# Finite Reflection Groups

Submitted April 2019

## 1 Introduction

The study of groups is a powerful tool to understand geometric structures as it allows one to consider the functions on a space that preserve a certain structure. In particular, the set of all isometries (fixing the origin) of a Euclidean space is the orthogonal group consisting of all orthogonal linear maps. In this group, and in more general affine linear maps in a Euclidean space, one type of element more fundamental to the structure is a reflection in the set. An affine linear isometry in a Euclidean space can be obtained by the composition of at most n+1 reflections. As such, we immediately see that one important example of a groups arising geometrically, the dihedral group, could theoretically be understood by examining reflections in $\mathbb{R}^2$. By restricting our attention to linear isometries (fixing the origin) we can attempt to develop some of the framework to study the theory of the structures that arise when we allow reflections to generate groups. Particularly, this allows us to use a geometric approach to prove purely algebraic statements. [2] This theory was first developed by H.S.M. Coxeter in 1934 when he completely classified such structures using a geometric approach. This theory has since been applied to many other problems in mathematics involving combinatorics as well as, more naturally, the study of polytopes and their symmetries. This theory was later generalized by Coxeter to the study of 'Coxeter groups' which gave rise to theories still applied to active areas of research today (Grove, Benson).

We will see that, not only can dihedral groups be realized in this form, but even the finite symmetric groups, which are ubiquitous in mathematics, are actually isomorphic to finite groups generated by reflections. The aim of this essay is to develop the geometric framework used to study the behaviour of these groups, primarily by closely examining the action of the group on $\mathbb{R}^n$. We will lead up to how one can find an efficient generating set for such groups as well as, more abstractly, the form of all defining relations in a finite reflection group.

## 2 Presentation of a Group

Before we can begin our geometric considerations, we must first give some preliminary algebraic notions to describe what our goal is in our treatment of reflection groups. We would like to describe what we mean by a presentation of a group. We give a fairly intuitive, but not completely precise, construction which is all that is necessary for our purposes where the description of a free group is adapted from a description by P. M. Cohn.

[1] A presentation of a group essentially tells us everything we would need to construct the multiplication table of a group. We have previously seen defining relations of a group

when a group has a specified number of elements which we use to determine when they are distinct. In a presentation, we are not specifying the size of a group but rather we say that elements are equal only if the equality can be shown directly from the relations. For a group presentation, we take a set $A$ from which we will construct formal words out of the elements of $A$ and their inverses. That is, $A$ will be the set of generators of our group. If these are not subject to any relations, we will call this group the free group on $A$. For example, the free group on $\{a, b, c\}$ would contain elements such as $a^3ba^{-2}c^4$ or $b^2a^{-1}$. We say that elements are only equal if they can be directly reduced to each other using only the relation (which we do not include in the presentation) $aa^{-1} = a^{-1}a = 1$ where we use 1 for the identity element which is just the empty word.

We let $R$ be a subset of the free group on $A$. That is, $R$ is a collection of expressions made out of our generators. By a presentation of a group $\langle A|R\rangle$, we mean that we allow the elements of $A$ to generate a group where $R$ gives us all the rules we are allowed to use to multiply elements. It is standard to let all relations be equal to the identity but we will sometimes rearrange these for clarity. More formally, a presentation is the quotient of the free group on $A$ by the normal subgroup generated by $R$ (Cohn).

We will take a familiar example to illustrate what is meant. We know (from Algebra 2) that any group of order $2n$ generated by two elements $a, b$ subject to the relations $a^n = b^2 = 1$ and $ba = a^{-1}b$ is the dihedral group $D_n$ where we use the subscript to denote the number of vertices as later we will like to focus on the geometric interpretation. This would be written in our notation as $\langle a, b|a^n = b^2 = 1, ba = a^{-1}b\rangle$. We know this group has at most $2n$ distinct elements of the form $a^ib^j$ with $0 \leq i < n, j = 0, 1$. However, no equality of two elements of this form follows from the relations so this group indeed has exactly $2n$ elements and is dihedral. A simpler example is if we take $\langle x|x^n = 1\rangle$ we would be able to write any element of this group in the form $x^k$ for $0 \leq k < n$ and this would give us precisely the cyclic group of order n as it has at most n distinct elements and no two of these can be shown to be equal from that relation.

The way we will use this concept to determine the presentation of a group is by showing that every single relation in a group can be determined solely by the relations given in our presentation. If this can be shown, then if all relations in the group are themselves true, we would have the result that the group admits that presentation. The goal of our essay will be to show that a reflection group can be uniquely characterized by the presentation stating the orders of products of any two reflections – which include the natural relation that the product of a reflection with itself is the identity. We also seek to study what the smallest generating sets would look like.

## 3 Reflections

We let $V$ be an n-dimensional Euclidean space ($V \cong \mathbb{R}^n$) with its usual inner product (in our coordinate system) denoted $\langle \cdot, \cdot \rangle$. We use the definition of angles from the inner product in a Euclidean space. First, we would like to define what is meant by a reflection. We will be ignoring affine transformations and so all reflecting hyperplanes must be linear subspaces and not affine subspaces. As all reflections are orthogonal transformations (isometries), they preserve the inner product. We call the group of orthogonal transformations of $V$, $\mathcal{O}(V)$. Results and definitions in this section, but not their proofs, are taken from Humphrey's text.

**Definition 3.1:** [3] A **reflection** is a linear map $T\colon V \to V$ such that, for some ordered orthonormal basis of $V$, $(e_1, ...e_n)$, one has that $T(e_1) = -e_1$ and $T(e_i) = e_i$ for $i \geq 2$. That is, $T$ maps some nonzero vector $\alpha$ to $-\alpha$ and fixes the hyperplane $H_\alpha$ which we define by $H_\alpha := \langle\alpha\rangle^\perp = \{v \in V | \langle\alpha, v\rangle = 0\}$ orthogonal to $\alpha$, where $\langle\alpha\rangle$ is the span $\{x\alpha | x \in \mathbb{R}\}$. We will denote reflections by $s_\alpha$ where $\alpha$ is some nonzero vector, as in our definition, mapped to $-\alpha$.

