Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 300 (2005) 571–589
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Constructing the Monster amalgam

A.A. Ivanov

Department of Mathematics, Imperial College, 180 Queen's Gate, London SW7 2BZ, UK

Received 4 July 2005
Available online 19 January 2006
Communicated by M. Aschbacher, G. Röhrle, and F. Timmesfeld

Dedicated to Professor Bernd Fischer on the occasion of his 70th birthday

Abstract

The Monster group M contains a pair $\{C, N\}$ of subgroups, where $C \sim 2^{1+24}_{+}.Co_1$ is the centralizer of an involution and $N \sim 2^{2+11+2\cdot 11}.(M_{24} \times Sym_3)$ is the normalizer of an elementary subgroup of order four with $N \cap C$ having index three in N. The amalgam $\{C, N\}$ plays an important role in the existing constructions and uniqueness proofs for the Monster. We suggest a transparent construction of this amalgam.

1. Introduction

The first evidence for the existence of the Monster group M was given independently by B. Fischer and R. Griess in 1973. During the 1970s a number of properties of the predicted group were unearthed (but mostly left unpublished) including (1) the lower bound 196,883 for the degree of a faithful complex representation; (2) the structure

$$C \sim 2^{1+24}_{+}.Co_1$$

of the centralizer in M of a central involution z and (3) the structure

E-mail address: a.ivanov@ic.ac.uk.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.08.039

$$N \sim 2^{2+11+2\cdot 11}.(M_{24} \times Sym_3)$$

of the normalizer in M of an elementary subgroup $\langle z, t\rangle$ of order 4 (here t is a conjugate of z contained in $O_2(C) \setminus Z(C)$).

In 1979 J.G. Thompson [13] has shown that the amalgam $\{C, N\}$ possesses (up to equivalence) at most one complex representation of degree 196,883. Thus he has established the uniqueness of the Monster subject to the condition that the lower bound for the minimal degree is attained.

In 1982 R. Griess [6] published an existence proof for the Monster which can be viewed as Thompson's uniqueness proof brilliantly transformed into a construction: Griess produces a 196,883-dimensional representation of C; adjoins an element σ which conjugates z to t and together with $C \cap N$ generates (a representation of) N and proves that the representations of C and N generate the Monster (inside the corresponding general linear group).

J. Tits [14] suggested extending $C \cap N$ to N in one go instead of adjoining a particular element σ. Starting with $C_C(t)$ (instead of $N \cap C$) one deals with a normal extension. In part III of [14] (where $D = C_C(t)$ and $D^\# = \{z_0, z_1, z_2\}$) it is stated as Proposition 1 that (i) every automorphism of D fixing each z_i is inner, and (ii) the group D possesses automorphisms permuting z_0, z_1, z_2 cyclically. After the proposition one reads 'The proof will be omitted in the present sketch, but I should emphasize that it does not necessitate the explicit construction of such an automorphism (it suffices for instance to give a characterization of D in which the z_i's play a symmetric role). Experience shows that explicit choices are a source of complications (e.g. sign complications).' We present here a proof of Tits' Proposition 1 which is indeed achieved via a characterization of $D/Z(D)$ from which the triality symmetry shows up.

J.H. Conway [2] gave a description of N in terms of Parker's loop. This description manifestly possesses a triality symmetry. Within Conway's approach the harder part of the construction lies within the identification of the two appearances of $C \cap N$ (as a subgroup of C and as a subgroup of N). Chapter 4 of M. Aschbacher's book [1] 'places the Conway construction in a larger context which hopefully makes the construction more natural and hence easier to understand.' We are trying to make a further step in this direction by showing that Parker's loop (at least its associator) can be recovered from the intrinsic structure of N.

It turns out an object similar to Parker's loop appears under rather general assumptions within the normalizer of an elementary subgroup of order four in a group with large extraspecial 2-subgroup [12]. Apparently the situation with extraspecial groups of odd order exhibits similar features [11]. We came across this observation when proving the following theorem (where the subgroups C and N of the Monster appear under the names G_1 and G_2, respectively).

Theorem 1. *Let G_1 be a group subject to the following*:

(i) $Q_1 := O_2(G_1)$ *is extraspecial of order* 2^{25} *and of* $+$ *type*;
(ii) $\bar{G}_1 := G_1/Q_1$ *is the first Conway group* Co_1;

(iii) *there is a surjective homomorphism* $\eta : Q_1 \to \bar{\Lambda}$ *with kernel* $Z_1 := Z(Q_1)$ *such that the induced isomorphism between* Q_1/Z_1 *and* $\bar{\Lambda}$ *commutes with the action of* $\bar{G}_1$ (*here* $\bar{\Lambda} = \Lambda/2\Lambda$ *and* Λ *is the Leech lattice*).

Let t *be an element from* Q_1 *with* $\eta(t) \in \bar{\Lambda}_4$. *Then for one and only one choice of the isomorphism type of* G_1 *there exists a group* G_2 *whose center is trivial and which contains* $C_{G_1}(\eta(t))$ *as a subgroup of index* 3.

The conditions (i) to (iii) in the above theorem allow exactly two possibilities for the isomorphism type of G_1 (cf. [7, Proposition 2.6] or [8, Lemma 5.13.1]). It is worth mentioning that similarly to Conway's construction when proving Theorem 1 we first construct a 4-fold cover of G_2 and then quotient out a suitable subgroup of order four.

The referee pointed out that Theorem 1 has been well known for 30 years (I have to take his word for this) and requested a declaration of what is new in the paper. Following referee's suggestion I would claim the characterization and the clarification of the structure of G_2 (accomplishing Tits' request) as new. A rigorous reader, which I am sure the referee must be, would certainly have found the useful by-products of the proof and the clarity of the exposition.

2. Golay code

In this section we briefly summarize notation, terminology and basic results concerning the binary Golay code (cf. [1] and [8] for details).

A Steiner system of type $S(5, 8, 24)$ is a pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a 24-element set and $\mathcal{B}$ is a collection of 8-element subsets of $\mathcal{P}$ (called *octads*) such that every 5-element subset of $\mathcal{P}$ is in a unique octad. This system is unique up to isomorphism and its automorphism group is the largest Mathieu group M_{24}. Let $V^{(24)}$ be the power set of $\mathcal{P}$ turned into a $GF(2)$-vector space with addition performed by the symmetric difference operator. Clearly $V^{(24)}$ carries the structure of the $GF(2)$-permutation module of M_{24} acting on $\mathcal{P}$. The $GF(2)$-valued function π on $V^{(24)} \times V^{(24)}$ defined by

$$\pi : (u, v) \mapsto |u \cap v| \bmod 2$$

is bilinear and M_{24}-invariant.

The M_{24}-module $V^{(24)}$ possesses a unique composition series

$$0 < V^{(1)} < \mathcal{C}_{12} < V^{(23)} < V^{(24)},$$

where $V^{(1)}$ is formed by the improper subsets of $\mathcal{P}$; $V^{(23)}$ is the set of even subsets of $\mathcal{P}$; $\mathcal{C}_{12}$ is the 12-dimensional Golay code (which is spanned by the octads). Then $\mathcal{C}_{12}$ and $\bar{\mathcal{C}}_{12} := V^{(24)}/\mathcal{C}_{12}$ are the 12-dimensional *Golay code* and *Todd* modules for M_{24}. The quotient $\mathcal{C}_{11} := \mathcal{C}_{12}/V^{(1)}$ of $\mathcal{C}_{12}$ and the submodule $\bar{\mathcal{C}}_{11} := V^{(23)}/\mathcal{C}_{12}$ of $\bar{\mathcal{C}}_{12}$ are irreducible M_{24}-modules called the 11-dimensional Golay code and Todd modules, respectively.

