Cambridge University Press
978-0-521-88994-0 - The Monster Group and Majorana Involutions
A. A. Ivanov
Excerpt
More information

1

M_{24} and all that

This chapter can be considered as a usual warming up with Mathieu and Conway groups, prior to entering the realm of the Monster. It is actually aimed at a specific goal to classify the groups which satisfy the following condition:

$$T \sim 2_+^{1+22}.M_{24}$$

The quotient $O_2(T)/Z(T)$ (considered as a $GF(2)$-module for $T/O_2(T) \cong M_{24}$) has the irreducible Todd module $\mathcal{C}_{11}^*$ as a submodule and the irreducible Golay code module $\mathcal{C}_{11}$ as the corresponding factor module. It turns out that there are exactly two such groups T: one splits over $O_2(T)$ with $O_2(T)/Z(T)$ being the direct sum $\mathcal{C}_{11}^* \oplus \mathcal{C}_{11}$, while the other does not split, and the module $O_2(T)/Z(T)$ is indecomposable. The latter group is a section in the group which is the first member $2_+^{1+24}.Co_1$ of the Monster amalgam.

1.1 Golay code

Let F be a finite field, and let (m, n) be a pair of positive integers with $m \leq n$. A linear (m, n)-code over F is a triple $(V_n, \mathcal{P}, \mathcal{C})$ where V_n is an n-dimensional F-space, $\mathcal{P}$ is a basis of V_n, and $\mathcal{C}$ is a m-dimensional subspace in V_n. Although the presence of V_n and $\mathcal{P}$ is always assumed, it is common practice to refer to such a code simply by naming $\mathcal{C}$. It is also assumed (often implicitly) that V_n is endowed with a bilinear form b with respect to which $\mathcal{P}$ is an orthonormal basis

$$b(p, q) = \delta_{pq} \text{ for } p, q \in \mathcal{P}.$$

The dual code of $\mathcal{C}$ is the orthogonal complement of $\mathcal{C}$ in V_n with respect to b, that is

$$\{e \mid e \in V_n, b(e, c) = 0 \text{ for every } c \in \mathcal{C}\}.$$

Since b is non-singular, the dual of an (m, n)-code is an $(n - m, n)$-code. Therefore, $\mathcal{C}$ is self-dual if and only if it is totally singular of dimension half the dimension of V_n. The weight $wt(c)$ of a codeword $c \in \mathcal{C}$ is the number of non-zero components of c with respect to the basis $\mathcal{P}$. The minimal weight of $\mathcal{C}$ is defined as

$$m(\mathcal{C}) = \min_{c \in \mathcal{C} \setminus \{0\}} wt(c).$$

The codes over the field of two elements are known as *binary codes*. In the binary case, the map which sends a subset of $\mathcal{P}$ onto the sum of its elements provides us with an identification of V_n with the power set of $\mathcal{P}$ (the set of all subsets of $\mathcal{P}$). Subject to this identification, the addition is performed by the symmetric difference operator, the weight is just the size and b counts the size of the intersection taken modulo 2, i.e. for $u, v \subseteq \mathcal{P}$ we have

$$u + v = (u \cup v) \setminus (u \cap v);$$
$$wt(u) = |u|;$$
$$b(u, v) = |u \cap v| \bmod 2.$$

A binary code is said to be *even* or *doubly even* if the weights (i.e. sizes) of all the codewords are even or divisible by four, respectively. Notice that a doubly even code is always totally singular with respect to b.

A binary (12, 24)-code is called a (binary) *Golay code* if it is doubly even, self-dual of minimal weight 8. Up to isomorphism there exists a unique Golay code which we denote by $\mathcal{C}_{12}$. In view of the above discussion, $\mathcal{C}_{12}$ can be defined as a collection of subsets of a 24-set $\mathcal{P}$ such that $\mathcal{C}_{12}$ is closed under the symmetric difference, the size of every subset in $\mathcal{C}_{12}$ is divisible by four but not four and $|\mathcal{C}_{12}| = 2^{12}$. The subsets of $\mathcal{P}$ contained in $\mathcal{C}_{12}$ will be called *Golay sets*.