We immediately see that $s_\alpha = s_\beta$ if and only if $\alpha$ and $\beta$ are linearly dependent and thus we may assume that $\alpha$ is a unit vector; had we defined reflections more generally without a specific origin, this would not be the case. As $\langle\alpha\rangle^\perp = H_\alpha$, we (from geometry) can decompose $V$ as: $V = \langle\alpha\rangle \bigoplus H_\alpha$. We also observe that for any $s_\alpha \in \mathcal{O}(V), s_\alpha^2$ fixes $\alpha$ as well as $H_\alpha$ and hence all reflections have order 2 in $\mathcal{O}(V)$. Given a reflection $s_\alpha$ we may take an orthonormal basis $e_2, ..., e_n$ of $H_\alpha$ so that adding $\alpha$ gives an orthonormal basis of $V$ by the definition of $H_\alpha$. Then, any vector $v \in V$ can be written as $v = a_1\alpha + \sum_{i=2}^n a_i e_i$ by our aforementioned decomposition of $V$. Therefore,

$$s_\alpha(v) = -a_1\alpha + \sum_{i=2}^n a_i e_i = -2a_1\alpha + v$$

But we also have that,

$$\langle v, \alpha\rangle = \langle a_1\alpha, \alpha\rangle + \sum_{i=2}^n a_i\langle e_i, \alpha\rangle = a_1$$

by the orthonormality of $\alpha, e_2, ..., e_n$. This proves the following result stated, but not proved, in (Humphreys):

**Proposition 3.2:** [3] Let $s_\alpha\colon V \to V$ be a reflection, where $\alpha$ is a unit vector, and let $v \in V$. Then,

$$s_\alpha(v) = v - 2\langle v, \alpha\rangle\alpha$$

The notation $s_\alpha$ is useful for emphasizing how a vector is changed by a reflection but a more geometric interpretation can be useful as reflections are often seen in terms of the fixed hyperplane. This is especially easy if $\dim(V) = 2$; that is, $V = \mathbb{R}^2$. One can always choose $H_\alpha = \langle(\cos\theta, \sin\theta)\rangle$ in which case, $\alpha$ would necessarily be a scalar multiple of $(\sin\theta, -\cos\theta)$. In this case we have the following:

**Proposition 3.3:** Let $\alpha = (\sin\theta, -\cos\theta)$. Then, $s_\alpha$ has matrix, with respect to the standard basis:

$$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

*Proof.* $\alpha$ is a unit vector and so we may apply proposition 3.2.

$$\begin{aligned} s_\alpha((1,0)) &= (1,0) - 2\langle(1,0), (\sin\theta, -\cos\theta)\rangle(\sin\theta, -\cos\theta) \\ &= (1 - 2\sin^2\theta, 2\sin\theta\cos\theta) \\ &= (\cos 2\theta, \sin 2\theta) \end{aligned}$$

One gets the second column by applying this argument to (0,1). □

# 4 Reflection Groups and Examples

**Definition 4.1:** [3] A **finite reflection group** is a finite subgroup of $\mathcal{O}(V)$ generated by reflections.

Clearly if we were to give a presentation of the group, we would need to specify that every generator has order 2 and so the relation $a^2 = 1$ for any generator $a$ of the group would need to be in our presentation. To understand these groups we will use both the geometric nature of the reflections that are in $G$ as well as their group structure. It is important to remember that a reflection group does not consist solely of reflections. We return to our motivating example of $D_m$.

**Example 4.2: (The Dihedral Group $D_m$ of order $2m$)** [3]
If V is the Euclidean plane, $\mathbb{R}^2$, then $D_m$ is the set of the $m$ rotations and $m$ reflections which are symmetries of a regular $m$-gon centred at the origin. The $m$ rotations are the anti-clockwise rotations through $2\pi i/m$ for $i = 1, ..., m$. These reflections are independent of the choice of vertices for our $m$-gon. These rotations are generated by a rotation about $2\pi/m$ so we need only consider this one. With respect to the standard basis, this has matrix:

$$\begin{pmatrix} \cos(2\pi/m) & -\sin(2\pi/m) \\ \sin(2\pi/m) & \cos(2\pi/m) \end{pmatrix}$$

Then, taking $\alpha = (\sin(\pi/m), -\cos(\pi/m))$ and $\beta = (0, 1)$, we can apply proposition 3.3 to obtain (Humphreys):

$$s_\alpha s_\beta = \begin{pmatrix} \cos(2\pi/m) & \sin(2\pi/m) \\ \sin(2\pi/m) & -\cos(2\pi/m) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\pi/m & -\sin 2\pi/m \\ \sin 2\pi/m & \cos 2\pi/m \end{pmatrix}$$

This shows that all rotations in $D_m$ can be obtained by a composition of reflections and so $D_m$ is a finite reflection group. Moreover, if $a$ is our rotation and $b$ is either of the two reflections used to generate it, we know (from Algebra 2) that every reflection in $D_m$ has the form $a^i b$ for $i = 0, 1, ..., m-1$. As such, $D_m$ is actually generated by our two reflections needed to obtain this rotation. We should note that, as the two lines needed are separated by an angle of $\pi/m$, we can simply choose our regular $m$-gon to have these two lines yielding symmetries. One such construction would be, for example, placing our vertices where the $m$-th roots of unity would be if we identify $\mathbb{C} \cong \mathbb{R}^2$. There will always be a point on the horizontal axis and they are each separated by angles $\pi/m$ and so they will always land on these lines. If $m$ is even, half the lines will have 2 points on them and the remaining ones will be our other symmetries. If $m$ is odd, all lines will have one point on them and they will be all reflections. In either case, these $m$ lines of reflection are precisely those in $D_m$.

**Example 4.3: Orthogonal Transformations** If $V \cong \mathbb{R}^n$ then every element of $\mathcal{O}(V)$ is a composition of reflections. This means that $\mathcal{O}(V)$ is generated by the set of all of its reflections and hence it is a reflection group (though not a finite one).

