5-17-2015

Generalized Symmetric Spaces of the Modular Group Mm(2)

Marc Julien Besson
Dickinson College

Generalized Symmetric Spaces of the Modular Group $M_m(2)$

By

Marc Besson

Submitted in partial fulfillment of the requirements
for departmental honors in Mathematics
Dickinson College, 2011-2015

Professor Jennifer Schaefer, Advisor
Professor Holley Friedlander, Reader
Professor Tracy McKay, Reader
Professor Barry Tesman, Reader

May 11, 2015

The Department of Mathematics and Computer Science at Dickinson College hereby accepts this senior honors thesis by Marc Besson, and awards departmental honors in Mathematics

---

Professor Jennifer Schaefer (Advisor) Date

Professor Holley Friedlander (Reader) Date

Professor Tracy McKay (Reader) Date

Professor Barry Tesman (Reader) Date

Professor Richard Forrester (Department chairperson) Date

Department of Mathematics and Computer Science
Dickinson College

May 11, 2015

Abstract

Generalized Symmetric Spaces of the Modular Group $M_m(2)$

by

Marc Besson

Symmetric spaces of Lie groups and Riemannian manifolds have been an area of study since the seminal work of Cartan in the early 19th century with applications to representation theory, geometry, and number theory. Though originally defined in terms of Lie groups, the idea of a symmetry space has been generalized to finite groups as well, opening up a new field of research. In this thesis we find the generalized symmetric spaces of the modular group $M_m(2)$. We begin by determining the structure of $M_m(2)$. We then establish the automorphism group of $M_m(2)$ and determine which of these automorphisms are involutions. Given an involution, ϕ, we determine the fixed-point group, the generalized symmetric space and the extended symmetric space. This work completes the categorization of generalized symmetric spaces for the class of non-Abelian 2-groups which contain a cyclic subgroup of index 2.

Acknowledgments

I would like to thank Professor Schaefer for her consistent advice, support, mentoring and mathematical guidance. I would furthermore like to thank Professor Friedlander, Professor McKay and Professor Tesman for taking their time to read over drafts and provide me with edits and notes. I'd also like to thank Professor Hermann, for inspiring my love of algebra. Lastly I'd like to thank my family.

Contents

1. Introduction

Since their introduction in the early 20^{th} century, symmetric spaces have played an important role in mathematics. The study of symmetric spaces has its origins in geometry, and can be approached either through the geometric methods of differential geometry or through the algebraic methods of Lie theory. Élie Cartan completed the classification of Riemannian symmetric spaces in the early 20^{th} century, and since then, symmetric spaces have become an important field of study with applications to differential geometry [3], harmonic analysis, algebraic geometry and representation theory. A symmetric space is a smooth manifold, such that at any point in the space there exists an inversion symmetry [13]. For example, n-dimensional Euclidean space and n-dimensional projective space are both symmetric spaces. While most research on symmetric spaces has focused on Lie groups, symmetric spaces defined over general groups have recently been studied. In particular, while the concept of a symmetric space is most intuitive over a Riemannian manifold, we can construct a similar object over finite groups, called the generalized symmetric space. The study of generalized symmetric spaces of finite groups is a new field of study. Among the finite groups whose spaces have already studied are the dicyclic groups [2], the dihedral groups [6], the semidihedral groups [11], the symmetry groups of the platonic solids [4], and some special cases of the special linear and general linear groups [5].

Generalized symmetric spaces are found using involutions in the automorphism group, $Aut(G)$, of a group G. Automorphisms are structure preserving bijective maps from a group G to itself, and an involution is a non-identity element of $Aut(G)$ of order two. For instance, if G is the Klein four-group, then the automorphism group $Aut(G)$ is isomorphic

to the symmetric group S_3. Thus, the involutions of the Klein four group can be thought of as the transpositions, $(1,2)$, $(1,3)$ and $(2,3)$ in S_3. These automorphisms have the effect of transposing two nonidentity elements of the Klein four-group, leaving the third non-identity element fixed (and mapping the identity to the identity).

We study involutions because given a group G, and an involution $\theta \in Aut(G)$, the generalized symmetric space defined by that involution is

$$Q = \{x\theta(x)^{-1} \mid x \in G\}.$$

Two other important spaces related to the generalized symmetric space are the fixed point subgroup H, and the extended symmetric space R. These two sets are defined with respect to an involution $\theta \in Aut(G)$ as follows:

$$H = \{g \in G \mid \theta(g) = g\}$$

$$R = \{g \in G \mid \theta(g) = g^{-1}\}.$$

In this thesis we determine the generalized symmetric spaces, the extended symmetric spaces, and the fixed point groups associated with the modular 2-group defined as

$$M_m(2) = \langle x, y | x^{2^{m-1}} = y^2 = e, yxy^{-1} = x^{1+2^{m-2}} \rangle, \text{where } m \geq 4.$$

This research is motivated by the following theorem.

Theorem 1.1. [8, p. 193] *Let P be a nonabelian 2-group of order 2^m which contains a cyclic subgroup G of order 2^{m-1}. Then if $m > 3$, P is isomorphic to the modular group*

$M_m(2)$, the dihedral group D_m, the generalized quaternion group Q_m or the semidihedral group S_m.

The symmetric spaces of D_m, Q_m and S_m have been studied in [2], [6] and [11]. Thus this work on $M_m(2)$ concludes the investigation of symmetric spaces of 2-groups of the above type. For more information on these groups, see [8].

To determine these spaces, first the structure of the $M_m(2)$ groups must be examined. Next, the structure of the general automorphism group $Aut(M_m(2))$ must be studied. Following this, the fixed-point groups, the general symmetric spaces, and the extended symmetric spaces will be found.

In Section One, we determine the commutation relation of the modular group, provide useful formulae regarding inverses and products of elements in the groups, find the center $Z(M_m(2))$, and determine the order of a general element. In Section Two, we determine the elements of $Aut(M_m(2))$ and determine which of these automorphisms are involutions. In Section Three we determine the fixed-point subgroup H, the generalized symmetric space Q, and the extended symmetric space R.

2. Structure of $M_m(2)$

We first define our main object of study, the modular 2-group.

Definition 2.1. For an integer $m \geq 4$, define the **modular 2-group**

$$M_m(2) = \langle x, y | x^{2^{m-1}} = y^2 = e, yx = x^{1+2^{m-2}} y \rangle$$

where e is the identity.

We begin our work by proving some general results about the structure of $M_m(2)$ that will be useful throughout this thesis. First, we define an expression for the elements of the modular 2-group $M_m(2)$.

Definition 2.2. An element $g \in M_m(2)$ is in **normal form** if $g = x^n y^k$ for $n \in \mathbb{Z}_{2^{m-1}}$ and $k \in \mathbb{Z}_2$.

Note that $yx = x^{1+2^{m-2}} y$ from the presentation implies that the modular group $M_m(2)$ is not Abelian. However, we will use the commutation relation given by the group presentation to prove any element can be written in normal form. We begin with a lemma.

Lemma 2.3. *For all integers $n \geq 1$, $yx^n = x^{n(1+2^{m-2})} y$.*

Proof. We prove this lemma by induction on n.

Basis Step: The basis step follows directly from the presentation of the group since $yx = x^{1+2^{m-2}} y$ is given.

Inductive Step: Assume that $yx^n = x^{n(1+2^{m-2})} y$ for an integer $n \geq 1$. We must show that $yx^{n+1} = x^{(n+1)(1+2^{m-2})} y$. By the Basis Step and the Inductive Hypothesis,

$$\begin{aligned} yx^{n+1} &= yx^n x \\ &= x^{n(1+2^{m-2})}yx \\ &= x^{n(1+2^{m-2})}x^{1+2^{m-2}}y \\ &= x^{(n+1)(1+2^{m-2})}y. \end{aligned}$$

Thus the result follows. □

With the help of this lemma, we can now prove the following theorem.

Theorem 2.4. *Every element of $M_m(2)$ can be written uniquely in normal form. Thus $M_m(2) = \{e, x, x^2 \dots x^{2^{m-1}-1}, xy, x^2y, \dots x^{2^{m-1}-1}y\}$.*

Proof. Let $g \in M_m(2)$. By definition, g can be written as a finite product of the generators x and y. Thus $g = x^{a_1}y^{b_1}x^{a_2}y^{b_2}\cdots x^{a_k}y^{b_k}$ for some $a_i, b_i \in \mathbb{Z}^+ \cup \{0\}$. We can repeatedly apply Lemma 2.3 to rewrite g as x^sy^t where $s, t \in \mathbb{Z}^+ \cup \{0\}$. Using the Quotient Remainder Theorem, we can write $s = k2^{m-1}+j$ and $t = w2+r$, where $k, w \in \mathbb{Z}$, $j \in \mathbb{Z}_{2^{m-1}}$ and $r \in \mathbb{Z}_2$ are unique. Then we have $g = x^sy^t = x^{k\cdot 2^{m-1}+j}y^{w\cdot 2+r}$. Using the relations $x^{2^{m-1}} = y^2 = e$ from Definition 2.1, g simplifies to $g = x^sy^t = x^{k\cdot 2^{m-1}+j}y^{w\cdot 2+r} = x^{k\cdot 2^{m-1}}x^jy^{w\cdot 2}y^r = x^jy^r$, which is in normal form as defined in Definition 2.2. □

Example 2.5. The modular 2-group $M_4(2)$ is of order 16 and consists of the following elements: $M_4(2) = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y\}$.