There are various constructions for the Golay code. We are going to review some basic properties of $\mathcal{C}_{12}$ and of its remarkable automorphism group M_{24}. The properties themselves are mostly construction-invariant while the proofs are not. We advise the reader to refer to his favorite construction to check the properties (which are mostly well-known anyway) while we will refer to Section 2.2 of [Iv99].

The weight distribution of $\mathcal{C}_{12}$ is

$$0^1\, 8^{759}\, 12^{2576}\, 16^{759}\, 24^1,$$

which means that besides the improper subsets $\emptyset$ and $\mathcal{P}$ the family of Golay sets includes 759 subsets of size 8 (called *octads*), 759 complements of octads, and 2576 subsets of size 12 called *dodecads* (splitting into 1288 complementary pairs). If $\mathcal{B}$ is the set of octads, then $(\mathcal{P}, \mathcal{B})$ is a Steiner system of type $S(5, 8, 24)$ (this means that every 5-subset of $\mathcal{P}$ is in a unique octad). Up to isomorphism $(\mathcal{P}, \mathcal{B})$ is the unique system of its type and $\mathcal{C}_{12}$ can be redefined as the closure of $\mathcal{B}$ with respect to the symmetric difference operator in the unique Steiner system of type $S(5, 8, 24)$.

If $(V_{24}, \mathcal{P}, \mathcal{C}_{12})$ is the full name of the Golay code, then

$$\mathcal{C}_{12}^* := V_{24}/\mathcal{C}_{12}$$

is known as the 12-dimensional *Todd module*. We continue to identify V_{24} with the power set of $\mathcal{P}$ and for $v \subseteq \mathcal{P}$ the coset $v + \mathcal{C}_{12}$ (which is an element of $\mathcal{C}_{12}^*$) will be denoted by v^*. It is known that for every $v \subseteq \mathcal{P}$ there is a unique integer $t(v) \in \{0, 1, 2, 3, 4\}$ such that $v^* = w^*$ for some $w \subseteq \mathcal{P}$ with $|w| = t(v)$. Furthermore, if $t(v) < 4$, then such w is uniquely determined by v; if $t(v) = 4$, then the collection

$$\mathcal{S}(v) = \{w \mid w \subseteq \mathcal{P}, |w| = 4, v^* = w^*\}$$

forms a *sextet*. The latter means that $\mathcal{S}(v)$ is a partition of $\mathcal{P}$ into six 4-subsets (also known as *tetrads*) such that the union of any two tetrads from $\mathcal{S}(v)$ is an octad. Every tetrad w is in the unique sextet $\mathcal{S}(w)$ and therefore the number of sextets is

$$1771 = \binom{24}{4}/6.$$

The automorphism group of the Golay code (which is the set of permutations of $\mathcal{P}$ preserving $\mathcal{C}_{12}$ as a whole) is the sporadic simple Mathieu group M_{24}. The action of M_{24} on $\mathcal{P}$ is 5-fold transitive and it is similar to the action on the cosets of another Mathieu group M_{23}. The stabilizer in M_{24} of a *pair* (a 2-subset of $\mathcal{P}$) is an extension of the simple Mathieu group M_{22} of degree 22 (which is the elementwise stabilizer of the pair) by an outer automorphism of order 2. The stabilizer of a *triple* is an extension of $L_3(4)$ (sometimes called the Mathieu group of degree 21 and denoted by M_{21}) by the symmetric group S_3 of the triple.

The sextet stabilizer $M(\mathcal{S})$ is an extension of a group $K_{\mathcal{S}}$ of order $2^6 \cdot 3$ by the symmetric group S_6 of the set of tetrads in the sextet. The group $K_{\mathcal{S}}$ (which is the kernel of the action of $M(\mathcal{S})$ on the tetrads in the sextet is a semidirect product of an elementary abelian group $Q_{\mathcal{S}}$ of order 2^6 and a group $X_{\mathcal{S}}$ of order 3 acting on $Q_{\mathcal{S}}$ fixed-point freely. If we put