**Example 4.4: Permutation Groups** [3] Let $e_1, ...e_n$ be the standard orthonormal basis of $\mathbb{R}^n$. We know that the symmetric group $S_n$ is generated by its transpositions as any permutation is the product of transpositions. Consider the family of reflections obtained by swapping the i-th and j-th columns of the identity matrix. These are all in the orthogonal group as their determinant is $-1$. This transformation precisely maps $e_i$ to $e_j$ and $e_j$ to $e_i$ while fixing all the other basis vectors since they are all orthogonal to $e_i - e_j$ by bilinearity of the inner product. We note that it carries $e_i - e_j$ to $-(e_i - e_j$; It also fixes $e_i + e_j$ which is orthogonal to $e_i - e_j$ and as $e_i + e_j$, along with the $e_k$ for $k \neq i, j$ are all linearly independent, they span the hyperplane normal to $e_i - e_j$. Therefore, we can conclude that this transformation is the reflection $s_{e_i - e_j}$. We can identify this reflection with the transposition (i, j) as it fixes all other basis vectors and just swaps the indices i and j. We can obtain a bijection by identifying any permutation with this corresponding composition of vectors permuting the basis elements. This is well-defined as any permutation determines the action of the composite map on the basis elements which determines any linear map. Moreover, the composition of permutations will necessarily yield the same permutation on the basis vectors so we see that this is indeed an isomorphism from $S_n$ to a reflection group. This tells us that all groups are isomorphic to a subgroup of a reflection group (as all groups are isomorphic to a subgroup of a symmetric group) which implies that finite reflection groups are similarly ubiquitous in finite group theory (Humphreys).

**Example 4.5: $A_n$ is not a reflection group** In general alternating groups are not reflection groups. It is sufficient to show they cannot be generated by their elements of order 2. $A_3$ has order 3 so it is cyclic and has no elements of order 2. We can also consider an alternating group of even order. $A_4$ has 3 elements of order 2 which are, when written as a product of transpositions, $(12)(34), (13)(24)$, and $(14)(23)$. However, these elements are closed under multiplication as $(12)(34)(13)(24) = (14)(23)$ and the others follow similarly. They are each of order two and so they generate a subgroup of order 4. Therefore $A_4$ is not generated by its elements of order 2 so it is not a reflection group.

# 5 Order Relations

To further study the behaviour of these groups we will need a particular definition of a total order which respects the vector space structure in a convenient way as well as an important example regarding total ordering on real vector spaces we will use. These are taken from Humphreys's text although the proof of theorem 5.3 is my own.

**Definition 5.1** [3] A **total order** on a vector space $V$ is a transitive relation '$<$' satisfying: (for any $a, b, c \in V$)
1. Exactly one of $a < b$, a = b, or $b < a$ holds.
2. $a < b \implies c + a < c + b$
3. If $\lambda \in \mathbb{R}$ then, if $\lambda > 0$ we have $a < b \implies \lambda a < \lambda b$ and if $\lambda < 0$ we have $a < b \implies \lambda b < \lambda a$.

**Definition 5.2:** [3] We define the **lexicographic ordering** on the vector space $V$ as follows: Let $(e_1, ..., e_n)$ be an ordered basis of $V$. Then, we say that $\sum_{i=1}^{n} a_i e_i < \sum_{i=1}^{n} b_i e_i$ if $a_k < b_k$ where $k$ is the least natural number such that $a_i \neq b_i$. It is not immediately clear that this is a total order on $V \cong \mathbb{R}^n$.

This is essentially just the numerical analogue of alphabetic order and we can safely assume we always define this with the standard basis. For example, we would have that $(1, 5, 7, 9) < (1, 5, 8, 3)$ and if we identified the numbers $0, ..., 9$ with $a, ..., j$ this would just say that “bfhj” comes before “bfid” alphabetically. We will generally use the standard basis; however, we will show that it is a total ordering for any basis.

**Theorem 5.3:** [3] The lexicographic ordering is a total order on $V$ (Humphreys).

*Proof.* Transitivity: If $\sum_{i=1}^{n} a_i e_i < \sum_{i=1}^{n} b_i e_i$ and $\sum_{i=1}^{n} b_i e_i < \sum_{i=1}^{n} c_i e_i$, then if the least digit, call it $k$, where $c_i > b_i$ is less than the digit for the $a_i$ and $b_i$ then we have that $c_k > b_k = a_k$ and the $c_i$ and $a_i$ must also be equal if i < k and we have transitivity. If this $k$ is greater than the first place they differ for $a_i$ and $b_i$ then, if l is the first place the $a_i$ and $b_i$ differ, we have that $c_l = b_l > a_l$ and if $i < l$ then $a_i = b_i = c_i$ and we once again have transitivity. We now show the three other requirements.

1) If $a \neq b$ then they differ in some place. These are both real numbers so we necessarily must have that one is more than the other and thus either $a < b$ or $b < a$. If $a = b$ neither of the other can hold since they differ nowhere.

2) We have that $a_i = b_i \iff c_i + a_i = c_i + b_i$ and thus the first index where they differ will remain unchanged. The above equivalence also holds for the standard order on the real numbers and thus $a < b \implies a + c < b + c$.

3) if $\lambda > 0$ then $a_i < b_i \iff \lambda a_i < \lambda b_i$ and $a_i = b_i \iff \lambda a_i = \lambda b_i$ and thus the index where they first differ as well as the order at this index is unchanged. The same holds if we reverse the order for $\lambda < 0$. □

We will use this to define several concepts related to reflection groups but we will mainly use this notion to derive contradictions involving whether an element is indeed ‘greater’ than 0 in this ordering which is always the case if all coefficients are nonnegative and at least one is nonzero.

# 6 Root Systems and Positive Reflection Groups

We will assume $G$ is a finite reflection group in this section. The main idea of this section is to understand $G$’s action on $V$ as a permutation on the lines $\langle \alpha \rangle$, where $s_\alpha \in G$. To avoid clutter, we will assume that $\alpha$ is always such that $s_\alpha \in G$.

