f(\zeta)-f(\zeta')=\langle\lambda_i+\lambda_\infty,\zeta-\zeta'\rangle+\langle\lambda_S+\lambda_x,\zeta-\zeta'\rangle\equiv 0+rs$ in $(S+S_x)\equiv 0(\mathrm{mod}\,2)$, as required.

The verification of this case is now complete.

Case 32. $(B_2^3, B_{\mathrm{even}})$. The associativity of the form makes this a consequence of Case 33, which we verify next.

Case 33. $(B_2^3,\ B_{\mathrm{odd}})$. We have

$$\begin{aligned}
&v(\lambda_{i,x})\,e(\tau y)\otimes x_j\\
&\quad=\sum_{k\in\Omega}\left[-3\delta_{jk}+\tfrac{9}{32}(u_0(u_{jk}),\ u(\lambda_{i,x}^2))\right]\varphi_{\lambda_{i,x}}(\tau y)\,e(xy)\otimes x_k\\
&\quad\overset{\sigma}{\longmapsto} a_1:=\sum_{k\in\Omega}\left[-3\delta_{jk}+\tfrac{9}{32}(u_0(u_{jk}),u(\lambda_{i,x}^2))\right]\varphi_{\lambda_{i,x}}(\tau y)\,(-1)^{\langle\lambda_\infty,\lambda_{k,xy}\rangle}\,e(xy)\otimes x_k.
\end{aligned}$$

Also,

$$\begin{aligned}
a_2&:=v(\lambda_{i,x})^\sigma\,(e(\tau y)\otimes x_j)^\sigma=(-1)^{\infty i\,\mathrm{in}\,S_x}(e(\tau x)\otimes x_i)\,(-1)^{\infty j\,\mathrm{in}\,S_y}v(\lambda_{j,y})\\
&=(-1)^{\infty i\,\mathrm{in}\,S_x+\infty j\,\mathrm{in}\,S_y}\sum_{k\in\Omega}\left[-3\delta_{ik}+\tfrac{9}{32}(u_0(u_{ik}),\ u(\lambda_{j,y}^2))\right]\varphi_{\lambda_{j,y}}(\tau x)\,e(xy)\otimes x_k.
\end{aligned}$$

Using H-action, we may arrange for $x=1$. We shall make this specialization within each of the subcases which arise.

For $r\in\Omega$, let $a_{s,r}$ be the coefficient of $e(xy)\otimes x_r$ in a_s, $s=1,2$. For $r\neq i,j$,

$$\begin{aligned}
a_{1,r}&=\tfrac{9}{32}(u_{jr},u(\lambda_{i,x}^2))\,\varphi_{\lambda_{i,x}}(\tau y)\,(-1)^{\langle\lambda_\infty,\lambda_{r,xy}\rangle}\\
a_{2,r}&=\tfrac{9}{32}(u_{ir},u(\lambda_{j,y}^2))\,\varphi_{\lambda_{j,y}}(\tau x)\,(-1)^{\infty i\,\mathrm{in}\,S_x+\infty j\,\mathrm{in}\,S_y}
\end{aligned}$$

For these to be equal, we need

$$\begin{aligned}
&jr\ \text{in}\ S_x+\langle\lambda_\infty,\lambda_{r,xy}\rangle+\langle\lambda_{i,x},\lambda_\infty\rangle+\langle\lambda_{i,x},\lambda_y\rangle\\
&\qquad\equiv ir\ \text{in}\ S_y+\langle\lambda_{j,y},\lambda_\infty\rangle+\langle\lambda_{j,y},\lambda_x\rangle+\infty i\ \text{in}\ S_x+\infty j\ \text{in}\ S_y(\mathrm{mod}\,2),
\end{aligned}$$

or

$$\begin{aligned}
&\infty ijr\ \text{in}\ S_{xy}+\langle\lambda_\infty,\lambda_{r,xy}\rangle+\langle\lambda_\infty,\lambda_{i,x}\rangle+\langle\lambda_\infty,\lambda_{j,y}\rangle+\langle\lambda_{i,x},\lambda_y\rangle+\langle\lambda_{j,y},\lambda_x\rangle\\
&\qquad\equiv 0(\mathrm{mod}\,2),
\end{aligned}$$

or

$$ij\ \text{in}\ S_{xy}+\langle\lambda_\infty,\lambda_{\infty,xy}\rangle+\langle\lambda_\infty,\lambda_{i,x}\rangle+\langle\lambda_\infty,\lambda_{j,y}\rangle+\langle\lambda_{i,x},\lambda_y\rangle+\langle\lambda_{j,y},\lambda_x\rangle\equiv 0(\mathrm{mod}\,2).$$

Using H-action, we may assume that $x=1$. The condition then reads

$$\begin{aligned}
0&\equiv ij\ \text{in}\ S_y+\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\langle\lambda_\infty,\lambda_{j,y}\rangle+\langle\lambda_i,\lambda_y\rangle\\
&\equiv ij\ \text{in}\ S_y+\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\infty j\ \text{in}\ S_y+\langle\lambda_\infty,\lambda_y\rangle+\infty i\ \text{in}\ S_y\\
&\equiv\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\langle\lambda_\infty,\lambda_y\rangle(\mathrm{mod}\,2),
\end{aligned}$$

which is true.

Suppose $r=i$. Then

$$a_{1,i}=[-3\delta_{ji}+\tfrac{9}{32}(u_0(u_{ji}),u(\lambda_{i,x}^2))]\,\varphi_{\lambda_{i,x}}(\tau y)(-1)^{\langle\lambda_\infty,\lambda_{i,xy}\rangle}$$
$$a_{2,i}=[-3+\tfrac{9}{32}(u_0(u_{ii}),u(\lambda_{j,y}^2))]\,\varphi_{\lambda_{j,y}}(\tau x)(-1)^{\infty i\,\mathrm{in}\,S_x+\infty j\,\mathrm{in}\,S_y}$$

First, let us treat the special case $i=j$. Then

$$[-3+\tfrac{9}{32}(u_0(u_{ii}),u(\lambda_{i,x}^2))]=-3+\tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii}-\sum_{k\neq i}u_{kk},u(\lambda_{i,x}^2))$$
$$=-3+\tfrac{9}{32}\cdot\tfrac{1}{24}(23\cdot 8\cdot 4)=\tfrac{45}{8}.$$

So $a_{1,i}=a_{2,i}$ if and only if

$$0\equiv\langle\lambda_{i,x},\lambda_\infty\rangle+\langle\lambda_{i,x},\lambda_y\rangle+\langle\lambda_\infty,\lambda_{i,xy}\rangle+\langle\lambda_{i,y},\lambda_\infty\rangle$$
$$+\langle\lambda_{i,y},\lambda_x\rangle+\infty i\text{ in }S_x+\infty i\text{ in }S_y\pmod 2.$$

Using H-action, we may assume that $x=1$. The condition then reads

$$0\equiv\langle\lambda_i,\lambda_\infty\rangle+\langle\lambda_i,\lambda_y\rangle+\langle\lambda_\infty,\lambda_{i,y}\rangle+\langle\lambda_{i,y},\lambda_\infty\rangle+\infty i\text{ in }S_y$$
$$\equiv 0+\langle\lambda_\infty,\lambda_y\rangle+\infty i\text{ in }S_y+\infty i\text{ in }S_y\pmod 2,$$

which is valid. Now let us treat the special case $i\neq j$. Then

$$\tfrac{9}{32}(u_{ij},u(\lambda_{i,x}^2))=\tfrac{9}{32}(u_{ij},(-6)(-1)^{ij\,\mathrm{in}\,S_x}u_{ij})=-\tfrac{27}{8}(-1)^{ij\,\mathrm{in}\,S_x}$$

and

$$-3+\tfrac{9}{32}(u_0(u_{ii}),u(\lambda_{j,y}^2))=-3+\tfrac{9}{32}\cdot\tfrac{1}{24}(23u_{ii}-\sum_{k\neq i}u_{kk},9u_{jj}+\sum_{k\neq j}u_{kk})$$
$$=-3+\tfrac{9}{32}\cdot\tfrac{1}{24}\cdot 4\cdot(23-9-22)=-3-\tfrac{3}{8}=-\tfrac{27}{8}.$$

So, $a_{1i}=a_{2i}$ if and only if

$$0\equiv ij\text{ in }S_x+\langle\lambda_{i,x},\lambda_\infty\rangle+\langle\lambda_{i,x},\lambda_y\rangle+\langle\lambda_\infty,\lambda_{i,xy}\rangle+\langle\lambda_{j,y},\lambda_\infty\rangle+\langle\lambda_{j,y},\lambda_x\rangle$$
$$+\infty i\text{ in }S_x+\infty j\text{ in }S_y\pmod 2.$$

Using H-action, we may assume that $x=1$. The condition then reads

$$0\equiv\langle\lambda_i,\lambda_\infty\rangle+\langle\lambda_i,\lambda_y\rangle+\langle\lambda_\infty,\lambda_{i,y}\rangle+\langle\lambda_{j,y},\lambda_\infty\rangle+\langle\lambda_{j,y},0\rangle+\infty j\text{ in }S_y$$
$$\equiv 0+\langle\lambda_\infty,\lambda_y\rangle+\infty i\text{ in }S_y+\langle\lambda_\infty,\lambda_{\infty,y}\rangle+\infty i\text{ in }S_y$$
$$+\langle\lambda_{\infty,y},\lambda_\infty\rangle+\infty j\text{ in }S_y+0+\infty j\text{ in }S_y\pmod 2,$$

which is valid.

Suppose that $r=j\neq i$. Then

$$a_{1,j}=[-3+\tfrac{9}{32}(u_0(u_{jj}),u(\lambda_{i,x}^2)]\,\varphi_{\lambda_{i,x}}(\tau y)(-1)^{\langle\lambda_\infty,\lambda_{j,xy}\rangle}$$
$$a_{2,j}=\tfrac{9}{32}(u_{ij},u(\lambda_{j,y}^2))\,\varphi_{\lambda_{j,y}}(\tau x)(-1)^{\infty i\,\mathrm{in}\,S_x+\infty j\,\mathrm{in}\,S_y}.$$

By calculating as above, we get $[-3+\tfrac{9}{32}(u_0(u_{jj}),u(\lambda_{i,x}^2)]=-\tfrac{27}{8}$ and $\tfrac{9}{32}(u_{ij},u(\lambda_{j,y}^2))=-\tfrac{27}{8}(-1)^{ij\,\mathrm{in}\,S_y}$. Thus $a_{1,j}=a_{2,j}$ if and only if

$$0\equiv\langle\lambda_{i,x},\lambda_\infty\rangle+\langle\lambda_{i,x},\lambda_y\rangle+\langle\lambda_\infty,\lambda_{j,xy}\rangle+ij\text{ in }S_y+\langle\lambda_{j,y},\lambda_\infty\rangle$$
$$+\langle\lambda_{j,y},\lambda_x\rangle+\infty i\text{ in }S_x+\infty j\text{ in }S_y\pmod 2.$$

Once we note that $\langle\lambda_\infty, \lambda_{j,xy}\rangle + ij$ in $S_y \equiv \langle\lambda_\infty, \lambda_{i,xy}\rangle + ij$ in $S_{xy} + ij$ in $S_y \equiv \langle\lambda_\infty, \lambda_{i,xy}\rangle + ij$ in $S_x \pmod 2$, the congruence becomes the one we verified in the last paragraph.

The verification of this case is now complete.

Case 34. $(B_{\text{even}}, B_{\text{even}})$. This is equivalent to earlier cases, by associativity of the form.

Case 35. $(B_{\text{even}}, B_{\text{odd}})$. This is equivalent to earlier cases.

Case 36. $(B_{\text{odd}}, B_{\text{odd}})$. This is equivalent to earlier cases.

The proof of Proposition 11.2 is now finished.

§12. The Identification of $G = \langle C, \sigma\rangle$

From Proposition 11.2, we know that $G(B) \cap \{g \in GO(B) \mid \underline{\underline{d}}^g = \underline{\underline{d}}\}$ is strictly larger than C. In fact, it contains C as a nonnormal subgroup, since σ can not normalize $C(z^\sigma = zz_1 \in Q - \langle z\rangle$; see Chap. 10). We define $G := \langle C, \sigma\rangle$, a subgroup of $G(B)$. In this section, we show that G is a finite simple group of order $2^{46}3^{20}5^9 7^6 11^2 13^3 . 17 . 19 . 23 . 29 . 31 . 41 . 47 . 59 . 71$.

Since it is not clear that G is finite, we temporarily transfer our attention to finite homomorphic images of G by reduction modulo $p \geqq 5$ (explained below). Techniques from the classification theory of finite simple groups are used to identify the centralizer of an involution in the image of G modulo p. Other results from the classification theory are then quoted to identify the images of G modulo the various primes, and they all turn out to be simple groups of the same order. This implies the required statements about G.

It is possible that finiteness and simplicity of G and a calculation of the order of G may be demonstrated without appealing to the classification theory. For instance, if a G-stable $\mathbb{Z}$-lattice in B is exhibited, positive definiteness of the form implies that G must be finite. Then, possibly, some analysis of the action of G on sets of vectors could be made to get simplicity and the order. Such an argument, however, may well be difficult. The description of G does not really require classification theorems (although we made reference to a few papers from the classification effort to verify a few points more quickly), and it would be desirable to maintain this independence throughout our analysis of G.

