1

The Mathieu Group M_{24} As We Knew It

In this chapter we start by reviewing the common way to describe the Mathieu group $G = M_{24}$ as the automorphism group of the binary Golay code and of the Steiner system formed by the minimal codewords in the Golay code. This discussion will lead us to the structure of the octad–trio–sextet stabilizers $\{G_1, G_2, G_3\}$. The starting point is the observation that, when forming a similar triple $\{H_1, H_2, H_3\}$ comprised of the stabilizers of one-, two- and three-dimensional subspaces in $H = L_5(2)$, we have

$$G_1 \cong H_1 \cong 2^4 : L_4(2), \quad G_2 \cong H_2 \cong 2^6 : (L_3(2) \times S_3),$$
$$[G_1 : G_1 \cap G_2] = [H_1 : H_1 \cap H_2] = 15,$$
$$[G_2 : G_1 \cap G_2] = [H_2 : H_1 \cap H_1] = 3,$$

so that the *amalgams* $\{G_1, G_2\}$ and $\{H_1, H_2\}$ have the *same type* according to Goldschmidt's terminology, although they are not isomorphic and differ by a *twist* performed by an outer automorphism of

$$H_1 \cap H_2 \cong G_1 \cap G_2 \cong (2^3 \times 2^3) : (L_3(2) \times 2),$$

which permutes conjugacy classes of $L_3(2)$-subgroups. This observation led us to the construction of M_{24} as the universal completion of a twisted $L_5(2)$-amalgam.

1.1 The Golay Code

Commonly the Mathieu group M_{24} is defined as the automorphism group of the Golay code, which by definition is a (a) binary (b) linear code (c) of length 24, which is (d) even, (e) self-dual and (f) has no codewords of weight 4.
By (a) we can identify a codeword with its support in the standard basis and view the Golay code as a pair $(\mathcal{P}, \mathcal{C})$, where $\mathcal{P}$ is a set and $\mathcal{C}$ is a collection

of subsets of $\mathcal{P}$, so that $\mathcal{P}$ together with an ordering can be identified with the standard basis of the vector space $2^{\mathcal{P}} := \{A \mid A \subseteq \mathcal{P}\}$ in which addition is performed by the symmetric difference operator:

$$A + B := (A \cup B) \setminus (A \cap B).$$

The *weight* of $A \subseteq \mathcal{P}$ is its cardinality $|A|$ and the remaining defining properties of the Golay code can be restated as follows:

(b) $\mathcal{C}$ is closed under addition;
(c) $|\mathcal{P}| = 24$;
(d) every subset in $\mathcal{C}$ has an even number of elements;
(e) a subset B of $\mathcal{P}$ intersects evenly every $A \in \mathcal{C}$ exactly when B is taken from $\mathcal{C}$;
(f) the minimal weight of $\mathcal{C}$ is 8.

It is convenient to deduce the numerology of the Golay code starting with consideration of its co-code $\mathcal{C}^* := 2^{\mathcal{P}}/\mathcal{C}$. For $A \subseteq \mathcal{P}$ let A^* denote the image of A in the co-code: $A^* = A + \mathcal{C}$. The following *cardinality* attribute is immediately evident from the minimal weight of $\mathcal{C}$ being 8.

Lemma 1.1 *Whenever two distinct subsets A and B in $\mathcal{P}$, each of cardinality at most 4, have the same image in $\mathcal{C}^*$, the equality $|A| = |B| = 4$ holds, and A is disjoint from B.* □

Let $\mathcal{P}_{(4)}$ be the set of all subsets of cardinality at most 4 in $\mathcal{P}$. Since it is not possible to find more than six pairwise disjoint 4-subsets in a 24-set, the *cardinality* attribute Lemma 1.1 gives the following lower bound on the size of the image $\mathcal{P}^*_{(4)}$ of $\mathcal{P}_{(4)}$ in $\mathcal{C}^*$:

$$|\mathcal{P}^*_{(4)}| \geq 1 + 24 + \binom{24}{2} + \binom{24}{3} + \frac{1}{6}\binom{24}{4} = 2^{12}.$$

On the other hand, the self-duality of $\mathcal{C}$ means that it is a maximal isotropic subspace in $2^{\mathcal{P}}$ with respect to the non-degenerate symplectic form

$$f : (A, B) \mapsto |A \cap B| \mod 2.$$

Thus the dimension of $\mathcal{C}$ is exactly *half* the dimension of $2^{\mathcal{P}}$, so that $|\mathcal{C}| = |\mathcal{C}^*| = 2^{12}$, and the above lower bound is attained. Therefore $\mathcal{C}^* = \mathcal{P}^*_{(4)}$, which brings about the following *representative* principle.

