IMPERIAL

Imperial College London

Department of Mathematics

Second-year Group Research Project

Title

Author:
Student name 1 (CID: ————-)
Student name 2 (CID: ————-)
Student name 3 (CID: ————-)
Student name 4 (CID: ————-)
Student name 5 (CID: ————-)

Supervisor(s):
Alessio Corti

June 9, 2025

Abstract

Type your abstract here. The abstract is a summary of the contents of the project. It should be brief but informative, and should avoid technicalities as far as possible.

Contents

1 Introduction

The introduction should attempt to set your work in the context of other work done in the field. It should demonstrate that you are aware of what you are doing, and how it relates to other work (with references). It should also provide an overview of the contents of the project. You should highlight your individual contributions and any novel result: which of the calculations, theorems, examples, proofs, conjectures, codes etc. are your own? This is how you cite a reference in the bibliography[1]. All of the commands and formatting are in ./style/header.sty

2 Polytopes

2.1 Polytopes

2.1.1 Dihedral groups

The dihedral group, D_{2n}, is the group of symmetries of a regular n-gon. Its standard presentation is given by

$$\langle r, s \mid r^3 = e,\ s^2 = e,\ (rs)^2 = e \rangle$$

where r is a rotation of $2\pi/n$ and s is a reflection.

Let l_1 and l_2 be two reflection axes with an angle θ between l_1 and l_2, and s_1 and s_2 be the respective reflections. After some algebra, the composition $s_1 s_2$ turns out to be a counterclockwise rotation through 2π.

Therefore, an alternative presentation of D_{2n} is given by

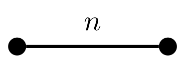
$$\langle s_1, s_2 \mid s_1^2 = e,\ s_2^2 = e,\ (s_1 s_2)^n = e \rangle$$

where s_1 and s_2 are adjacent reflections.

This shows that D_{2n} is an example of a reflection group.

Example 2.1.2. The coxeter diagram for the symmetries of a regular n-gon, also known as $I_2(n)$, looks like

$I_2(n)$



$(n \geq 4)$

Theorem 2.1.3. Let $G \curvearrowright X$ be an action of a finite group G on a finite set X. Then the number of G-orbits in X is given by:

$$\text{Number of orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

where $\text{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.

Example 2.1.4. How many distinguishable necklaces can be made using seven different colored beads of the same size?
Let X be the 7! possible arrangements. The necklace can be turned over (a reflection) as well as rotated so we consider the dihedral group D_{14} acting on X. Using the previous theorem,

$$\text{Number of orbits} = \frac{7!}{14} = 360$$

as only the identity leaves any arrangement fixed.

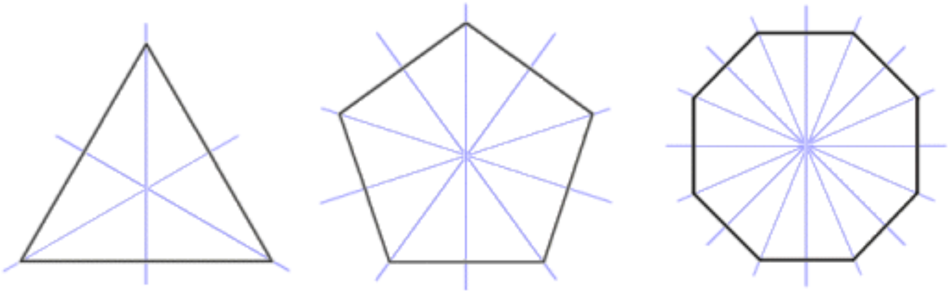


Figure 1 The lines of symmetry of a regular 3-,4- and 7-gon.

Theorem 2.1.5. Let p be a prime. Then any group G of order $2p$ is isomorphic to either the cyclic group C_{2p} or the dihedral group D_{2p}.
Proof. By Cauchy's theorem, there exists an element $a \in G$ of order p and an element $b \in G$ of order 2. Let

$$H = \langle a \rangle,$$

so H is a subgroup of G of index 2, so $H \trianglelefteq G$.
Since $H \trianglelefteq G$, conjugation by b sends H to itself. Thus, there exists $k \in \{1, 2, \ldots, p-1\}$ such that

$$bab^{-1} = a^k.$$

Applying conjugation by b twice to a gives

$$a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^kb^{-1} = (bab^{-1})^k = (a^k)^k = a^{k^2}.$$

Therefore,

$$a = a^{k^2} \implies a^{k^2-1} = e.$$

Since a has order p, this implies

$$p \mid (k^2 - 1),$$

or equivalently,

$$k^2 \equiv 1 \pmod{p}.$$

Because p is prime, this implies

$$k \equiv \pm 1 \pmod{p}.$$

- If $k \equiv 1$, then

  $$bab^{-1} = a,$$

  and b commutes with a. Hence G is abelian, and since a has order p and b has order 2, G is cyclic of order $2p$.