Now we proceed to a description of the "reduction modulo p" process and the determination of the centralizer of an involution in our quotient groups.

The definitions of C and σ with respect to our basis of B show that, in matrix form, the linear transformations in $G = \langle C, \sigma\rangle$ may be written over the ring $\mathbb{Z}[\frac{1}{2}]$; see Table 10.2. Furthermore, Table 6.1 shows that all structure constants for B lie in the ring $\mathbb{Z}[\frac{1}{6}]$. Thus, we get an algebra $B_{\mathbb{Z}[\frac{1}{6}]}$ over the ring $\mathbb{Z}[\frac{1}{6}]$ having our $\mathbb{Q}$-basis of B as a free $\mathbb{Z}[\frac{1}{6}]$-basis. Furthermore, G acts on $B_{\mathbb{Z}[\frac{1}{6}]}$. By reduction modulo $p \geqq 5$, p prime, we get algebras $B(p) := B_{\mathbb{Z}[\frac{1}{6}]}/pB_{\mathbb{Z}[\frac{1}{6}]}$ over $\mathbb{F}_p$ and natural homomorphisms $G \rightarrow G(B(p)) \leqq GO(B(p))$ (the bilinear form on B gives us some bilinear form on $B(p)$; it is nonzero since $(e(x), e(y)) = \delta_{xy}$ and $(v(\lambda), v(\mu)) = \delta_{\bar{\lambda}, \bar{\mu}}$, for instance; we do not assert anything about nondegeneracy and so $GO(B(p))$ means the subgroup of $GL(B(p))$ preserving a possibly degenerate form). We shall use the suffix (p) to indicate images in $B(p)$ or in $G(B(p))$. Generalizing slightly, we define $S(p)$ for $S \subseteq B$ by $(S \cap B_{\mathbb{Z}[\frac{1}{6}]})(p)$, and thereby define $U(p)$, $V(p)$, $W(p)$. Note that $\mathbb{Z}[\frac{1}{2}]\Lambda$ and $\bigoplus_{i\in\Omega} \mathbb{Z}[\frac{1}{2}]x_i$ are the same subset of $\bigoplus_{i\in\Omega} \mathbb{Q}x_i$. Since $\hat{C} = \langle \hat{Q}, \hat{N}_0, \hat{s}_0 \rangle = \langle \hat{Q}, \hat{P}, \hat{s}_0 \rangle$ (see Sect. 4, 7 and 10 and use the fact that N_{24} is maximal in .0 [11]), it follows that $T_{\mathbb{Z}[\frac{1}{2}]} := \bigoplus_{i\in\Omega} \mathbb{Z}[\frac{1}{2}]\, e(x)$ is stable under $\hat{C}$: this is easy to check for elements of $\hat{Q}\hat{P}$ (see Sect. 8), and for $\hat{s}_0$ see Lemma 9.2 (iv) (take $\hat{g} = \hat{s}_0$ and use $e(x)^{s_0} = e(1)^{x s_0} = e(1)^{s_0 x^{s_0}} = (\sum_{y\in F} \pm\frac{1}{2}\, e(y))^{x^{s_0}} \in T_{\mathbb{Z}[\frac{1}{2}]})$. So, we may define $\Lambda(p) := \Lambda/p\Lambda$, $T(p) := T_{\mathbb{Z}[\frac{1}{2}]}/p\,T_{\mathbb{Z}[\frac{1}{2}]}$ and we may identify $W(p)$ with $\Lambda(p) \bigotimes_{\mathbb{F}_p} T(p)$.

Fix a prime $p \geqq 5$. Set $C_1 = C_{G(p)}(z(p))$, $N_1 = N_{G(p)}(Q(p))$.

Lemma 12.1. $C(p) = N_1$.

Proof. In this proof, we use bars to indicate the application of $\overline{\mathbb{F}}_p \bigotimes_{\mathbb{F}_p}$- to a finite dimensional $\mathbb{F}_p$- module for some group.

Let $\hat{N}_1$ be a covering group of N_1, $Q_1 := O_2(\hat{N}_1)$. Use ˆ to indicate preimages under $\hat{N}_1 \to N_1$.

As a module for $Q \cong Q(p)$, $W(p) \cong \bigoplus_1^{24} T(p)$. Define $A := \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{W(p)})$. Think of N_1 as a subgroup of the group of units of A. Let A_1 be the subalgebra of A spanned over $\overline{\mathbb{F}}_p$ by $Q(p)$ and let A_2 be the commuting algebra of A_1 in A. We have A_1, A_2 isomorphic to full matrix algebras of degrees 2^{12}, 24, respectively, over $\overline{\mathbb{F}}_p$, and A, A_1 and A_2 have a common unit element. The double centralizer theorem ([42], p. 25) asserts that A_1 is the commuting algebra of A_2 in A.

Since $Q(p) \lhd N_1$, A_1 and A_2 are stable under conjugation by N_1. Therefore, we have a projective representations $N_1 \to PGL(d_i, \overline{\mathbb{F}}_p)$, $d_1 = 2^{12}$, $d_2 = 24$, and a corresponding homomorphism $\rho_i : \hat{N}_1 \to GL(24, \overline{\mathbb{F}}_p)$, $i = 1, 2$ (see [39], p. 216). Let M_i be the $\overline{\mathbb{F}}_p\hat{N}_1$-module associated to ρ_i, $i = 1, 2$.

Define $N_2 := C_{\hat{N}_1}(M_2) \lhd \hat{N}_1$, $N_2^* := Z(\hat{N}_1 \bmod N_2)$ and $N_3 := C_{\hat{N}_1}(Q(p))$. Then N_2, N_2^*, N_3 and Q_1 are normal subgroups of $\hat{N}_1$. We apply Lemmas 2.19 and 2.20 several times. For the action of $N_3 Q_1 \lhd \hat{N}_1$ on M_2, we get $N_3 Q_1 \leqq N_2^*$. For the action of $N_2^* \lhd \hat{N}_1$ on $Q(p)/Q(p)'$, we get $N_2^* \leqq N_3 \widehat{Q(p)} \leqq N_3 Q_1$, whence $N_2^* = N_3 Q_1 = N_3 \widehat{Q(p)}$.

Since $(N_3 Q_1)^{\rho_2}$ is scalar, the image of $N_3 Q_1$ in A lies in A_1. Therefore, elements of N_3 operate as scalars on $W(p)$. Let $g \in N_3$ act as the scalar c on $\overline{W(p)}$. Since g preserves the form and $(e(x) \otimes x_i, e(x) \otimes x_i) = 1$, $c^2 = 1$, whence $c = \pm 1$ and g is trivial on $\overline{U(p) + V(p)}$ because $\overline{W(p)^2} = \overline{U_0(p) + V(p)}$ and G fixes the vector $\underline{\underline{d}}$. It follows that g acts as 1 or $z(p)$ does on $B(p)$. Thus, $N_2^* = \widehat{Q(p)}\, N_4$, where N_4 is the kernel of the action on $B(p)$. Since N_1 acts faithfully on $B(p)$, $N_4 \leqq Z(\hat{N}_1)$. So, $N_3 = Z(\widehat{Q(p)})\, N_4$.

A consequence of this paragraph is that $Q(p) = O_2(N_1)$ and N_1 is 2-constrained.

It remains to identify $N_1/Q(p)$, which has a 24-dimensional projective representation over $\bar{\mathbb{F}}_p$ and is embedded in $\mathrm{Out}(Q(p))\cong O^+(24,2)$. This identification follows at once from Lemma 2.21, and we are done.

Lemma 12.2. *Q is the unique subgroup in $S\in\mathrm{Syl}_2(C)$ which contains $\langle z\rangle$ as its center and is isomorphic to Q. Consequently, $Q(p)$ is weakly closed in $S(p)$ with respect to C_1 and $S(p)\in\mathrm{Syl}_2(C_1)\subseteq\mathrm{Syl}_2(G(p))$.*

Proof. The second statement follows from the first and Lemma 12.1. So, let us verify the first statement. Note that $S\cong S(p)$ since p is odd.

Suppose that $\langle z\rangle=Q_1'$, $Q_1\leqq S$, $Q_1\cong Q$, $Q_1\neq Q$.

For $t\in S$, $m(C_{Q/\langle z\rangle}(t))\leqq 16$ (see Lemma 2.30). Define $2^a=|Q\cap Q_1/\langle z\rangle|$ and $2^b=|Q_1/Q_1\cap Q|$. We have $a\leqq 16$ and $1\leqq b\leqq 11$, since $m(S/Q)=11$; see Lemma 2.15. Also $a+b=24$, so that $b\geqq 8$ and $a\geqq 13$. Since $a>\frac{1}{2}(24)$, there is an extraspecial group $Q^*\leqq Q\cap Q_1$, $|Q^*|=2^{2c+1}$, $c\geqq 1$. We have $2c\leqq a$. Choose Q^* to maximize c. Set $R^*=\langle Q,Q_1\rangle=QQ_1$. Then $|R^*|=2^{49-a}=2^{a+2b+1}$. Also, $Q^*\lhd R$ because $Q\cap Q_1/\langle z\rangle$ is central in $R^*/\langle z\rangle$ as $R^*=QQ_1$ and $Q/\langle z\rangle\cong Q_1/\langle z\rangle$ are abelian. Since $Q\cap Q_1/\langle z\rangle$ is central in $R^*/\langle z\rangle$, $R^*=C_{R^*}(Q^*)Q^*$. Also, $|C_{R^*}(Q^*)|=2^{a+2b-2c+1}$ and $|C_Q(Q^*)|=2^{1+24-2c}=2^{1+a+b-2c}$ so that $|C_{R^*}(Q^*)/C_Q(Q^*)|=2^b\geqq 2^8$. Since Q^* is extraspecial, there is a vector $\xi\in\Lambda_3$ with $q(\xi)\in Q^*$. The shape of $C_{R^*}(Q^*)$ indicates that the stabilizer in $\cdot 1$ of $\langle\xi,-\xi\rangle$ contains an elementary abelian group of order 2^b, $b\geqq 8$. However, the 2-rank of $\cdot 3$ is at most 6, by Lemma 2.22, a contradiction. This completes the proof.

Lemma 12.3. *$Q(p)$ is strongly closed in $S(p)$ with respect to C_1.*

Proof. We let bars denote images in $\overline{C}_1=C_1/\langle z(p)\rangle$. Lemma 12.2 shows that $\overline{Q(p)}$ is weakly closed in $S(p)$. It suffices to prove that $\overline{Q(p)}$ is strongly closed in $\overline{S(p)}$, and to do so, we assume otherwise and use Lemma 2.14 to get a contradiction. In that notation, we take $\overline{C}_1$ for G, $\overline{S(p)}$ for T, $\overline{Q(p)}$ for $A=W$ and we have $r\leqq 11$ (see Lemma 2.15).

We establish some notation relevant to the use of Lemma 2.14. Let φ: $\overline{C(p)}\to\cdot 1$ and ψ: $N_{24}/\{\pm 1\}\to(N_{24}/\{\pm 1\})/O_2(N_{24}/\{\pm 1\})\cong M_{24}$ be the natural maps. We may replace S with a conjugate to assume that $S(p)^\varphi\leqq N_{24}/\{\pm 1\}$. Let $\mathcal{S}=\{B\leqq\overline{S(p)}\,|\,B$ is conjugate in $\overline{C}_1$ to a subgroup of $\overline{Q(p)}$, $B\nleqq\overline{Q(p)}\}$, $r=\max\{m(B^\varphi)\,|\,B\in\mathcal{S}\}$, $\mathcal{S}_{\max}=\{B\in\mathcal{S}\,|\,m(B^\varphi)=r\}$, $\mathcal{S}^*=\{B\in\mathcal{S}\,|\,m(B)+r\geqq 24\}$. Then $\mathcal{S}$, $\mathcal{S}_{\max}$ and $\mathcal{S}^*$ are nonempty, although we do not know whether $\mathcal{S}_{\max}\cap\mathcal{S}^*$ is empty or not.

For $\tilde{B}\leqq\overline{S(p)}$, let $c(\tilde{B}):=\dim C_{\overline{Q(p)}}(\tilde{B})=\dim C_{\Lambda/2\Lambda}(\tilde{B})$. Then $m(B)\leqq c(B)+m(B^\varphi)$. Also,

$$(*)\qquad 24\leqq r+c(B)+m(B^\varphi)\quad\text{for } B\in\mathcal{S}^*.$$

We claim that

$$(**)\qquad \text{if } B\in\mathcal{S},\ (B^\varphi)^\#\text{ consists of 2-central involutions of }\overline{C}_1\text{ and }8\leqq r\leqq 10.$$

The first part and $r \geqq 8$ follow from $r \leqq 11$, Corollary 2.30 and Lemma 2.14(ii.2). Suppose that $r=11$. Take $B \in \mathscr{S}_{\max}$. By Lemma 2.15, $B^{\varphi}=O_2(N_{24}/\{\pm 1\})$, which contains non-2-central involutions, a contradiction.

Let V be the subspace of $\mathscr{C}$ corresponding to the subgroup $B_0:=B^{\varphi} \cap O_2(N_{24}/\{\pm 1\})$ of $O_2(N_{24}/\{\pm 1\})$, $m(V)=m(B_0)+1$. In an obvious way, an element of B_0 corresponds to a pair $\{S, S+\Omega\}$ of $\mathscr{C}$-sets in V. Lemma 2.25 and $(**)$ imply that such an S must be $\emptyset$, Ω, an octad or a 16-set and $m(B_0) \leqq 5$.