$$Y_{\mathcal{S}} = N_{M(\mathcal{S})}(X_{\mathcal{S}}),$$

then $Y_{\mathcal{S}} \cong 3 \cdot S_6$ is a complement to $Q_{\mathcal{S}}$ in $M(\mathcal{S})$; $Y_{\mathcal{S}}$ does not split over $X_{\mathcal{S}}$ and $C_{Y_{\mathcal{S}}}(X_{\mathcal{S}}) \cong 3 \cdot A_6$ is a perfect central extension of A_6. Furthermore, $Y_{\mathcal{S}}$ is the stabilizer in M_{24} of a 6-subset of $\mathcal{P}$ not contained in an octad (there is a single M_{24}-orbit on the set of such 6-subsets).

Because of the 5-fold transitivity of the action of M_{24} on $\mathcal{P}$, and since $(\mathcal{P}, \mathcal{B})$ is a Steiner system, the action of M_{24} on the octads is transitive. The stabilizer of an octad is the semidirect product of an elementary abelian group $Q_{\mathcal{O}}$ of order 2^4 (which fixes the octad elementwise) and a group $K_{\mathcal{O}}$ which acts faithfully as the alternating group A_8 on the elements in the octad and as the linear group $L_4(2)$ on $Q_{\mathcal{O}}$ (the latter action is by conjugation). Thus, the famous isomorphism $A_8 \cong L_4(2)$ can be seen here. The action of M_{24} on the dodecads is transitive, with the stabilizer of a dodecad being the simple Mathieu group M_{12} acting on the dodecad and on its complement as on the cosets of two non-conjugate subgroups each isomorphic to the smallest simple Mathieu group M_{11}. These two M_{11}-subgroups are permuted by an outer automorphism of M_{12} realized in M_{24} by an element which maps the dodecad onto its complement.

The following lemma is easy to deduce from the description of the stabilizers in M_{24} of elements in $\mathcal{C}_{12}$ and in $\mathcal{C}_{12}^*$.

Lemma 1.1.1 *Let u and v be elements of $\mathcal{C}_{12}$, and let $M(u)$ and $M(v)$ be their respective stabilizers in M_{24}. Then:*

(i) *$M(u)$ does not stabilize non-zero elements of $\mathcal{C}_{12}^*$;*
(ii) *if u and v are octads, then $(u \cap v)^*$ is the only non-zero element of $\mathcal{C}_{12}^*$ stabilized by $M(u) \cap M(v)$.* □

A presentation $d = u + v$ of a dodecad as the sum (i.e. symmetric difference) of two octads determines the pair $u \cap v$ in the dodecad complementary to d and also a partition of d into two *heptads* (6-subsets) $u \setminus v$ and $v \setminus u$. If $\mathcal{K}$ is the set of all heptads obtained via such presentations of d, then $(d, \mathcal{K})$ is a Steiner system of type $S(5, 6, 12)$ (every 5-subset of d is in a unique heptad). There is a bijection between the pairs of complementary heptads from $\mathcal{K}$ and the set of pairs in $\mathcal{P} \setminus d$ such that if $d = h_1 \cup h_2$ corresponds to $\{p, q\}$, then $h_1 \cup \{p, q\}$ and $h_2 \cup \{p, q\}$ are octads, and d is their symmetric difference.

Lemma 1.1.2 *Let d be a dodecad, $\{p, q\}$ be a pair disjoint from d, and let $d = h_1 \cup h_2$ be the partition of d into heptads which correspond to $\{p, q\}$. Let A be the stabilizer in M_{24} of d and $\{p, q\}$, and let B be the stabilizer in M_{24} of h_1, h_2, and $\{p, q\}$. Then:*

(i) $A \cong \mathrm{Aut}(S_6)$, *while* $B \cong S_6$*;*
(ii) $A \setminus B$ *contains an involution.*

Proof. (i) is Lemma 2.11.7 in [Iv99] while (ii) is a well-known property of the automorphism group of S_6. □

Lemma 1.1.3 ([CCNPW]) *The following assertions hold:*

(i) *the outer automorphism group of M_{24} is trivial;*
(ii) *the Schur multiplier of M_{24} is trivial.* □