**Lemma 6.1** Let $t \in \mathcal{O}(V)$ and let $G$ be a finite reflection group; let $\alpha \in V$ be nonzero. Then, $ts_\alpha t^{-1} = s_{t(\alpha)}$

*Proof.* [3] $ts_\alpha t^{-1}(t(\alpha)) = ts_\alpha(\alpha) = -t(\alpha)$. Now, it suffices to show that this map has the same action on $H_{t(\alpha)}$ as $s_{t(\alpha)}$ since this means they have the same action on a basis of $\mathbb{R}^n$ and so they must be the same map. Then, we note that $\langle v, t(\alpha) \rangle = \langle t^{-1}(v), \alpha \rangle$ for any $v, \in V$ as $t$ is an orthogonal transformation and so $t^{-1}$ is as well. Hence, if $v \in H_{t(\alpha)}$, then $t^{-1}(v) \in H_\alpha$. Then, if $v \in H_{t(\alpha)}$, $ts_\alpha t^{-1}(v) = t(t^{-1}(v)) = v$ and so the transformation fixes $H_{t(\alpha)}$. Therefore, $ts_\alpha t^{-1} = s_{t(\alpha)}$. □

A remark about group actions can be made following this lemma. With the way we have defined reflection groups it is natural to associate the group with the vector space the reflections naturally act on. However, this lemma suggests it may be more efficient to restrict our view to the lines spanned by the vectors orthogonal to the reflecting hyperplanes. That is, if $t, s_\alpha \in G$ then so is $ts_\alpha t^{-1}$ so $s_{t(\alpha)} \in G$ for all $t \in G$. This allows us to consider the action of $G$ on the lines $\langle \alpha \rangle$ by $t(\langle \alpha \rangle) = \langle t(\alpha) \rangle$. As $s_{t(\alpha)} \in G$, this is indeed still a line in this set and so this is indeed a group action as it clearly respects the group operation. This means that all reflection groups can actually be seen as a set of permutations on these lines and we can simply choose pairs of unit vectors (varying in sign) on each line to be able to represent them. Because the action of $G$ maps the lines to each other, this set of unit vectors will also be preserved under the action of $G$ as, by permuting the lines, we are effectively permuting these vectors (and changing signs so we need pairs). As with any group action, the elements of $G$ act as permutations on the set.

**Example 6.2:** [3] We would like to consider $D_4$, more particularly which points in $\mathbb{R}^2$ are permuted by the action of the group besides the vertices. That is, on what points can we define an action of $D_4$? We will assume our square has vertices where the fourth roots of unity are located. The isometries in $D_4$ permute the vertices $\pm(0,1)$ and $\pm(1,0)$. The elements of $D_4$ preserve (permute) the points $\pm(1,1)$ and $\pm(1,-1)$ as well as the vertices. This is because rotations simply cyclically permute these and two of our reflections are actually lines through pairs of these. Both of those reflections actually preserve all those points and in fact our other two reflections simply swap pairs of them as well. Therefore, these 4 points would clearly be stable under $D_4$. That is, the vectors $\pm(1,0), \pm(0,1), \pm(1,1), \pm(-1,1)$ being preserved by $D_4$ (they are mapped to each other). This collection of vectors is actually enough to specify the reflections in $D_4$ and hence the group itself as all reflections are through a pair of them. We use $\pm$ in order to emphasize that the pairs of vectors give only one reflection. A figure (made in Geogebra) showing these for $D_4$ is given below:

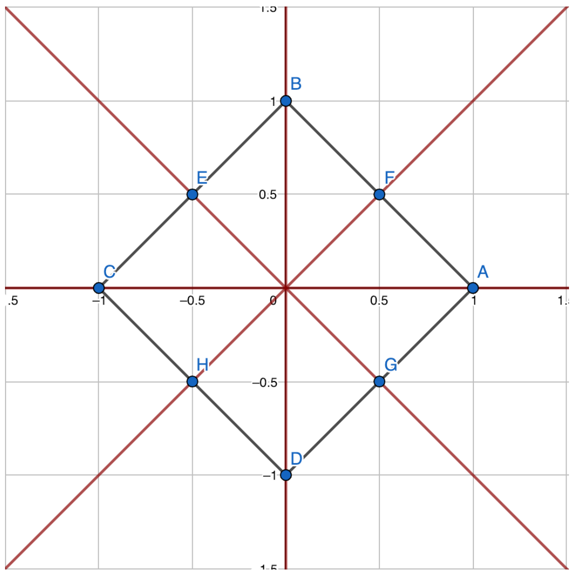


Figure 1: Vertices at roots of unity. Axes of reflection shown in red, stable points in blue.

We would like to generalize this notion of stability under the action of a finite reflection group to study a general group. This motivates the following definition to associate a group with a set of lines (or equivalently, antipodal points):

**Definition 6.3 (Root systems):** [3] A nonempty, finite, set $\Phi$ of nonzero vectors in $V$ is a **root system** with associated finite reflection group $G$ generated by $\{s_\alpha | \alpha \in \Phi\}$ if:
1. $\Phi \cap \langle \alpha \rangle = \{\pm\alpha\}$ for any $\alpha \in \Phi$
2. If $\alpha \in \Phi$, then $s_\alpha(\Phi) = \Phi$
We see that condition 2 essentially states that $G$ will always define a group on action on this set.

**Remark 6.4** $\Phi$ is a finite set but, as reflections do not commute, it is not obvious that the associated reflection group should be finite as well. We give the following argument adapted from [3] (Humphreys) as well as a specific case proven in [2] . Similar to our remarks following Lemma 6.1, we can associate every element of $G$ with a permutation on the set $\Phi$ because of the second requirement. Moreover, if a vector is orthogonal to all of $\Phi$, then $G$ must necessarily fix it and so no transformation other than the identity could also fix all of $\Phi$. This is because, for any subspace $W$ of $V$, $V = W \bigoplus W^{\perp}$ and we may take $W$ to be the span of the vectors in $\Phi$ and so it is sufficient to consider where $\Phi$ and vectors orthogonal to it are mapped. Therefore, the kernel of our group action consists solely of the identity. Then, we may apply the first isomorphism theorem to the homomorphism carrying elements of $G$ to their corresponding permutation to obtain that $G$ is isomorphic to a subgroup of the symmetric group on $\Phi$ (the image of the homomorphism). As such, we can associate every root system to a finite reflection group.

To be able to completely study finite reflection groups by studying root systems we would like to be able to associate each group to a root system as well. This can be done as the set of lines fixed by the reflections in our group gives us a root system by simply choosing antipodal points on each of these lines. If we rescale all of $\Phi$ we are still left with a root system and so, when necessary, we can always choose a root system consisting of unit vectors. It is worth noting that the $\{s_\alpha | \alpha \in \Phi\}$ may not give all reflections in the corresponding group – the choice of root system is not always strict. However, this lack of uniqueness is not an issue for the essay as what matters is the stability and the fact that the reflections generate the group.