We argue that we may assume $B_0 \neq 1$. Any involution $z \in (B^{\varphi})^{\#}$ is 2-central in $\bar{C}_1^{\varphi} \cong \cdot 1$ and $B^{\varphi} \leqq C_{C_1^{\varphi}}(z) \cong 2_+^{1+8} \cdot D_4(2)$, which has a subgroup $2_+^{1+8} \cdot 2^6 \cdot A_8$, of odd index, conjugate to a subgroup of $N_{24}/\{\pm 1\}$. Sylow's theorem gives the result. So, we do assume $B_0 \neq 1$.

Now take $B \in \mathscr{S}_{\max}$. We shall argue that $m(B)=r=8$.

Suppose that B_0 is of octad type (in the sense of Definition 2.27), based on the octad $\mathcal{O}_0$. Let H_0 be the stabilizer of $\mathcal{O}_0$ in $(N_{24}/\{\pm 1\})^{\psi} \cong M_{24}$, $H_0 \cong 2^4 . A_8$, and let $H_1 \leqq H_0$ be the centralizer of B_0. We have $m_2(H_1) \geqq r-m(B_0)$ since $B^{\varphi}/B_0 \hookrightarrow H_1$, whence, by Corollary 2.24, $6 \geqq m_2(H_1) \geqq 8-m(B_0)$ and $m(B_0) \geqq 2$. Thus, B_0 has an element associated to an octad $\mathcal{O}$ disjoint from $\mathcal{O}_0$, and so H_1 lies in the stabilizer H_2 of each member of the trio $\{\mathcal{O}, \mathcal{O}_0, \mathcal{O}+\mathcal{O}_0+\Omega\}$, $H_2 \cong 2^3 . 2^3 . L_3(2)$. Note that $H_1=1$ if $m(B_0)=5$, so that $2 \leqq m(B_0) \leqq 4$. If $m(B_0)=2$, Corollary 2.24 gives $m(B^{\varphi}/B_0) \leqq 6$ and $r=m(B) \leqq 8$, as desired. So, we may assume $m(B_0) \geqq 3$. Therefore, B_0 contains elements associated to octads $\mathcal{O}_1$, $\mathcal{O}_2$ disjoint from $\mathcal{O}_0$, so that $\mathcal{O}_1 \cap \mathcal{O}_2 \neq \emptyset$. Thus, H_1 lies in the stabilizer of the associated sextet and fixes the tetrads $\mathcal{O}_1-\mathcal{O}_2$, $\mathcal{O}_2-\mathcal{O}_1$, $\mathcal{O}_1 \cap \mathcal{O}_2$ and $\mathcal{O}_0+(\mathcal{O}_1 \cup \mathcal{O}_2)+\Omega$ i.e. H_1 lies in a subgroup $H_3 \cong 2^6 . 3 . 2$ (see Lemma 2.31). If $m(B^{\varphi}/B_0) \geqq 5$, $B^{\varphi}/B_0 \leqq O_2(H_3)$, a contradiction to $(**)$ and Lemmas 2.29 and 2.31 (iii). Thus, $m(B^{\varphi}/B_0) \leqq 4$. Since $m(B^{\varphi})=r \geqq 8$, $m(B_0) \geqq 4$, so that $m(B_0)=4$ and $r=8$.

Next suppose that our $B \in \mathscr{S}_{\max}$ has B_0 of sextet type, (thus not of octad type). If $m(B_0) \leqq 2$, $r=8$ by Corollary 2.24. So, $m(B_0) \geqq 3$, without loss. Let Ξ be the relevant sextet, with tetrads $T_1, \ldots, T_6$ (Ξ is unique since $m(B_0) \geqq 3$). Let $\mathscr{A}$ be the set of octads associated to elements of B_0 and $\mathscr{B}$ the set of tetrads involved in members of $\mathscr{A}$. We have $|\mathscr{B}| \geqq 4$ and since B_0 is not of octad type, $|\mathscr{B}| \geqq 5$ and every member of $\mathscr{B}$ is expressible as an intersection of two members of $\mathscr{A}$. Therefore, the stabilizer in $(N_{24}/\{\pm 1\})^{\psi}$ of B_0 is simply the setwise stabilizer of all of the members of B_0 and it has shape $2^6 . 3$ since $|\mathscr{B}| \geqq 5$ (see Lemma 2.31). So, $m(B_0)=4$ and $m(B^{\varphi}/B_0) \leqq 4$ by Lemma 2.29 and 2.31 (iii) and $(**)$. Therefore, $r=8$ in this case as well.

We have $r=8$. We now take $B \in \mathscr{S}^*$ and analyze $C_{\Lambda/2\Lambda}(B)$ carefully. Unfortunately, we don't know that $B \in \mathscr{S}_{\max}$, so that the preceeding paragraphs may not apply to B. We do have $c(B)+m(B^{\varphi}) \geqq m(B) \geqq 16$. Without loss, $B_0 \neq 1$, as before. We complete the search for a contradiction by analyzing cases. Define $B_1=\{b \in B \mid b^{\varphi\psi} \in O_2(N_{24})/\{\pm 1\}\}$, $m_1=m(B_1/B_0)$, $m_2=m(B/B_1)$.

Case 1. $m(B^{\varphi}) \geqq 3$. Take $\overline{Q(p)} \leqq \tilde{B} \leqq B$ such that $\tilde{B}^{\varphi} \cap B_0$ has order 2 and $\tilde{B}$ covers B/B_0 (this can be done since B is elementary abelian). Then $\tilde{B} \in \mathscr{S}$. By Lemmas 2.28 and 2.32, $c(B) \leqq 12$, so that $m(B^{\varphi}) \geqq 4$. Note that $m(B_0)=5$ implies $B^{\varphi}=B_0$, $c(B)=8$ so that $m(B) \leqq 13$ and $(*)$ fails for B. Therefore, $m(B_0) \leqq 4$.

Suppose $m(B_0) \geqq 2$. We claim that $m_1 \leqq 3$. Suppose $m_1 = 4$. Since B_1 operates regularly on $\Omega + \mathcal{O}_0$ (via ψ), the only $\mathscr{C}$-sets fixed modulo $\langle \Omega \rangle$ by B_1 are $\mathcal{O}_0$ and $\Omega + \mathcal{O}_0$. Therefore, $|C_{\mathscr{C}}(B_1)| \leqq 2$, contradicting $m(B_0) \geqq 2$.

Suppose $m(B_0) \geqq 3$. By Lemma 2.28, $c(B) \leqq 10$, implying $m(B^{\varphi}) \geqq 6$ so that $m_1 + m_2 \geqq 6 - m(B_0) \geqq 6 - 4 = 2$. From Lemma 2.32, we get the contribution of $A(4) + 2A/2A$ to $c(\tilde{B})$ and since $c(B) \geqq 8$ and $d \leqq 1$ in the notation of 2.28, we get $c(B) = 8$, $m_1 = 0$, $m_2 = 2$, $d = 1$ and $c(\tilde{B}) = 8$. Therefore, $m(B^{\varphi}) \geqq 8$, a contradiction to $m_1 + m_2 = 2$ and $m(B_0) \leqq 4$.

We have $m(B_0) \leqq 2$. Suppose $m(B_0) = 2$. Then $m_1 + m_2 \geqq 3 - 2 = 1$, whence $c(\tilde{B}) \leqq 12$ by Lemma 2.32 and so $m_1 + m_2 \geqq 2$. Again, 2.32 gives $c(\tilde{B}) \leqq 11$ and $m_1 + m_2 \geqq 3$. So, $c(\tilde{B}) \leqq 10$ or $m_1 = 0$ and $m_2 = 3$ and $c(\tilde{B}) = 11$. Note that $m_2 \geqq 1$ in any case because $c(\tilde{B}) \leqq 10$ implies that $m(B^{\varphi}) \geqq 6$, whence $m_1 + m_2 \geqq 4$ and $m_2 \geqq 1$ because $m_1 \leqq 3$ when $m(B_0) \geqq 2$. Since $m_2 \geqq 1$ and $m_1 + m_2 \geqq 3$, the contribution $c_1(\tilde{B})$ of $A(4) + 2A/2A$ to $c(\tilde{B})$ is at most 7, whence $d = 3$ (in the notation of 2.28) gives $c(B) \leqq 10$. Then $m_1 + m_2 \geqq 4$ and $c_1(\tilde{B}) \leqq 6$, so that $c(B) \leqq 6 + d = 9$ and $m_1 + m_2 \geqq 5$. Again, $c_1(\tilde{B}) \leqq 5$, so that $c(B) \leqq 5 + d = 8$ and $c(B) = 8$, $m(B^{\varphi}) = 8$ and $m_1 + m_2 = 6$. If $m_2 = 4$, this gives $c_1(\tilde{B}) \leqq 2$ and $c(B) \leqq 2 + d = 5$, a contradiction. So, $1 \leqq m_2 \leqq 3$, $m_1 \geqq 3$ and we get $c(\tilde{B}) \leqq 10 - m_1 \leqq 7$, a contradiction.

We have $m(B_0) = 1$ and $\tilde{B} = B$. Since $m_1 + m_2 \geqq 2$, $c(B) \leqq 11$, implying $m(B^{\varphi}) \geqq 5$, $m_1 + m_2 \geqq 4$ and $c(B) \leqq 9$ or $c(B) = 10$, $m_1 = 0$, $m_2 = 4$ (see 2.28 and 2.32). If $c(B) \leqq 9$, another round with $(*)$ and Lemma 2.32 gives $m_1 + m_2 \geqq 6$ and $c(B) \leqq 8$ and $m(B^{\varphi}) \geqq 8$, a contradiction to $m(B_0) = 1$ and Corollary 2.24. So, $c(B) = 10$, $m_1 = 0$, $m_2 = 4$. Then $(*)$ fails.

Case 2. $m(B^{\varphi}) = 2$. By $(*)$, we must have $c(B) \geqq 14$. If $B_0 = B^{\varphi}$, Lemma 2.28 implies that $c(B) = 13$, a contradiction. So, $|B_0| = 2$. Then Lemma 2.32 applies to give a contradiction.

Case 3. $m(B^{\varphi}) = 1$. Then $B^{\varphi} = B_0$, $c(B) = 16$ and, from $(*)$, $m(B) = 16$ or 17. So, $B = \langle R, t \rangle$, where $R = B \cap \overline{Q(p)}$ and t is an involution. We have $|R| = 2^{15}$ or 2^{16}. Set $K_1 = N_{\overline{Q(p)}}(B)$, $K = K_1 B$. Then $|\overline{Q(p)} : K_1| \leqq 2$ and $|K_1 : R| = 2^8$; see $(**)$ and Corollary 2.30. By 2.14(i), there is $g \in C_1$ such that $B^g \leqq \overline{Q(p)}$ and $K^g \leqq \overline{S(p)}$. Set $2^a = |K_1^g : K_1^g \cap \overline{Q(p)}|$, $\bar{L} = K_1^g \cap \overline{Q(p)}$. Since $|[K_1, t]| = 2^7$ or 2^8 and $|K_1 : \bar{L}^{g^{-1}}| = |K_1^g : \bar{L}| = 2^a$, $|[\bar{L}^{g^{-1}}, t]| \geqq 2^{7-a}$. Since $\langle \bar{L}^{g^{-1}}, t \rangle^g \leqq \overline{Q(p)}$, we get $2^{7-a} \leqq 1$ or $a \geqq 7$. In particular, $K_1^g \nleqq \overline{Q(p)}$. So $K_1^g \in \mathscr{S}$ and since $m(K_1^g) + r \geqq 23 + 8 \geqq 24$, $K_1^g \in \mathscr{S}^*$. Therefore, one of the previous cases applies to K_1^g (as $m((K_1^g)^{\varphi}) = a \geqq 7$) and we get our contradiction.

Lemma 12.4. *In $G(p)$, $C(p)$ is the centralizer of $z(p)$, for all primes $p \geqq 5$.*

Proof. By Lemma 12.3 and [26] and the irreducible action of N_1 on the commutator quotient group of $Q(p) \cong Q$, $Q(p)$ is a Sylow 2-group of its normal closure N_p in C_1, and N_p is solvable of 2-length one. If $Q(p) \lhd N_p$, we are done by Lemma 12.1; so, let us assume that $Q(p) \ntriangleleft N$. Then $O_2(N_p) = \langle z(p) \rangle$. For some odd prime $r \neq p$, $[O_r(N_p), Q(p)] \neq 1$. Let R be a subgroup of $O_r(N_p)$ which is minimal with respect to being normalized by, but not centralized by, $C(p)$. Then R is a special r-group (modify the argument of [27], p. 181). If $C_R(Q(p)) \neq 1$, we contradict Lemma 12.1. So, $C_R(Q(p)) = 1$ and $R = [R, Q(p)]$ is elementary abelian. Thus, on R, $Q(p)$ acts by a collection of linear characters, which must form at least one nontrivial orbit under the action of $C(p)$. The orbits for $C(p)$ on the nonprincipal linear characters of $Q(p)$ have lengths 98,280, 8,292,375 and 8,386,560 (see the proof of Lemma 5.1 (iv)), whence $m(R) \geqq 98{,}280$. The smallest degree of a representation for $R.C(p)$ over $\overline{\mathbb{F}}_p$ nontrivial on R is at least $2 \cdot 98{,}280 > 98{,}304 = \dim \overline{W(p)}$, a contradiction.