- If $k \equiv -1$, then

$$bab^{-1} = a^{-1},$$

  which is the defining relation for the dihedral group D_{2p}:

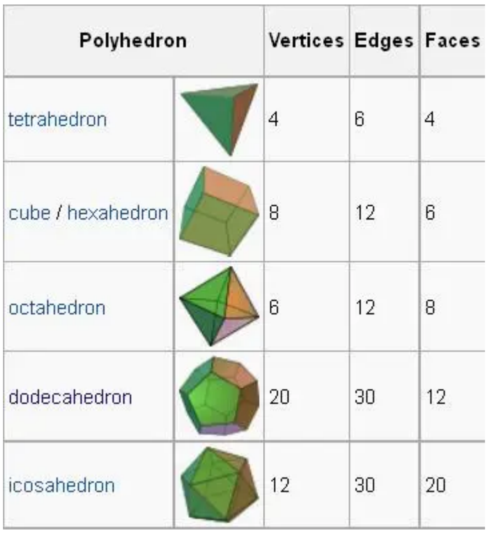
$$D_p = \langle a, b \mid a^p = e, b^2 = e, bab = a^{-1} \rangle.$$

Thus, G is isomorphic to either C_{2p} or D_{2p}.

$\square$

2.2 The Infinite dihedral group

3 Platonic solids and reflections



Polyhedron		Vertices	Edges	Faces
tetrahedron		4	6	4
cube / hexahedron		8	12	6
octahedron		6	12	8
dodecahedron		20	30	12
icosahedron		12	30	20

Figure 2 The five Platonic solids.

Definition 3.0.1. A polyhedron is regular if its faces are regular polygons, all with the same number of sides, and also each vertex belongs to the same number of edges.

Theorem 3.0.2. The only regular convex polyhedra are the five Platonic solids.
Proof. Before writing the proof, we introduce some notations. V, the number of vertices;
E, the number of edges;
F, the number of faces;
n, the number of sides on a face;
r, the number of edges to which each vertex belongs.
Observe that

$$2E = nF \tag{1}$$

and

$$2E = rV \tag{2}$$

(1) comes from counting the number of pairs (e,f) where e is an edge and f is a face and e lies on f; (2) comes from counting the number of pairs (v,e) where v is a vertex and v lies on e. Substitute into Euler's formula, we get

$$\frac{1}{r} + \frac{1}{n} = \frac{1}{2} + \frac{1}{E} \tag{3}$$

Now $n \geq 3$, as a polygon must have at least 3 sides and $r \geq 3$, since in a polyhedron a vertex must belong to at least 3 edges. By (3), we can't have both $n \geq 4$ and $r \geq 4$, since this would make the left-hand side of (3) at most $\frac{1}{2}$. It follows that either $n = 3$ or $r = 3$. If $n = 3$, then (3) becomes

$$\frac{1}{r} = \frac{1}{6} + \frac{1}{E} \tag{4}$$

The right-hand side is greater than $\frac{1}{6}$, and hence $r < 6$. Therefore, $r = 3$, 4 or 5 and $E = 6$, 12 or 30, respectively. If $r = 3$, (3) becomes

$$\frac{1}{n} = \frac{1}{6} + \frac{1}{E} \tag{5}$$

Similarly, n = 3,4 or 5 and E = 6,12 or 30, respectively. These parameters are coincide with those in the table above.

Example 3.0.3. Let G be the group of symmetries of a dodecahedron. What is $|G|$?
Let G act on the 12 faces of the dodecahedron and fix a face. There are $|D_{10}| = 10$ symmetries which fix this face and our action is clearly transitive. By Orbit-Stabiliser theorem, $|G| = 10 \times 12 = 120$. Alternatively, this can be done by considering the fundamental domain, which is a triangle that uniquely determines the reflection. There are 120 such triangles.

We would like to study the group of symmetries of these Platonic solids.

3.1 Tetrahedron

Each face has D_6 as a group of symmetries.
Before moving on to the other solids, we first introduce the concept of dual.

Definition 3.1.1. The dual of a Platonic solid is a new Platonic solid where the faces and vertices are interchanged with those of the original.

Remark 3.1.2. The tetrahedron is self-dual. The cube and the octahedron form a dual pair. The dodecahedron and the icosahedron form a dual pair.

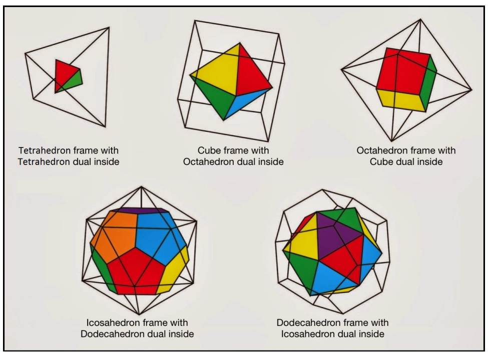


Figure 3 Duals of each Platonic solid.

