CAMBRIDGE TRACTS IN MATHEMATICS

176

THE MONSTER GROUP AND MAJORANA INVOLUTIONS

A. A. IVANOV

CAMBRIDGE UNIVERSITY PRESS

The Monster Group and Majorana Involutions

A. A. IVANOV
Imperial College of Science, London
and
Institute for System Analysis, Moscow

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521889940

First published 2009

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-88994-0 hardback

CAMBRIDGE TRACTS IN MATHEMATICS

General Editors

176 The Monster Group and Majorana Involutions

To Love and Nina

Preface

The *Monster* is the most amazing among the finite simple groups. The best way to approach it is via an amalgam called the *Monster amalgam*.

Traditionally one of the following three strategies are used in order to construct a finite simple group H:

(I) realize H as the automorphism group of an object Ξ;
(II) define H in terms of generators and relations;
(III) identify H as a subgroup in a 'familiar' group F generated by given elements.

The strategy offered by the *amalgam method* is a symbiosis of the above three. Here the starting point is a carefully chosen generating system $\mathcal{H} = \{H_i \mid i \in I\}$ of subgroups in H. This system is being axiomatized under the name of *amalgam* and for a while lives a life of its own independently of H. In a sense this is almost like (III) although there is no 'global' group F (familiar or non-familiar) in which the generation takes place. Instead one considers the class of all *completions* of $\mathcal{H}$ which are groups containing a quotient of $\mathcal{H}$ as a generating set. The axioms of $\mathcal{H}$ as an abstract amalgam do not guarantee the existence of a completion which contains an isomorphic copy of $\mathcal{H}$. This is a familiar feature of (II): given generators and relations it is impossible to say in general whether the defined group is trivial or not. This analogy goes further through the *universal completion* whose generators are all the elements of $\mathcal{H}$ and relations are all the identities hold in $\mathcal{H}$. The *faithful* completions (whose containing a generating copy of $\mathcal{H}$) are of particular importance. To expose a similarity with (I) we associate with a faithful completion X a combinatorial object $\Xi = \Xi(X, \mathcal{H})$ known as the *coset geometry* on which X induces a flag-transitive action. This construction equips some group theoretical notions with topological meaning: the homomorphisms of faithful completions correspond to local isomorphisms of the coset geometries; if X is the universal completion of $\mathcal{H}$, then $\Xi(X, \mathcal{H})$ is simply connected and vice versa. The ideal outcome is when the group H we are after is the universal completion of its subamalgam $\mathcal{H}$. In the classical situation, this is always the case whenever H is taken to be the universal central cover of a finite simple group of Lie type of rank at least 3 and $\mathcal{H}$ is the amalgam of parabolic subgroups containing a given Borel subgroup.

By the classification of flag-transitive Petersen and tilde geometries accomplished in [Iv99] and [ISh02], the Monster is the universal completion of an amalgam formed by a triple of subgroups

$$G_1 \sim 2_+^{1+24}.Co_1,$$
$$G_2 \sim 2^{2+11+22}.(M_{24} \times S_3),$$
$$G_3 \sim 2^{3+6+12+18}.(3 \cdot S_6 \times L_3(2)),$$

where $[G_2 : G_1 \cap G_2] = 3$, $[G_3 : G_1 \cap G_3] = [G_3 : G_2 \cap G_3] = 7$. In fact, explicitly or implicitly, this amalgam has played an essential role in proofs of all principal results about the Monster, including discovery, construction, uniqueness, subgroup structure, Y-theory, moonshine theory.

The purpose of this book is to build up the foundation of the theory of the Monster group adopting the amalgam formed by G_1, G_2, and G_3 as the first principle. The strategy is similar to that followed for the fourth Janko group J_4 in [Iv04] and it amounts to accomplishing the following principal steps:

(A) 'cut out' the subset $G_1 \cup G_2 \cup G_3$ from the Monster group and axiomatize the partially defined multiplication to obtain an abstract *Monster amalgam* $\mathcal{M}$;
(B) deduce from the axioms of $\mathcal{M}$ that it exists and is unique up to isomorphism;
(C) by constructing a faithful (196 883-dimensional) representation of $\mathcal{M}$ establish the existence of a faithful completion;
(D) show that a particular subamalgam in $\mathcal{M}$ possesses a unique faithful completion which is the (non-split) extension $2 \cdot BM$ of the group of order 2 by the Baby Monster sporadic simple group BM (this proves that every faithful completion of $\mathcal{M}$ contains $2 \cdot BM$ as a subgroup);
(E) by enumerating the suborbits in a graph on the cosets of the $2 \cdot BM$-subgroup in a faithful completion of $\mathcal{M}$ (known as the *Monster graph*), show that for any such completion the number of cosets is the same (equal to the index of $2 \cdot BM$ in the Monster group);

(F) defining G to be the universal completion of $\mathcal{M}$ conclude that G is the Monster as we know it, that is a non-abelian simple group, in which G_1 is the centralizer of an involution and that

$$|G| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

In terms of the Monster group G, the Monster graph can be defined as the graph on the class of $2A$-involutions in which two involutions are adjacent if and only if their product is again a $2A$-involution. The centralizer in G of a $2A$-involution is just the above-mentioned subgroup $2 \cdot BM$. It was known for a long time that the $2A$-involutions in the Monster form a class of 6-transpositions in the sense that the product of any two such involutions has order at most 6. At the same time the $2A$-involutions act on the 196 884-dimensional G-module in a very specific manner, in particular we can establish a G-invariant correspondence of the $2A$-involutions with a family of so-called *axial vectors* so that the action of an involution is described by some simple rules formulated in terms of the axial vector along with the G-invariant inner and algebra products on this module (the latter product goes under the name of *Griess algebra*). The subalgebras in the Griess algebra generated by pairs of axial vectors were calculated by Simon Norton [N96]: there are nine isomorphism types and the dimension is at most eight. By a remarkable result recently proved by Shinya Sakuma in the framework of the Vertex Operator Algebras [Sak07], these nine types as well as the 6-transposition property are implied by certain properties of the axial vectors and the corresponding involutions. In this volume we axiomatize these properties under the names of *Majorana axial vectors* and *Majorana involutions*. The fact that the Monster is generated by Majorana involutions will certainly dominate the future studies.

Contents

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