Now that we understand the commutation relation of this group and how to write elements in normal form, we find an expression for an element raised to a power, a calculation we will require frequently in later sections.

Lemma 2.6. *If k is odd, a product of the form $(x^a y^b)^k$ can be rewritten as $x^{ak+a(k-1)b2^{m-3}}y^b$.*

Proof. Consider $(x^a y^b)^k \in M_m(2)$ where $a \in \mathbb{Z}_{2^{m-1}}$, $b \in \mathbb{Z}_2$ and $k \in \mathbb{Z}^+$ is odd. We can expand $(x^a y^b)^k$ as $\underbrace{(x^a y^b)(x^a y^b)\cdots(x^a y^b)}_{k \text{ factors of } (x^a y^b)}$. Each pair of these terms can be written as $(x^a y^b)(x^a y^b) = x^a \cdot x^{a(1+2^{m-2})^b} y^{2b}$. Thus far we have been entirely general, but we now note that b must be either 0 or 1, since $y^2 = e$. We break this into the two corresponding cases.

Case 1: Assume $b = 0$. Then $(x^a y^b)(x^a y^b) = x^a x^{a(1+2^{m-2})^0} = x^{2a} = x^{2a+ab2^{m-2}}$.

Case 2: Assume $b = 1$. Then $(x^a y^b)(x^a y^b) = x^a \cdot x^{a(1+2^{m-2})^1} = x^{2a+ab2^{m-2}}$.

Regardless of case, $(x^a y^b)^2 = x^{2a+ab2^{m-2}}$. Since there are $\frac{k-1}{2}$ pairs of the form $(x^a y^b)(x^a y^b)$, we have $(x^a y^b)^k = x^{(2a+ab2^{m-2})\cdot\frac{k-1}{2}} \cdot x^a y^b = x^{(k-1)(a+ab2^{m-3})+a} y^b = x^{ak+a(k-1)b2^{m-3}} y^b$ as desired. □

Lemma 2.7. *If k is even, a product of the form $(x^a y^b)^k$ can be rewritten as $x^{ak+kab2^{m-3}}$.*

Proof. Consider $(x^a y^b)^k \in M_m(2)$ where $a \in \mathbb{Z}_{2^{m-1}}$, $b \in \mathbb{Z}_2$ and $k \in \mathbb{Z}^+$ is even. We can expand $(x^a y^b)^k$ as $\underbrace{(x^a y^b)(x^a y^b)\cdots(x^a y^b)}_{k \text{ factors of } (x^a y^b)}$. We break into two cases.

Case 1: Assume $b = 0$. Then $(x^a y^b)(x^a y^b) = x^{2a} = x^{2a+ab2^{m-2}}$.

Case 2: Assume $b = 1$. Then $(x^a y^b)(x^a y^b) = x^a \cdot x^{a(1+2^{m-2})} = x^{2a+ab2^{m-2}}$.

This time there are $\frac{k}{2}$ pairs, so $(x^a y^b)^k = x^{(2a+ab2^{m-2})\cdot\frac{k}{2}} = (x^a y^b)^k = x^{ak+kab2^{m-3}}$. □

Example 2.8. In the group $M_4(2)$, the element $(x^3y)^3 = (x^3y)(x^3y)(x^3y) = x^3x^{15}yyx^3y = x^{21}y = x^5y$ by definition of the group, or $(x^3y)^3 = x^{3\cdot3+3(2)1\cdot2^{4-3}}y^1 = x^{9+12}y = x^5y$ by Lemma 2.6.

Next, we determine the order of any element of $M_m(2)$. This helps us understand the structure of $M_m(2)$ and will prove useful when we determine the automorphism group $Aut(M_m(2))$. Recall the following definition and notation of order for an arbitrary group element.

Definition 2.9. The **order** of an element g in a group G is defined to be the smallest integer $n \geq 1$ such that $g^n = e$, the identity. The order of an element is denoted $O(g)$.

In order to determine the order of elements in $M_m(2)$, we require the following result and definition.

Definition 2.10. Let G be a group and $g \in G$. Then we define the **cyclic group** generated by g as $< g >= \{g^n | n \in \mathbb{Z}\}$.

Theorem 2.11. *The order of the subgroup generated by g, denoted* $| < g > |$*, is equal to the order of an element* $O(g)$*.*

Proof. See proof in [10, Theorem 1.3.3] □

Definition 2.12. Given two integers a and b, the **greatest common divisor** of a and b is the largest integer n such that $n|a$ and $n|b$ and is denoted as (a, b).

To calculate the order of elements in $M_m(2)$, we use the following two theorems.

Theorem 2.13. *In a finite group, if* $O(x) = n$*, then* $O(x^k) = \frac{n}{(k,n)}$*.*

Proof. See proof in [12]. □

Definition 2.14. The **index** of a subgroup H in a group G is the number of left cosets of H in G and is denoted $|G : H|$.

Theorem 2.15 (Lagrange's Theorem)**.** *If G is a group and H is a subgroup of G, then $|G| = |G : H| \cdot |H|$. If G is finite, $|G : H| = |G|/|H|$. Hence the order of a subgroup always divides the order of the group if the latter is finite.*

Proof. See proof in [10, Theorem 1.3.6] □

We can now calculate the order of elements in $M_m(2)$.

Theorem 2.16. *The order of an element of the form x^k where $k \in \mathbb{Z}_{2^{m-1}}$ is $O(x^k) = \frac{2^{m-1}}{(2^{m-1},\ k)}$, and the order of an element of the form $x^k y$ where $k \in \mathbb{Z}_{2^{m-1}}$ is $O(x^k y) = \frac{2^{m-1}}{(2^{m-2},\ k+2^{m-3}k)}$.*

Proof. We will break this proof into the two cases of elements of the form x^k and $x^k y$. The order of x and y are given in the presentation of the group such that $O(x) = 2^{m-1}$ and $O(y) = 2$.

Case 1: Consider an element of the form $x^k \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-1}}$. Then we can use the result in Theorem 2.13: if $O(x) = n$ then $O(x^k) = \frac{n}{(k,n)}$. Since $O(x) = 2^{m-1}$ in $M_m(2)$, it follows that $O(x^k) = \frac{2^{m-1}}{(2^{m-1},k)}$.

Case 2: Consider an element of the form $x^k y$ where $k \in \mathbb{Z}_{2^{m-1}}$. Then $(x^k y)^2 = x^{2k+2^{m-2}k}$ by Lemma 2.3, and $O(x^{2k+2^{m-2}k}) = \frac{2^{m-1}}{(2^{m-1},2k+2^{m-2}k)}$ by Theorem 2.16. By Lagrange's Theorem, we know that $O(g^2)|O(g)$, from which it follows that $O(g^2) \leq O(g)$ for any element g in a group G. Thus, $O((x^k y)^2) \leq O(x^k y)$ by Lagrange's Theorem.

Furthermore, $O(x^k y) \leq 2O((x^k y)^2)$ by Theorem 2.13. Since $|M_m(2)| = 2^m$, we know that $O(x^k y)$ is a power of 2, because the order of an element must divide the order of the group by Lagrange's Theorem. So either $O(x^k y) = O((x^k y)^2)$ or $O(x^k y) = 2O((x^k y)^2)$. We can easily rule out the first case, because $< (x^k y)^2 >$ is a proper subgroup of $< x^k y >$, seeing as it does not contain $x^k y$, for instance. Thus $O(x^k y) = 2O((x^k y)^2) = 2 \cdot \frac{2^{m-1}}{(2^{m-1}, 2k+2^{m-2}k)} = \frac{2^{m-1}}{(2^{m-2}, k+2^{m-3}k)}$. □

Next we find the inverse of any element in $M_m(2)$. This is necessary for understanding the structure of $M_m(2)$ and will also prove important when we begin to find the fixed-point groups and the extended symmetric spaces.