The Golay code module $\mathcal{C}_{12}$ is totally singular with respect to π and therefore π induces a well-defined map $\mathcal{C}_{12} \times \bar{\mathcal{C}}_{12} \to GF(2)$. Furthermore, $V^{(1)}$ is the radical of π restricted to $V^{(23)}$ and hence π induces also a well-defined bilinear map $\mathcal{C}_{11} \times \bar{\mathcal{C}}_{11} \to GF(2)$. For each of these three maps we use the same symbol π and the concrete meaning will be clear from the context. From the above discussions it is clear that $(\mathcal{C}_{12}, \bar{\mathcal{C}}_{12})$ and $(\mathcal{C}_{11}, \bar{\mathcal{C}}_{11})$ are dual pairs.

The subsets of $\mathcal{P}$ contained in $\mathcal{C}_{12}$ are called *Golay sets*. Besides the empty set and the whole set $\mathcal{P}$ the Golay sets include the octads and their complements as well as the *dodecads* (which are 12-element subsets of $\mathcal{P}$). The dodecads come in complementary pairs. Let $\mathcal{S}$ be the subsets of $\mathcal{P}$ of size at most 4. Then every element of $\bar{\mathcal{C}}_{12}$ (which is a coset of $\mathcal{C}_{12}$ in $V^{(24)}$) intersects $\mathcal{S}$ either in a single subset of size less than 4 or in exactly six subsets of size 4 forming a *sextet*.

The *Parker loop* [1,2] is an extension of $GF(2)$ by $\mathcal{C}_{12}$. The power map P, the commutator map C and the associator map A of the Parker loop are defined by

$$P(u) = \frac{1}{4}|u| \bmod 2,$$

$$C(u, v) = \frac{1}{2}|u \cap v| \bmod 2,$$

$$A(u, v, w) = |u \cap v \cap w| \bmod 2$$

for $u, v, w \in \mathcal{C}_{12}$. The symbols P, C and A will also denote the corresponding maps induced on the powers of $\mathcal{C}_{11}$.

The map τ of $\mathcal{C}_{12} \times \mathcal{C}_{12}$ onto $\bar{\mathcal{C}}_{11}$ defined by

$$\tau : (u, v) \mapsto \overline{u \cap v}$$

(here for a subset x of $\mathcal{P}$ by $\bar{x}$ we denote the image of x in $\bar{\mathcal{C}}_{12}$) is bilinear and

$$A(u, v, w) = \pi\big(u, \tau(v, w)\big).$$

The first and the second cohomology groups of the Golay code and Todd modules are known.

Lemma 2.1. *The following assertions hold*:

(i) *both* $H^1(\mathcal{C}_{11}, M_{24})$ *and* $H^2(\mathcal{C}_{11}, M_{24})$ *are trivial*;
(ii) *both* $H^1(\bar{\mathcal{C}}_{11}, M_{24})$ *and* $H^2(\bar{\mathcal{C}}_{11}, M_{24})$ *are of order* 2.

Proof. (i) was already known to Thompson [13]. Since $\bar{\mathcal{C}}_{12}$ is an indecomposable extension of $\bar{\mathcal{C}}_{11}$ by a trivial module, $H^1(\bar{\mathcal{C}}_{11}, M_{24})$ is non-zero. The dimensions of $H^1(\mathcal{C}_{11}, M_{24})$ and $H^1(\bar{\mathcal{C}}_{11}, M_{24})$ have been calculated in Section 9 of [5]. Finally, $H^2(\bar{\mathcal{C}}_{11}, M_{24})$ was calculated by Derek Holt using his cohomology package. For the proof of our main result we do not need to know $H^2(\bar{\mathcal{C}}_{11}, M_{24})$ but we present it here for completeness.[1] □

3. The anti-heart module for M_{24}

The heart $V^{(23)}/V^{(1)}$ of the $GF(2)$-permutation module of M_{24} acting on $\mathcal{P}$ is an indecomposable extension of $\mathcal{C}_{11}$ by $\bar{\mathcal{C}}_{11}$. In this section we study an indecomposable extension of $\bar{\mathcal{C}}_{11}$ by $\mathcal{C}_{11}$ which can be termed the *anti-heart module*. We show (Lemma 3.2) that the anti-heart module is in fact the unique such indecomposable extension which carries a non-zero invariant quadratic form.

Lemma 3.1. *For $\varepsilon \in \{0, 1\}$ let U^ε be the set $\mathcal{C}_{11} \times \bar{\mathcal{C}}_{11}$ together with addition defined via*

$$(u, \bar{v}) + (t, \bar{s}) = (u + t, \bar{v} + \bar{s} + \varepsilon \cdot \overline{u \cap t}),$$

where $u, t \in \mathcal{C}_{11}$, $\bar{v}, \bar{s} \in \bar{\mathcal{C}}_{11}$ and the operations on the right are in the corresponding modules. Then

- (i) *U^ε is a $GF(2)$-vector space and the natural action of M_{24} turns it into a module for this group*;
- (ii) *the $GF(2)$-valued function q^ε on U^ε defined by*

$$q^\varepsilon(u, \bar{v}) = \pi(u, \bar{v}) + \varepsilon \cdot P(u)$$

is an M_{24}-invariant quadratic form on U^ε and the associated bilinear form is

$$f^\varepsilon\big((u, \bar{v}), (t, \bar{s})\big) = \pi(u, \bar{s}) + \pi(t, \bar{v}) + \varepsilon \cdot C(u, t);$$

- (iii) *the action of $\mathcal{C}_{11}$ on U^ε defined by*

$$u : (t, \bar{s}) \mapsto (t, \bar{s} + \overline{u \cap t})$$

preserves the vector space structure and the form q^ε; furthermore, this action is normalized by the action of M_{24}.

Proof. For $\varepsilon = 0$ the module U^ε is the direct sum of $\mathcal{C}_{11}$ and $\bar{\mathcal{C}}_{11}$, so the assertions are quite obvious in this case since π establishes the duality between $\mathcal{C}_{11}$ and $\bar{\mathcal{C}}_{11}$. For the case $\varepsilon = 1$ the result is a truncated and specialized version of [1, Exercise 4.6 and Lemma 23.10] (see also the paragraph after Lemma 4.1 below). □

Let $S^\varepsilon = \{(u, 0) \mid u \in \mathcal{C}_{11}\}$ and $\bar{S}^\varepsilon = \{(0, \bar{v}) \mid \bar{v} \in \bar{\mathcal{C}}_{11}\}$ be subsets of U^ε. By Lemma 3.1 $\bar{S}^\varepsilon$ is a submodule isomorphic to $\bar{\mathcal{C}}_{11}$, which is totally isotropic with respect to q^ε and centralized by the action of $\mathcal{C}_{11}$. On the other hand, S^ε is M_{24}-invariant, but it is closed under

[1] It was pointed out by the referee that both these second cohomology groups were calculated by D.J. Jackson in his PhD thesis (circa 1980).

the addition only if $\varepsilon = 0$. Since the stabilizer in M_{24} of a Golay subset does not stabilize proper subsets of $\mathcal{P}$ other than the subset itself and its complement, it is clear that S^ε is the only M_{24}-invariant subset of U^ε which projects bijectively onto $\mathcal{C}_{11}$. In particular U^1 (called the *anti-heart module*) is indeed indecomposable.

The next two lemmas provide us with a characterization of the anti-heart module.

Lemma 3.2. *The following assertions hold*:

(i) *the exterior square* $\bar{\mathcal{C}}_{11} \wedge \bar{\mathcal{C}}_{11}$ *contains* $\mathcal{C}_{11}$ *as a submodule*;
(ii) *the quotient* $V^{(44)} := (\bar{\mathcal{C}}_{11} \wedge \bar{\mathcal{C}}_{11})/\mathcal{C}_{11}$ *is irreducible*;
(iii) $H^1(V^{(44)}, M_{24})$ *has order* 2.