1.2 Todd module

The 24-dimensional space V_{24} containing $\mathcal{C}_{12}$ and identified with the power set of $\mathcal{P}$ carries the structure of the $GF(2)$-permutation module of M_{24} acting on $\mathcal{P}$. With respect to this structure, $\mathcal{C}_{12}$ is a 12-dimensional submodule known as the *Golay code module*. Let $V^{(1)}$ and $V^{(23)}$ be the subspaces in V_{24} formed by the improper and even subsets of $\mathcal{P}$, respectively. Then $V^{(1)}$ and $V^{(23)}$ are the M_{24}-submodules contained in $\mathcal{C}_{12}$ and containing $\mathcal{C}_{12}$, respectively. Put

$$\mathcal{C}_{11} = \mathcal{C}_{12}/V^{(1)} \text{ and } \mathcal{C}_{11}^* = V^{(23)}/\mathcal{C}_{12}.$$

The elements of $V_{24}/V^{(1)}$ are the partitions of $\mathcal{P}$ into pairs of subsets. There are two M_{24}-orbits on $\mathcal{C}_{11} \setminus \{0\}$. One of the orbits consists of the partitions involving octads and other one the partitions into pairs of complementary dodecads. Acting on $\mathcal{C}_{11}^* \setminus \{0\}$, the group M_{24} also has two orbits, this time indexed by the pairs and the sextets

$$|\mathcal{C}_{11}| = 1 + 759 + 1288; \quad |\mathcal{C}_{11}^*| = 1 + 276 + 1771.$$

Already from this numerology it follows that both $\mathcal{C}_{11}$ and $\mathcal{C}_{11}^*$ are irreducible and not isomorphic to each other. The modules $\mathcal{C}_{11}$ and $\mathcal{C}_{11}^*$ are known as the *irreducible Golay code and Todd modules* of M_{24}, respectively.

Since $\mathcal{C}_{12}$ is totally singular and $V^{(1)}$ is the radical of b, the bilinear form b establishes a duality between $\mathcal{C}_{12}$ and $\mathcal{C}_{12}^*$ and also between $\mathcal{C}_{11}$ and $\mathcal{C}_{11}^*$. Since M_{24} does not stabilize non-zero vectors in $\mathcal{C}_{12}^*$, the latter is indecomposable. Because of the dually, $\mathcal{C}_{12}$ is also indecomposable.

Lemma 1.2.1 *The series*

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

is the only composition series of V_{24} *considered as the module for* M_{24}.

Proof. We have seen that the above series is indeed a composition series. Since both $\mathcal{C}_{12}$ and $\mathcal{C}_{12}^*$ are indecomposable, in order to prove the uniqueness it is sufficient to show that $V_{24}/V^{(1)}$ does not contain $\mathcal{C}_{11}^*$ as a submodule. Such a submodule would contain an M_{24}-orbit X indexed by the pairs from $\mathcal{P}$. On the other hand, by the 5-fold transitivity of M_{24} on $\mathcal{P}$, the stabilizer of a pair stabilizes only one proper partition of $\mathcal{P}$ (which is the partition into the pair and its complement). Therefore, X has no choice but to consist of all such partitions. But then X would generate the whole of $V^{(23)}/V^{(1)}$, which proves that X does not exist. □

If K is a group and U is a $GF(2)$-module for K, then $H^1(K,U)$ and $H^2(K,U)$ denote the first and the second cohomology groups of U. Each of these groups carries a structure of a $GF(2)$-module, in particular it is elementary abelian. The order of $H^1(K,U)$ is equal to the number of classes of complements to U in the semidirect product $U : K$ of U and K (with respect to the natural action), while the elements of $H^2(K,U)$ are indexed by the isomorphism types of extensions of U by K with the identity element corresponding to the split extension $U : K$. If W is the largest indecomposable extension of U by a trivial module, then $W/U \cong H^1(K,U)$ and all the complements to W in the semidirect product $W : K$ are conjugate and $H^1(K,W)$ is trivial. Dually, if V is the largest indecomposable extension of a trivial module V_0 by U, then $V_0^* \cong H^1(K,U^*)$ (here U^* is the dual module of U)