Theorem 2.17. *The elements of $M_m(2)$ have the following inverses:*

$(x^k)^{-1} = x^{2^{m-1}-k}$ *and* $(x^k y)^{-1} = x^{(2^{m-1}-k)(1+2^{m-2})} y$ *where* $k \in \mathbb{Z}_{2^{m-1}}$.

Proof. Using the group presentation

$$M_m(2) = \langle x, y | x^{2^{m-1}} = y^2 = e, yx = x^{1+2^{m-2}} y \rangle,$$

we can determine the inverse of any element.

Given an element of the form x^k, we have $x^k \cdot x^{2^{m-1}-k} = x^{2^{m-1}} = e$. It follows that $(x^k)^{-1} = x^{2^{m-1}-k}$.

Given an element of the form $x^k y$, since $x^{(2^{m-1}-k)\cdot(1+2^{m-2})} y = y x^{2^{m-1}-k}$ by Lemma 2.3, we see $x^k y \cdot y x^{2^{m-1}-k} = x^k y^2 x^{2^{m-1}-k} = x^{k+2^{m-1}-k} = x^{2^{m-1}} = e$. Thus $(x^k y)^{-1} = x^{(2^{m-1}-k)(1+2^{m-2})} y$. □

Example 2.18. The following table provides the order of every element in the group $M_4(2)$, as well as inverses.

Element	Order	Inverse
e	1	e
x	8	x^7
x^2	4	x^6
x^3	8	x^5
x^4	2	x^4
x^5	8	x^3
x^6	4	x^2
x^7	8	x
xy	8	x^3y
x^2y	4	x^6y
x^3y	8	xy
x^4y	2	x^4y
x^5y	8	x^7y
x^6y	4	x^2y
x^7y	8	x^5y
y	2	y

Another important quality of our group is its center, $Z(M_m(2))$. We recall its definition:

Definition 2.19. The **center** of a group G, denoted $Z(G)$, is the set $Z(G) = \{x \in G \mid xy = yx \text{ for all } y \in G\}$.

Determining the center of the group will help us with computation in later sections.

Theorem 2.20. *The center of $M_m(2)$ consists of all elements of the form x^{2k} where $k \in \mathbb{Z}_{2^{m-2}}$. Thus $Z(M_m(2))$ is a cyclic subgroup of order 2^{m-2}.*

Proof. We break this proof into four cases, determining if elements of the form x^{2k}, x^{2k+1}, $x^{2k}y$, and $x^{2k+1}y$ are central, where $k \in \mathbb{Z}_{2^{m-2}}$.

Case 1: Consider $x^{2k} \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-2}}$. We must determine if elements of this form commute with both generators, x and y. Clearly $x \cdot x^{2k} = x^{1+2k} = x^{2k+1} = x^{2k} \cdot x$, so elements of the form x^{2k} commute with all elements generated by x. Next, we show that x^{2k} commutes with y. By Lemma 1.1, $y \cdot x^{2k} = x^{2k\cdot(1+2^{m-2})}y$.

But note that $x^{2k\cdot(1+2^{m-2})}y = x^{2k} \cdot x^{k\cdot 2^{m-1}}y = x^{2k}y$. Thus x^{2k} commutes with all elements generated by y, and $\{x^{2k}\} \subseteq Z(M_m(2))$.

Case 2: Consider $x^{2k+1} \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-2}}$. Using the commutation relations, $y \cdot x^{2k+1} = x^{(2k+1)(1+2^{m-2})}y = x^{2k+1}x^{2^{m-2}}y$. Since $x^{2^{m-2}} \neq e$, we see that x^{2k+1} is *not* central.

Case 3: Consider $x^{2k}y \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-2}}$. To determine if elements of this form commute with x, we see $x \cdot x^{2k}y = x^{2k+1}y$, and $x^{2k}y \cdot x = x^{2k+1}x^{1+2^{m-2}}y = x^{2k+2^{m-2}+1}y$. These two expressions cannot be equal because $x^{2^{m-2}}$ is not the identity. Thus elements of the form $x^{2k}y$ are *not* central.

Case 4: Consider $x^{2k+1}y \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-2}}$. To determine if elements of this form commute with x, we see $x \cdot x^{2k+1}y = x^{2(k+1)}y$ and $x^{2k+1}y \cdot x = x^{2k+1}x^{1+2^{m-2}}y = x^{2k+2+2^{m-2}}y$. Since $x^{2^{m-2}}$ is not the identity, this demonstrates that elements of the form $x^{2k+1}y$ are *not* central.

Thus $Z(M_m(2)) =< x^2 >$. □

Example 2.21. The center of $M_4(2)$ is $Z(M_4(2)) = \{e, x^2, x^4, x^6\}$.

3. Automorphisms of $M_m(2)$

The goal of this work is to determine the fixed-point group, the generalized symmetric spaces, and extended symmetric spaces of $M_m(2)$. Because all of these spaces are defined with respect to automorphisms, we first determine the automorphism group of $M_m(2)$. Automorphisms of finitely generated groups are characterized by their actions on the group's generators, we first determine the possible images of the generators x and y and their corresponding homomorphisms. We will then show which of these homomorphisms are indeed automorphisms. Recall the following definition:

Definition 3.1. An **automorphism** of a group G is a bijective homomorphism $\phi : G \to G$, and the set of all automorphisms of G is denoted $Aut(G)$.

The following results hold for automorphisms.

Theorem 3.2. *Let G be a group. Then $Aut(G)$ is a group under the operation of function composition.*

Proof. See proof in [10, p.26]. □

Theorem 3.3. *Let G be a group and $\phi \in Aut(G)$. Then $O(g) = O(\phi(g))$ for all $g \in G$.*

Proof. See proof in [7, Ch. 4.4, Cor. 14]. □

Using Theorem 2.16, we can determine the possible images of the generators x and y.

Theorem 3.4. *If ϕ is an automorphism of $M_m(2)$, then $\phi(x) = x^k y^j$ where k is odd, and $j = 0$ or $j = 1$.*

Proof. Consider $x \in M_m(2)$. By definition we have that $O(x) = 2^{m-1}$. We now split into cases and examine first elements of the form x^k and then elements of the form $x^k y$.

Case 1: We know by Theorem 2.16 that $O(x^k) = \frac{2^{m-1}}{(2^{m-1},k)}$. If k is even then we know it can be written as $k = 2a$ for some integer a. In this case $\frac{2^{m-1}}{(2^{m-1},2a)} = \frac{2^{m-2}}{(2^{m-2},a)} \leq 2^{m-1}$. Thus, if k is even, $O(x^k) < O(x)$. Alternatively, if k is odd, we have $O(x^k) = \frac{2^{m-1}}{(2^{m-1},2a+1)}$. But $(2^{m-1}, 2a+1) = 1$, so $O(x^k) = O(x)$ when k is odd.

Case 2: We know by Theorem 2.16 that $O(x^k y) = \frac{2^{m-1}}{(2^{m-2},\ k+2^{m-3}k)}$. When k is even, we have $O(x^k y) = \frac{2^{m-1}}{(2^{m-2},\ 2a+2^{m-3}2a)} = \frac{2^{m-2}}{(2^{m-2},\ a+2^{m-3}a)} < O(x)$. However, if k is odd, then we see that $(2^{m-2},\ 2a+1+2^{m-3}(2a+1)) = 1$, and once again $O(x^k y) = 2^{m-1} = O(x)$.

□

Next, we examine what the image of y may be under an automorphism. This is a slightly more involved matter. For the modular group $M_m(2)$, there are only three elements with order 2: the elements y, $x^{2^{m-2}}$ and $x^{2^{m-2}}y$ by Theorem 2.16. For elements of the form x^k, this follows because if $2 = \frac{2^{m-1}}{(2^{m-1},x)}$, we have $(2^{m-1}, x) = 2^{m-2}$. The only solution for $x \in Z_{2^{m-1}}$ is 2^{m-2}. Alternatively, for elements of the form $x^k y$, we use Theorem 2.16 to find the elements of order 2, i.e. we solve $2 = \frac{2^{m-1}}{(2^{m-1},k+2^{m-3}k)}$ for k. This implies $2^{m-2} = (2^{m-1}, k + 2^{m-3}k)$, which is only satisfied if $k = 2^{m-2}$. This shows that y, $x^{2^{m-2}}$ and $x^{2^{m-2}}y$ are possible images of y under an automorphism. We will demonstrate that there exists no automorphism ϕ such that $\phi(y) = x^{2^{m-2}}$. We do this by showing that any homomorphism that sends y to $x^{2^{m-2}}$ is not injective. First we prove a lemma. The proof of this lemma requires Cauchy's Theorem, which we state.

Theorem 3.5 (Cauchy's Theorem)**.** *If a prime p divides the order of a finite group G, then G contains an element of order p.*

Proof. See proof in [1, Theorem 6.4.4.3]. □

Lemma 3.6. *For all* $t \in \mathbb{Z}_{2^{m-1}} - \{0\}, x^{2^{m-2}} \in < x^t >$.