Proof. The trilinear form A on $\mathcal{C}_{11}$ defines a surjective bilinear map $\mathcal{C}_{11} \wedge \mathcal{C}_{11} \to \bar{\mathcal{C}}_{11}$. Applying the duality we obtain (i). The composition factors of the exterior square can be calculated by decomposing the Brauer character of $\bar{\mathcal{C}}_{11} \times \bar{\mathcal{C}}_{11}$ using [10]. This gives (ii). Finally (iii) is the result of computer calculations with the cohomology package by Derek Holt performed by Dima Pasechnik. □

Lemma 3.3. *Let* U *be a* 22*-dimensional* $GF(2)$*-space and* q *be a non-singular quadratic form of type* $+$ *on* U. *Let* H *be a subgroup of the orthogonal group* $O(U,q) \cong O_{22}^{+}(2)$ *such that*

(i) H *is the semidirect product with respect to the natural action of* $R \cong \mathcal{C}_{11}$ *and* $K \cong M_{24}$;
(ii) H *stabilizes a maximal totally isotropic subspace* S;
(iii) R *centralizes both* S *and* U/S *while* K *acts on* S *and* U/S *as on* $\bar{\mathcal{C}}_{11}$ *and* $\mathcal{C}_{11}$, *respectively.*

Then U, *as a module for* K, *is isomorphic to* U^ε *for* $\varepsilon = 0$ *or* 1 *and* R *acts on* U *according to the rule given in Lemma* 3.1(iii). *In particular* (*up to conjugation*) *there are exactly two choices for* H.

Proof. The stabilizer L of S in $O(U,q)$ is the semidirect product of X and Y, where $X = O_2(L) \cong S \wedge S$ is the centralizer of S in L and $Y \cong GL(S)$ is a Levi complement. By the hypothesis $HX/X \cong M_{24}$ and by Lemma 3.2(ii) $H \cap X$ is the only 11-dimensional H-submodule in X. Finally K is a complement to $X/R \cong 2^{44}$ in $HX/R \cong 2^{44} : M_{24}$. By Lemma 3.2(iii) up to conjugation there are two choices K^0 and K^1 for this complement. If we assume that K^0 is contained in the Levi complement Y then it preserves a direct sum decomposition of U and therefore acts on U as M_{24} acts on U^0. By the pigeonhole principle the action of K^1 on U must be isomorphic to the action of M_{24} on U^1. □

Lemma 3.4. *The only non-zero* M_{24}*-invariant quadratic form on* U^ε *is* q^ε *and the only non-zero* M_{24}*-invariant bilinear form is* f^ε.

Proof. The uniqueness of the quadratic form follows from Lemma 3.3, while that of the bilinear form is due to the fact that π establishes the only duality between $\mathcal{C}_{11}$ and $\bar{\mathcal{C}}_{11}$. □

4. Trident groups

In this section we construct a family of groups (called the *trident groups*) of the shape $2^{11}.(2^{11} \times 2^{11}).M_{24}$ which includes the section $C_N(\langle z,t\rangle)/\langle z,t\rangle$ of the normalizer N in the Monster group M of an elementary subgroup $\langle z,t\rangle$ of order 4 (N appears in Theorem 1 under the name G_2).

We show (Lemma 4.4 together with the equality $|H^2(\bar{\mathcal{C}}_{11}, M_{24})| = 2$) that (up to isomorphism) there are exactly four trident groups. In order to identify $C_N(\langle z,t\rangle)/\langle z,t\rangle$ among them we calculate the automorphism groups (Subsection 4.1) and estimate the Schur multipliers (Subsection 4.2) of the trident groups.

Let F^δ be an extension of $\bar{\mathcal{C}}_{11}$ by M_{24}, so that $O_2(F^\delta)$ is isomorphic to $\bar{\mathcal{C}}_{11}$ as a module for $F^\delta/O_2(F^\delta) \cong M_{24}$ and $\delta \in H^2(\bar{\mathcal{C}}_{11}, M_{24})$ specifies the type of the extension. In view of Lemma 2.1(ii) δ is either 0 or 1, so that F^0 is the semidirect product and F^1 is the only non-split extension.

For $\alpha, \beta \in \{0,1\}$ and $\delta \in H^2(\bar{\mathcal{C}}_{11}, M_{24})$ let $T = T(\alpha,\beta,\delta)$ be a group which is a product of three of its subgroup A^α, B^β and F^δ such that (1) A^α and B^β are normal elementary abelian of order 2^{22} each; (2) $E := A^\alpha \cap B^\beta$ coincides with $O_2(F^\delta)$; (3) there are isomorphisms $a : U^\alpha \to A^\alpha$ and $b : U^\beta \to B^\beta$ which commute with the actions of $F^\delta/E \cong M_{24}$ (so that $E = a(\bar{S}^\alpha) = b(\bar{S}^\beta)$); (4) for $u, t \in \mathcal{C}_{11}$, $\bar{v}, \bar{s} \in \bar{\mathcal{C}}_{11}$ we have

$$\bigl[a(u,\bar{v}), b(t,\bar{s})\bigr] = e(\overline{u \cap t}),$$

where e is the isomorphism of $\bar{\mathcal{C}}_{11}$ onto E commuting with the actions of F^δ. Notice that $Q := O_2(T)$ is of order 2^{33}; $Q = A^\alpha B^\beta$, $E = Z(Q)$ and $T/Q \cong F^\delta/E \cong M_{24}$.

The group $T(\alpha,\beta,\delta)$ exists and unique up to isomorphism. It can be obtained in two stages by constructing partial semidirect products (cf. [3, p. 27] for the definition). Start by taking disjoint copies A^α and B^β of U^α and U^β, respectively, with a and b being the identity maps. Construct the semidirect product X of A^α and B^β with $b(\bar{S}^\beta)$ centralizing A^α and $B^\beta/b(\bar{S}^\beta) \cong \mathcal{C}_{11}$ acting as in Lemma 3.1(iii). Take Y to be the quotient of X over the subgroup $\{a(0,\bar{v})b(0,\bar{v}) \mid \bar{v} \in \bar{\mathcal{C}}_{11}\}$ (which is the *diagonal* copy of $\bar{\mathcal{C}}_{11}$). Identify A^α and B^β with their respective images in Y. Construct a semidirect product Z of Y and F^δ with $O_2(F^\delta)$ acting trivially and $F^\delta/O_2(F^\delta) \cong M_{24}$ acting on A^α and B^β as on U^α and U^β, respectively. Finally, quotient out the diagonal copy of $\bar{\mathcal{C}}_{11}$ (which is the unique normal subgroup of order 2^{11} in Z which is neither in $Y = A^\alpha B^\beta$ nor in F^δ). In terms of Lemma 3.3 the semidirect product of U and H is $T(0,0,0)$ or $T(1,0,0)$ depending on whether or not the M_{24}-subgroup K from H is contained in a Levi complement of $O(U,q)$.

Lemma 4.1. *Let $T = T(\alpha,\beta,\delta)$ be the above defined group. Let*

$$\gamma = (1 + \alpha + \beta) \bmod 2,$$

let c be the mapping of U^γ *into* T *defined by*

$$c:(u,\bar{v})\mapsto a(u,0)b(u,0)e(\bar{v}),$$

and let $C^\gamma=\mathrm{Im}(c)$. *Then*

(i) c *is an injective homomorphism*;
(ii) C^γ *is a normal subgroup in* T *containing* E;
(iii) c *commutes with the actions of* $F^\delta/O_2(F^\delta)\cong M_{24}$;
(iv) *for* $u,t\in\mathcal{C}_{11}$, $\bar{v},\bar{s}\in\bar{\mathcal{C}}_{11}$ *we have*

$$\big[c(u,\bar{v}),a(t,\bar{s})\big]=\big[c(u,\bar{v}),b(t,\bar{s})\big]=e(\overline{u\cap t});$$

(v) A^α, B^β *and* C^γ *are the maximal elementary abelian normal subgroups in* T.