If $\Phi$ is a root system, then every one of its elements is a pair of elements varying in sign, it can be convenient to only consider half of the vectors by choosing one from each pair. In any lexicographic ordering, precisely one from each pair will be positive and it will just be whichever has a positive component appear first when written in terms of some basis. We will fix an arbitrary basis for our lexicographic order for the purposes of our following definitions from [3] which we will then fix for the rest of the essay unless otherwise specified.

**Definition 6.5:** $\alpha \in V$ is **positive** if $\alpha > 0$. If $\Phi$ is a root system then we call a subset $\Pi \subset \Phi$ a **positive system** if it consists of all positive roots in $\Phi$. We define **negative systems** analogously. We note that $\Phi$ is a disjoint union of a positive and negative system. We will use the positive system for further definitions and results. It is a completely arbitrary choice and the following definition, and hence the results that use this concept, can just as easily be defined for negative systems. If we assume we have a positive system then, unless we specify otherwise or it is arbitrary, we shall assume that we are applying lexicographic ordering with the same basis as the one used to define the positive system.

**Definition 6.6:** Let $\Phi$ be a root system with positive system $\Pi$. A subset $\Delta$ of $\Pi$ is a **simple system** if $\Delta$ is a basis for the vector space spanned by the elements of $\Phi$ and if every element $\alpha \in \Phi$, when written in terms of the basis $\Delta$, has coefficients all of the same sign (or equivalently, every element of $\Pi$).

We should note that these coefficients in this expansion are unique by the definition of a basis. We will call the sum of these coefficients the **height** of that vector. To show why simple systems are useful, we will show the following result from [3] which implies that simple systems exist. Along with theorem 6.9 it is one of the two main results from this chapter:

**Theorem 6.7:** Any positive system contains a unique simple system.

*Proof.* [3] As mentioned previously, we may safely assume that our positive system consists entirely of unit vectors. We first show existence. Let $\Pi$ be our positive system. We first choose a subset of $\Pi$, $\Delta$, such that every element of $\Pi$ can be written as a linear combination of these elements with no coefficients being negative. Clearly $\Pi$ itself will work as $\alpha = \alpha$ satisfies these requirements. We then choose this subset to have as few elements as possible. We must now show that it is linearly independent. This follows from a geometric argument given by (Humphreys). We first claim that, for any distinct $\alpha, \beta \in \Delta$,

$$\langle \alpha, \beta \rangle \leq 0$$

If $\alpha, \beta \in \Delta$, then we would have, from proposition 3.2,

$$s_\alpha(\beta) = \beta - 2\alpha\langle \alpha, \beta \rangle$$

This element lies in $\Phi$ from the definition of a root system. If this inner product were not less than or equal to zero, this would not be a linear combination of vectors with coefficients of the same sign. However, this element (or its negative) can be written as a linear combination of elements from $\Delta$ with coefficients of the same sign by the definition of a simple system. Call the coefficient of $\beta$, $a_\beta$ in this linear combination. Call the remaining terms $v$ so that $s_\alpha(\beta) = \beta a_\beta + v$. We treat the case where $s_\alpha$ is positive as the negative case is analogous. This means the coefficients of $v$ must all be nonnegative.

We now consider the case where $a_\beta < 1$, and so $1 - a_\beta > 0$. Here, we would have that $\beta(1 - a_\beta) = 2\alpha\langle \alpha, \beta \rangle + v$ where $v$ is the other terms in our linear combination. Everything on the right-hand side has coefficients of the same sign. Now, dividing through by $1 - a_\beta > 0$ we can write $\beta$ as a linear combination of elements in $\Delta$ with coefficients of the same sign which contradicts its minimality as we could now remove $\beta$ and still have the desired property.

Otherwise, if $a_\beta \geq 1$ we would have that $0 = \beta(a_\beta - 1) + 2\alpha\langle \alpha, \beta \rangle + v$ as before where all the coefficients on the right are nonnegative as $a_\beta - 1$ is positive. However, we can apply lexicographic ordering to this sum with respect to the linearly independent elements of $\Delta$ used here (note that this can be a different basis to the one used to define our positive system). As this contains only nonnegative coefficients with one positive coefficient, it can never be 0. Therefore, this inequality does not hold and we have that this case cannot occur. We now argue that this shows linear independence:

Suppose that $\sum_{\alpha\in\Delta} a_\alpha\alpha = 0$ where not all coefficients are 0. Then, call $A$ and $B$ the subsets of $\Delta$ such that $a_\alpha > 0$ if $\alpha \in A$ and $a_\alpha < 0$ if $\alpha \in B$. Then we can rewrite this as

$$\sum_{\beta\in B}(-a_\beta)\beta = \sum_{\alpha\in A} a_\alpha\alpha$$

where now all coefficients on either side are positive. We know from positive definiteness that, as these two sums are equal,

$$0 \leq \left\langle \sum_{\beta\in B}(-a_\beta)\beta, \sum_{\alpha\in A} a_\alpha\alpha \right\rangle$$

However, by using bilinearity, we can expand this inner product as the sum of the products of positive coefficients with an inner product of an element in A with an element in B. By our aforementioned result, as $A$ and $B$ must be disjoint by their definition so all vectors are distinct in the inner products, all of these are less than or equal to 0 and hence we obtain:

$$0 \leq \left\langle \sum_{\beta\in B}(-a_\beta)\beta, \sum_{\alpha\in A} a_\alpha\alpha \right\rangle \leq 0$$

Therefore, this inner product is equal to 0 and so the sums are 0 by positive definiteness of an inner product. Now, suppose that there were at least two nonzero coefficients in one of the sums. We could rewrite one of the vectors as a linear combination of the others with coefficients all of the same sign which would once again contradict our minimality as we could remove this one. Therefore all coefficients must be 0 (as if just one were nonzero then that vector would be equal to the 0 vector). Therefore, they are linearly independent.