Proof. Let $t \in \mathbb{Z}_{2^{m-1}} - \{0\}$. By Lagrange's Theorem, all subgroups of $< x >$ have order n such that $n|2^{m-1}$. In other words, every subgroup of $< x >$ besides the trivial group is a 2-group. Then by Cauchy's Theorem [1, Theorem 6.4.4.3], we know that the subgroup $< x^t >$ where $j \neq 0$ contains a subgroup of order 2. Equivalently, we know $< x^t >$ contains an element of order 2. Let this element be denoted x^s. From Theorem 2.16, we know that $O(x^s) = \frac{2^{m-1}}{(2^{m-1},s)} = 2$. Hence $(2^{m-1}, s) = 2^{m-2}$, which implies $s = 2^{m-2}$. Thus, $x^{2^{m-2}} \in < x^t >$. □

We use this lemma to prove the following result.

Theorem 3.7. *For all* $\phi \in Aut(M_m(2)),\ \phi(y) \neq x^{2^{m-2}}$.

Proof. Let $\phi \in Aut(M_m(2))$. We prove this theorem in two parts. First we show that $x^{2^{m-2}} \in < \phi(x) >$, and second we show that if $\phi(y) = x^{2^{m-2}}$, then ϕ is not injective. By Theorem 3.4, the image of x under ϕ is of the form x^k or $x^k y$, where k is an odd integer.

Case 1: Suppose $\phi(x) = x^k$ for k odd. Then it follows directly by Lemma 3.6 that $x^{2^{m-2}} \in < x^k > = < \phi(x) >$.

Case 2: Suppose $\phi(x) = x^k y$ for k odd. Then by Lemma 2.3, $(x^k y)^2 = x^{2k+k2^{m-2}}$. Note that $x^{2k+k2^{m-2}} \neq e$ because then $x^k y$ would not have order 2^{m-1} as required. Thus, $< x^{2k+k2^{m-2}} > \subseteq < x^k y >$ where $2k + k2^{m-2} \not\equiv 0\ (2^{m-1})$. So by Lemma 3.6, $x^{2^{m-2}} \in < x^{2k+k2^{m-2}} > \subseteq < x^k y > = < \phi(x) >$. Thus, $x^{2^{m-2}} \in < \phi(x) >$.

Since regardless of case we have $x^{2^{m-2}} \in < \phi(x) >$, we have that $(\phi(x))^n = x^{2^{m-2}}$ for some n. Then by properties of homomorphisms, we have $\phi(x^n) = x^{2^{m-2}}$. But then if $\phi(y) = x^{2^{m-2}}$, ϕ would not be injective, and thus ϕ would not be an automorphism. $\square$

Corollary 3.8. *If ϕ is an automorphism of $M_m(2)$, then $\phi(y) = x^{c2^{m-2}}y$ where $c \in \mathbb{Z}_2$.*

Now we know that if ϕ is an automorphism, then $\phi(x) = x^k y^j$ and $\phi(y) = x^{c2^{m-2}}y$ where $k \in \mathbb{Z}$ odd and $j, c \in \mathbb{Z}_2$.

Definition 3.9. For a odd in $\mathbb{Z}_{2^{m-1}}$ and $b, c \in \mathbb{Z}_2$, we define a function $\phi_{a,b,c} : G \to G$ such that $\phi_{a,b,c}(x) = x^a y^b$ and $\phi_{a,b,c}(y) = x^{c2^{m-2}}y$.

Our next task is to show that any homomorphism of this form is indeed an automorphism. The proof strategy will be to show that the homomorphisms $\phi_{a,0,c}$ and $\phi_{a,1,c}$ are surjective. Generally, automorphisms are bijective homomorphisms. However, in our case, proving surjectivity implies injectivity as well.

Lemma 3.10. *A homomorphism ϕ from a finite group G to itself is an automorphism if it is surjective or injective.*

Proof. Let G be a finite group and suppose $\phi : G \to G$ is a homomorphism such that ϕ is surjective. Since G is finite, we know it has finite order n. Then we know that for any element $g_2 \in G$, there exists $g_1 \in G$ such that $\phi(g_1) = g_2$. We now demonstrate that surjectivity implies injectivity. Let g and g' be elements in G such that $\phi(g) = \phi(g')$, but $g \neq g'$. Then this function cannot be surjective, because there remain $n-2$ elements of $G - \{g, g'\}$ which must be mapped into the $n-1$ elements of $G - \{\phi(g)\}$. But this

contradicts our hypothesis that ϕ is surjective. Thus, for a finite group G, surjective homomorphisms from G to G are automorphisms.

Alternatively, suppose that G is a finite group and $\phi : G \to G$ is a homomorphism which is injective but not surjective. Then there exists some element $g \in G$ such that $g \notin Im(\phi)$. Then ϕ maps n elements in G to no more than $n-1$ elements in the set $G - \{g\}$. This function ϕ cannot be injective, contradicting the hypothesis. Thus for a homomorphism of a finite group to itself, injectivity or surjectivity are sufficient is the homomorphism to be an automorphism. □

We require one more theorem on the solutions of Diophantine equations:

Theorem 3.11. *If (a,n) =1, then the equation* $ax \equiv b\ (n)$ *has a solution, and that solution is unique modulo n .*

Proof. See [12, p. 23]. □

We now have all the tools necessary to demonstrate that the homomorphisms $\phi_{a,b,c} : M_m(2) \to M_m(2)$ are indeed automorphisms.

Theorem 3.12. *The automorphisms of* $M_m(2)$ *are the homomorphisms* $\phi_{a,b,c} : M_m(2) \to M_m(2)$ *such that* $\phi_{a,b,c}(x) = x^a y^b$ *and* $\phi_{a,b,c}(y) = x^{c2^{m-2}} y$*, where* $a \in \mathbb{Z}_{2^{m-1}}$ *is odd and* $b, c \in \mathbb{Z}_2$.

Proof. Let $\phi_{a,b,c} : M_m(2) \to M_m(2)$ such that $a \in \mathbb{Z}_{2^{m-1}}$ is odd and $b, c \in \mathbb{Z}_2$ be a homomorphism. Then $b \in \mathbb{Z}_2$ implies $b = 0$ or $b = 1$. We wish to show that $|ker(\phi)| = 1$, which implies injectivity, and thus implies that these homomorphisms are automorphisms. We split into the two cases where $b = 0$ and $b = 1$.

Case 1: Let $b = 0$. We set $\phi_{a,0,c}(x^k y^j) = e$ and expand to get

$$\phi_{a,0,c}(x^k y^j) = (x^a)^k (x^{cj2^{m-2}} y^j) = x^{ak+cj2^{m-2}} y^j = e.$$

Setting $x^{ak+cj2^{m-2}} y^j$ equal to e, we see that $j = 0$ and $ak + cj2^{m-2} \equiv 0\ (2^{m-1})$. Thus to find elements mapped by ϕ to the identity, we must solve $ak \equiv 0\ (2^{m-1})$. Since a is always odd by definition, $(a, 2^{m-1}) = 1$ and Theorem 3.11 implies we can always find a unique k which solves this equation. Thus homomorphisms of the form $\phi_{a,0,c}$ are injective and must be automorphisms by Lemma 3.10.

Case 2: Let $b = 1$. We must show that $|ker(\phi_{a,1,c})| = 1$. Expanding out, we find that

$$\phi_{a,1,c}(x^k y^j) = (x^a y)^k (x^{cj2^{m-2}} y^j) = e.$$

To make further progress, we subdivide further into subcases corresponding to whether k is even or k is odd.

Subcase a: Assume k is even. In this case, we use Theorem 2.7 to find

$$\begin{aligned}\phi_{a,1,c}(x^k y^j) &= (x^a y)^k (x^{cj2^{m-2}} y^j) \\ &= (x^{ak+ak2^{m-3}})(x^{cj2^{m-2}} y^j) \\ &= x^{ak+ak2^{m-3}+cj2^{m-2}} y^j.\end{aligned}$$

Setting this equal to e, we find that $j = 0$ and $ak+ak2^{m-3}+cj2^{m-2} \equiv 0\ (2^{m-1})$. Thus to find the kernel, we must solve $ak+ak2^{m-3} = k(a+a2^{m-3}) \equiv 0\ (2^{m-1})$. Since a is odd, $a+a2^{m-3}$ is odd and $(a+a2^{m-3}, 2^{m-1}) = 1$, so there is a unique k which solves this equation.