Proof. Directly from the definitions of T, c and C^γ we have the following equalities:

$$\begin{aligned}c(u,\bar{v})c(t,\bar{s})&=a(u,0)b(u,0)e(\bar{v})a(t,0)b(t,0)e(\bar{s})\\&=a(u,0)a(t,0)b(u,0)b(t,0)e(\overline{u\cap t})e(\bar{v}+\bar{s})\\&=a(u+t,0)e(\overline{u\cap t})^\alpha b(u+t,0)e(\overline{u\cap t})^\beta e(\overline{u\cap t})e(\bar{v}+\bar{s})\\&=c(u+t,\bar{v}+\bar{s})e(\overline{u\cap t})^{1+\alpha+\beta}.\end{aligned}$$

This proves the assertions (i) to (iii). The assertion (iv) is now immediate, since both A^α and B^β are abelian. Since Q/E is the direct sum of two copies of $\mathcal{C}_{11}$, (v) follows. □

The groups T are analogous to the so-called tri-extraspecial groups introduced and studied by S.V. Shpectorov and the present author in [9]. The group T will be said to be a *trident group*. A maximal abelian normal subgroup in T will be called a *dent* (by Lemma 4.1(v) there are exactly three dents in T which explains the name trident). Any two different dents intersect in E which is the center of $Q=O_2(T)$. A subgroup K of T is called a *quasi-complement* if $K\cap Q=E$ and $KQ=T$. In particular F^δ is a quasi-complement. By Lemma 4.1 when $\alpha=\beta=0$ the value of γ is 1. Hence even the group $T(0,0,0)$, which is a plain semidirect product, contains a copy of U^1. This construction can be used as an alternative definition of the anti-heart module.

For the proof of our crucial Proposition 6.4 we need the following characterization of the trident groups.

Lemma 4.2. *Let* X *be a group, satisfying the following*:

(i) $Q:=O_2(X)$ *is of order* 2^{33} *and* $X/Q\cong M_{24}$;
(ii) $Q=AB$, *where* A *and* B *are self-centralizing elementary abelian normal subgroup in* X *of order* 2^{22} *each*;
(iii) *there are non-zero quadratic forms* q^A *and* q^B *on* A *and* B *which are invariant under the actions of* X *on these subgroups*;
(iv) *if* $E=A\cap B$ *then* $E\cong\bar{\mathcal{C}}_{11}$ *and* $A/E\cong B/E\cong\mathcal{C}_{11}$ *as* X/Q*-modules.*

Then X *is a trident group.*

Proof. Since $H^2(\mathcal{C}_{11}, M_{24})$ is trivial, X/E splits over $Q/E = A/E \times B/E \cong \mathcal{C}_{11} \times \mathcal{C}_{11}$. Applying Lemma 3.3 to A and B, and the images of X in $O(A, q^A)$ and $O(B, q^B)$, respectively, we observe that the properties of X match the defining properties of a trident group with F^δ being the preimage in X of a complement to Q/E in X/E. □

Lemma 4.3. *All the quasi-complements in a trident group T are conjugates of F^δ.*

Proof. A quasi-complement is the preimage in T of a complement to Q/E in T/E. By the definition of T the quotient T/E is the semidirect product of $Q/E \cong \mathcal{C}_{11} \times \mathcal{C}_{11}$ and $F^\delta/E \cong M_{24}$. Since $H^1(\mathcal{C}_{11}, M_{24})$ is trivial (cf. Lemma 2.1(i)) the result follows. □

Let $\mathcal{D} = \{A^\alpha, B^\beta, C^\gamma\}$ be the set of dents in T. Define $\theta : \mathcal{D} \to GF(2)$ to be a function such that $D \in \mathcal{D}$ is isomorphic to $U^{\theta(D)}$ as a module for $K/E \cong M_{24}$, where K is a quasi-complement. By Lemma 4.3 θ is well defined (independent of the choice of the quasi-complement). The definition of a trident group involves a pair of dents and a quasi-complement, and by Lemma 4.1 any pair of dents can be taken. On the other hand, the function θ is determined by its values on a pair of dents. Thus every trident group is isomorphic either to $T(0, 0, \delta)$ or to $T(1, 1, \delta)$ for some δ. We rephrase this observation in the following lemma.

Lemma 4.4. *For a given isomorphism type of F^δ there are exactly two possibilities for the isomorphism type of T:*

- (i) *$T = T^+(\delta)$ is of plus type: two dents are semi-simple and the third one is indecomposable;*
- (ii) *$T = T^-(\delta)$ is of minus type: each of the three dents is the indecomposable anti-heart module.*

If we consider $\mathcal{D}$ as the set of non-zero vectors of a 2-dimensional $GF(2)$-space then by Lemma 4.1 θ is a non-singular quadratic form and the type of T in the above lemma is exactly the type of the form.

4.1. Automorphisms

In this subsection we calculate the automorphism groups of the trident groups.

Lemma 4.5. *Let T be a trident group. Let ρ be a permutation of the set of dents $\mathcal{D}$ which preserves the function θ. For $D \in \mathcal{D}$ and d being the F^δ/E-invariant isomorphism of $U^{\theta(D)}$ onto D let $\rho(d)$ denote the similar isomorphism of $U^{\theta(\rho(D))}$ onto $\rho(D)$. Define a map $\mu(\rho)$ which fixes every element of F^δ and sends $d(u, \bar{v})$ onto $\rho(d)(u, \bar{v})$ for all $u \in \mathcal{C}_{11}$, $\bar{v} \in \bar{\mathcal{C}}_{11}$. Then $\mu(\rho)$ extends uniquely to an (outer) automorphism of T.*

Proof. The result is immediate from Lemma 4.1(iv) and the definition of T. Notice that the automorphism (which extends) $\mu(\rho)$ permutes the dents according to ρ. □

Define L^δ to be a partial semidirect product of $\bar{\mathcal{C}}_{12}$ and F^δ. As usual to construct this group we first take the semidirect product of $\bar{\mathcal{C}}_{12}$ and F^δ with $O_2(F^\delta)$ acting trivially and $F^\delta/O_2(F^\delta) \cong M_{24}$ acting naturally, and then quotient out the diagonal copy of $\bar{\mathcal{C}}_{11}$. Then L^δ is an extension of $\bar{\mathcal{C}}_{12}$ by M_{24} and it contains (an isomorphic copy of) F^δ with index 2.

Lemma 4.6. $L^\delta = \mathrm{Aut}(F^\delta)$.

Proof. Since F^δ has trivial center it can be identified with $\mathrm{Inn}(F^\delta)$. In view of the existence of L^δ it is sufficient to show that the index of F^δ in $\mathrm{Aut}(F^\delta)$ is at most 2. Let ψ be an automorphism of F^δ. Since the action of $F^\delta/O_2(F^\delta) \cong M_{24}$ on $O_2(F^\delta)$ is absolutely irreducible and the outer automorphism group of M_{24} is trivial, ψ can be adjusted by inner automorphisms to centralize $O_2(F^\delta)$ and to commute with $F^\delta/O_2(F^\delta)$. Then $\langle O_2(F^\delta), \psi\rangle$ is abelian and can be considered as a module for $F^\delta/O_2(F^\delta)$. Since a power of ψ must not commute with the whole of F^δ unless this power is the identity element, the module must be an indecomposable extension of $\bar{\mathcal{C}}_{11}$ by a trivial $GF(2)$-module. By Lemma 2.1(ii) the largest such extension is $\bar{\mathcal{C}}_{12}$ which gives the result. □

Proposition 4.7. *The following assertions hold*:

(i) $\mathrm{Out}(T^+(\delta)) \cong 2^2$;
(ii) $\mathrm{Out}(T^-(\delta)) \cong Sym_3 \times 2$.