Lemma 1.2.2 *The following assertions hold:*

(i) $H^1(M_{24},\mathcal{C}_{11})$ *is trivial;*
(ii) $H^2(M_{24},\mathcal{C}_{11})$ *is trivial;*
(iii) $H^1(M_{24},\mathcal{C}_{11}^*)$ *has order* 2*;*
(iv) $H^2(M_{24},\mathcal{C}_{11}^*)$ *has order* 2. □

Proof. The first cohomologies were computed in Section 9 in [Gri74]. The second cohomologies calculations are commonly attributied to D.J. Jackson [Jack80] (compare [Th79a]). All the assertions were rechecked by Derek Holt using his computer package for cohomology calculating. □

In view of the paragraph before the lemma, by (ii) every extension of $\mathcal{C}_{11}$ by M_{24} splits; by (i) all the M_{24}-subgroups in the split extension $\mathcal{C}_{11} : M_{24}$ are conjugate; by (iv) there exists a unique non-split extension (denoted by

Cambridge University Press
978-0-521-88994-0 - The Monster Group and Majorana Involutions
A. A. Ivanov
Excerpt
More information

$\mathcal{C}_{11}^* \cdot M_{24}$), while by (iii) the split extension $\mathcal{C}_{11}^* : M_{24}$ contains two classes of complements (these classes are fused in $\mathcal{C}_{12}^* : M_{24}$). Furthermore, every extension by $\mathcal{C}_{11}^*$ of a trivial module is semisimple (which means decomposable), while $\mathcal{C}_{12}$ is the largest indecomposable extension by $\mathcal{C}_{11}$ of a trivial module.

The following result has been recently established by Derek Holt using computer calculations and in a sense it assures success of our construction of the Monster amalgam.

Lemma 1.2.3 *The following assertions hold* (*where $\otimes$ and $\wedge$ denote the tensor and exterior products of modules*)*:*

(i) $H^1(M_{24}, \mathcal{C}_{11}^* \otimes \mathcal{C}_{11}^*)$ *has order* 2*;*
(ii) $H^1(M_{24}, \mathcal{C}_{11}^* \wedge \mathcal{C}_{11}^*)$ *has order* 2. □

The following assertion is a rather standard consequence of the above statement but a sketch of a proof might be helpful.

Corollary 1.2.4 *The following hold:*

(i) *there exists a unique indecomposable extension of $\mathcal{C}_{11}^*$ by $\mathcal{C}_{11}$;*
(ii) *the extension in* (i) *carries a non-singular invariant quadratic form of plus type.*

Proof. To prove (i) we need to enumerate (up to the obvious equivalence) the pairs (V, M) where $M \cong M_{24}$ and V is an M-module having $\mathcal{C}_{11}^*$ as a submodule and $\mathcal{C}_{11}$ as the corresponding factor module. We should keep in mind that exactly one such pair corresponds to the decomposable extension (where $V = \mathcal{C}_{11}^* \oplus \mathcal{C}_{11}$). We start with a 22-dimensional $GF(2)$-space V and enumerate the suitable subgroups M in the general linear group $G = GL(V) \cong GL_{22}(2)$. Let U_1 and U_2 be a pair of disjoint 11-dimensional subspaces in V. Then $N_G(U_1)$ is a semidirect product of

$$C = C_G(U_1) \cap C_G(V/U_1) \cong U_1 \otimes U_2^*$$

and

$$K = N_G(U_1) \cap N_G(U_2) \cong GL(U_1) \times GL(U_2).$$

Let M_0 be a subgroup of K isomorphic to M_{24} which acts on U_1 as on $\mathcal{C}_{11}^*$ and on U_2 as on $\mathcal{C}_{11}$. It is easy to see that up to conjugation in K such subgroup M_0 can be chosen uniquely. Then (V, M_0) is the pair corresponding to the decomposable extension and any other M which suits the requirements is a complement to C in CM_0. Since $C \cong \mathcal{C}_{11}^* \otimes \mathcal{C}_{11}^*$ (as an M_0-module), (1.2.3 (i)) shows that there is exactly one further complement M_1. The action of M_1 on V is indecomposable.