The proof is complete.

Lemma 12.5. *For all primes $p \geqq 5$, $G(p)$ is a simple group of order* $2^{46}3^{20}5^9 7^6 11^2 13^3 17.19.23.29.31.41.47.59.71$.

Proof. Lemmas 12.4, 2.16 and the fact that σ causes z and z_1 to fuse (this shows that conclusion (ii) of Lemma 2.16 does not hold in our case).

Proposition 12.6. *The group $G = \langle C, \sigma \rangle$ is simple of order* $2^{46}3^{20}5^9 7^6 11^2 13^3 17.19.23.29.31.41.47.59.71$.

Proof. Lemmas 12.5 and 2.33.

13. Consequences

From our construction of G, we may deduce existence of other sporadic simple groups and the existence of certain nonsplit group extensions.

In this section our dependency on the classification of finite simple groups increases. We also require work on F_1 and its subgroups done by other authors (some of this material is not yet published).

Notation 13.1. Let $G := \langle C, \sigma \rangle$, as in Sect. 12. We pick out certain elements $a \in C$ of odd order. It suffices to give the class of the element $a^{\hat{\pi}} \in \cdot 0$ in the notation of [12]. We do so with a subscript: a_{3A}, a_{5A}, etc.

Lemma 13.2. (i) $C_C(a_{3C}) \cong \mathbb{Z}_3 \times 2_+^{1+8} A_9$.

(ii) $C_C(a_{3D}) \cong (\mathbb{Z}_3 \times 2_+^{1+12}) 3U_4(3)2$.

(iii) $C_C(a_{5C}) \cong \mathbb{Z}_5 \times (2_+^{1+8})(A_5 \wr \mathbb{Z}_2)$.

(iv) $C_C(a_{7B}) \cong \mathbb{Z}_7 \times (2_+^{1+6}) GL(3, 2)$.

(v) $C_C(q(\lambda)) \cong (\mathbb{Z}_2 \times 2_+^{1+22})(\cdot 2)$, *for* $\lambda \in \Lambda_2$.

Proof. For the first four assertions, see [11, 12]. The last statement follows from [11], p. 240, or [36].

Remark. It would take additional work to determine the precise isomorphism types of the groups in 13.2. From [12], these groups are 2-constrained.

Lemma 13.3. *The groups $C_G(a)/\langle a \rangle$ of Lemma* 13.2 *are all simple (for $a = a_{3C}$, etc.). Their orders are as follows:*

(i) $2^{15}3^{10}5^3 7^2 13.19.31$ (*Thompson's group F_3*),

(ii) $2^{21}3^{16}5^2 7^3 11.13.17.23.29$ (*Fischer's group F_{24}'*),

(iii) $2^{14}3^6 5^6 7.11.19$ (*the Harada-Norton group F_5*),

(iv) $2^{10}3^3 5^2.7^3.17$ (*Held's group, Held*),

(v) $2^{41}3^{13}5^6 7^2 11.13.17.19.23.31.47$ (*Fischer's $\{3, 4\}$-transposition group, F_2*).

Proof. Since we have not determined the precise isomorphism types of the groups in 13.2, we get the conclusions most quickly by referring to the solution of the so-called "O_2 extraspecial problem" from the classification theory. For a discussion of this problem, we refer to survey articles [62], p. 111, and [73] and the references contained therein.

In all these cases we must eliminate the trivial possibility $C_G(a) = O(C_G(a))\, C_C(a)$. This can be done if we can take a conjugate of a in C which lies in the group H of Sect. 10 (because $H \leqq C_C(\sigma)$ and $z^\sigma = zz_1$). This is clear for (ii), (iii), (iv) and (v). For (i) it can not be done. Instead, we replace σ by $\sigma' \in O_2(X)\sigma$ such that $|C_X(\sigma')|_3 = 3^3$ (such σ' exist because a Sylow 3-group of X has order 3^3 and must centralize an element of the coset $O_2(X)\sigma$). Taking $a = a_{3C} \in C_X(\sigma')$, we get $\sigma' \in C_G(a) \not+ O(C_G(a))\, C_C(a)$, as required.

Finally, we must show that $C(a_{7B})/\langle a_{7B}\rangle$ is not isomorphic to M_{24} or $GL(5, 2)$ (these groups have some involutions whose centralizers are isomorphic to one in Held [41]). Take $b \in C$, b conjugate to a_{3D}, such that $a^b = a^2$, $a = a_{7B}$, $[C_C(a)', b] = 1$. If $C(a)/\langle a\rangle \cong M_{24}$ or $GL(5, 2)$, the structure of $\mathrm{Aut}(C(a)/\langle a\rangle)$ implies that $C(a)/\langle a\rangle$ is embedded in $C_G(b) \cong 3\,.\,F'_{24}$, a perfect group. Since $31 \in \pi(GL(5, 2)) - \pi(3\,.\,F'_{24})$, $C(a)/\langle a\rangle \ncong GL(5, 2)$. Suppose $C_G(a)/\langle a\rangle \simeq M_{24}$. Since a is a rational element of C [12] and since $\mathrm{Out}(M_{24}) = 1$ [4], there is an involution $t \in C_G(L(C_G(a))) \cap C_G(b)$ such that $a^t = a^{-1}$. It follows that $C_G(t)/\langle t\rangle$ contains a subgroup isomorphic to $\mathbb{Z}_3 \times \mathrm{M}_{24}$, a contradiction to [12, 22] and Lemma 2.41.

Remark. It seems reasonable that, with our representation of G on B and knowledge of $|G|$, a reasonably direct calculation of these orders would be possible.

By studying local subgroups of G, one can find sporadic simple groups other than the ones listed above. However, we cannot claim new existence proofs of them since they are involved in $\cdot 1$ or F'_{24} in natural ways, and their description involves only the groups $\cdot 1$ or F'_{24} rather than F_1. See Table 14.1 for a description of involvement of sporadic groups in one another.

The embedding of Held into F'_{24} was first proved by Simon Norton in 1975 [53] by studying linear groups of dimension 783 over $\mathbb{Q}(e^{2\pi i/3})$. Such an embedding was suspected to exist by Fischer about 1970. The existence of F_1 implies this embedding, because we may choose a_{3D} to normalize $\langle a_{7B}\rangle$ and to satisfy $C_C(\langle a_{7B}, a_{3D}\rangle) = C_C(a_{7B})'$ [12], [41]. The structure of Aut(Held) [38] implies that $C_G(a_{7B})' \leqq C_G(a_{3D})$.

We can also obtain embeddings of F_3 and $F_5 \cdot 2 \cong \mathrm{Aut}\, F_5$ [40] into $2F_2 = \hat{F}_2 \cong C_G(q(\lambda))$, $\lambda \in \Lambda_2$, by choosing appropriate involutions in C which invert a_{3C} and a_{5C}, respectively. To carry out these arguments, we require the discussion of fusion of involutions of C in G found in [36], mainly the fact that G has two classes of involutions; or see [22].

Say u is a 2-element in C inverting a_{3C}. Since $\mathrm{Out}(F_3) = 1$ [69], we may assume that $[L(C(a_{3C})), u] = 1$. So $|F_3|$ divides $|C(u)|$. Since $19 \mid |F_3|$ but $19 \nmid |C|$, the involution of $\langle u\rangle$ lies in $2A$. If $|u| \geqq 4$, $\mathbb{Z}_3 \times F_3$ is embedded in F_2, against Lemma 2.41. So $|u| = 2$, and we have our embedding.

A similar argument does the job for a_{5C}, taking $u \in C$ so that $(a_{5C})^u = (a_{5C})^2$ and using $\mathrm{Out}(F_5) \cong \mathbb{Z}_2$.

A bit more care in selecting u yields an embedding of Σ_{10} into $F_4(2)$ [40, 53].

Remark. The next result shows that some interesting examples of nonsplit group extensions may be found among the subgroups of F_1. Of particular significance is 13.4(i) because, among all the known finite simple groups, only F_2 has not had its multiplier settled. In [36], an upper bound of $\mathbb{Z}_2$ was obtained for the multiplier. It was well known that, if F_1 exists, the multiplier of F_2 must be $\mathbb{Z}_2$. However, an independent construction of a nonsplit extension $1 \to \mathbb{Z}_2 \to \hat{F}_2 \to F_2 \to 1$ has not been done, and seems to be very difficult. See [35] for a recent commentary on the multiplier situation.

Fischer was the first to notice the nonsplit sequences of 13.4(ii). Kusefoglu [46, 47] has shown that $H^2(O(7,3), \mathbb{F}_3^7) \cong H^2(\Omega(7,3), \mathbb{F}_3^7) \cong \mathbb{F}_3$ and, moreover, has settled all $H^2(O^\varepsilon(n,3), \mathbb{F}_3^n)$ and $H^2(\Omega^\varepsilon(n,3), \mathbb{F}_3^n)$ except for $(n, \varepsilon) = (8, -)$. The only solid information we have about the degree 2 cohomology group for $(n, \varepsilon) = (8, -)$ is that it is nonzero (and 13.4(ii) is the only proof we know of).

The multiplier of F_{24}' was settled originally by Griess [33] and Norton [54], and that of ${}^2E_6(2)$ by Griess [32].

Proposition 13.4. (i) *The Schur multiplier of F_2 has order* 2, *and $C_G(q(\lambda))$, $\lambda \in \Lambda_2$, is a covering group of F_2.*

(ii) *There is a subgroup $E \cong \mathbb{Z}_3^8$ of G such that $E = C_G(E)$, $N_G(E)/E \cong O^-(8,3)$ and $1 \to E \to N_G(E) \to O^-(8,3) \to 1$ is nonsplit. Also, there is $E_1 \leqq E$, $|E_1| = 3$ so that $1 \to E/E_1 \to N_G(E) \cap N_G(E_1) \to O(7,3) \to 1$ is nonsplit.*

(iii) *The Schur multiplier of F_{24}' has order* 3.

(iv) *The Schur multiplier of ${}^2E_6(2)$ is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Proof. (i) In [36], it is shown that the Schur multiplier has order at most 2. Also, in [36] it is shown that the action of $\cdot 2$ on $\Lambda/2\Lambda$ is uniserial with Loewey factors of dimensions 1, 22, 1, in that order. Consequently, $1 \to \langle q(\lambda) \rangle \to C_G(q(\lambda)) \to F_2 \to 1$ is a nonsplit extension, and (i) follows.

(ii) Take $A \leqq C$ such that $|A| = 3$, $C_Q(A) = \langle z \rangle$ and $N_C(A) \cong 2 \cdot 3 \cdot \mathrm{Suz} \cdot 2$ [22, 36]. From [36], $N_C(A)' = C_C(A) = 6 \cdot \mathrm{Suz}$ is perfect. By [19, 60], $N_G(A) = O(N_G(A)) \cdot N_G(A\langle z \rangle)$ and $O(N_G(A))/A$ must be abelian and is inverted by z.

If $O(N_G(A)) > A$, $N_C(A)/A$ acts faithfully on $O(N_G(A))$. We argue that this is the case. Since we know $|G|_3 = 3^{20}$, we shall get $O_3(N_G(A)) > A$ by Sylow's theorem. Let $R \leqq N_C(A)$, $R \cong \mathbb{Z}_3^6$ so that $N_{N_C(A)}(R)/C_C(R) \cong M_{11}$. Since R has a 4-dimensional $\mathbb{F}_3 A_6$-constituent in common with the usual 6-dimensional permutation module for $\mathbb{F}_3 A_6$ [11], where we take $A_6 \leqq M_{10} \leqq M_{11}$, identified with $N_{N_C(A)}(R)/C_C(R)$, we get that R is the J-subgroup ([27], p. 271) of $P \in \mathrm{Syl}_3(N_{N_C(A)}(R))$. Thus, R is characteristic in P, and so $|N_G(R)|_3 > |P| = 3^8$. Since $\langle z \rangle \in \mathrm{Syl}_2(C_G(R))$, a Frattini argument shows that C covers $N_G(R)/C_G(R)$, giving $|N_G(R)/C_G(R)|_3 = 3^2$ and $|C_G(R)|_3 > 3^6$. The structure of $N_G(A)$ given above shows that $O_3(N_G(A)) > A$, as required.