Proof. It is easy to see that every automorphism of the quasi-complement F^δ which commutes with $E = O_2(F^\delta)$ extends uniquely to an automorphism of T which commutes with Q. Then from Lemmas 4.4 and 4.5 we obtain all the required outer automorphisms. Since all the quasi-complements are conjugate by Lemma 4.3, it only remains to show that an automorphism of T which centralizes F^δ and stabilizes every dent as a whole must be trivial. But this is indeed the case since for every dent D the group F^δ/E acts absolutely irreducibly on each composition factors of D and these (two) composition factors are non-isomorphic. □

Thus the trident groups of minus type possess the triality symmetry between the dents. This triality is essential for constructing the group G_2 in Theorem 1.

4.2. Schur multipliers

In this subsection we estimate the order of the Schur multiplier of a trident group T. Since T is perfect, the standard theory of Schur multipliers applies. Let $\tilde{T}$ be the covering group of T which is the largest perfect group possessing a surjective homomorphism

$$\chi : \tilde{T} \to T$$

such that $\ker(\chi) = Z(\tilde{T})$ (recall that $Z(T) = 1$). Then $Z(\tilde{T})$ is the Schur multiplier of T. For a subgroup X of T let $\tilde{X}$ denote the preimage of X in $\tilde{T}$. Since the Schur multiplier of $M_{24} \cong T/O_2(T)$ is trivial it is easy to see that $Z(\tilde{T})$ is a 2-group.

Lemma 4.8. *Let* $Y = [\tilde{Q}, \tilde{E}]$. *Then* $Z(\tilde{T})/Y$ *is elementary abelian of order* 2^2.

Proof. By the definition Y is the smallest normal subgroup of $\tilde{T}$ contained in $Z(\tilde{T})$ such that $\tilde{E}/Y$ is the center of $\tilde{Q}/Y$. Therefore $\tilde{E}/Y$ is a T/Q-module which is an extension of a trivial module by E. Since $E \cong \bar{\mathcal{C}}_{11}$ is dual to $\mathcal{C}_{11}$ and $H^1(\mathcal{C}_{11}, M_{24})$ is trivial by Lemma 2.1(i), there are no proper indecomposable extensions of trivial modules by $\bar{\mathcal{C}}_{11}$. Hence there is a complement I to $Z(\tilde{T})/Y$ in $\tilde{E}/T$ which is normal in $\tilde{T}/Y$. The quotient of $\tilde{T}/Y$ over I is a perfect central extension of $T/E \cong (\mathcal{C}_{11} \times \mathcal{C}_{11}) : M_{24}$. Since (1) the Schur multiplier of M_{24} is trivial; (2) M_{24} does not preserve non-zero bilinear forms on $\mathcal{C}_{11}$, (3) $H^1(\bar{\mathcal{C}}_{11}, M_{24})$ is of order 2 and $\bar{\mathcal{C}}_{11}$ is the dual of $\mathcal{C}_{11}$; we conclude that the Schur multiplier of T/E has order at most 4. Thus it only remains to show that the upper bound for the order of $Z(\tilde{T})/Y$ is attained. For this purpose we apply a standard pull back construction. First, let X be the semidirect product with respect to the natural action of the direct sum of two copies of $\mathcal{C}_{12}$, and M_{24}. Second, consider the subdirect product $X^{(1)}$ of X and T with respect to their homomorphisms onto $T/E \cong (\mathcal{C}_{11} \times \mathcal{C}_{11}) : M_{24}$. Then $X^{(1)}$ is a perfect group with center of order 4 possessing a homomorphism onto T and the preimage of E with respect to this homomorphism is the center of $X^{(1)}$. Hence the result follows. □

Lemma 4.9. *The order of* $Y = [\tilde{Q}, \tilde{E}]$ *is at most* 2^2.

Proof. Let D be a dent. Let $\zeta(D) : \tilde{D} \times \tilde{D} \to Z(\tilde{T})$ be the commutator map, so that

$$\zeta(D) : (\tilde{d}_1, \tilde{d}_2) \mapsto [\tilde{d}_1, \tilde{d}_2].$$

Since D is an elementary abelian 2-group, so is the image $I(D)$ of $\zeta(D)$. Let J be a hyperplane in $I(D)$. Since Y is in the center of $\tilde{T}$ the mapping $\tilde{D} \times \tilde{D} \to I(D)/J$ induced by $\zeta(D)$ induces in its turn a bilinear form $D \times D \to GF(2)$ which is invariant under the action of $F^\delta/E \cong M_{24}$. By Lemma 3.4 this implies that $I(D)$ is of order at most 2. Let $\mathcal{D} = \{A^\alpha, B^\beta, C^\gamma\}$. Since $Q = A^\alpha B^\beta$, the group Y is generated by $I(A^\alpha)$ and $I(B^\beta)$ (both of order at most 2). Considering elements $a \in A^\alpha \setminus E$, $b \in B^\beta \setminus E$, $c \in C^\gamma \setminus E$ with $abc = 1$, it is easy to see that Y is elementary abelian of order at most 2^2. □

Lemma 4.10. *If* T *is of plus type then the order of* $Y = [\tilde{Q}, \tilde{E}]$ *is at most* 2.

Proof. Let T be a trident group of plus type and assume without loss that $\alpha = \beta = 0$, $\gamma = 1$. For $D \in \mathcal{D}$ let $\omega(D) : \tilde{D} \to Z(\tilde{T})$ be the squaring map. We claim that image of $\omega(D)$ is contained in the commutator $I(D)$ of $\tilde{D}$ and that $\omega(D)$ induces on D a quadratic form associated with the bilinear form induced by the commutator map $\zeta(D)$. In order to prove the claim it is sufficient to show that $\tilde{D}/I(D)$ has exponent 2. The group $\tilde{D}/I(D)$ is abelian and hence it is a direct product of cyclic groups. By Lemmas 4.8 and 4.9 $|Z(\tilde{T})/I(D)| \leqslant 2^3$, and therefore there are at most three direct factors of orders greater than 2. Hence the images in D of the involutions from $\tilde{D}/I(D)$ generate a submodule in D of codimension at most 3. Since there are no such proper submodules the claim follows.

Let u be an element of $\mathcal{C}_{11}$ which is a pair of complementary dodecads. Then by Lemma 3.1(ii) the elements $a(u,0)$ and $b(u,0)$ are isotropic with respect to the invariant quadratic forms on A^0 and B^0, respectively. By the first paragraph of the proof this implies that both $a(u,0)^2$ and $b(u,0)^2$ are equal to the identity element. By Lemma 4.1 $c(u,0) = a(u,0)b(u,0) = b(u,0)a(u,0)$ and therefore $c(u,0)^2$ is the identity as well. On the other hand, by Lemma 3.1(ii) the element $c(u,0)$ is not isotropic with respect to the non-zero invariant quadratic form on C^1. This means that $I(C^1)$ is trivial and hence the order of Y is at most 2. □

In Section 6 we will see that the upper bound 2^4 for the Schur multiplier is attained for a particular trident group of minus type. It is well known that every automorphism of T can be lifted to an automorphism of $\tilde{T}$ (a proof can be seen on pp. 356–357 of [4]).

Lemma 4.11. *Suppose that T is a trident group with $Z(\tilde{T})$ of order 2^4. Then the automorphism group of dent permutations acts faithfully on $Z(\tilde{T})$ with every permutation of order* 3 *acting fixed-point freely.*

Proof. If $Y = [\tilde{Q}, \tilde{E}]$ has order 4 then by the proof of Lemma 4.9 there is a natural bijection between the dents and the non-identity elements of Y. Similarly by the proof of Lemma 4.8 there is a natural bijection between the dents and the non-identity elements of $Z(\tilde{T})/Y$. □

It does not appear to be obvious (even when $|Z(\tilde{T})| = 2^4$) whether the automorphism of T which centralizes Q and induces an outer automorphism of a quasi-complement acts non-trivially on $Z(\tilde{T})$. We do not need to answer this question in order to prove Theorem 1. The affirmative answer will be given at the very end of the paper (in Lemma 7.1(i)) for the sake of completeness.