To establish (ii) we enumerate the triples (V, M, q) where V and M are as above and q is an M-invariant non-singular quadratic form on V. In this case we start with an orthogonal space (V, q) and enumerate the suitable subgroups M in the orthogonal group $H = O(V, q)$. Since $\mathcal{C}_{11}^*$ is irreducible and since it is not self-dual, the submodule in V isomorphic to $\mathcal{C}_{11}^*$ must be totally isotropic. Therefore, we choose U_1 and U_2 as in (i) and assume that each of them is totally isotropic with respect to q. Then $N_H(U_1)$ is a semidirect product of

$$D = C_H(U_1) \cong U_1 \wedge U_1$$

and

$$L = N_H(U_1) \cap N_H(U_2) \cong GL(U_1).$$

Take M_0 to be the subgroup in L isomorphic to M_{24} which acts on U_1 as on $\mathcal{C}_{11}^*$ (since the bilinear form associated with q establishes a duality between U_1 and U_2, M_0 acts on U_2 as on $\mathcal{C}_{11}$). By (1.2.3 (ii)) up to conjugation, $DL \cong (\mathcal{C}_{11}^* \wedge \mathcal{C}_{11}^*) : M_0$ contains, besides M_0, exactly one further complement which must be M_1. By (i) the pair (V, M_1) corresponds to the unique indecomposable extension. □

In the next section the indecomposable extension of $\mathcal{C}_{11}^*$ by $\mathcal{C}_{11}$ will be constructed explicitly along with the invariant quadratic form on it.

Let U be a $GF(2)$-module for K and let $U : K$ denote the semidirect product of U and K with respect to the natural action. Then (since U is abelian) all the complements to U in $U : K$ are conjugate in the automorphism group of $U : K$. Therefore, $H^1(K, U)$ 'contributes' to the outer automorphism group of $U : K$. In fact this contribution takes place for any extension of U by K. In order to explain this phenomenon (which is probably well-known), we recall the notion of *partial semidirect product* (cf. p.27 in [G68]).

Let X, Y, Z be groups, let

$$\varphi_X : Z \to X,$$
$$\varphi_Y : Z \to Y$$

be monomorphisms whose images are normal in X and Y, respectively, and let

$$\alpha : X \to \mathrm{Aut}(Y)$$

be a homomorphism such that for every $x \in X$ and $z \in Z$ the following equality holds

$$\varphi_X^{-1}(x^{-1}\varphi_X(z)x) = \varphi_Y^{-1}(\varphi_Y(z)^{\alpha(x)})$$

(notice that the equality implies that $\alpha(X)$ normalizes $\varphi_Y(Z)$). The usual semidirect product $S = Y : X$ of Y and X associated with the homomorphism α is the set

$$S = \{(x, y) \mid x \in X, y \in Y\}$$

together with the multiplication rule

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1^{\alpha(x_2)} y_2).$$

The *partial semidirect product* of Y and X over Z is the quotient of S/Z_S where

$$S_Z = \{(\varphi_X(z), \varphi_Y(z^{-1})) \mid z \in Z\}$$

is a 'diagonal' subgroup of S isomorphic to Z.

Lemma 1.2.5 *Let U be a $GF(2)$-module for a group K and let E be an extension (split or non-split) of U by K. Then there is an injective homomorphism of $H^1(K, U)$ into* $\mathrm{Out}(E)$.

Proof. Let W be the largest indecomposable extension of U by a trivial module, so that $W/U \cong H^1(K, U)$ and let P be the partial semidirect product of W and E over U with respect to the homomorphism $\alpha : E \to GL(W)$ such that U acts trivially and $E/U \cong K$ acts naturally. Then E is (isomorphic to) a self-centralizing normal subgroup in P (so that $P/E \le \mathrm{Out}(E)$) and $P/E \cong W/U \cong H^1(K, U)$, which gives the result. □

The partial semidirect product of $\mathcal{C}_{11}^* \cdot M_{24}$ and $\mathcal{C}_{12}^*$ over $\mathcal{C}_{11}^*$ is a non-split extension of $\mathcal{C}_{12}^*$ by M_{24} and we denote the extension by $\mathcal{C}_{12}^* \cdot M_{24}$. The following result is not difficult to deduce from the data on M_{24} and its modules we have revealed already.