Finally, we show uniqueness. Suppose $\Delta$ is a simple system of $\Pi$. Then, take some $\alpha \in \Delta$. Suppose that $\alpha$ can be expressed as a linear combination of two or more elements in $\Pi$, $a_1, ..., a_n$, with strictly positive coefficients, $\beta_1, ..., \beta_n$. We claim that $\alpha$ cannot be in $\Delta$. Write the $a_i$ as linear combinations of elements of $\Delta$. If $\alpha$ appears in any of them we have two cases. If the sum of the coefficients of $\alpha$ are greater than 1, we can subtract alpha from our equation and may apply lexicographic ordering to an ordered basis beginning with $\alpha$ to derive a contradiction as it would yield a positive vector being equal to 0. If it's less than 1 but not 0, we can subtract and divide by the new coefficient of $\alpha$ in the equality to write $\alpha$ as a positive linear combination of elements of $\Delta$ hence showing that if $\alpha \in \Delta$, then $\Delta$ cannot be a basis for the span of the elements of $\Pi$. Then, if $\alpha$ cannot be written in such a way, clearly it must be in $\Delta$ so we have that $\Delta$ is precisely the set of such elements of $\Pi$ where this property holds showing that $\Delta$ must be a unique set.

□

Before we state and prove the final theorem from this section, we will need a lemma.

**Lemma 6.8:** Let $\Delta$ be a simple system for a positive system $\Pi$. Then, one has that $\alpha \in \Delta \implies s_\alpha(\Pi\backslash\{\alpha\}) = \Pi\backslash\{\alpha\}$.

*Proof.* [3] Let $\beta \in \Pi\backslash\{\alpha\}$. $\beta$ is positive. Without loss of generality, $\Pi$ consists of unit vectors and so, by proposition 3.2, $s_\alpha(\beta) = \beta - 2\langle\alpha, \beta\rangle\alpha$. $\langle\alpha, \beta\rangle\alpha$ can be expanded by bilinearity into a sum of inner products of elements of $\Delta$ with coefficients all positive.

Hence, by our remark about these inner products in the proof of theorem 6.7, we have that $\langle \alpha, \beta \rangle \alpha$ must be 0 or negative. Thus, all the coefficients in our expression of $s_\alpha(\beta)$ are nonnegative which means that $s_\alpha(\beta)$ is positive (and $s_\alpha(\beta)$ must be a root by the definition of a root system). If it were equal to $\alpha$, then we would have that $s_\alpha s_\alpha(\beta) = \beta = -\alpha$ but $-\alpha$ is negative and not in $\Pi$ so it can't be $\beta$. Therefore, $s_\alpha(\beta)$ is in $\Pi \backslash \{\alpha\}$ and since this reflection determines a permutation on the roots, this is sufficient to show the image will in fact be equal to this set and not simply contained in it. □

Now that we have this, we further wish to prove the following theorem to conclude the section along with an example. This demonstrates that we are able to associate a finite reflection group's generating set (and hence its root system) to a specific simple system by fixing a basis to determine our positive system.

**Theorem 6.9:** Let $G$ be a finite reflection group with root system $\Phi$ which has a simple system, $\Delta$ for some positive system $\Pi$. Then, $G$ is generated by $\{s_\alpha | \alpha \in \Delta\}$.

*Proof.* [3] Let $G'$ be the subgroup of $G$ generated by these reflections. $G$ is finitely generated and it is sufficient to show that any generator of $G$ lies in $G'$. To do this we consider the orbit of elements in $\Phi$ under the action of $G'$ by first considering positive and negative roots. We know that $G$ is generated by the reflections $\{s_\alpha | \alpha \in \Phi\}$ as it is a reflection group. Therefore, it is sufficient to show that any element $\alpha \in \Phi$ lies in the orbit of some element of $\Delta$ under the action of $G'$ as Lemma 6.1 guarantees that, if this is the case, then $s_\alpha$ lies in $G'$. This means that $G'$ contains $G$'s generating set and hence the groups are equal.

Let $\alpha \in \Pi$ and consider $A := G'\alpha \cap \Pi = \{t(\alpha) | t \in G'\} \cap \Pi$. $\alpha \in A$ as $G'$ contains the identity element. Let $c \in A$ be the element with smallest possible height (or any such element with minimal height if there is not just one). We can choose such a $c$ as $A$ is a finite set. We claim that $c \in \Delta$. We can write

$$c = \sum_{\beta \in \Delta} c_\beta \beta$$

where the $c_\beta$ are all nonnegative. As $c$ is nonzero, we have that:

$$0 < \langle c, c \rangle = \sum_{\beta \in \Delta} c_\beta \langle c, \beta \rangle$$

And hence at least one $\langle c, \beta \rangle$ must be strictly positive for some $\beta \in \Delta$. This holds for $c \in \Delta$ as we could take $\beta = c$. Otherwise $\beta \neq c$ and, by Lemma 6.7, $s_\beta(c) \in \Pi \backslash \{\beta\}$ and from proposition 3.2, this is $c - 2\langle c, \beta \rangle \beta$ where $-\langle c, \beta \rangle < 0$. This new element would have a height less than that of c and it is still in $\Pi$. This contradicts our minimality of height and so we must have that $c \in \Delta$.

We have shown that any positive element of $\Phi$ can be mapped to a simple root by $G'$ and hence any element of $\Pi$ lies in the orbit of some element of $\Delta$ under the action of $G'$ as $c = t(\alpha) \implies \alpha = t^{-1}(c)$. If we have a negative root, say $\beta$, then $-\beta \in \Pi$ can be mapped to some $\alpha \in \Delta$ by an element of $G'$, say $t$. In this case, $\alpha = t(-\beta)$ so $-\alpha = -s_\alpha t(\beta)$ and so $\beta$ can also be carried to an element of $\Delta$ by $G'$. Therefore, $G'$ maps $\Delta$ into all of $\Phi$ as any root has a simple root that maps to it by an element of $G'$. This is precisely what we needed to show. □

**Example 6.10:** One use of this result is being able to find all finite reflection groups on 2-dimensional vector spaces. We claim that every finite reflection group such that their root system spans a 2-dimensional vector space is dihedral which follows from our work in section 3 as well as an argument from [2].