5. Leech lattice

The Leech lattice Λ is commonly defined with respect to a basis identified with the element set $\mathcal{P}$ of the Steiner system $S(5,8,24)$ (cf. [1, Chapter 8] or [8, Chapter 4]). The coordinates of a Leech vector $\lambda \in \Lambda$ in this basis are integers and therefore λ can be considered as a function

$$\lambda : \mathcal{P} \to \mathbf{Z}.$$

The Leech vectors are characterized by the following three conditions:

(i) there is $m \in \{0,1\}$ such that $\lambda(a) \equiv m \bmod 2$;
(ii) $\{a \mid \lambda(a) \equiv m \bmod 4\}$ is a Golay set;
(iii) $\sum_{a\in\mathcal{P}} \lambda(a) \equiv 4m \bmod 8$.

Define

$$\Lambda_i = \left\{ \lambda \;\middle|\; \lambda \in \Lambda,\ \sum_{a \in \mathcal{P}} \lambda(a)^2 = 16i \right\}.$$

The group C_0 of automorphisms of Λ preserving the origin is a non-split extension by the first Conway group Co_1 of the group of (± 1)-scalar transformations. The stabilizer N_0 in C_0 of the frame

$$\mathcal{F} = \{\pm a \mid a \in \mathcal{P}\}$$

is the semidirect product of $O_2(N_0) \cong \mathcal{C}_{12}$ and $K \cong M_{24}$. The elements of K permute the coordinates of the Leech vectors in the natural way and a Golay set $u \in O_2(N_0)$ acts by sign changes:

$$u : \lambda(a) \to (-1)^{|u \cap \{a\}|} \lambda(a).$$

In particular $\mathcal{P}$ (considered as an element of $O_2(N_0)$) acts as the (-1)-scalar operator.

Put $\bar{\Lambda} = \Lambda / 2\Lambda \cong 2^{24}$ and adopt the bar convention for the images in $\bar{\Lambda}$ of elements and subsets of Λ. Then

$$\bar{\Lambda} = \bar{\Lambda}_0 \cup \bar{\Lambda}_2 \cup \bar{\Lambda}_3 \cup \bar{\Lambda}_4$$

($\Lambda_1 = \emptyset$, since Λ contains no roots). The group $\bar{G}_1 := C_0/\{\pm 1\} \cong Co_1$ acts faithfully and irreducibly on $\bar{\Lambda}$ preserving a unique non-zero quadratic form $\theta_{\bar{\Lambda}}$ (which is non-singular) defined by

$$\theta_{\bar{\Lambda}} : \bar{\Lambda}_i \to i \bmod 2$$

for $i = 0, 2, 3, 4$. If $a \in \mathcal{P}$ the vector $\lambda_0 := 8a$ is contained in Λ_4, $\bar{\lambda}_0$ is independent of the choice of a and

$$\bar{G}_{12} := N_0/\{\pm 1\} \cong \mathcal{C}_{11} : M_{24}$$

is the stabilizer of $\bar{\lambda}_0$ in $\bar{G}_1$. Let K also denote a complement to $O_2(\bar{G}_{12})$ in $\bar{G}_{12}$ (since $H^1(\mathcal{C}_{11}, M_{24})$ is trivial, all the complements are conjugate). The following result is well known (cf. [8, Lemma 4.6.2]).

Lemma 5.1. *The Leech lattice $\bar{\Lambda}$ as a module for $\bar{G}_{12}$ possesses a unique composition series*

$$0 < \bar{\Lambda}^{(1)} < \bar{\Lambda}^{(12)} < \bar{\Lambda}^{(23)} < \bar{\Lambda},$$

and

(i) $\bar{\Lambda}^{(1)} = \langle\bar{\lambda}_0\rangle$ *is the centralizer of* $O_2(\bar{G}_{12})$ *in* $\bar{\Lambda}$;
(ii) $\bar{\Lambda}^{(12)}/\bar{\Lambda}^{(1)}$ *is the centralizer of* $O_2(\bar{G}_{12})$ *in* $\bar{\Lambda}/\bar{\Lambda}^{(1)}$ *and* $\bar{\Lambda}^{(12)}$ *is totally isotropic with respect to* $\theta_{\bar{\Lambda}}$;
(iii) $\bar{\Lambda}^{(23)}$ *is the dual of* $\bar{\Lambda}^{(1)}$ *with respect to the bilinear form associated with* $\theta_{\bar{\Lambda}}$.

The actions of K and $O_2(\bar{G}_{12})$ on $\bar{\Lambda}$ are described in [1, Lemma 23.10]. The next two lemmas are extractions from that description.

Lemma 5.2. *Consider* $\bar{\Lambda}$ *as a module for a complement* $K \cong M_{24}$ *to* $O_2(\bar{G}_{12})$ *in* $\bar{G}_{12}$. *Then* (*besides the composition series in Lemma* 5.1) *there is a composition series*:

$$0 < \bar{\Lambda}^{(11)} < \bar{M}^{(12)} < \bar{M}^{(13)} < \bar{\Lambda}$$

and the following assertions hold:

(i) $\bar{M}^{(12)} \cong \bar{\mathcal{C}}_{12}$;
(ii) $\bar{\Lambda}/\bar{M}^{(12)} \cong \mathcal{C}_{12}$;
(iii) $\bar{\Lambda}^{(23)}/\bar{\Lambda}^{(1)}$ *is isomorphic to the anti-heart module*;
(iv) $\bar{M}^{(12)}/\bar{\Lambda}^{(11)}$ *and* $\bar{M}^{(13)}/\bar{M}^{(12)}$ *are trivial* 1*-dimensional.*

Notice that the subset of $\bar{\Lambda}^{(23)}/\bar{\Lambda}^{(1)}$ on which K acts as on $\mathcal{C}_{11} \cup \bar{\mathcal{C}}_{11}$ is formed by the images of the Leech vectors from

$$\left\{\sum_{a\in u} 2a \,\middle|\, u \in \mathcal{C}_{12}\right\} \cup \left\{\sum_{a\in s} 4a \,\middle|\, s \subseteq \mathcal{P},\ |s| \in \{0, 2, 4\}\right\}.$$

Thus the anti-heart module can also be defined as the 22-dimensional section of the Leech lattice modulo 2 (considered as a module for $K \cong M_{24}$). Since $H^1(\mathcal{C}_{11}, M_{24})$ is trivial and $H^1(\bar{\mathcal{C}}_{11}, M_{24})$ has order 2, it is easy to see that the assertions (i) to (iv) in Lemma 5.2 specify $\bar{\Lambda}$ uniquely as an M_{24}-module.

Lemma 5.3. *In terms of Lemma* 5.1 *the group* $O_2(\bar{G}_{12}) \cong \mathcal{C}_{11}$ *acts*

(i) *on* $\bar{\Lambda}^{(12)}$ *by transvections with center* $\bar{\lambda}_0$;
(ii) *on* $\bar{\Lambda}/\bar{\Lambda}^{(12)}$ *by transvections with axis* $\bar{\Lambda}^{(23)}/\bar{\Lambda}^{(12)}$;
(iii) *on* $\bar{\Lambda}^{(23)}/\bar{\Lambda}^{(1)}$ *according to the rule given in Lemma* 3.1(iii).

Each of the above three actions is faithful.

6. Proof of Theorem 1

Let G_1 be a group satisfying the hypothesis of Theorem 1. As was mentioned in the paragraph following Theorem 1, there are two such groups. To obtain the other one we first construct the universal cover $\hat{G}_1$ which is the subdirect product of G_1 and the automorphism group $C_0 \cong 2.Co_1$ of the Leech lattice with respect to their homomorphisms onto $\bar{G}_1 \cong Co_1$, and then quotient out the diagonal central subgroup of order 2.