Lemma 1.2 *For every $X \subseteq \mathcal{P}$ the coset X^* contains a subset A of cardinality at most 4. The cardinality of such a subset A is uniquely determined by X. If the cardinality of A is strictly less than 4 then A itself is uniquely determined by*

X, but if the cardinality is 4 *then there are precisely six choices for A forming a partition of $\mathcal{P}$ into six disjoint* 4*-subsets.* □

Let us introduce some further terminology by calling the minimal non-empty subsets of $\mathcal{C}$ (having size eight) *octads*, and denoting by $\mathcal{B}$ the set of octads. A partition of $\mathcal{P}$ into six 4-subsets such that the union of any two of them is an octad is known as a *sextet*. Notice that the partition which appeared in the last sentence of the *representative* principle Lemma 1.2 is a sextet. A partition of $\mathcal{P}$ into three disjoint octads is called a *trio*. Let $\mathcal{S}$ and $\mathcal{T}$ denote the sets of sextets and trios, respectively. Given a sextet, one can easily construct a trio by taking a sub-partition of the sextet, and then $\mathcal{P}$ is an element of $\mathcal{C}$, since it is the sum of the octads in a trio. Also two distinct octads cannot share a 5-set, because of the minimal weight property. These observations, together with the *representative* principle, give the following *Steiner* attribute.

Lemma 1.3 *Every* 4*-subset of $\mathcal{P}$ is a member of a unique sextet, and every* 5*-subset is contained in a unique octad. Furthermore, trios exist and $\mathcal{P}$, viewed as an element from $2^{\mathcal{P}}$, is contained in $\mathcal{C}$.* □

Now easy combinatorial counting demonstrates the equalities

$$|\mathcal{S}| = \frac{1}{6}\binom{24}{4} = 1771 \text{ and } |\mathcal{B}| = \frac{\binom{24}{5}}{\binom{8}{5}} = 759.$$

The pair $(\mathcal{P}, \mathcal{B})$ is a Steiner system of type $S(24, 8, 5)$, which by definition is a collection of 8-subsets in a 24-set such that every 5-subset is covered by exactly one 8-subset from the collection.

In order to calculate the number of trios we first analyze how two octads can intersect. Let n_i denote the number of octads intersecting a given octad B in exactly i elements. Clearly $n_8 = 1$, while $n_i = 0$ whenever i is odd by the self-duality condition, and $n_6 = 0$ by the minimal weight condition. A 4-subset X is contained in five octads which are unions of the pairs of 4-subsets in the sextet determined by X and B is one of them. This readily gives the equality

$$n_4 = \binom{8}{4}(5 - 1) = 280.$$

In order to calculate n_2 we consider a 5-subset Q which intersects B in exactly two elements. The unique octad $B(Q)$ containing Q might intersect B in four points, but all such subsets Q can be counted, since n_4 is known. For the remaining Qs we have $|B \cap B(Q)| = 2$, which gives

$$n_2 = \left[\binom{8}{2}\binom{16}{3} - n_4\binom{4}{2}\binom{4}{3}\right] \Big/ \binom{6}{3} = 448.$$

Finally,

$$n_0 = |\mathcal{B}| - n_8 - n_4 - n_2 = 30.$$

Since $\mathcal{C}$ is linear and contains $\mathcal{P}$, the complement of the union of two disjoint octads is again an octad, so that an octad is contained in $15 = n_0/2$ trios and

$$|\mathcal{T}| = |\mathcal{B}| \cdot n_0/(2 \cdot 3) = 3795.$$

Any two disjoint octads determine a trio, which implies that any two octads that are disjoint from a given octad B are either disjoint forming a trio with B, or intersect each other in a 4-subset. Since an octad is contained in more than one trio, this demonstrates that every trio is sub-partitioned by a sextet. There are 15 partitions of a six-element set into three disjoint pairs, therefore every sextet sub-partitions 15 trios. In view of the equality

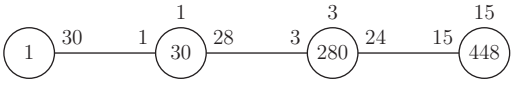
$$15 \cdot |\mathcal{S}| = 7 \cdot |\mathcal{T}|,$$

this implies that every trio is sub-partitioned by exactly seven sextets.