If $p \in \pi(O(N_G(A)))$, the p-rank of $O(N_G(A))/A$ must be at least 8 since a subgroup $T \cong 2_-^{1+6}$ of $N_C(A)$ acts faithfully on $O(N_G(A))/A$. Since $|G| = 2^{46} 3^{20} 5^9 7^6 11^2 13^3 m$ where m is squarefree, we have $p = 3$ or 5. If $p = 5$, we observe that the faithful action of a $3^5 M_{11}$ subgroup of $N_C(A)/A$ on $O_{3'}(O(N_G(A)))$ forces the 5-rank to be at least 11, a contradiction. So $O(N_G(A)) = O_3(N_G(A))$. Since $t \in Z(T)^{\#}$ fuses in $N_G(A)$ to an element $t' \in \langle T, z\rangle - Z(\langle T, z\rangle)$ (see Lemma 2.10 and [25]), a comparison of the traces of t and t' shows that $m(O_3(N_G(A))/A) \geqq 12$. Since $|G|_3 = 3^{20}$ and $|\mathrm{Suz}|_3 = 3^7$, we get $|O_3(N_G(A))| = 3^{13}$. We claim that $O_3(N_G(A))$ is extraspecial. Suppose false. Then the action of z implies that $O_3(N_G(A)) \cong \mathbb{Z}_3^{13}$ and that $N_G(A)$ leaves $C_{O_3(N_G(A))}(z)$ and $[O_3(N_G(A)), z]$ invariant; in particular, a Sylow 3-group of $N_G(A)$ has noncyclic center. By looking in F'_{24}, we find that a Sylow 3-normalizer looks like $3^{1+10} U_5(2) \cdot 2$ [20] and that in $C(a_{3D}) \cong 3F'_{24}$ the corresponding subgroup is $K = (3 \times 3^{1+10}) U_5(2) \cdot 2$ [33]. If $P \in \mathrm{Syl}_3(K)$, $Z(P) \cong \mathbb{Z}_3^2$. Our remarks about $N_G(A)$ then imply that $Z(P)$ is in the center of a Sylow 3-group of G, a contradiction to $|C(a_{3D})|_3 = 3^{17} < |G|_3$. So $O_3(N_G(A))$ is extraspecial.

Take $B \leqq N_C(A)$ so that $C_C(\langle A, B\rangle)$ is the perfect group $2 \cdot 3 \cdot 3 \cdot U_4(3)$ and such that A and B are conjugate in C. Set $R = O_3(N_G(A))$. Since $N_G(A)$ is 3-constrained, $C_C(\langle A, B\rangle)$ acts nontrivially on $C_R(B)$ ([27], p. 179). Therefore, if $3^k = |C_R(B)/A|$, $k \geqq 6$ because $7 \nmid |GL(5, 3)|$. So, $C_R(B) \simeq \mathbb{Z}_3^7$ and $[R, B] = C_R(B)$. Set $E = \langle C_R(B), B\rangle \cong \mathbb{Z}_3^8$. In each of $N_{N_G(X)}(E)$, $X = A$ or B, the group of automorphisms effected on E is $3^6 \cdot SO^-(6, 3) \cdot 2 \cdot 2$ (to see this, look at the normal 3-subgroups of $O_3(C_G(X))\, C_C(\langle A, B\rangle)$, $X = A, B$). Thus $Y := N_G(E)/C_G(E)$ satisfies $O_3(Y) = 1$ and $F^*(Y)$ quasisimple. To identify Y, the quickest method is to quote the standard form problem for $L(C_Y(zC_G(E))) \cong SO^-(6, 3) \cong 2 \cdot U_4(3)$ to get $Y \simeq O^{\varepsilon}(8, 3)$, $\varepsilon = +$ or $-$ [3]. If the extension $1 \to E \to N_G(E) \to Y \to 1$ were split,

$$1 \to \langle A, B\rangle \to C_G(\langle A, B\rangle) \to 2U_4(3) \to 1$$

would be split, which is not the case. Therefore, $\varepsilon = -$ (if ε were $+$, $Z(Y) \simeq \mathbb{Z}_2$ by [2], p. 196, and the extension would be split) and we get the first part of (ii). The second part follows by considering the preceding statements and realizing that we may take $a_{3D} \in \langle A, B\rangle - (A \cup B)$.

(iii) In [33], it is shown that the Schur multiplier of F'_{24} has order at most 3. We get that $1 \to \langle a_{3D}\rangle \to C_G(a_{3D}) \to F'_{24} \to 1$ is nonsplit from the fact that $a_{3D} \in C_C(a_{3D})'$; see above remarks.

(iv) It is relatively easy to see that $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ is an upper bound for $H^2({}^2E_6(2), \mathbb{Q}/\mathbb{Z})$ [32]. The hard part of settling this Schur multiplier is to show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the 2-part of the multiplier. We do this as follows. Let i, j, k be distinct indices in Ω, and let $V = \langle q(\lambda_{ij'}, \lambda_{jk'})\rangle \leqq Q$. Then $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $V^{\#}$ is in the class $2A$; see Lemma 13.3(v). Set $M = C_C(V)$. Then $M/M \cap Q \cong U_6(2)$ [11] and $M \cap Q \cong 2_+^{1+20} \times 2 \times 2$. We claim that $V \leqq [M \cap Q, M \cap C]$. Let $Y \geqq Q$, $Y \leqq C$ map onto the natural M_{21} subgroup of $N_{24}/\{\pm 1\}$ fixing i, j and k. Note that a natural M_{21} subgroup of M_{24} fixes a 2-dimensional submodule of $P(\Omega)_{\mathrm{even}}/\mathscr{C}$ but that this module has no trivial quotient module since a natural M_{21} fixes no $\mathscr{C}$-set other than Ω and ϕ. Thus, $\langle z, V\rangle \leqq \langle z, [E, Y]\rangle$ (this "E" is $q(\Lambda(4))$, as in earlier sections), implying the claim. Thus, $C_G(V)' = C_G(V)$.

We obtain $C_G(V)/V \cong {}^2E_6(2)$ from the solution of the "O_2 extraspecial" problem ([67], specifically), using $z^{\sigma} = zz_1$, $\sigma \in C_G(V)$ as before to eliminate the trivial case $C_G(V) = O(C_G(V))\, C_C(V)$.

The proof of Proposition 13.4 is complete.

Remark. From the existence of the perfect group $2.2.2E_6(2)$ one may derive the existence of the perfect groups $2.F_4(2)$, $2.2^2A_5(2)$, $2.F_{22}$, $2.2.A_2(4)$ and from the existence of the perfect group $3.F'_{24}$, one may derive the existence of the perfect groups $3.B_3(3)$, $3.G_2(3)$ as sections, which also occur within the group $3^8.O^-(8,3)$ of Proposition 13.4(ii). The existence of $\cdot 0$ implies the existence of a number of nonsplit extensions, as noted in [11].

More than ten years ago, Jack McLaughlin observed that the sporadic groups are connected with many examples of nonvanishing low degree cohomology. In F_3 we find Dempwolff's nonsplit extension $2^5.GL(5,2)$ [16] and in LyS we find the nonsplit extension $5^3.SL(3,5)$, which had been shown to exist abstractly by McLaughlin. For an example of nonvanishing degree 1 cohomology, look at a particular section of $\cdot 0$ isomorphic to $3^5.M_{11}$. Not only can we observe subgroups of sporadic groups which exhibit nonvanishing cohomology of degrees 1 and 2, but such examples in the groups of Lie type seem to be connected to sporadic phenomena which lead to sporadic groups. A "nonstandard" complement in $3^4.A_6 \leqq U_4(3)$ is contained in $L_3(4)$-subgroup of $U_4(3)$, and these two maximal subgroups of $U_4(3)$ are "tied together" by McLaughlin's group. We once observed that the "sporadic" nonvanishing of degree 1 cohomology for a group of Lie type seems to be connected to a "sporadic" maximal subgroups. For example, $A_7 \leqq A_8$ "explains" $H^1(\Omega^+(6,2), 2^6) \cong \mathbb{Z}_2$; see [57]. The most obvious examples of extensions in groups of Lie type are the parabolic subgroups. They split over the maximal normal unipotent subgroup by virtue of the Levi complement. In contrast, the candidates for "parabolic subgroups" in sporadic groups often involve nonsplit extensions. See [59]. However, it is not always true that $H^1(L,F)=0$ in a group G of Lie type, for L the commutator subgroup of a Levi complement and F an L-chief factor within the normal unipotent subgroup of a parabolic subgroup of G. There are a number of counterexamples, including infinite families of counterexamples, such as $L=Sp(2n,q)$, $F=\mathbb{F}_q^{2n}$, $G=Sp(2n+2,q)$, $q=2^m$, $n \geqq 2$ or $L=Sp(6,q)$, $F=\mathbb{F}_q^6$, $G=F_4(q)$, $q=2^m$.

It is tempting to think that the sporadic groups and the exceptional low degree cohomology groups are linked in some deep way. Because of the great importance of centralizers of involutions in the classification of finite simple groups, the occurrence of nonsplit central extensions of simple groups (classified by $H^2(-,\mathbb{Q}/\mathbb{Z})$) within sporadic groups strongly suggests that there is some connection. If there is a theory explaining such connections, the role in it of cohomology with coefficients in nontrivial modules is less clear.

For Sect. 14, we need a result.

Lemma 13.5. *Let $Qt \in C/Q$ be an involution.*

(i) *If Qt is 2-central, Qt contains involutions;*

(ii) *If Qt is not 2-central, Qt does not contain involutions if $C_{C/Q}(Qt)$ has shape $(2 \times 2 \times G_2(4))2$ and Qt does contain involutions if $C_{C/Q}(Qt)$ has shape $2^{11}.M_{12}.2$.*

Proof. Certainly, $C-Q$ contains involutions since $R_0^\sigma = R_1$ and $R_1 \cap Q = E$, in the notation of Chap. 10. In fact, R_1Q/Q corresponds to $O_2(N_{24}/\{\pm 1\})$ under the natural map $\phi: C \to \cdot 1$. Thus, Qt contains involutions if $C_{C/Q}(Qt) \cong 2_+^{1+8}.D_4(2)$ or $2^{11}M_{12}.2$.

Consider the remaining case. We refer to [11, 12] for the information we require about $\cdot 0$. Suppose t^ϕ is in the remaining class. Then $C(t^\phi) = (V \times L)\langle u \rangle$, $V \cong \mathbb{Z}_2^2$, $L \cong G_2(4)$, $|u| = 2$, and there is $V_1 \leqq L$, V_1 conjugate to V in C/Q. There is an element h of order 3 in $\cdot 1$ centralizing L and fixed point free on $\Lambda/2\Lambda$. In G, the structure of $C_G(\theta)$ for $\theta \in C$, $|\theta| = 3$ with $\theta^\phi = h$, is as described in the proof of 13.4(ii), i.e., $3^{1+12}.2.\mathrm{Suz}$. The structure of $2.\mathrm{Suz}$ implies that V_1 corresponds to a quaternion group of order 8 in $C(\theta)/O_3(C(\theta))$. Thus, Qt contains an element with square z. Since $\Lambda/2\Lambda$ is a free $F_2\langle t^\phi \rangle$-module (Corollary 2.30), Qt contains no involution, as required.

14. The Happy Family and the Pariahs

It is clear from Sect. 13 and a study of subgroups of F_2, F_{24} and $\cdot 1$ that we have 20 sporadic groups involved in the Friendly Giant. We call the set of sporadic groups which are involved in the Friendly Giant and *Happy Family*. There are 20 or 21 sporadics involved in the Happy Family - whether J_1 belongs or not is unsettled as of this writing. The sporadics outside the Happy Family are called the *Pariahs*. Since $\pi(\mathrm{LyS}) - \pi(F_1) = \{37, 67\}$ and $\pi(J_4) - \pi(F_1) = \{37, 43\}$, Lagrange's theorem implies that LyS and J_4 are Pariahs. It is not obvious how to show that J_3, $O'S$ and Ru are Pariahs. We do so in this section.

We conclude this section with a table of involvements of sporadic groups in one another and with a table giving fusion information for possible embeddings of J_1 in F_1.

Lemma 14.1. *Ru is a Pariah.*

Proof. Suppose that X is a quasi-simple subgroup of F_1, $X/Z(X) \cong Ru$. Then $|Z(X)| = 1$ or 2.

Suppose $Z(X) = \langle u \rangle$ has order 2. If u is 2-central, we get an embedding $Ru \to \cdot 1$, which is impossible since $29 \in \pi(\mathrm{Ru}) - \pi(\cdot 1)$. If u is not 2-central, we get an embedding $\mathrm{Ru} \to F_2$, which is impossible since $29 \in \pi(\mathrm{Ru}) - \pi(F_2)$.

We have $Z(X) = 1$. Take a four-group $V \leqq X$ so that $C_X(V) \cong \mathbb{Z}_2^2 \times Sz(8)$. Suppose that $v \in V^\#$ is 2-central in F_1. We may suppose that $v = z$, $C_X(V) \leqq C$. Since $13 \mid |Sz(8)|$, $C_X(V)$ fixes no element of $Q/\langle z \rangle$. Thus, $C_X(V)/\langle z \rangle$ is embedded in $\cdot 1$ and $Sz(8)$ is involved in the centralizer of an involution, t, of $\cdot 1$. A look at [12] shows that $13 \mid |C_{\cdot 1}(t)|$ implies $C_{\cdot 1}(t) \cong (\mathbb{Z}_2^2 \times G_2(4)) \cdot 2$. But 7 does not divide the order of a 2-local in $G_2(4)$, a contradiction. So $V^\#$ lies in the class of u, where $C_{F_1}(u) \cong 2F_2$. The centralizers of involutions in F_2 have shape $(2 \times 2 \times F_4(2))2$, $(2^{1+22})(\cdot 2)$, $2 \cdot {}^2E_6(2) \cdot 2$ and $2^9 \cdot 2^{16} \cdot D_4(2) \cdot 2$; see Lemma 2.41. Since $13 \mid |Sz(8)|$, we get an embedding of $Sz(8)$ into $F_4(2)$ or ${}^2E_6(2)$, a contradiction to Lemma 2.36.