Let $\eta : Q_1 \to \bar{\Lambda}$ be the G_1-invariant homomorphism as in the hypothesis of Theorem 1 and adopt the notation for the Leech lattice from Section 5. Let t be an element from $Q_1 \setminus Z_1$ with $\eta(t) = \bar{\lambda}_0$. Put $Z_2 = \langle z, t\rangle$, $G_{12} = N_{G_1}(Z_2)$, $G_{12}^0 = C_{G_1}(Z_2)$, and $Q_2 = O_2(G_{12}^0)$. Then G_{12} is the preimage in G_1 of the stabilizer $\bar{G}_{12} \cong 2^{11} : M_{24}$ of $\bar{\lambda}_0$ in $\bar{G}_1 \cong Co_1$.

Lemma 6.1. *Let E_2 and $\hat{A}$ be the preimages with respect to η of $\bar{\Lambda}^{(12)}$ and $\bar{\Lambda}^{(23)}$, respectively. Then*

- (i) $G_{12}^0 \cap Q_1 = Q_2 \cap Q_1 = \hat{A}$, $Q_2 Q_1 = O_2(G_{12})$, $G_{12}^0/Q_2 \cong M_{24}$, *and* G_{12}^0 *is the commutator subgroup of* G_{12};
- (ii) *elements from* $Q_1 \setminus \hat{A}$ *conjugate* t *to* tz;
- (iii) E_2 *is a maximal elementary abelian normal subgroup in* Q_1 *of order* 2^{13}, E_2 *is the centralizer of* Q_2/Z_2 *in* Q_1, *and* E_2/Z_2 *is isomorphic to* $\bar{\mathcal{C}}_{11}$ *as a module for* $G_{12}^0/Q_2 \cong M_{24}$;
- (iv) Q_2 *induces on* E_2 *the group generated by the transvections whose centers are contained in* Z_2;
- (v) $[E_2, Q_2] = Z_2$.

Proof. The assertions (i) to (iii) follow from Lemma 5.1(iii). Since $\theta_{\bar{\Lambda}}$ is non-singular, $\bar{\Lambda}^{(12)}$ is a maximal totally singular subspace in $\bar{\Lambda}$. Therefore an element from $Q_2 \setminus E_2$ acts on E_2 as a transvection with center t. In view of this observation (iv) follows from Lemma 5.3(i). Finally (v) is immediate from (iv). □

Lemma 6.2. *Let $\hat{B}$ and $\hat{C}$ be the centralizers in Q_2 of $E_2/\langle t\rangle$ and $E_2/\langle tz\rangle$, respectively. Then*

- (i) $\hat{B} \cap Q_1 = \hat{C} \cap Q_1 = E_2$ *and* $\hat{A}\hat{B} = \hat{A}\hat{C} = Q_2$;
- (ii) $[\hat{B}, \hat{B}] = \langle t\rangle$, $[\hat{C}, \hat{C}] = \langle tz\rangle$;
- (iii) Q_2/E_2, *as a module for* $G_{12}^0/Q_2 \cong M_{24}$, *is the direct sum of two copies of* $\mathcal{C}_{11}$;
- (iv) G_{12}^0/E_2 *splits over* Q_2/E_2.

Proof. The assertion (i) is immediate from Lemma 6.1(iv). Notice that $\hat{B}$ and $\hat{C}$ are the subgroups in Q_2 which act on E_2 by transvections with centers t and tz, respectively. Thus (ii) follows. By (i) $Q_2/E_2 = \hat{A}/E_2 \times \hat{B}/E_2$. The factors are isomorphic to $\mathcal{C}_{11}$ by Lemmas 5.2(ii) and 5.3. This gives (iii). Finally (v) is by (iv) and Lemma 2.1(i). □

Lemma 6.3. $\hat{B}/\langle z\rangle \cong \hat{C}/\langle z\rangle \cong 2_+^{1+22}$.

Proof. In view of Lemmas 6.1(iv) and 6.2(ii) (and the obvious symmetry between $\hat{B}$ and $\hat{C}$) all we have to show is that the abelian group $\hat{B}/Z_2$ has exponent 2. The group (as a module for $G_{12}^0/Q_2 \cong M_{24}$) is an extension of $E_2/Z_2 \cong \bar{\mathcal{C}}_{11}$ by $O_2(\bar{G}_{12}) \cong \mathcal{C}_{11}$. Since E_2/Z_2 must be in the center of $\hat{B}/Z_2$, the squares of the elements from a coset of E_2/Z_2 are the same element of E_2/Z_2. On the other hand, the stabilizer in M_{24} of an element from $\mathcal{C}_{11}$ does not stabilize non-trivial elements in $\bar{\mathcal{C}}_{11}$. Thus $\hat{B}/Z_2$ is indeed has exponent 2. □

If G is a group such that $G_1 = C_G(z)$ and in which t is a conjugate of z, then

$$\hat{B} = O_2\big(C_G(t)\big) \cap G_1, \qquad \hat{C} = O_2\big(C_G(tz)\big) \cap G_1$$

and the above three lemmas are rather standard in the theory of groups with large extraspecial 2-subgroup (cf. [1,12]).

Now we are ready to proof our crucial result.

Proposition 6.4. $G_{12}^0/Z_2 \cong T^-(\delta)$ *for some* $\delta \in H^2(\bar{\mathcal{C}}_{11}, M_{24})$.

Proof. For $T = G_{12}^0/Z_2$ we check the hypothesis of Lemma 4.2 with $Q = Q_2/Z_2$, $A = \hat{A}/Z_2$, $B = \hat{B}/Z_2$. Then (i) is by Lemma 6.1(i); (ii) is by Lemmas 6.2(i) and 6.3; and (iv) is by Lemmas 6.1(iii) and 6.2(iii). The quadratic forms needed for (iii) are induced by the squaring maps in the extraspecial groups $\hat{A}/\langle t\rangle$ and $\hat{B}/\langle z\rangle$ (compare Lemma 6.3 and the definition of $\hat{A}$). We claim that G_{12}^0 is of minus type. Indeed, G_{12}^0 is perfect central extension of T with center Z_2 of order 4. Now it only remains to compare Lemma 4.10 with Lemma 6.1(v). □

A quasi-complement F^δ is the preimage in T of an M_{24}-complement to Q_2/E_2 in G_{12}^0/E_2 (such a complement exists by Lemma 6.2(iv)). Within our treatment it is irrelevant whether F^δ splits or not. It is known in the theory of the Monster that F^δ does not split (cf. [13, Property (16)]).

In order to prove Theorem 1 we need to construct a group G_2 containing G_{12} with index 3. Since G_{12}^0 is the only subgroup of index 2 in G_{12}, it must be normal in G_2. Therefore $Z_2 = Z(G_{12}^0)$ is also normal in G_2. Since G_2 is supposed to have trivial center, we conclude that G_2 acts transitively on $Z_2^\# = \{z, t, tz\}$. By Lemma 6.1(ii) G_{12} permutes t and tz centralizing z. Hence $G_2/G_{12}^0 \cong Sym_3$.

Lemma 6.5. G_2/Z_2 *is a subgroup of* Aut(T) *satisfying the following*:

- (i) G_2/Z_2 *contains the group of inner automorphisms*;
- (ii) *the image of* G_2/Z_2 *in* Out(T) *is* Sym_3;
- (iii) G_2/Z_2 *contains* G_{12}/Z_2 *with index* 3;
- (iv) *the isomorphism type of* G_2/Z_2 *is uniquely determined.*

Proof. Since $Z(T) = 1$ the assertion (i) to (iii) follow from the paragraph before the lemma. By Lemmas 4.7(ii) and 6.4 Out(T) contains precisely two subgroups Sym_3 which have different subgroups of order 2. Since the image of G_{12}/Z_2 in Out(T) is such a subgroup of order 2, (iv) follows. □

It is implicit in the proof of Lemma 6.5 that G_2/Z_2 is independent of the choice of the isomorphism type of G_1. This is indeed the case since Z_2 contains Z_1 and the two groups suitable for G_1 are isomorphic modulo their centers.