Subcase b: Assume k is odd. In this case, we use Lemma 2.6 to find

$$\begin{aligned}\phi_{a,1,c}(x^k y^j) &= (x^a y)^k (x^{cj2^{m-2}} y^j) \\ &= (x^{ak+a(k-1)2^{m-3}} y)(x^{cj2^{m-2}} y^j) \\ &= x^{ak+a(k-1)2^{m-3}+cj2^{m-2}} y^{j+1}\end{aligned}$$

Setting this equal to e, we find that $j = 1$ and $x^{ak+a(k-1)2^{m-3}+cj2^{m-2}} \equiv 0\ (2^{m-1}$. Then we can rewrite the equation as $ak \equiv -a(k-1)2^{m-3} - c2^{m-2}\ (2^{m-1})$. This is a contradiction because a and k are odd, so their product is odd. If ak is odd, it cannot equal an even number modulo 2^{m-1}. Thus when k is odd, no elements of the form $x^k y^j$ are in the kernel of $\phi_{a,1,c}$. We are left with $|ker(\phi)| = 1$, which shows that $\phi_{a,1,c}$ is injective and thus an automorphism by Lemma 3.10.

This proof shows that $\phi_{a,b,c}$ as defined above are automorphisms. But it also shows that these are *all* of the automorphisms. This is because these homomorphisms are all of the structure-preserving homomorphisms from $M_m(2)$ to itself, except for the homomorphisms which map y to $x^{2^{m-2}}$. This, as we have shown, is not an automorphism. □

Determining the automorphism group in this fashion provides information on where an element is sent under an automorphism. We make this explicit in the following theorem.

Theorem 3.13. *Let $\phi_{a,b,c} \in Aut(M_m(2))$ be an automorphism, where $a \in \mathbb{Z}_{2^{m-1}}$ is odd and $b, c \in \mathbb{Z}_2$. Then for an element $x^k y^j \in M_m(2)$ where $k \in \mathbb{Z}_{2^{m-1}}$ and $j \in \mathbb{Z}_2$,*

$$\phi_{a,b,c}(x^k y^j) = \begin{cases} x^{ak+akb2^{m-3}+jc2^{m-2}} y^j, & \textit{when } k \textit{ is even} \\ x^{ak+a(k-1)b2^{m-3}+jc2^{m-2}} y^{j+b}, & \textit{when } k \textit{ is odd} \end{cases}$$

Proof. Let $x^k y^j \in M_m(2)$ and $\phi_{a,b,c} \in Aut(M_m(2))$. Then by Theorem 3.12 we have $\phi_{a,b,c}(x^k y^j) = (x^a y^b)^k (x^{c2^{m-2}} y)^j$. Note that since $j = 0$ or 1, $(x^{c2^{m-2}} y)^0 = 1 = x^{0c2^{m-2}} y^0$ and $(x^{c2^{m-2}} y)^1 = x^{c2^{m-2}} y$. Thus $(x^{c2^{m-2}} y)^j = x^{jc2^{m-2}} y^j$. To understand the term $(x^a y^b)^k$, we split into the two cases: k even and k odd.

Case a: Let k be even. Then using Lemma 2.7,

$$\begin{aligned} \phi_{a,b,c}(x^k y^j) &= (x^a y^b)^k x^{jc2^{m-2}} y^j \\ &= x^{ak+akb2^{m-3}+jc2^{m-2}} y^j. \end{aligned}$$

Case b: Let k be odd. Then using Lemma 2.6,

$$\begin{aligned} \phi_{a,b,c}(x^k y^j) &= (x^a y^b)^k x^{jc2^{m-2}} y^j \\ &= x^{ak+ak(-1)b2^{m-3}+jc2^{m-2}} y^j. \end{aligned}$$

□

Now that we have the general form of the automorphisms of $M_m(2)$, we determine the composition of two automorphisms. In particular, this will allow us to find the automorphisms of order two, namely, the involutions. Because fixed-point groups, generalized symmetric spaces, and extended symmetric spaces are all defined using involutions, this is an important step.

Theorem 3.14. *The composition $\phi_{a,b,c} \circ \phi_{d,e,f}$ of the automorphisms $\phi_{a,b,c}$ and $\phi_{d,e,f}$ is $\phi_{ad+ab(d-1)2^{m-3}+ec2^{m-2},\ b+e,\ c+f}$.*

Proof. Let $\phi_{a,b,c}$ and $\phi_{d,e,f} \in Aut(M_m(2))$. To determine $\phi_{a,b,c} \circ \phi_{d,e,f}$, we examine $\phi_{a,b,c} \circ \phi_{d,e,f}(x)$ and $\phi_{a,b,c} \circ \phi_{d,e,f}(y)$.

By Theorem 3.12,

$$\phi_{a,b,c} \ \circ \ \phi_{d,e,f}(x) = \phi_{a,b,c}(x^d y^e) = \phi_{a,b,c}(x)^d \phi_{a,b,c}(y)^e = (x^a y^b)^d (x^{2^{m-2}})^{ce} y^e.$$

Since d is odd, by Lemma 2.6,

$$(x^a y^b)^d (x^{ce2^{m-2}} y^e) = x^{ad+ab(d-1)2^{m-3}} y^b (x^{ce2^{m-2}}) y^e = x^{ad+ab(d-1)2^{m-3}+ce2^{m-2}} y^{b+e}.$$

This result follows from Lemmas 2.6 and 2.7. The last step uses the fact that $x^{ce2^{m-2}} \in Z(M_m(2))$ from Theorem 2.20.

Thus under composition, $\phi_{a,b,c}(\phi_{d,e,f}(x)) = x^{ad+ab(d-1)2^{m-3}+ce2^{m-2}} y^{b+e}$.

Next, by Theorem 3.9,

$$\phi_{a,b,c} \ \circ \ \phi_{d,e,f}(y) = \phi_{a,b,c}((x^{2^{m-2}})^f y) = (x^a y^b)^{f2^{m-2}} (x^{c2^{m-2}}) y.$$

Using Lemma 2.7 and $x^{af2^{m-2}2^{m-3}} = e$, we have

$$(x^a y^b)^{f2^{m-2}} (x^{c2^{m-2}}) y = x^{a2^{m-2}f+af2^{m-2}2^{m-3}} (x^{c2^{m-2}}) y = x^{a2^{m-2}f+c2^{m-2}} y,$$

Because a is odd, we rewrite $a = 2k+1$ for $k \in \mathbb{Z}$. From this we have $x^{(a2^{m-2}f+c2^{m-2})} y = x^{(2k+1)2^{m-2}f+c2^{m-2}} y = (x^{2^{m-2}})^{f+c} y$. Thus $\phi_{a,b,c} \ \circ \phi_{d,e,f}(y) = x^{(c+f)2^{m-2}} y$.

Combining the two previous results, we get the general form of automorphism composition : $\phi_{a,b,c} \ \circ \ \phi_{d,e,f} = \phi_{ad+ab(d-1)2^{m-3}+ce2^{m-2},\ b+e,\ c+f}$. □

The fixed-point group, generalized symmetric spaces, and extended symmetric spaces are all defined on involutions, a special subset of automorphisms.

Definition 3.15. Let G be a group. An **involution** is a non-identity element $\phi \in Aut(G)$ such that $\phi^2 = e$, where e is the identity in $Aut(G)$.

Theorem 3.16. *If $\phi_{a,b,c} \in Aut(M_m(2))$ is an involution, then $a^2 + ab(a-1)2^{m-3} + bc2^{m-2} \equiv 1(2^{m-1})$.*

Proof. Using Theorem 3.14, if $\phi_{a,b,c}$ is an involution, then

$$\phi_{a,b,c} \circ \phi_{a,b,c} = \phi_{a^2+ab(a-1)2^{m-3}+bc2^{m-2},2b,2c} = \phi_{1,0,0}.$$

Note that since $b, c \in \mathbb{Z}_2$, $2b = 2c = 0$ (2) by definition. Thus, to find the involutions of $M_m(2)$, we must solve the equation

$$a^2 + ab(a-1)2^{m-3} + bc2^{m-2} \equiv 1(2^{m-1}). \qquad \square$$

Example 3.17. We now determine the involutions for $M_4(2)$. We begin by finding the involutions of the form $\phi_{a,0,c} \in Aut(M_4(2))$. When $b = 0$, the above equation becomes $a^2 \equiv 1$ (8). Then we can see that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$ (8). No even square will satisfy this equation, because squares of even integers are even, and if $n \equiv 1$ (8), n is odd. Thus we find that the following elements are the only involutions of the form $\phi_{a,0,c} \in Aut(M_4(2))$: $\phi_{1,0,0}$, $\phi_{3,0,0}$, $\phi_{5,0,0}$, $\phi_{7,0,0}$, $\phi_{1,0,1}$, $\phi_{3,0,1}$, $\phi_{5,0,1}$, $\phi_{7,0,1}$.