Now take $B \lhd A \leqq F_1$ with $A/B \cong Ru$ and $|A|$ minimal. By the Frattini argument, B is nilpotent. Since the Schur multiplier of Ru is $\mathbb{Z}_2$, minimality of

A implies that $O(B) \leqq [B, A]$. Let $\pi = \pi(B)$, $\pi_1 = \pi - \{2\}$. The action of $H \leqq A/B$, $H \cong 2^6 \cdot G_2(2)$, on B/B' shows that $m_p(B/B') \geqq 63$ for $p \in \pi_1$, whence $\pi_1 = \phi$ and $\pi = \{2\}$. Since the order of 2 modulo 29 is 28, $m_2(B/B') \geqq 28$. Since 29 does not divide $|\cdot 1|$ or $|F_2|$, an element of order 29 is fixed point free on B. Since $|F_1|_2 = 2^{46} < 2^{56}$, $B \cong \mathbb{Z}_2^{28}$. Take $h \in A$, $|h| = 13$. Then $B_1 := C_B(h)$ has order 2^4 or 2^{16}. Let $x \in B_1^{\#}$. If x is 2-central in F_1, we may assume that $x = z \in Z(C)$. Then $\langle B_1, h \rangle \leqq C$ and h fixed point free on Q/Q' imply that the centralizer of an element of order 13 in $\cdot 1$ contains a copy of $\mathbb{Z}_2^3$ a contradiction [12]. So x is in the class $2A$, implying that F_2 contains a copy of $\mathbb{Z}_2^3$ whose centralizer has order divisible by 13. Since the centralizers of involutions in F_2 look like $2 \cdot {}^2E_6(2) \cdot 2$, $(2^{1+22})(\cdot 2)$, $(2 \times 2 \times F_4(2))2$ and $2 \cdot 2^8 \cdot 2^{16} \cdot D_4(2) \cdot 2$ and 13 does not divide the order of $D_4(2)$ or of a parabolic subgroup of ${}^2E_6(2)$, we have a contradiction. The proof is complete.

Definition 14.2. Let X, Y be a pair of finite groups. An (X, Y)-*fusion pattern* is a class function $f\colon X \to Y$ such that x and $f(x)$ have the same order, for all $x \in X$. The *fusion pattern test for the fusion pattern* f is the test that $x \mapsto \chi(f(x))$ be a character of X, for all irreducible characters χ of Y.

Note that these tests are lengthy but mechanical in nature. They can be verified in a straightforward way with a computer since one simply checks whether the inner product of $x \mapsto \chi(f(x))$ with every irreducible character of X is a nonnegative integer.

Lemma 14.3. *Exactly* 18 *fusion pattern tests for* (J_1, F_1) *are satisfied. If* J_1 *is involved in* F_1, *it is contained in* F_1.

Proof. The fact that fusion pattern tests for (J_1, F_1) are passed by exactly 18 fusion patterns has been established by Charles C. Sims and Steven D. Smith, independently, with computer programs. These fusion patterns are listed in Table 14.2.

To prove the second statement, we assume that J_1 is involved in but not contained in F_1, then derive a contradiction.

Take $B \lhd A \leqq G \cong F_1$, $A/B \cong J_1$, $|A|$ minimal. Then, by the Frattini argument, B is nilpotent. By the fact that J_1 has trivial Schur multiplier [35], [43], $B = [B, A]$. Let $\pi = \pi(B)$, $\pi_1 = \pi - \{2\}$. If $p \in \pi_1$, the action of a $2^3 \cdot 7 \cdot 3$ subgroup of A/B on $O_p(B)/\Phi(O_p(B))$ shows that $m_p(B/B') \geqq 7$, whence $p = 3$ or 5 by Lemma 12.6. The order of 3, 5 modulo 19 is 18, 9, respectively. Considering the action of an element of order 19, we get $m_p(B/B') \geqq 18$, 9 for $p = 3, 5$ respectively. If $p = 5$, we contradict Lemma 12.6. So $p = 3$, and we find that $m_3(B/B') \geqq 18$. So $|O_3(B)| = 3^{18}$ or 3^{19} as $|F_1|_3 = 3^{20}$ and $|J_1|_3 = 3$. The action of a $2^3 \cdot 7 \cdot 3$ subgroup on $O_3(B/B')$ shows that an element x of order 7 centralizes a subgroup B_1 of $O_3(B)$ with the property $m_3(B_1/B_1 \cap B') \geqq 6$ or $O_3(B)$ is elementary abelian of order 3^{19} (use the fact that 3 has order 6 modulo 7). In the former case, we quote the work of [22] to get $C(x) \cong \mathbb{Z}_7 \times \text{Held}$ or $7^{1+6}2A_7$; in either case a Sylow 3-group of $C(x)$ has order dividing 3^3, a contradiction. So $O_3(B) \cong \mathbb{Z}_3^{19}$. Thus, a Sylow 3-group of F_1 has an elementary abelian maximal subgroup. This is certainly false, since the section $C/O_2(C) \cong \cdot 1$ contains a subgroup $3^{1+4} \cdot Sp(4, 3)$. Therefore, $\pi_1 = \emptyset$, and B is a 2-group.

Let $\mathscr{A}$ be the set of $\mathbb{F}_2 J_1$-irreducible modules which occur as A-chief factors within B. If no module in $\mathscr{A}$ lies in the principal 2-block for J_1, the extension $1 \to B \to A \to J_1 \to 1$ splits, and we contradict Lemma 14.3. Thus, $\mathscr{A}_0 = \{X \in \mathscr{A} \mid X$ is in the principal 2-block$\}$ is nonempty. Since J_1 has trivial Schur multiplier, $\mathscr{A}_1 = \{X \in \mathscr{A}_0 \mid X$ is not the trivial module$\}$ is nonempty. By Lemma 2 $\mathscr{A}_0$, $\dim X = 20$ for $X \in \mathscr{A}_1$. Let $x \in A$, $|x| = 19$. From [22] and since the order of 2 modulo 19 is 18, $\dim C_X(x) = 2$, and $B \cong \mathbb{Z}_2^{20}$. Set $V = C_B(x)$, $B_1 = [B, x]$. Then $C_G(V) \cong 2 \cdot 2 \cdot {}^2E_6(2)$ and $B_1 \langle x \rangle$ maps to a 2-local of $C_G(V)/V \cong {}^2E_6(2)$. This is a contradiction since 19 does not divide the order of any parabolic subgroup of ${}^2E_6(2)$.

Lemma 14.4. J_3 *is a Pariah.*

Proof. Suppose that X is a quasisimple subgroup of $G \simeq F_1$ with $X/Z(X) \simeq J_3$; then $|Z(X)| = 1$ or 3 [52], [35]. If $|Z(X)| = 3$, $19 \in \pi(J_3) \cap \pi(C_G(Z(X)))$ implies that $C_G(Z(x)) \simeq \mathbb{Z}_3 \times F_3$ [12], a contradiction since $Z(X) \leqq X'$. So, $Z(X) = 1$.

The following statement was kindly supplied by Steven D. Smith, who used the character table of J_3 from Janko's paper [44] and the class list and certain characters ("head characters") of F_1 found in Conway and Norton's paper [13]:

We used simple FORTRAN programs at the IBM 370 installation at the California Institute of Technology to study (J_3, F_1) fusion patterns.

For convenience, the calculation was done in three stages. First, for each fusion pattern, the power map in F_1 was applied and the result checked for agreement with the power map of J_3; just 156 patterns survived this test. Then for these patterns a "crude" character-theoretic test was applied - computing the sums only modulo $|J_3|$ for the inner products (χ_{J_3}, η) with χ the 196,883-character of F_1, and η each irreducible character of J_3 (in effect, requiring χ_{J_3} to be a generalized character). Just 84 patterns survived this test. Finally for these patterns the multiplicities (χ_{J_3}, η) were computed in full, and required to be nonnegative integers; and just 12 patterns remained. (These 12 patterns were then tested with the next-larger F_1-irreducible, and all survived.) As a precaution, several of the computed multiplicities were re-verified by hand.

From this work of Smith, we know that the involutions of X must be conjugate in G to z, that all elements of order 5 in X are 5-central in G and that all the elements of order 3 are 3-central in G. These facts will suffice to obtain a contradiction.

We may assume that $z \in X$. Take $h \in C_X(z)$, $|h| = 3$. Then $C_X(h) \cong \mathbb{Z}_3 \times A_6$. We have $C_G(h) \cong 3^{1+12}.2.\mathrm{Suz}$. Take $S \leqq C_G(h)$, $S = 6.\mathrm{Suz}$. Then $L{:} = S \cap O_3(C_G(h))\, C_X(h)' \cong \mathbb{Z}_3 \times A_6$ or $3.A_6$. Since elements of order S in X lie in the class $5B$ of G (the 5-central class), the same is true of elements of order 5 in L. Thus, if $S \leqq \cdot 0$ is the natural embedding, and $y \in L$, $|y| = 5$, y is either 5-central in $\cdot 0$ or fixed point free on the Leech lattice. A look at the class list [12] reveals that $y \in S$ implies y acts fixed point freely on Λ. Let M be a natural 12 dimensional module for $\mathbb{C}S$. Since the traces lie in $\mathbb{Q}(e^{2\pi i/3})$, the remarks about y imply that the irreducible $\mathbb{C}L$-constituents or M have degrees divisible by 4. A look at the character tables of A_6 and $3.A_6$ shows that all these conditions may not be met. Therefore, G contains no subgroup isomorphic to J_3.

Suppose that $B \lhd A \leqq F_1$, $A/B \cong J_3$ and $|A|$ minimal. Then, by the Frattini argument, B is nilpotent. Since the multiplier of J_3 is $\mathbb{Z}_3$ [52], [35], $O_{3'}(B) \leqq [B, A]$. Also, $\pi(B/[B, A]) \subseteq \{3\}$ by minimality of A. Let $\pi = \pi(B)$, $\pi_0 = \{p \in \pi \mid p > 2$ and $[O_p(B), A] \neq 1\}$. Considering the action of a $2^4(3 \times A_5)$ subgroup of A/B on $O_p(B/B')$, we find that $m_p(B/B') \geqq 15$ for $p \in \pi_0$. Thus, $\pi_0 \subseteq \{3\}$. Suppose $\pi_0 = \{3\}$. Then $|J_3|_3 = 3^5$ implies that $O_3(B) \cong \mathbb{Z}_3^{15}$. Since the order of 3 modulo 19 is 18, we have a contradiction. Suppose $2 \in \pi$. Then, considering the action of a $3^2 \cdot 3 \cdot 3^2 \cdot 8$ subgroup of A/B on $O_2(B)$, we get $m_2(B/B') \geqq 24$. Since an element of order 19, 17 in F_1 has centralizer of shape $\mathbb{Z}_{19} \times A_5$ and $\mathbb{Z}_{17} \times L_2(7)$, respectively (see [22]) we get $m_2(B/B') \geqq 36, 40$, then $m_2(B/B') \geqq 54$, and a contradiction. The proof is complete.

Lemma 14.5. *$O'S$ is a Pariah.*

Table 14.1. Involvement of Sporadic Groups in One Another

($* =$yes, $\cdot =$no, ? $=$unsettled)

	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	J_1	$J_2=HJ$	J_3	Held	HiS	McL	Suz	·1	·2	·3	F_{22}	F_{23}	F'_{24}	LyS	Ru	$O'S$	F_2	F_1	F_3	F_5	J_4
M_{11}	*	*	·	*	*	·	·	·	·	*	*	*	*	*	*	*	*	*	*	·	?	*	*	·	*	*
M_{12}	·	*	·	·	*	·	·	·	·	·	·	*	*	·	*	*	*	*	·	·	·	*	*	·	*	*
M_{22}	·	·	*	*	*	·	·	·	·	*	*	·	*	*	*	*	*	*	*	·	?	*	*	·	*	*
M_{23}	·	·	·	*	*	·	·	·	·	·	·	·	*	*	*	·	*	*	·	·	·	*	*	·	·	*
M_{24}	·	·	·	·	*	·	·	·	·	·	·	·	*	·	·	·	·	*	·	·	·	?	*	·	·	*
J_1	·	·	·	·	·	*	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	?	?	·	·	·
$J_2=HJ$	·	·	·	·	·	·	*	·	·	·	·	*	*	·	·	·	?	?	·	·	·	?	*	·	·	·
J_3	·	·	·	·	·	·	·	*	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
Held	·	·	·	·	·	·	·	·	*	·	·	·	·	·	·	·	·	*	·	·	·	·	*	·	·	·
HiS	·	·	·	·	·	·	·	·	·	*	·	·	*	*	*	·	·	·	·	·	·	*	*	·	*	·
McL	·	·	·	·	·	·	·	·	·	·	*	·	*	*	*	·	·	·	*	·	·	*	*	·	·	·
Suz	·	·	·	·	·	·	·	·	·	·	·	*	*	·	·	·	·	·	·	·	·	·	*	·	·	·
·1	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·	·	·	·	·	·	·	*	·	·	·
·2	·	·	·	·	·	·	·	·	·	·	·	·	*	*	·	·	·	·	·	·	·	*	*	·	·	·
·3	·	·	·	·	·	·	·	·	·	·	·	·	*	·	*	·	·	·	·	·	·	·	*	·	·	·
F_{22}	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	*	*	·	·	·	*	*	·	·	·
F_{23}	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	*	·	·	·	*	*	·	·	·
F'_{24}	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·	·	*	·	·	·
LyS	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·	·	·	·	·
Ru	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·	·	·	·
$O'S$	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·	·	·
F_2	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	*	·	·	·
F_1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	·	·	·
F_3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	*	*	·	·
F_5	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*	*	·	*	·
J_4	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	*