As we saw in example 4.2, the root system of a dihedral group consists of vectors in $\mathbb{R}^2$ which are not all collinear and hence these groups do indeed satisfy this property. Suppose we had such a root system. Then, the simple system (for some arbitrary basis for our ordering, say the standard basis) has two elements and our group is generated by the reflections from the simple system by theorem 6.9 (existence of a system is theorem 6.7). Without loss of generality, we may assume that one of the vectors in our system is $a = (1, 0)$ (as this is positive) by rotating our Euclidean space and the other has the form $b = (\sin\theta, -\cos\theta)$ as any vector can be written in this form. As root systems give finite reflection groups, $(ab)^m = 0$ for some m as all elements of a finite group have finite order. From example 4.2 and proposition 3.3, $ab$ is a rotation about $2\theta$ and it has finite order m. Therefore, $2\theta = 2k\pi/m$ for some $k$ coprime to m and this element lies in the cyclic group generated by a rotation about $\pi/m$ which also has order m so they generate the same cyclic group and thus our reflection group contains a rotation by $2\pi/m$. As these two mentioned rotations have the same order and generate the same cyclic group, then the elements obtained by applying the reflection about $2\theta$ and its powers to the reflections will be the same as applying the rotation about $2\pi/m$ and so by our argument in example 4.2, our group is isomorphic to $D_m$.

The key thing about this result is that the finiteness of the reflection group means that $ab$ must have finite order so the rotation can't be about an irrational angle (leading to an infinite group which certainly isn't dihedral). Composing any two of these kinds of reflections has to give a rotation since the orientation preserving isometries of $\mathbb{E}^2$ are rotations and translations. Once we know that we have a rotation by a rational angle, we simply have to label our regular polygon according to the two lines of reflection and we are guaranteed to have a dihedral group.

# 7 Construction of Elements from Generators

So far, we have found an effective way to study the elements in a finite reflection group that are reflections as well as the reflections which generate the group. We would like to look at the kind of structure the other elements in the group can have. What we would like to do is find ways to reduce elements to express them in their simplest form. Following the results in this section we will be able to give a list of all the kinds of relations that are present in presentations of finite reflection groups. We adapt our definitions and take the proofs of these theorems from (Humphreys).

Let $G$ be a finite reflection group with positive system and simple system $\Pi$ and $\Delta$ respectively. Let $t \in G$; then, $t = \prod_{i=1}^{m} r_i$ where the $r_i$ are all reflections in the generating set. We define the **length** of $t$, $l(t)$ to be the smallest $m$ for which such an expression exists. If $t$ is in this form we will call the expression **reduced**. We've found our generating set for $G$ by examining root systems so we would like a way to talk about the elements in terms of how they will permute roots. For this we introduce the notation $n(t)$ which will be the number of negative roots which $t$ carries to some positive root. As $t$ is a linear map, this is identical to the number of positive roots carried to negative roots since if $\alpha \in \Pi$, we have $-\alpha \in -\Pi := \{-\alpha | \alpha \in \Pi\}$ as $-\Pi$ is precisely the negative system. We would first like a lemma to discuss how building up a term with reflections can change the number of positive roots taken to negative ones.

**Lemma 7.1:** If $\alpha \in \Delta, t \in G$ then if $t(\alpha) \in \Pi$, then $n(ts_\alpha) = n(t) + 1$.

*Proof.* [3] $t(-\alpha) = -t(\alpha) \in -\Pi$ so $-\alpha$ is not a negative root that $t$ carries to a positive root. If we recall Lemma 6.8, we know that $s_\alpha$ maps all positive roots other than $\alpha$ to other positive roots. As such, the only negative root that $s_\alpha$ carries to a positive root is $-\alpha$ as $s_\alpha$ permutes these roots. $ts_\alpha(-\alpha) = t(\alpha) \in \Pi$ so $-\alpha$ is carried to a positive root by $ts_\alpha$. Let $\beta$ be any negative root other than $\alpha$. If $t(\beta) \in -\Pi$ then $s_\alpha t(\beta) \in -\Pi$ by our observation about Lemma 6.7. Similarly, if $\beta$ is carried to a positive root by $t$, then $s_\alpha$ will keep it a positive root. Therefore, the set of all negative roots taken to positive roots by $s_\alpha t$ is precisely all such roots for t as well as $-\alpha$ which we know is not one of the roots for t. This gives us the statement.

□

An immediate consequence of this is that, as all simple reflections satisfy the condition on $t$, then an expression in terms of simple reflections of length r can map at most r negative roots to positive roots.

**Theorem 7.2** Let $t = s_1 ... s_r$ be an expression in terms of simple reflections such that $n(t) < r$. Then, if $s_i = s_{\alpha_i}$ for each $i$ where the $\alpha_i$ are simple roots which need not be distinct, we have that there exist some $i, j \in \{1, 2, ..., r\}$ with $i < j$ such that:

$$\alpha_i = s_{i+1} s_{i+2} ... s_j(\alpha_j)$$

Moreover,

$$s_{i+1} ... s_j = s_i s_{i+1} ... s_{j-1}$$

*Proof.* [3] If $n(t) < r$, then as the expression was built up in stages of $s_1 ... s_k$ for $k \leq r$, adding $s_k$ could not have resulted in $s_1 ... s_{k-1}(\alpha_k) \in \Pi$ for each $k$ as if this were always the case, then by Lemma 7.1, we would have $n(t) = r$. Let $j$ be some such index for which $s_1 ... s_{j-1}(\alpha_j) \notin \Pi$. We know, from Lemma 6.8, that simple reflections only change the sign of one root. Therefore, since $\alpha_j \in \Pi$, at some point as we apply the reflections starting with $s_{j-1}$, we must have one for which the right to left composition eventually carries $\alpha_j$ to some negative root but never did for any reflections to the right of this. That is, there is some $i < j$ such that $s_{i+1} ... s_{j-1}(\alpha_j) \in \Pi$ but $s_i s_{i+1} ... s_j - 1(\alpha_j) \in -\Pi$. Lemma 6.7 again implies that, as $s_i$ only changes the sign of $\pm\alpha_i$, we must have that $s_{i+1} ... s_{j-1}(\alpha_j) = \alpha_i$ as required.

Then, if $t' := s_{i+1} ... s_{j-1}$, we may apply Lemma 6.1 to obtain:

$$t' s_j (t')^{-1} = s_i$$

And thus, as $(t')^{-1} = s_{j-1}^{-1} ... s_{i+1}^{-1} = s_{j-1} ... s_{i+1}$, we have that the above expression says:

$$s_{i+1} ... s_{j-1} s_j s_{j-1} ... s_{i+1} = s_i$$

And so,

$$s_{i+1} ... s_j = s_i s_{i+1} ... s_{j-1}$$

□

We can now find a form of presentation all finite reflection groups admit which is the main theorem of this essay.