One can apply Lemma 5.2(i) to show that it is not possible to choose an element in $G_{12} \setminus G_{12}^0$ to centralize a quasi-complement in T. Therefore G_2/G_{12}^0 is not the group of 'pure' dent permutations as in Lemma 4.5.

Now it remains 'to bring back' Z_2. By Lemma 6.1(i) we know that G_{12}^0 is a perfect central extension of T and by the universality principle there is a surjective homomorphism

$$\varphi : \tilde{T} \to G_{12}^0.$$

By Lemmas 4.8 and 6.1(v) $|Z(\tilde{T})| = 2^4$. Therefore $\ker(\varphi)$ is of order 2^2 and G_2 exists if and only if $\ker(\varphi)$ is invariant under the action on $Z(\tilde{T})$ of $G_2/G_{12}^0 \cong Sym_3$. This is the point where the choice between the two possibilities for G_1 becomes essential.

Let $\hat{G}_1$ be the covering group of G_1 as in the first paragraph of this section, and let $\hat{T}$ be the preimage of G_{12}^0 in $\hat{G}_1$. Since the stabilizer N_0 in C_0 of the frame $\mathcal{F}$ is a perfect group, it is easy to see that $\hat{T}$ is also perfect and hence there is a surjective homomorphism

$$\psi : \tilde{T} \to \hat{T}.$$

The group $Z(\hat{T})$ is elementary abelian of order 2^3. In view of Lemma 4.11 this shows that $Z(\tilde{T})$ is also elementary abelian. Furthermore, $\ker(\psi)$ is of order 2 contained in $\ker(\varphi)$. Let χ be the homomorphism of $\hat{G}_1$ onto G_1. Then $\ker(\chi)$ is a subgroup of order 2 in the center of $\hat{G}_1$ which is not the commutator of the preimage of Q_1 in $\hat{G}_1$. Clearly this kernel is contained in $\hat{T}$. Let

$$\chi^{(i)} : \hat{T} \to G_{12}^0$$

be the homomorphism induced by χ, so that φ is the composition of φ and $\chi^{(i)}$ (we have introduced the superscript to make explicit the two choices for G_1).

Lemma 6.6. *Let r be an element of order 3 from G_2/G_{12}^0 and d be a generator of G_{12}/G_{12}^0. Then r has five orbits on $Z(\tilde{T})^\#$, say $S_1, \ldots, S_5$. These orbits can be renumbered so that*

(i) *$S_1 = Y^\#$ where $Y = [\tilde{Q}, \tilde{E}]$;*
(ii) *d has one fixed point in each of S_1, S_2, S_3 and no further fixed points in $Z(\tilde{T})^\#$.*

Proof. By Lemma 4.11 t acts on $Z(\tilde{T})$ fixed-point freely which gives the five orbits. It it clear that $Y^\#$ is one of them. The action of t defines on $Z(\tilde{T})$ a structure of a 2-dimensional $GF(4)$-space. Since d inverts t, it acts on $Z(\tilde{T})$ as a field automorphism which gives (ii). □

Let f_1, f_2 and f_3 be the vectors fixed by d and contained in the orbits S_1, S_2 and S_3, respectively. Since Y maps onto Z_2, we have $\ker(\varphi) \cap S_1 = \emptyset$. Therefore without loss we assume that

$$\ker(\psi) = \langle f_2 \rangle.$$

There are the following three subspaces of dimension 2 in $Z(\tilde{T})$ which are d-invariant and contain $\ker(\psi)$:

$$\langle f_1, f_2 \rangle, \ \langle S_2 \rangle, \ \langle f_2, f_3 \rangle.$$

We have seen that the former one cannot be the kernel of φ, while the last one is not t-invariant, which leaves us one and only possibility: $\ker(\varphi) = \langle S_2 \rangle$. This completes the proof of Theorem 1.

7. Conclusion

We conclude the article by the following.

Lemma 7.1. *Let G_2 be as in Theorem* 1 *and $T = G_{12}^0/Z_2$. Then*

(i) $\mathrm{Out}(T) \cong Sym_3 \times 2$ *acts faithfully on* $Z(\tilde{T}) \cong 2^4$;
(ii) $\mathrm{Out}(G_{12}^0) = Sym_3$.

Proof. By Lemma 4.11 in order to prove (i) all we have to show is that the automorphism ν which centralizes Q_2/Z_2 and induces an outer automorphism of a quasi-complement does not centralize $Z(\tilde{T})$. Suppose it does. Then ν stabilizes $\ker(\varphi) = \langle S_2 \rangle$ and hence it induces an (outer) automorphism of G_2. The induced automorphism (which we also denote by ν) centralizes Z_2 and therefore it normalizes Q_1. Consider the image of ν in the automorphism group of Q_1. Since ν is not inner, it acts non-trivially on $Q_1/Z_1 \cong \bar{\Lambda}$ and commutes with the action of $\bar{G}_{12} \cong 2^{11} : M_{24}$. It is easy to deduce from Lemmas 5.1 and 5.2 that the only non-identity element in $GL(\bar{\Lambda})$ commuting with the action of $\bar{G}_{12}$ is the transvection τ with center $\bar{\lambda}_0$ and axis $\bar{\Lambda}^{(23)}$. However $\bar{\lambda}_0$ is isotropic with respect to $\theta_{\bar{\Lambda}}$ and therefore τ does not preserve $\theta_{\bar{\Lambda}}$. Since $\theta_{\bar{\Lambda}}$ is induced by the squaring map in Q_1, it is preserved by every automorphism of Q_1. This proves (i). Since every automorphism of G_2 can be lifted to an automorphism of $\tilde{T}$, (i) implies (ii). □

Lemma 7.1(i) is precisely the assertion (i) in Tits' [14, Proposition 1], III; the assertion (ii) is the essence of our Theorem 1.

Acknowledgments

The layout of the present article has emerged during the Groups and Geometries meeting in Oberwolfach in March 2005. I am thankful to Bernd Fischer for sharing his memories of the early days of the Monster, to Michael Aschbacher for his stimulating interest, and to Sergey Shpectorov for showing me how to relate the situation to the structure of tri-extraspecial groups.

References

[1] M. Aschbacher, Sporadic Groups, Cambridge Univ. Press, Cambridge, 1994.
[2] J.H. Conway, A simple construction of the Fischer–Griess Monster group, Invent. Math. 79 (1985) 513–540.
[3] D. Gorenstein, Finite Groups, Happer & Row, New York, 1968.
[4] R.L. Griess Jr., Schur multipliers of finite simple groups of Lie type, Trans. Amer. Math. Soc. 183 (1973) 355–421.
[5] R.L. Griess Jr., Schur multipliers of some sporadic simple groups, J. Algebra 32 (1974) 445–466.
[6] R.L. Griess Jr., The friendly giant, Invent. Math. 69 (1982) 1–102.
[7] R.L. Griess Jr., U. Meierfrankenfeld, Y. Segev, A uniqueness proof for the monster, Ann. of Math. 130 (1989) 567–602.
[8] A.A. Ivanov, Geometry of Sporadic Groups I, Petersen and Tilde Geometries, Cambridge Univ. Press, Cambridge, 1999.
[9] A.A. Ivanov, S.V. Shpectorov, Tri-extraspecial groups, J. Group Theory 8 (2005) 395–413.
[10] G. James, The modular characters of the Mathieu groups, J. Algebra 27 (1973) 57–111.
[11] T.M. Richardson, Local subgroups of the Monster and odd code loops, Trans. Amer. Math. Soc. 347 (1995) 1453–1531.
[12] St.D. Smith, Large extraspecial subgroups of width 4 and 6, J. Algebra 58 (1979) 251–281.
[13] J.G. Thompson, Uniqueness of the Fischer–Griess Monster, Bull. London Math. Soc. 11 (1979) 340–346.
[14] J. Tits, Remarks on Griess' construction of the Griess–Fischer sporadic group I, II, III, IV, Mimeographs letters, December 1982–July 1983.