Now consider the automorphisms of the form $\phi_{a,1,c}$. Since $b = 1$, the above equation becomes $a^2 + a(a-1)2^{m-3} + c2^{m-2} \equiv 1$ (2^{m-1}). For the automorphism$\phi_{1,1,0}$, we have $1^2 + (1)(0)(2) + (0)(4) \equiv 1$ (8), so $\phi_{1,1,0}$ is an involution. For the automorphism $\phi_{5,1,0}$

we have $5^2 + (5)(4)(2) + 0 \equiv 1\ (8)$, so it is an involution. For the automorphism $\phi_{3,1,1}$, we have $3^2 + (3)(2)(2) + 2^2 \equiv 1\ (8)$, so it is an involution. Lastly, for $\phi_{7,1,0}$ we have $7^2 + (7)(6)(2) + 2^2 \equiv 1\ (8)$ so it is an involution.

It can be shown that the combinations of $a = 1,\ c = 1$, $a = 5,\ c = 1$, $a = 3,\ c = 0$ and $a = 7,\ c = 0$ do not satisfy the equation. Thus the only elements of $Aut(M_4(2))$ which are not involutions are $\phi_{1,1,1}$, $\phi_{5,1,1}$, $\phi_{3,1,0}$, and $\phi_{7,1,0}$.

4. Fixed-Point Groups, Generalized Symmetric Spaces and Extended Symmetric Spaces

We now proceed to finding the spaces outlined in the introduction: the fixed-point groups H, the generalized symmetric spaces Q, and the extended symmetric spaces R. Since all of these spaces are defined for a a fixed involution, our results rely heavily on Theorem 3.13. In particular, our proof strategy must often be broken up into cases dictated by the nature of automorphisms. In general, it is very easy to find the fixed point spaces, generalized symmetric spaces, and extended symmetric spaces for involutions of the form $\phi_{a,0,c}$. For an element $x^k y^j$ and an automorphism $\phi_{a,1,c}$, we will split into two cases, one where k is even and one where k is odd. This fundamental difference comes from the commutation relations and, in particular, Theorems 2.6 and 2.7. We begin by determining the fixed-point group of a given involution.

4.1. **Fixed-point group.**

Definition 4.1. Let G be a group and $\phi \in Aut(G)$ be an involution. The **fixed-point group** of the involution ϕ is the set of elements $H_\phi = \{x \in G \mid \phi(x) = x\}$.

Let $\phi_{a,b,c} \in Aut(M_m(2))$. Then we know by Theorem 3.13 that $b = 0$ or $b = 1$. We first investigate involutions of the form $\phi_{a,0,c}$.

Theorem 4.2. *For an involution $\phi_{a,0,c} \in Aut(M_m(2))$, the fixed point group is*

$$H_{\phi_{a,0,c}} = \{x^k y^j | (a-1)k + jc2^{m-2} \equiv 0 \ (2^{m-1})\}.$$

Proof. Let $\phi_{a,0,c} \in Aut(M_m(2))$ be an involution. By definition, if an element $x^k y^j$ is in the fixed-point group of $\phi_{a,0,c}$, we have $\phi_{a,0,c}(x^k y^j) = x^k y^j$. By Theorem 3.13, this implies

that

$$\phi_{a,0,c}(x^k y^j) = x^{ak+jc2^{m-2}} y^j = x^k y^j.$$

For $x^k y^j$ to satisfy this equation, $ak + jc2^{m-2} \equiv k \ (2^{m-1})$, or $(a-1)k + jc2^{m-2} \equiv (2^{m-1})$. □

We now consider the fixed-point groups of involutions of the form $\phi_{a,1,c}$.

Theorem 4.3. *For an involution $\phi_{a,1,c} \in Aut(M_m(2))$, the fixed-point group is*

$$H_{\phi_{a,1,c}} = \{x^k y^j \mid (a-1)k + ak2^{m-3} + jc2^{m-2} \equiv 0 \ (2^{m-1}) \text{ for } k \text{ even}\}.$$

Proof. Consider two cases: k even and k odd.

Case 1: Assume k is even. Then Theorem 3.13 implies that

$$\phi_{a,1,c}(x^k y^j) = x^{ak+ak2^{m-3}+jc2^{m-2}} y^j = x^k y^j.$$

Thus, an element $x^k y^j$ is fixed when $ak + ak2^{m-3} + jc2^{m-2} \equiv k \ (2^{m-1})$, or $(a-1)k + ak2^{m-3} + jc2^{m-2} \equiv 0 \ (2^{m-1})$.

Case 2: Assume k is odd. Then Theorem 3.13 implies that that

$$\phi_{a,1,c}(x^k y^j) = x^{ak+a(k-1)2^{m-3}+jc2^{m-2}} y^{j+1} = x^k y^j.$$

Because $j+1 \neq j$, elements of the form $x^k y^j$ with k odd are *never* in the fixed-point group of $\phi_{a,1,c}$. □

Corollary 4.4. *For an involution $\phi_{a,1,c} \in Aut(M_m(2))$, the fixed point group is $H_{\phi_{a,1,c}} = \{x^k | (a-1)k + ak2^{m-3} \equiv 0\ (2^{m-1})$ and k is even$\} \cup \{x^k y | (a-1)k + ak2^{m-3} + c2^{m-2} \equiv 0\ (2^{m-1})$ and k is even$\}$.*

Example 4.5. We now determine the fixed-point groups of involutions $\phi \in Aut(M_4(2))$. Let us examine the fixed-point groups of the following involutions: $\phi_{3,0,0}$, $\phi_{5,0,1}$, $\phi_{1,1,0}$, and $\phi_{7,1,1}$.

Subcase a: By Theorem 4.2, we have that $H_{\phi_{3,0,0}} = \{x^k y^j | 2k \equiv 0\ (8)\}$. This is satisfied when $k = 0$ or $k = 4$, so $H_{\phi_{3,0,0}} = \{e, x^4, x^4 y, y\}$.

Subcase b: By Theorem 4.2, we have that $H_{\phi_{5,0,1}} = \{x^k | 4k \equiv 0\ (8)\} \cup \{x^k y | 4k + 4 \equiv 0\ (8)\}$. When $j = 0$, the equation is satisfied when $k = 0, 2, 4$ or 6 and when $j = 1$, the equation is satisfied for $k = 1, 3, 5$ or 7. Thus $H_{\phi_{5,0,1}} = \{e, x^2, x^4, x^6, xy, x^3 y, x^5 y, x^7 y\}$.

Subcase c: By Theorem 4.3, we have that $H_{\phi_{1,1,0}} = \{x^k y^j | 2k \equiv 0\ (8)\}$. This equation is satisfied whenever $k = 0$ or 4. Thus $H_{\phi_{1,1,0}} = \{e, x^4, x^4 y, y\}$.

Subcase d: By Theorem 4.3, we have that $H_{\phi_{7,1,1}} = \{x^k | 6k + 6k \equiv 0\ (8)\} \cup \{x^k y | 6k + 6k + 4 \equiv 0\ (8)\}$. These equations are satisfied with even k in the first set and odd k in the second set, but we know k must be even. Thus $H_{\phi_{7,1,1}} = \{e, x^2, x^4, x^6\}$.

The rest of the fixed-point groups are found in a similar manner and are shown below.

$H_{\phi_{3,0,0}} = \{e, x^4, x^4 y, y\}$

$H_{\phi_{5,0,0}} = \{e, x^2, x^4, x^6, x^2 y, x^4 y, x^6 y, y\}$

$H_{\phi_{7,0,0}} = \{e, x^4, x^4 y, y\}$

$H_{\phi_{1,0,1}} = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7\}$

$H_{\phi_{3,0,1}} = \{e, x^4, x^2 y, x^6 y\}$

$H_{\phi_{5,0,1}} = \{e, x^2, x^4, x^6, xy, x^3 y, x^5 y, x^7 y\}$

$H_{\phi_{7,0,1}} = \{e, x^4, x^2y, x^6y\}$

$H_{\phi_{1,1,0}} = \{e, x^4, x^4y, y\}$

$H_{\phi_{5,1,0}} = \{e, x^4, x^4y, y\}$

$H_{\phi_{3,1,1}} = \{e, x^2, x^4, x^6\}$

$H_{\phi_{7,1,1}} = \{e, x^2, x^4, x^6\}$

4.2. **Generalized symmetric spaces.** We now determine the generalized symmetric space of a given involution.

Definition 4.6. Let G be a group and $\phi \in Aut(G)$ be an involution. The **generalized symmetric space** of ϕ is the set $Q_\phi = \{\ g(\phi(g))^{-1} \mid g \in G\ \}$.