**Theorem 7.3** Let $\Delta$ be a simple system for a root system $\Phi$ with finite reflection group $G$. Then, let $S := \{s_\alpha | \alpha \in \Delta\}$. Then, $G$ is isomorphic to the free group on S with its defining relations being: $(s_\alpha s_\beta)^{m(\alpha,\beta)} = 1$ for $\alpha, \beta, \in \Delta$ where we must have $m(\alpha, \alpha) = 1$. That is, the order of the compositions of two reflections are what define the reflection group uniquely up to isomorphism.

By speaking of the free group on $S$, we are just specifying the size of generating set our group needs. When dealing with presentations, since we only care about words out of our generating set, we could equivalently use $\Delta$. We use $S$ so that our notation emphasizes that it's those relations in $G$ that need to follow from these relations. To prove this theorem, all we need to do is show that every equality of elements in $G$ can be shown to be true solely from these relations. This is an equivalent statement to showing that any product of elements in $G$ being the identity follows from the relations since we can always take inverses to move everything to one side of an equality. The previous results in this section can't immediately be used when doing this. We know that they are true in a finite reflection group but we can only use the theorems to show something in terms of relations if we know that equality (specifically the one in Theorem 7.2) does indeed already follow from the relations. The proof below is given by Humphreys and relies very heavily on Theorem 7.2:

*Proof.* [3] Take some equality $s_1...s_r = 1$. The identity map is orientation preserving so $r$ must be even. Suppose $r = 2q$, we proceed by induction on $q$.

If r=2, we have $(s_1 s_2)^1 = 1$ which follows from a relation of the desired form. Then, if it holds for all naturals less than q, we have:

$$s_1....s_q s_{q+1}...s_r = 1 \tag{1}$$

or equivalently,

$$s_1...s_{q+1} = s_r...s_{q+2} \tag{2}$$

The right-hand side of this is a composition of $q-1$ reflections while the right is of $q+1$; therefore, the left-hand side cannot be in reduced form. If we call $t$ the expression on the left, then $n(t) < q+1$ since $t$ can be built out of $q-1$ simple reflections so $n(t) \leq q-1$. We can apply Theorem 7.2 to yield the existence of $i, j \in \{1, ..., q+1\}$ with $i < j$ such that:

$$s_{i+1}...s_j = s_i s_{i+1}...s_{j-1}$$

However, we do not know that this follows from the relation; we only know that it is true in $G$ so if our induction hypothesis were possible to apply, we would be able to as it is a relation in $G$. If the total number of reflections on each side adds up to less than $r$ this will also be a consequence of the relations so we may use it. In this case, we can substitute the right hand side in place of the left in (1) to get:

$$s_1...s_q s_{q+1}...s_r = 1 \iff s_1....s_i s_i s_{i+1}...s_{j-1} s_{j+1}...s_r = 1$$

The left hand side of our new expression has fewer than $r$ simple reflections as we know $s_i^2 = 1$ from our relations so we can apply the induction hypothesis. We now have to consider the case where our expression we substituted has $r$ elements and so we weren't able to substitute it. This is the case precisely if $i = 1, j = q+1$. In this case the relation we need is:

$$s_2 ... s_{q+1} = s_1 .... s_q \tag{3}$$

What we wish to do now is continually substitute new expressions in (1) until we can show two terms are equal and then apply the identical argument to the shifted expression $1 = s_2 ..... s_r s_1$ to exhaust all digits to get that all even reflections are equal and all odd ones are equal. At each stage, we only need to consider the case where the original argument fails as if it ever didn't we could apply the induction hypothesis and be done. We can rewrite (1) as $s_2 ... s_r s_1 = 1$. If we apply the identical argument to this new expression, then if it is unsuccessful we must have: $s_3 ... s_{q+2} = s_2 .... s_{q+1}$ or equivalently,

$$s_3 s_2 s_3 s_4 ... s_{q+2} s_{q+1} ... s_4 = 1$$

Obtained by multiplying on the left by $s_3 s_2$ and multiplying on the right by by the rest of the right hand side. The original argument could theoretically apply to this and its failure would imply that

$$s_2 s_3 ... s_{q+1} = s_3 s_2 s_3 s_4 .... s_q$$

However, the left hand side of this appears in (3) where it is equal to $s_1 ... s_q$ but,

$$s_1 s_2 s_3 s_4 .... s_q = s_3 s_2 s_3 s_4 .... s_q \iff s_1 = s_3$$

We can shift our indices along as described earlier (starting with $s_3 ... s_r s_1 s_2 = 1$) to get that $s_2 = s_4, s_3 = s_5$ and so on to find that (1) is just $(s_1 s_2)^q = 1$ which is precisely a relation of the desired form.

□

This yields an efficient way of finding a presentation of any finite reflection group. All one would need to do is compute the orders of pairs of reflections and we would know the presentation; in fact, it is sufficient to only look at unordered pairs because $(ab)^m = 1 \implies (b^{-1}a^{-1})^m = 1$ but $a, b$ are of order 2 so this tells us that $ba$ has order m. An example of this is the dihedral group generated by two elements. It can be written as: $\langle a, b | a^2 = b^2 = (ab)^m = 1 \rangle$ which is different from our presentation in section 2 but defines the same group.

# 8 Concluding Remarks

We have examined some of the geometric tools used to study reflection such as how they act on certain subsets of $\mathbb{R}^n$, how the reflection groups can be viewed as permutations on a set of lines (or equivalently unit roots) as well as how reflections behave under conjugation with other isometries. We've also gone through how one can find efficient generating sets for such groups as well as a way to find their presentations. Moreover, we've gained some insight into some of the ways compositions of reflections can be reduced to make them easier to understand.

[3] A more general theory leading from what was developed here follows from the relations we found in Theorem 7.3. After finite reflection groups were studied by H. S. M. Coxeter, he naturally generalized them to what are known as Coxeter groups. In those, the elements still are subject to the same relations as in our presentations only we no longer require that the order of products of distinct reflections be finite (Humphreys).

## References


[1] P. M. Cohn. *Classic Algebra.* John Wiley, 2000.

[2] Larry C. Grove and C. T. Benson. *Finite Reflection Groups.* Springer, 2010.

[3] James E. Humphreys. *Reflection groups and coxeter groups.* Cambridge University Press, 1990.