Most of the involvements are "obvious" and many noninvolvements are easy to verify by looking at local information or standard representations. The referee has helped fill in the table and cites work of Enright which shows that M_{12} is embedded in $2F_{22}$ as the intersection of copies of $2F_{22}$ and Σ_{12} in F_{23}. The referee has furnished "character restriction" arguments as proof of the noninvolvements $(M_{12}, \cdot 2)$, (M_{24}, F_{23}), (J_2, F_{22}), (J_2, Ru), (J_2, F_{23}), (McL, F_5), (Suz, F'_{24}), (Suz, F_2). Thanks go also to Ronald Solomon for spotting an error in an early version of this table

Proof. Suppose that $X \leqq G \simeq F_1$, X quasisimple and $X/Z(X) \simeq O'S$. Let $Z \leqq X$, $Z \simeq \mathbb{Z}_4$ such that $C_X(Z)/Z(X)$ is the perfect group $4.L_3(4)$. Set $\langle t \rangle = \Omega_1(Z)$. If $C_G(t) \simeq 2F_2$, then Z maps to a group of order 2 with centralizer $(2 \times 2 \times F_4(2))2$ in F_2, a contradiction since $Z \leqq C_X(Z)'$. So, $C_G(t) \simeq C$ and we may as well take $t = z$. The structures of the centralizers of elements of order 2 in $\cdot 1$ [12] show that $Z \leqq Q$, so that $Z = \langle q(\xi) \rangle$, for some vector ξ of type 3. Thus, we have an embedding of $C_X(Z)Q/Q \simeq C_X(Z)/Z \simeq L_3(4)$ or $3.L_3(4)$ into $\cdot 3$. By [12], $C_X(Z)/Z \simeq L_3(4)$, i.e., $Z(X) = 1$. Let $K := C_X(Z)^{\hat{\pi}} \leqq \cdot 0$. Then $K' \simeq L_3(4)$ since the Schur multiplier of $\cdot 3$ is trivial [33, 35].

According to the character table of $L_3(4)$, there are two irreducible characters of degrees less than 24; they have degrees 1 and 20. So, $L := C_\Lambda(K')$ has rank 4 and is a $\mathbb{Z}$-direct summand of Λ. By looking at $P(\Omega)$, a module extension of $\mathscr{C}$ by $P(\Omega)/\mathscr{C}$, one sees that the modular irreducible constituents of the degree 20 irreducible taken modulo 2 have dimensions 1, 1, 9 and 9, and, in particular, if $h \in K$, $|h| = 7$, then $\dim C_{\Lambda/2\Lambda}(h) = 6$. Set $R := \langle q(C_\Lambda(h)) \rangle \simeq 2^{1+6}_+$. Since $R_1 := \langle q(L), z \rangle \leqq R$ and $|\mathrm{R}_1| = 2^5$, R_1 is nonabelian. Set $R_2 := \langle R_1, z \rangle \leqq R$. Since $\mathrm{Out}(R_2)$ is solvable or has every nonsolvable composition factor isomorphic to $L_3(2)$ or A_5, $[R_2, C_X(Z)] \leqq [R_2, R_2] \leqq \langle z \rangle$, whence $[R_2, C_X(Z)] = 1$ by the three subgroups lemma and $C_X(Z) = C_X(Z)'$.

We now obtain a contradiction. Since $L_3(4)$ is not involved in M_{11} and $\cdot 333 \simeq 3^5 \cdot M_{11}$, R_2 does not contain a quaternion group. Since R_1 is non-

Table 14.2. Fusion Maps for (J_1, F_1) (see Lemma 14.3)

Rational class for J_1 (designated by order of element):	1	2	3	5	6	7	10	11	15	19
Fusion pattern (class in F_1):	$1A$	$2B$	$3A$	$5A$	$6C$	$7A$	$10B$	$11A$	$15A$	$19A$
			$3A$	$5A$	$6C$	$7B$	$10B$		$15A$	
			$3B$	$5A$	$6B$	$7A$	$10B$		$15B$	
			$3B$	$5A$	$6B$	$7B$	$10B$		$15B$	
			$3B$	$5A$	$6E$	$7A$	$10B$		$15B$	
			$3B$	$5A$	$6E$	$7B$	$10B$		$15B$	
			$3B$	$5B$	$6B$	$7A$	$10D$		$15C$	
			$3B$	$5B$	$6B$	$7A$	$10E$		$15C$	
			$3B$	$5B$	$6B$	$7B$	$10D$		$15C$	
			$3B$	$5B$	$6B$	$7B$	$10E$		$15C$	
			$3B$	$5B$	$6E$	$7A$	$10D$		$15C$	
			$3B$	$5B$	$6E$	$7A$	$10E$		$15C$	
			$3B$	$5B$	$6E$	$7B$	$10D$		$15C$	
			$3B$	$5B$	$6E$	$7B$	$10E$		$15C$	
			$3C$	$5B$	$6F$	$7A$	$10D$		$15D$	
			$3C$	$5B$	$6F$	$7A$	$10E$		$15D$	
			$3C$	$5B$	$6F$	$7B$	$10D$		$15D$	
			$3C$	$5B$	$6F$	$7B$	$10E$		$15D$	

(Columns 1, 2, 11 and 19 are constant).

The referee has furnished a character restriction argument which eliminates the cases with $3A$ (one examines the 19-local structure of $\Sigma_3 \times F_3$)

abelian, $R_1 = R_2 \simeq D_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and any element of order 4 in R_1 is conjugate in R_1 to its inverse. Take $x \in R_1$ so that x inverts $Z \leqq R_1$ under conjugation. Then, $[C_X(Z), x] \leqq [C_X(Z), R_1] = 1$ gives a contradiction.

We are now left with the case that $O'S$ or its 3-fold cover are involved in F_1 but not by containment. We take $A \leqq F_1$ of minimal order with $B \lhd A$ so that $A/B \simeq O'S$. Then B is nilpotent and $[B, A] \leqq O_{3'}(B)$. Since J_1 is contained in $O'S$, we get a contradiction to this situation as follows. We repeat the arguments of Lemmas 14.3 to get $[B, A] \leqq O_2(B)$. Then $O_2(B) \neq 1$ and 2-constraint of A imply that an element x of order 19 in A acts nontrivially on B. Since $|C(x)| = 2^2.3.5.19$ [22], $|F_1|_2 = 2^{46}$, $|\mathcal{O}'S|_2 = 2^9$ and $46 - 9 < 2 \cdot 19$, we get $|B|_2 = 2^{18}$, 2^{19} *or* 2^{20}. But now, the nontrivial action of an extraspecial group of order 7^3 in A/B on B shows that $|B|_2 \geqq 2^{3 \cdot 7} = 2^{21}$, a contradiction.

15. Concluding Remarks

As stated in the introduction, work on the putative simple group F_1 began in November, 1973. Bernd Fischer suggested the possibility of a finite simple group having a 3-local subgroup of shape $3^{1+12}.2.\mathrm{Suz}.2$. A number of other group theorists got involved at this point, mainly Conway, Harada, Norton and Thompson. Many properties of this hypothetical simple group were derived, including shapes of various local subgroups and a correct guess of its order, using the result of Frobenius which says that the cardinality of $\{g \in G \mid g^n = 1\}$ is divisible by n, for any finite group G and integer dividing $|G|$ (a proof that its order is the number of Sect. 1 was written down by Griess [36]). The existence of several additional simple groups was derived (see Sect. 13). Coincidentally, Harada had been working on a standard form problem for a component of shape $2.\mathrm{HiS}$, exactly the situation which comes up in the group F_5. Norton's thesis was concerned with properties of F_5 and an existence and uniqueness proof (based on a complex representation of degree 133). The group of Thompson, F_3, was constructed by Thompson and Peter Smith, who did some computer work, as a linear group of degree 248. The group F_2, while noticed as a subquotient of F_1, had been proposed by Fischer during the summer of 1973 as a group generated by a class of $\{3, 4\}$-transpositions. Indeed, F_2 appeared to have a perfect central extension $2F_2$ and the possibility of a simple group having $2F_2$ and $C \simeq (2^{1+24}).(\cdot 1)$ as centralizers of involutions is what led this author to his investigations [37], independently of the work of the aforementioned individuals.

The group F_2 was constructed a few years later by Jeffrey Leon and Charles Sims with the aid of a computing machine [51].

Norton and others at Cambridge did some preliminary work on characters and conjugacy classes for F_1, notably the facts discussed in Sect. 1. Ultimately, combined work of Fischer, Livingstone and Thorne led to a complete determination of the character table[1]. It must be pointed out that all this work

[1] It should be pointed out that the notations for conjugacy classes in [13] and [22] differ; we use that of [13] in this paper

was made under the assumption that F_1 has an irreducible complex character of degree 196,883. That 196,883 is a lower bound for the degree of a nontrivial complex character was pointed out by Griess [37] and was also noticed by Conway and Norton [13].

Norton has recently announced a uniqueness proof of F_1. He studied a graph on the class of involutions $2A$ in which two distinct involutions are joined by an edge if and only if their product lies in $2A$ and found a matrix in the commuting algebra of the group action on the permutation module within an eigenvalue of multiplicity 196,883. It follows that any finite simple group with an involution whose centralizer is isomorphic to C must have an irreducible character of degree 196,883. Thus, the "hard" assumption of Thompson's uniqueness proof [71] is valid; formal proofs of the remaining assumptions should not be difficult to write out. Granting this, we summarize: A finite simple group which contains C as the centralizer of an involution must be isomorphic to the Friendly Giant.

The algebra B which figures so importantly in our construction of G is a somewhat mysterious object. We can state no homogeneous linear identity, linearly independent of $xy=yx$, which is satisfied by elements of B. The classical theories of linear algebras use such identities as starting points. In our case, we use an automorphism group as the starting point (and never stray too far from it). The presence of the algebra was a guide in defining G. Once we had $G \leqq G(B)$, the algebra was used only to make a few points in Sect. 12.

After Norton's finding (see Sect. 1), some attention was directed to commutative nonassociative algebras with certain finite groups as automorphisms. Such algebras were irreducible as modules, or were the direct sum of a module and its dual, and were often connected to some rank 3 permutation representation of the group [54, 61]. The term "Norton algebra" has been applied to some of these examples. As with B, no axioms for these algebras were given and no characterizations were made. These investigations were interesting and encouraging but had no direct bearing on the discussion of B in this paper.

It is natural to ask whether any of the Pariahs (see Sect. 14) can be constructed explicitly as automorphisms of some kind of linear algebra. Indeed, Frohardt has completed such a construction of J_3; the algebra is commutative and nonassociative and is the direct sum of an 85-dimensional complex irreducible module with its dual. Similar constructions for the other Pariahs will surely be available in due course. One result will be more controlled settings in which to study the sporadic groups. Another will be that the theory of these groups will be relatively free of dependence on computers.

We conclude by expressing our hope that the ideas in this paper will lead to further methods for studying the finite simple groups.

List of Notations and Definitions

We give at least the first occurrences of notations used in this paper which are not in general use. Among the more standard definitions are $x^y = y^{-1}xy$, $[x, y] = x^{-1}y^{-1}xy$ for group elements x, y; ε_G, $\underset{G}{\leq}$, $\underset{G}{=}$ for membership, containment and equality, up to G-conjugacy; $|X|$ for the cardinality of X; $\mathrm{Sol}(G)$ for the largest solvable normal subgroup of G; $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Section 1
$X \,.\, Y$, a group extension with normal subgroup X and quotient Y
B
C
$G = \langle C, \sigma \rangle$
F_1
S^n, the n-th symmetric tensor power functor on modules
M_{24}
$\cdot 0$
Λ, the Leech lattice
Conway groups
F
β
Happy Family
Pariahs

Section 2
$\cdot 1$
$\Omega = \mathbb{F}_{23} \cup \{\infty\}$
$\mathscr{S} = \mathscr{S}(5, 8, 24)$
$P(\Omega)$, $P(\Omega)_{\text{even}}$
$\mathscr{C}$
$\bar{\mathscr{C}} = \mathscr{C}/\langle \Omega \rangle$
octad, dodecad, special 16-set
$ij\ldots$ in S
$\{x_i \mid i \in \Omega\}$
$(\, , \,)$
$\langle \, , \, \rangle$
N_{24}
ε_S
Λ_n
$\Lambda_2 = \Lambda_2^4 \cup \Lambda_2^2 \cup \Lambda_2^3$
$\tilde{L}$, $\tilde{\lambda}$, $\tilde{\Lambda}_2$
triangle of type abc
λ_i, $\lambda_{i,S}$, $\lambda_{i,x}$
λ_{ij}, $\lambda_{ij'}$
$i(\lambda)$
$\mathscr{O}$, $\mathscr{O}_\lambda$
$\operatorname{supp}(\lambda)$
$\operatorname{Pos}(\lambda)$, $\operatorname{Neg}(\lambda)$
$F(2)$
S_x, x_S
$\Lambda(n)$
$H^n(G, M)$, degree n cohomology
$m(X)$, the minimal number of generators of the group X
$c(X)$, $c_1(X)$
tetrad
Ξ, a sextet
weakly closed, strongly closed
λ_S, $\lambda_{\mathscr{O}}$