As with the fixed-point groups, we first consider the generalized symmetric spaces associated with involutions of the form $\phi_{a,0,c}$.

Theorem 4.7. *For an involution $\phi_{a,0,c} \in Aut(M_m(2))$, the generalized symmetric space is $Q_{\phi_{a,0,c}} = \{x^{k(1-a)-jc2^{m-2}} \mid k \in \mathbb{Z}_{2^{m-1}}\}$.*

Proof. Let $\phi_{a,0,c} \in Aut(M_m(2))$ be an involution and let $x^ky^j \in M_m(2)$. Using Theorem 3.13 and Theorem 2.17, we have

$$\begin{aligned} x^ky^j(\phi_{a,0,c}(x^ky^j))^{-1} &= x^ky^j(x^{ak+jc2^{m-2}}y^j)^{-1} \\ &= x^ky^j(y^jx^{2^{m-1}-(ak+jc2^{m-2})}) \\ &= x^{k(1-a)-jc2^{m-2}}. \end{aligned}$$

□

Recall by Theorem 2.20 that elements of the form x^k where k is even are in the center $Z(M_m(2))$. Since for any involution $\phi_{a,b,c}$, the value of a is odd, we have the following corollary:

Corollary 4.8. *For an involution $\phi_{a,0,c} \in Aut(M_m(2))$, the generalized symmetric space $Q_{\phi_{a,0,c}} \subseteq Z(M_m(2))$.*

Now we examine the generalized symmetric spaces on involutions of the form $\phi_{a,1,c}$.

Theorem 4.9. *For an involution $\phi_{a,1,c} \in Aut(M_m(2))$, the generalized symmetric space arising from x^k is $Q_{\phi_{a,1,c}} = \{x^{k-ak2^{m-2}-ak-a(k-1)2^{m-3}}y | k \text{ is odd}\} \cup \{x^{k-ak-ak2^{m-3}} | k \text{ is even}\}$. For an involution $\phi_{a,1,c} \in Aut(M_m(2))$, the generalized symmetric space arising from $x^k y$ is $Q_{\phi_{a,1,c}} = \{x^{k-ak2^{m-2}-ak-a(k-1)2^{m-3}-c2^{m-2}}y | k \text{ is odd}\} \cup \{x^{k-ak-ak2^{m-3}-c2^{m-2}} | k \text{ is even}\}$.*

Proof. Let $\phi_{a,1,c} \in Aut(M_m(2))$ and $x^k y^j \in M_m(2)$.

Case 1: Assume k is even and $j = 0$. Using Theorem 3.13 and Theorem 2.17, we have

$$\begin{aligned} x^k(\phi_{a,1,c}(x^k))^{-1} &= x^k(x^{ak+ak2^{m-3}})^{-1} \\ &= x^{k-ak-ak2^{m-3}}. \end{aligned}$$

Case 2: Assume k is odd and $j = 0$. We use Theorem 3.13, Theorem 2.17, and the commutation relation to obtain the following:

$$\begin{aligned} x^k(\phi_{a,1,c}(x^k))^{-1} &= x^k(x^{ak+a(k-1)b2^{m-3}}y)^{-1} \\ &= x^k y x^{-(ak+a(k-1)2^{m-3})} \\ &= x^k x^{(-ak-a(k-1)2^{m-3})(2^{m-2}+1)} y \\ &= x^{k-ak2^{m-2}-a(k-1)2^{2m-5}-ak-a(k-1)2^{m-3}} y. \end{aligned}$$

Furthermore, since k is odd, the term $a(k-1)2^{2m-5}$ can be rewritten as $at2^{2m-4}$ for some $t \in \mathbb{Z}$. Then $m \geq 4$ implies $2m-4 \geq m-1$ holds. Thus $x^{-a(k-1)2^{2m-5}} = e$, which implies

$$x^k(\phi_{a,1,c}(x^k))^{-1} = x^{k-ak2^{m-2}-ak-a(k-1)2^{m-3}} y.$$

We now examine the involutions of the form $\phi_{a,1,c} \in Aut(M_m(2))$.

Case 3: Assume k is even and $j = 1$. Using Theorem 3.13 and Theorem 2.17, we have

$$\begin{aligned} x^k y(\phi_{a,1,c}(x^k y))^{-1} &= x^k y(x^{ak+ak2^{m-3}+c2^{m-2}}y)^{-1} \\ &= x^k(y^2)x^{-ak-ak2^{m-3}-c2^{m-2}} \\ &= x^{k-ak-ak2^{m-3}-c2^{m-2}}. \end{aligned}$$

Case 4: Assume k is odd and $j = 1$. Using Theorems 3.13, 2.20 and 2.17, we have

$$\begin{aligned} x^k y(\phi_{a,1,c}(x^k y))^{-1} &= x^k y(x^{ak+a(k-1)2^{m-3}+c2^{m-2}})^{-1} \\ &= x^k(x^{-(ak-a(k-1)2^{m-3}-c2^{m-2})(2^{m-2}+1)})y \\ &= x^{k-ak2^{m-2}-ak-a(k-1)2^{m-3}-c2^{m-2}}y. \end{aligned}$$ □

Though split into four cases for easier analysis, we can now combine the results into a more comprehensive equation.

Corollary 4.10. *The generalized symmetric space of an involution $\phi_{a,1,c}$ is equal to* $Q_{\phi_{a,1,c}} = \{x^{k-ak-ak2^{m-3}+a2^{m-3}-jc2^{m-2}-ak2^{m-2}}y|\ k \text{ is odd}\} \cup \{x^{k-ak-ak2^{m-3}-jc2^{m-2}}|\ k \text{ is even}\}$.

Example 4.11. We now determine the generalized symmetric spaces of involutions $\phi \in Aut(M_4(2))$.

Let us examine the generalized symmetric spaces of the following involutions: $\phi_{3,0,0}$, $\phi_{5,0,1}$, $\phi_{1,1,0}$, and $\phi_{7,1,1}$.

Subcase a: By Theorem 4.7, we have $Q_{\phi_{3,0,0}} = \{x^{k(-2)}|k \in \mathbb{Z}_8\}$. This equation is satisfied when $k = 0, 2, 4, 6$. Thus $Q_{\phi_{3,0,0}} = \{e, x^2, x^4, x^6\}$.

Subcase b: By Theorem 4.7, we have $Q_{\phi_{5,0,1}} = \{x^{-4k}|k \in \mathbb{Z}_8\} \cup \{x^{-4k+4}|k \in \mathbb{Z}_8\}$. Thus we have $Q_{\phi_{5,0,1}} = \{e, x^4\}$.

Subcase c: By Theorem 4.9, we have $Q_{\phi_{1,1,0}} = \{x^{-6k+2}y|\ k \text{ is odd}\} \cup \{x^{-2k}|\ k \text{ is even}\} \cup \{x^{-6k+2}y|\ k \text{ is odd}\} \cup \{x^{k-k-2k}|\ k \text{ is even}\}$. Note in this case that the elements in Q arising from elements of the form $x^k y$ are identical to the elements in Q arising from elements of the form x^k. When k is odd, $-6k+2$ (8) ranges through $\{4, 0\}$ and when k is even, $-2k$ (8) ranges through the set $\{4, 0\}$. Thus $Q_{\phi_{1,1,0}} = \{e, x^4, x^4y, y\}$.

Subcase d: By Theorem 4.9, we have $Q_{\phi_{7,1,1}} = \{x^6y|\ k \text{ is odd}\} \cup \{x^{4k}|\ k \text{ is even}\} \cup \{x^8y|\ k \text{ is odd}\} \cup \{x^{4k-4}|\ k \text{ is even}\}$. Thus we have $Q_{\phi_{7,1,1}} = \{e, x^4, x^2y, x^6y\}$.

The rest of the generalized symmetric spaces are found in a similar manner and are shown below.

$Q_{\phi_{3,0,0}} = \{e, x^2, x^4, x^6\}$

$Q_{\phi_{5,0,0}} = \{e, x^4\}$

$Q_{\phi_{7,0,0}} = \{e, x^2, x^4, x^6\}$

$Q_{\phi_{1,0,1}} = \{e, x^4\}$

$Q_{\phi_{3,0,1}} = \{e, x^2, x^4, x^6\}$

$Q_{\phi_{5,0,1}} = \{e, x^4\}$

$Q_{\phi_{7,0,1}} = \{e, x^2, x^4, x^6\}$

$Q_{\phi_{1,1,0}} = \{e, x^4, x^4y, y\}$

$Q_{\phi_{5,1,0}} = \{e, x^4, x^4y, y\}$

$Q_{\phi_{3,1,1}} = \{e, x^4, x^2y, x^6y\}$

$Q_{\phi_{7,1,1}} = \{e, x^4, x^2y, x^6y\}$

4.3. **Extended symmetric spaces.** We conclude this section by determining the extended symmetric space of a given involution.