1.2 The Octad Graph

Define the *octad graph* Γ to be the graph having the set $\mathcal{B}$ of octads as the vertex set, in which two vertices are adjacent whenever they are disjoint as octads. From the discussion in the previous section, we have that Γ is regular of valency $n_0 = 30$ and every edge is contained in a unique triangle corresponding to a trio, and hence there are 15 triangles through a given vertex.

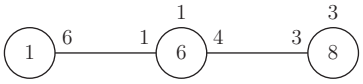
Theorem 1.4 *The octad graph Γ is distance-regular with the following intersection diagram:*



The intersection diagram indicates that the diameter of Γ is 3, while the number of vertices at distance i from any given vertex-octad B is 1, 30, 280 and 448 for $i = 0$, 1, 2 and 3, respectively. These numbers appear inside the circles read from left to right. If B' is a vertex at distance i from B then, among the 30 vertices adjacent to B', exactly c_i vertices are at distance $i-1$ from B, a_i at distance i and b_i at distance $i+1$. The parameters c_i, a_i and b_i depend not

on the individual choices of B and B', but only on the distance between them, and on the diagram they are drawn around the ith circle at 9, 12 and 3 o'clock, respectively.

Proof of Theorem 1.4 The values $b_0 = n_0 = 30$, $c_1 = 1$, $a_1 = 1$ and $b_1 = n_0 - c_1 - a_1 = 24$ have already been justified. For a sextet S the subgraph induced by the vertices or octads which are unions of pairs of 4-subsets in S is a 15-vertex subgraph of valency 6. This subgraph is the graph on 2-subsets of a six-element set in which two subsets are adjacent whenever they are disjoint. These subgraphs will be called *quads*, with every quad being distance-regular as described by the following diagram:



Since any two octads intersecting in four elements are unions of pairs of 4-subsets in the sextet determined by the intersection, we conclude that such octads are at distance 2 in Γ and are contained in a common quad. The diagram of the quad shows that $c_2 \geq 3$ and $a_2 \geq 3$, and hence $b_2 \leq 24$. Notice that at this stage the parameters c_2, a_2 and b_2 might still depend on the particular choice of the pair of vertices at distance 2 in Γ, but for any vertex of Γ the number $N_{2,3}$ of edges joining vertices at distance 2 with vertices at distance 3 from that vertex satisfies the inequality

$$N_{2,3} \leq 280 \cdot 24.$$

Suppose that B and B' are octads intersecting in a 2-subset, and let $T = \{B, B_1, B_2\}$ be a trio containing B. Then the 6-set $B' \setminus B$ splits between B_2 and B_3. Since any two octads intersect evenly and never share a 6-set, up to reordering the splitting is $6 = 4+2$. Therefore, in every triangle-trio containing B there is exactly one vertex at distance 2 from B' and the other two vertices, including B, are at distance 3, so that $c_3 = a_3 = 15$ and

$$N_{2,3} = 448 \cdot 15.$$

Since the value of $N_{2,3}$ attains the above upper bound, the equality $c_2 = a_2 = 3$ holds and the proof of distance-regularity is complete. □

1.3 A Review

In this section we reveal the existence and uniqueness features of the Golay code $\mathcal{C}$ and discuss the automorphism group of $\mathcal{C}$ along with some of

its important subgroups. In all the uniqueness statements the caveat *up to isomorphism* is implicit. The following statement of *existence-uniqueness* was first established by E. Witt in 1938 for the Steiner system.[1] The construction of the Golay code in 1949[2] extends it to the code, and for the octad graph the uniqueness was proved by A. E. Brouwer.[3]

Theorem 1.5 *There exists exactly one Steiner system* $(\mathcal{P}, \mathcal{B})$ *of type* $S(24, 8, 5)$. *The span of* $\mathcal{B}$ *in the power space* $2^{\mathcal{P}}$ *is the unique Golay code, and the octad graph* Γ *is the unique distance-regular graph with its intersection diagram subject to the existence of the quads.* □