Section 3
p^{1+2n}, extraspecial p-group
2_ε^{1+2n}
$Q = EF$
$\langle z \rangle$
$e(x)$, $x \in F$
ϕ_x
A_ϕ
T

Section 4
q
C_∞
$\hat{C}$
C^*
C
C_0
U
V
W
C_2
$T(i)$, $i = 0, 2, 3, 4$
$V(\phi)$
π_1
π_∞
π_0
π
$\bar{\pi}$
$-$
$\hat{\pi}$
E_0
λ_x
u_{ij}
$u : S^2(\mathbb{Q} \otimes \Lambda) \xrightarrow{\sim} U$
$\underline{\underline{d}}$
u_0
U_0

Section 5
$\langle A_1, A_2 \rangle$
ϕ_λ
x_λ
$v(\lambda) = v(\tilde{\lambda})$
$p(u, x)$
$\beta'(\lambda, \mu)$

Section 6
$\beta(\lambda, \mu)$

Section 7
$E_0 = C_E(e(1))$
$E(2)$
z_1
X
$F(2)$
S_λ, $\lambda \in \Lambda(2)$
S_x, x_S
h
$\mathscr{Q}$, $\mathscr{Q}^x$
$\mathscr{N}$, $\mathscr{N}^x$
$\mathscr{D}$
E_1

θ
s
J
L
Q_0
Q_1
s_0
F
Γ_1, Γ_2
J_1, J_2
λ_x
$\Delta(2, 2)$, $\Delta(2, 3)$
$J(i, S)$
$\gamma(i, S)$
$E(v, \mathscr{D}, \varepsilon)$
$E(\lambda)$
$E^*(\lambda)$
$i(\Delta_\eta)$
E_*
s_1
$\delta(\lambda, \mu)$

Section 8
z_1
P
$\hat{z}$
$\hat{E}$
$x \circ g$
i^g, $i \in \Omega$, $g \in N_{24}$
N_{23}
$\tau = q(\lambda_\infty)$
$a(x, i, g)$, $a_T(x, g)$, $a_\Lambda(i, g)$
g_S
$b(\lambda, g)$
S_g, $g \in O_2(P)$
S_λ, $\lambda \in \Lambda_2^2 \cup \Lambda_2^4$

Section 9
$u(x, g)$, $v(x, g)$

Section 10
σ
N
N_0
$v_{\iota j}$, $v_{\iota j'}$
B_{24}, B_{276}, $B_2^{4,+}$, $B_2^{4,-}$, B_2^2, B_2^3,
B_{even}, B_{odd}
R_0
N_0
R
R_1
$d(\lambda_{\iota, x})$
H_∞
F-triple

Section 11
λ over S, the coordinates
of λ indexed by $S \subseteq \Omega$

Section 12
$G = \langle C, \sigma \rangle$
$G(p)$, $C(p)$, $z(p)$
$B(p)$
C_1, N_1
weakly closed, strongly closed

Section 13
a_{3A}, a_{5A}, etc.
F_1, F_2, F_3, F_5
F_{22}, F_{23}, F_{24}
Held
$\pi(G)$, the set of prime divisors of $|G|$

Section 14
(X, Y)-fusion pattern
fusion pattern test

Section 15
class of $\{3, 4\}$-transpositions
Norton algebras

List of Tables

References

1. Alperin, J., Gorenstein, D.: A vanishing theorem for cohomology. Proc. Amer. Math. Soc. **32**, 87–88 (1972)
2. Artin, E.: Geometric Algebra. New York: Interscience 1957
3. Aschbacher, M.: private communication
4. Aschbacher, M., Seitz, G.: On groups with a standard component of known type. Osaka J. Math. **13**, 439–482 (1976)
5. Borel, A.: Seminar on algebraic groups and related finite groups. Lecture Notes in Mathematics, vol. 131. Berlin-Heidelberg-New York: Springer 1973
6. Brauer, R., Nesbitt, C.: On the modular representation of groups of finite order, I, University of Toronto Studies, No. 4, 21 pp. (1937)
7. Burgoyne, N., Fong, P.: Schur multipliers of the Mathieu groups. Nagoya Math. J. **27**, 733–745 (1966); Correction, ibid **31**, 297–304 (1968)
8. Burgoyne, N., Griess, R., Lyons, R.: Maximal subgroups and automorphisms of Chevalley groups. Pacific J. of Math. **71**, 365–403 (1977)
9. Carter, R.: Simple groups of Lie type. New York: Wiley - Interscience 1972
10. Conway, J.: A group of order 8, 315, 553, 613, 086, 720, 000. Bull. L.M.S. **1**, 79–88 (1969)
11. Conway, J.: Three lectures on exceptional groups in Higman-Powell, pp. 215–247. Finite simple groups. London: Academic Press 1971
12. Conway, J., Guy, M., Patterson, N.: The characters and conjugacy classes of $\cdot 0$, $\cdot 1$, $\cdot 2$, $\cdot 3$ and Suz. unpublished
13. Conway, J., Norton, S.: Monstrous moonshine. Bull. London Math. Soc. **11**, 303–339 (1979)
14. Curran, P.: Fixed point free action on a class of abelian groups. Proc. Amer. Math. Soc. **57**, 189–193 (1976)
15. Curtis, C., Reiner, I.: Representation theory of finite groups and associative algebra. New York: Interscience 1962
16. Dempwolf, U.: On extensions of an elementary abelian group of order 2^5 by $GL(5, 2)$, Rendiconti del Seminario Matematico della Universita di Padova **48**, 359–364 (1973)
17. Dickson, L.E.: Linear groups. New York: Dover 1968
18. Dieudonne, J.: La geometrie des groups classiques. Berlin-Heidelberg-New York: Springer 1971
19. Finkelstein, L., Solomon, R.: Standard components of type M_{12} and .3. Osaka J. Math. **16**, 759–774 (1979)
20. Fischer, B.: Private correspondence. 1971
21. Fischer, B.: Privately circulated note. 1973
22. Fischer, B., Livingstone, D., Thorne, M.P.: The character table of F_1. unpublished
23. Fong, P.: On decomposition numbers of J_1 and $R(q)$, Instituto Nazionale di Alta Mathematica, Symposia Mathematica, volume XII, 415–422 (1973)
24. Gilman, R., Griess, R.: A characterization of finite groups of Lie type in characteristic 2. submitted to J. of Algebra
25. Glauberman, G.: Central elements in corefree groups. J. of Algebra **4**, 403–420 (1966)
26. Goldschmidt, D.: 2-fusion in finite groups. Annals of Math. **99**, 70–117 (1974)
27. Gorenstein, D.: Finite Groups. New York: Harper and Row 1968
28. Gorenstein, D., Walter, J.: The characterization of finite groups with dihedral Sylow 2-subgroups, I, II and III. J. of Algebra **2**, 85–151; 218–270; 354–293 (1965)
29. Griess, R.: A construction of F_1 as automorphisms of a 196,883 dimensional algebra. Proc. Natl. Acad. Sci. USA **78**, 689–691 (1981)
30. Griess, R.: A subgroup of order $2^{15}|GL(5,2)|$ in $E_8(\mathbb{C})$, the Dempwolff group and $\mathrm{Aut}(D_8 \circ D_8 \circ D_8)$. J. of Algebra **40**, 271–279 (1976)
31. Griess, R.: Automorphisms of extra special groups and nonvanishing degrees 2 cohomology. Pacific J. of Math. **28**, 403–422 (1973)
32. Griess, R.: Schur multipliers of finite simple groups of Lie type. Trans. Amer. Math. Soc. **183**, 355–421 (1973)
33. Griess, R.: Schur multipliers of some sporadic simple groups. J. of Algebra **32**, 445–466 (1974)
34. Griess, R.: Schur multipliers of the known finite simple groups I. Bull. Amer. Math. Soc. **78**, 78–71 (1972)

35. Griess, R.: Schur multipliers of the known finite simple groups II, in the Santa Cruz Conference on Finite Groups, edited by B. Cooperstein and G. Mason
36. Griess, R.: Structure of the Friendly Giant. In preparation
37. Griess, R.: Structure of the monster simple group. Proceedings of the Conference in Finite Groups. New York: Academic Press 1976
38. Griess, R., Solomon, R.: Finite groups with unbalancing 2-components of $\{L_3(4), He\}$-type. J. Algebra **60**, 92–125 (1979)
39. Gruenberg, K.: Cohomological topics in group theory. Berlin-Heidelberg-New York: Springer 1970
40. Harada, K.: On the simple group F of order $2^{14}3^6 5^6.7.11.19$. Proc. of a Conference on Finite Groups, pp. 119–276
41. Held, D.: The simple groups related to M_{24}. J. Algebra **13**, 253–296 (1969)
42. Jacobson, N.: The theory of rings. Amer. Math. Soc., Providence 1943
43. Janko, Z.: A new finite simple group with abelian Sylow 2-subgroups and its characterization. J. of Algebra **3**, 147–186 (1966)
44. Janko, Z.: Inst. Natl. Alta Math. Symposia Math. Odensi, Gubbio, **1**, 25–64 (1968)
45. Jordan, C.: Traité des substitutions et des èquations algêbriques. Paris: Gauthiers-Villars 1870
46. Kusefoglu, A.: Cohomology of finite orthogonal groups. I: J. of Algebra **56**, 207–220; II: J. of Algebra **67**, 88–109 (1980)
47. Kusefoglu, A.: Thesis, University of Michigan 1976
48. Lang, S.: Algebraic groups over finite fields. Amer. J. of Math. **78**, 555–563 (1956)
49. Leech, J.: Notes on sphere packings. Can. J. Math. **19**, 251–267 (1967)
50. Leech, J.: Some sphere packings in higher space. Can. J. Math. **16**, 657–682 (1964)
51. Leon, J.S., Sims, C.C.: The existence and uniqueness of a simple group generated by $\{3, 4\}$-transpositions. Bull. Amer. Math. Soc. **83**, 1039–1040 (1977)
52. McKay, J., Wales, D.: The multipliers of the simple groups of order 604,800, and 50,232,960. J. of Algebra **17**, 262–272 (1971)
53. Norton, S.: Thesis, University of Cambridge 1975
54. Norton, S.: Transposition algebras and the group F_{24}, to appear
55. Niemeyer, H.V.: Definite Quadratische Formen der Diskriminante 1 und Dimension 24. Doctoral Dissertation, Göttingen, 1968
56. Patterson, N.J.: On Conway's group .0 and some subgroups. Thesis, University of Cambridge, 1972
57. Pollatsek, H.K.: Cohomology groups of some linear groups over fields of characteristic 2, Ill. J. of Math. **15**, 393–417 (1971)
58. Robinson, D.: The vanishing of certain homology and cohomology groups. J. of Pure and Applied Algebra **7**, 145–167 (1976)
59. Ronan, M.A., Smith, S.D.: 2-local geometries for some sporadic groups. The Santa Cruz Conference on Finite Groups, edited by B. Cooperstein and G. Mason. Amer. Math. Soc. Providence, 1980
60. Seitz, G.: Standard subgroups in finite groups. Finite simple groups II, M.J. Collins, (ed.). London: Academic Press 1980
61. Smith, S.: Nonassociative commutative algebras for triple covers of 3-transposition groups. Michigan Math. J. **24**, 273–287 (1977)
62. Smith, S.: The classification of finite groups with large extraspecial 2-subgroups. The Santa Cruz Conference on Finite Groups, edited by B. Cooperstein and G. Mason. Amer. Math. Soc., Providence, 1980
63. Smith, S.: Large extraspecial subgroups of width 4 and 6. J. of Algebra **58**, 251–281 (1979)
64. Steinberg, R.: Generators, relations, and coverings of algebraic groups II. to appear
65. Steinberg, R.: Lectures on Chevalley groups, lecture notes, Mathematics Department, Yale University
66. Steinberg, R.: Representation of algebraic groups. Nagoya Math. J. **22**, 33–56 (1963)
67. Stroth, G.: Eine Kennzeichnung der Gruppen ${}^2E_6(2^n)$. J. of Algebra **35**, 534–547 (1975)
68. Suzuki, M.: On a class of doubly transitive groups. Ann. of Math. **75**, 105–145 (1962)
69. Thompson, J.: A simple subgroup of $E_8(3)$. Finite Groups, Iwahori, N. (ed.). Japan Society for Promotion of Science, Tokoyo, 1976

70. Thompson, J.: Nonsolvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. **74**, 383–437 (1968)
71. Thompson, J.: Uniqueness of the Fischer-Griess monster. Bull. London Math. Soc. **11**, 340–346 (1979)
72. Timmesfeld, F.: Groups generated by root involutions. I, II. J. of Algebra **33**, 75–135 (1975); **35**, 367–441 (1975)
73. Timmesfeld, F.: Groups of $GF(2)$-type and related problems. Finite Simple Groups II, Collins, M.J. (ed.). London: Academic Press 1980
74. Todd, J.: A representation of the Mathieu group M_{24} as a collineation group. Annali di Mathematica Pura ed Applicata. **71**, 199–238 (1966)
75. Walter, J.: The characterization of finite groups with abelian Sylow 2-groups. Ann. of Math. **89**, 405–514 (1969)

Oblatum 4-VI-1981 & II-1982