Definition 4.12. Let G be a group and $\phi \in Aut(G)$ be an involution. The **extended symmetric space** of ϕ is the set $R_\phi = \{g \in G | \phi(g) = g^{-1}\}$.

Note that it can be shown that the generalized symmetric space Q of an involution is a subset of the extended symmetric space R. As with the fixed-point group and the generalized symmetric space, we begin with involutions of the form $\phi_{a,0,c}$.

Theorem 4.13. *For an involution $\phi_{a,0,c} \in Aut(M_m(2))$, the extended symmetric space is*

$$R_{\phi_{a,0,c}} = \{x^k y^j | ak + jc2^{m-2} + k(2^{m-2}+1)^j \equiv 0 \ (2^{m-1})\}.$$

Proof. Let $\phi_{a,0,c} \in Aut(M_m(2))$ and $x^k y^j \in M_m(2)$. The statement $\phi_{a,0,c}(x^k y^j) = (x^k y^j)^{-1}$ is equivalent to $\phi_{a,0,c}(x^k y^j)(x^k y^j) = e$, where e is the identity. We will use this formulation.

By Theorem 3.13, the commutation relation and Theorem 2.20, we have

$$\begin{aligned}
\phi_{a,0,c}(x^k y^j) x^k y^j &= x^{ak+jc2^{m-2}} y^j x^k y^j \\
&= x^{ak+jc2^{m-2}} x^{k(2^{m-2}+1)^j} y^{2j} \\
&= x^{ak+jc2^{m-2}+k(2^{m-2}+1)^j} \\
&= e,
\end{aligned}$$

which implies

$$ak + jc2^{m-2} + k(2^{m-2}+1)^j \equiv 0 \ (2^{m-1}). \qquad \square$$

We now turn our attention to the extended symmetric spaces of involutions of the form $\phi_{a,1,c}$. As in the case of fixed point groups, we find that no element $x^k y^j$ with k odd is in the extended symmetric space of these involutions.

Theorem 4.14. *For an involution $\phi_{a,1,c} \in Aut(M_m(2))$, the extended symmetric space is $R_{\phi_{a,1,c}} = \{x^k y^j | ak + ak2^{m-3} + jc2^{m-2} + k(2^{m-2}+1)^j \equiv 0 \ (2^{m-1})$ and k is even.$\}$*

Proof. We again split into two cases: k even and k odd.

Case 1: Assume k is even. Using Theorem 3.13 and our commutation relation, we have

$$\begin{aligned}\phi_{a,1,c}(x^k y^j)x^k y^j &= x^{ak+ak2^{m-3}+jc2^{m-2}} y^j x^k y^j \\ &= x^{ak+ak2^{m-3}+jc2^{m-2}+k(2^{m-2}+1)^j} y^{2j} \\ &= x^{ak+ak2^{m-3}+jc2^{m-2}+k(2^{m-2}+1)^j} = e.\end{aligned}$$

This leads us directly to the condition $ak + ak2^{m-3} + jc2^{m-2} + k(2^{m-2}+1)^j \equiv 0\ (2^{m-1})$.

Case 2: Assume k is odd. Using Theorem 3.13 and the commutation relation, we have

$$\begin{aligned}\phi_{a,1,c}(x^k y^j)x^k y^j &= x^{ak+a(k-1)b2^{m-3}} y x^{jc2^{m-2}} y^j x^k y^j \\ &= x^{ak+a(k-1)2^{m-3}+c2^{m-2}} x^{k(2^{m-2}-1)^j} y^{2j+1}.\end{aligned}$$

An element of this form can never be equivalent to the identity e. Thus, when k is odd, elements of the form $x^k y^j \notin R_{\phi_{a,1,c}}$. □

Example 4.15. We now determine the extended symmetric spaces for involutions $\phi \in Aut(M_4(2))$. Let us first examine the extended symmetric spaces corresponding to the following involutions : $\phi_{3,0,0}, \phi_{5,0,1}, \phi_{1,1,0}$ and $\phi_{7,1,1}$.

Subcase a: By Theorem 4.13, we have $R_{\phi_{3,0,0}} = \{x^k | 4k \equiv 0\ (8)\} \cup \{x^k y | 8k \equiv 0\ (8)\}$. The first equation is satisfied when k is even, and the second is satisfied for all k. Thus $R_{\phi_{3,0,0}} = \{e, x^2, x^4, x^6, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y\}$.

Subcase b: By Theorem 4.13, we have $R_{\phi_{5,0,1}} = \{x^k | 6k \equiv 0\ (8)\} \cup \{2k+4 \equiv 0\ (8)\}$. The first equation is satisfied by $k = 0$ or 4 and the second is satisfied for $k = 2$ or 6. Thus, $R_{\phi_{5,0,1}} = \{e, x^4, x^2y, x^6y\}$.

Subcase c: By Theorem 4.14, we have $R_{\phi_{1,1,0}} = \{x^k | 4k \equiv 0\ (8)$ and k is even$\} \cup \{x^k y | 8k \equiv 0\ (8)$ and k is even$\}$. The first equation is satisfied for all even k in both cases. Thus $R_{\phi_{1,1,0}} = \{e, x^2, x^4, x^6, x^2y, x^4y, x^6y, y\}$.

Subcase d: By Theorem 4.14, we have $R_{\phi_{7,1,1}} = \{x^k | 6k \equiv 0\ (8)$ and k is even$\} \cup \{x^k y | 2k+4 \equiv 0\ (8)$ and k is even$\}$. The first equation is satisfied for $k = 0$ or 4, and the second is satisfied for $k = 2$ or 6. Thus $R_{\phi_{7,1,1}} = \{e, x^4, x^2y, x^6y\}$.

The rest of the extended symmetric spaces are found in a similar way, and are shown below.

$R_{\phi_{3,0,0}} = \{e, x^2, x^4, x^6, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y\}$

$R_{\phi_{5,0,0}} = \{e, x^4, x^4y, y\}$

$R_{\phi_{7,0,0}} = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7, x^2y, x^4y, x^6y, y\}$

$R_{\phi_{1,0,1}} = \{e, x^4, x^2y, x^6y\}$

$R_{\phi_{3,0,1}} = \{e, x^2, x^4, x^6\}$

$R_{\phi_{5,0,1}} = \{e, x^4, x^2y, x^6y\}$

$R_{\phi_{7,0,1}} = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7, xy, x^3y, x^5y, x^7y\}$

$R_{\phi_{1,1,0}} = \{e, x^2, x^4, x^6, x^2, x^4y, x^6y, y\}$

$R_{\phi_{5,1,0}} = \{e, x^2, x^4, x^6, x^2, x^4y, x^6y, y\}$

$R_{\phi_{3,1,1}} = \{e, x^4, x^2y, x^6y\}$

$R_{\phi_{7,1,1}} = \{e, x^4, x^2y, x^6y\}$

References

[1] M. Artin. *Algebra*. Prentice Hall, 1991.

[2] A. Bishop, C. Cyr, J. Hutchens, C. May, N. Schwartz, and B. Turner. On involutions and generalized symmetric spaces of dicyclic groups. *ArXiv e-prints*, September 2013.

[3] W.M. Boothby. *An Introduction to Differentiable Manifolds and Riemannian Geometry*. Pure and Applied Mathematics Series. Academic Press, 2003.

[4] C. Buell, B. Carrillo, M. Lewis, and J. Woelfel. The classification of involutions of symmetry groups and their generalized symmetric spaces. *Pre-Print*, Unpublished.

[5] C. Buell, A. G. Helminck, V. Klima, J. Schaefer, C. Wright, and E. Ziliak. On the structure of generalized symmetric spaces of $\mathbf{SL}_2(\mathbb{F}_q)$ and $\mathbf{GL}_2(\mathbb{F}_q)$. *Pre-Print*, 2014.

[6] K. K. A. Cunningham, T. J. Edgar, A. G. Helminck, B. F. Jones, H. Oh, R. Schwell, and J. F. Vasquez. On the structure of involutions and symmetric spaces of dihedral groups. *ArXiv e-prints*, May 2012.

[7] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[8] D. Gorenstein. *Finite Groups*. AMS Chelsea Publishing, 2 edition, 2007.

[9] A. Papantonopoulou. *Algebra: Pure and Applied*. Pearson, 2001.

[10] D. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1996.

[11] J. Schaefer and K. Schlechtweg. On the structure of symmetric spaces of semidihedral groups. *Pre-Print*, 2014.

[12] W. Stein. *Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach*. Undergraduate Texts in Mathematics. Springer, 2008.

[13] Wolfgang Ziller. Lie groups, representation theory and symmetric spaces. 2010.