The Steiner system $(\mathcal{P}, \mathcal{B})$ is uniquely reconstructible from the Golay code $\mathcal{C}$. In fact $\mathcal{C}$ can be recovered from the octad graph Γ, although we postpone the explanation of this procedure. In any event, all of the three objects $(\mathcal{P}, \mathcal{B})$, $\mathcal{C}$ and Γ have the same automorphism group G. The following 5-*transitivity* attribute is the central point of the review. This and further theorem attributes in this section will be proved later in the book within our construction of the Mathieu group M_{24} by group amalgams (see Theorem 2.2 and sections after that theorem). Other proofs can be found in M. Aschbacher's book,[4] in Chapter 6 of the book by J. D. Dixon and B. Mortimer,[5] in my book[6] and in many other books and journal articles.

Theorem 1.6 *The automorphism group* G *of* $(\mathcal{P}, \mathcal{B})$, $\mathcal{C}$ *and* Γ *is the Mathieu group* M_{24} *discovered by É. Mathieu in 1873.*[7] *It is simple of order*

$$|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$$

and acts 5*-fold transitively on the* 24*-set* $\mathcal{P}$. □

The 5-fold transitivity is by definition the transitivity of G on the set of ordered 5-subsets of $\mathcal{P}$. The following *flag-transitivity* attribute is the foundation of our treatment of G. Here a *flag* $\Phi = \{B, T, S\}$ is an octad–trio–sextet triple such that S sub-partitions T, and B is one of the three octads in T.

[1] E. Witt, Über Steinersche Systeme, *Abh. Math. Seminar Hamburg* **12** (1938), 265–275.
[2] M. J. E. Golay, Notes on digital coding, *Proc. IRE* **37** (1949), 657.
[3] A. E. Brouwer, The uniqueness of the near hexagon on 759 points, in *Finite Geometries*, ed. N. L. Johnson, M. J. Kallaher and C. T. Long, Marcel Dekker, New York, 1982, pp. 47–60.
[4] M. Aschbacher, *Sporadic Groups*, Cambridge University Press, Cambridge, 1994.
[5] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, Berlin, 1996.
[6] A. A. Ivanov, *Geometry of Sporadic Groups* I, Cambridge University Press, Cambridge, 1999.
[7] É. Mathieu, Sur la fonction cinq fois transitive de 24 quantités, *J. Math. Pures Appl.* **18** (1873), 25–46.

Theorem 1.7 *The group G acts transitively on the set of flags Φ, the stabilizer of Φ has order $2^{10}\cdot 3$, and thus contains a Sylow 2-subgroup of G as a subgroup of index 3.* □

With the flag $\Phi = \{B, T, S\}$ as above, let G_1, G_2 and G_3 be the stabilizers in G of B, T and S, respectively. Then we have the following *parabolic structure* attribute formulated in the standard group-theoretical terms.

Theorem 1.8 *The following isomorphisms hold:*

$$G_1 \cong 2^4 : L_4(2), \quad G_2 \cong 2^6 : (L_3(2) \times S_3), \quad G_3 \cong 2^6 : 3 \cdot S_6. \qquad \square$$

By the *flag-transitivity* attribute, G acts transitively on each of the sets $\mathcal{B}$, $\mathcal{T}$ and $\mathcal{S}$ as on the cosets of G_1, G_2 and G_3, respectively. In particular, the action of G on Γ is vertex-transitive. Furthermore, the following *distance-transitivity* property holds.

Theorem 1.9 *The action of M_{24} on the octad graph Γ is distance-transitive, and so it is vertex-transitive, and G_1 permutes transitively the vertices at distance i from B for every $i = 0,\ 1,\ 2$ and 3.* □

The following *simple connectedness* attribute proved by M. Ronan[8] assures the success of our construction of the Mathieu group M_{24} as the universal completion of the Mathieu amalgam $\{G_1, G_2, G_3\}$.

Theorem 1.10 *The octad–trio–sextet geometry of the Mathieu group M_{24} is simply connected.* □

[8] M. A. Ronan, Locally truncated buildings and M_{24}, *Math. Z.* **180** (1982), 469–501.