Lemma 1.2.6 *The following assertions hold:*

(i) $\mathcal{C}_{12}^* \cdot M_{24} = \mathrm{Aut}(\mathcal{C}_{11}^* \cdot M_{24})$;
(ii) *$\mathcal{C}_{12}^* \cdot M_{24}$ is the only non-split extension of $\mathcal{C}_{12}^*$ by M_{24};*
(iii) *the Schur multiplier of $\mathcal{C}_{11}^* \cdot M_{24}$ is trivial.* □

We will make use of the following result of a combinatorial nature:

Lemma 1.2.7 *Let X be a subgroup of the general linear group $GL(\mathcal{C}_{11})$ containing M_{24} and having on the element set of $\mathcal{C}_{11}$ the same orbits as M_{24} does (with lengths* 1, 759, *and* 1288*). Then $X = M_{24}$.*

Proof. The semidirect product $\mathcal{C}_{11} : X$ acting on the cosets of X is an affine rank three permutation group. All such groups were classified in [Lie87] and the assertion can be deduced as a consequence of that classification (of course the assertion can be proved independently as a pleasant combinatorial exercise). □

1.3 Anti-heart module

The *intersection map* $\mathcal{C}_{12} \times \mathcal{C}_{12} \to \mathcal{C}_{12}^*$, defined by

$$(u, v) \mapsto (u \cap v)^*$$

is bilinear. Since any two Golay sets intersect evenly the image of the intersection map is $\mathcal{C}_{11}^*$. The intersection map (considered as a cocycle) determines an extension W_{24} of $\mathcal{C}_{12}^*$ by $\mathcal{C}_{12}$

$$W_{24} = \{(u, v^*) \mid u \in \mathcal{C}_{12}, v^* \in \mathcal{C}_{12}^*\}$$

with

$$(u_1, v_1^*) + (u_2, v_2^*) = (u_1 + u_2, v_1^* + v_2^* + (u_1 \cap u_2)^*).$$

By (1.2.1), the permutation module V_{24} is an indecomposable extension of $\mathcal{C}_{12}$ by $\mathcal{C}_{12}^*$. We call W_{24} the *anti-permutation* module. As the next lemma shows, the anti-permutation module is also indecomposable.

Lemma 1.3.1 *Let W_{24} be the above-defined anti-permutation module of M_{24}. Put*

$$W^{(1)} = \{(u, 0) \mid u \in V^{(1)}\},$$
$$W^{(23)} = \{(u, v^*) \mid u \in \mathcal{C}_{12}, v^* \in \mathcal{C}_{11}^*\},$$
$$\mathcal{S}_{12}^* = \{(0, v^*) \mid v^* \in \mathcal{C}_{12}^*\}, \quad \mathcal{S}_{12} = \{(u, 0) \mid u \in \mathcal{C}_{12}\}.$$

The following assertions hold:

(i) *$W^{(1)}$ and $W^{(23)}$ are the only submodules in W_{24} of dimension and co-dimension* 1, *respectively;*
(ii) *$\mathcal{S}_{12}^*$ is a submodule in W_{24} isomorphic to $\mathcal{C}_{12}^*$;*
(iii) *$\mathcal{S}_{11}^* := \mathcal{S}_{12}^* \cap W^{(23)}$ is a submodule isomorphic to $\mathcal{C}_{11}^*$;*
(iv) *$\mathcal{S}_{12}$ is M_{24}-invariant; it maps bijectively onto $W_{24}/\mathcal{S}_{12}^* \cong \mathcal{C}_{12}$, although $\mathcal{S}_{12}$ is not closed under the addition in W_{24};*
(v) *$W^{(23)}/W^{(1)}$ is an indecomposable extension of $\mathcal{C}_{11}^*$ by $\mathcal{C}_{11}$.*

Proof. Since $\mathcal{C}_{12}$ and $\mathcal{C}_{12}^*$ are indecomposable containing one trivial composition factor each, (i) follows. Now (ii), (iii), and (iv) are easy to check using