4 Classification of finite reflection groups

The plan is to show all finitely generated reflection groups are in fact Coxeter groups, which admit a nice geometric classification. This follows[1]
This is a rough outline of the structure:

4.1 Reflection groups

work in n-dimensional euclidean space E. This may be spoken about in the previous section?
The origin preserving reflections of E are all contained in $O(E)$, this is also the smallest group containing all of these reflections.[citation-needed](easy induction i think?) We also want to consider reflections that don't preserve the origin, or *affine reflections* these will, similarly, all lie in the **affine orthogonal group**

$$AO(E) := E \rtimes O(E)$$

where E acts on itself by translation.
A reflection in E is an affine transformation $r \in AO(E)$ that fixes some affine hyperplane H (some translation of codimension 1 subspace).
A group $W \leq AO(E)$ is a **reflection group** if it is generated by affine reflections. If we have $W \leq O(E) \leq AO(E)$ then we recover the definition used for reflection groups of regular polytopes discussed earlier.
From now on we will fix a reflection group W and start referring to affine reflections as just reflections.
Let $\mathcal{H}$ be the set of affine hyperplanes fixed by some reflection in W.

Lemma 4.1.1. If $H \in \mathcal{H}$ is an affine hyperplane and $s \in W$ is a reflection, sH is also an affine hyperplane.

Proof. A hyperplane in any euclidean space is equivalently the locus

$$\{v \in E \mid (v, \alpha) = 0\}$$

where α is the normal vector to the hyperplane. Thus an affine hyperplane with normal α and minimal distance from the origin k will be

$$\{v \in E \mid (v, \alpha) = k\}$$

Now sH will consists of points sv such that $(v, \alpha) = k$, but as s is $AO(E)$, it preserves the inner product so $(sv, s\alpha) = (v, \alpha) = k$ so

$$sH = \{v \in E \mid (sv, s\alpha) = k\} = \{v \in E \mid (v, s^* s\alpha) = k\}$$

where s^* is the adjoint map. □

Let Φ be the set of unit normal vectors to hyperplanes $H_i \in \mathcal{H}$.

Lemma 4.1.2. For all affine hyperplanes $H \in \mathcal{H}$ with corresponding reflection $r \in W$, and reflections $s \in W$ the map srs^{-1} is a reflection over the affine hyperplane sH.

Proof. □

Proposition 4.1.3. The action of W on E stabilises Φ and $\mathcal{H}$.

Proof. Start by considering some affine hyperplane $H \in \mathcal{H}$ with corresponding reflection $r \in W$, then for all $s \in W$ the map srs^{-1} fixes sH and has determinant -1 so is a reflection, therefore $sH \in \mathcal{H}$ □

We can derive the Coxeter relations from Φ, a group satisfying such relations is called Coxeter.

Definition 4.1.4. We call a group W **Coxeter** if it admits a presentation of the form:

$$\langle r_1, \dots, r_n \mid (r_i r_j)^{m_{ij}} \text{ for all } i, j \rangle$$

where each $m_{ij} \in \mathbb{N} \cup \{\infty\}$, and $m_{ii} = 1$ for all i. For formal reasons, we will consider the pair (W, R), where R is the set of generators in the presentation, and call this a **Coxeter system**. We call a Coxeter system finite if R is finite.

4.2 The fundamental domain

The action of W fixes Φ and $\mathcal{H}$ so acts on the connexted componenets $E \setminus \mathcal{H}$ called the set of **fundamental domains** for W.
The reflections fixing hyperplanes bounding any single fundamental domain will generate W, such reflections (hyperplanes, roots) are called **simple**.
Show the action of W on the fundamental domains is transitive

4.3 Words

The length of a word in terms of simple reflections corresponds to the number of plane between a fundamental domain and its image. This implies the action on fundamental domains is in fact **simply** transitive.

Proposition 4.3.1 (Deletion condition)**.** Given an unreduced expression $w = r_1 \cdots r_k$ there exists $1 \leq i < j \leq k$ such that $w = r_1 \cdots \hat{r_i} \cdots \hat{r_j} \cdots r_k$, where the hat means ommitance.

Proposition 4.3.2 (Exchange condition)**.** For $w = r_1 \cdots r_k$ a not necessarily reduced expression and some simple $r \in W$ with $l(wr) < l(w)$, then there exists an $1 \leq i \leq k$ s.t. $wr = r_1 \cdots \hat{r_i} \cdots r_k$.

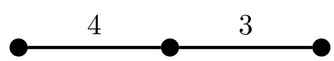
Theorem 4.3.3. Any non-trivial relation in a reflection group is a consequence of the Coxeter relations.

4.4 Classification

To any finite Coxeter system (W, R) we can associate an undirected graph called its **Coxeter diagram** by the following rules:

- Draw a node i for each $r_i \in R$;
- For each relation $(r_i r_j)^{m_{ij}}$ with $m_{ij} > 2$ draw an edge between i and j and label it with m_{ij}.

This process can be reversed to obtain a Coxeter system from any Coxeter diagram. This correspondence will associate the graph:



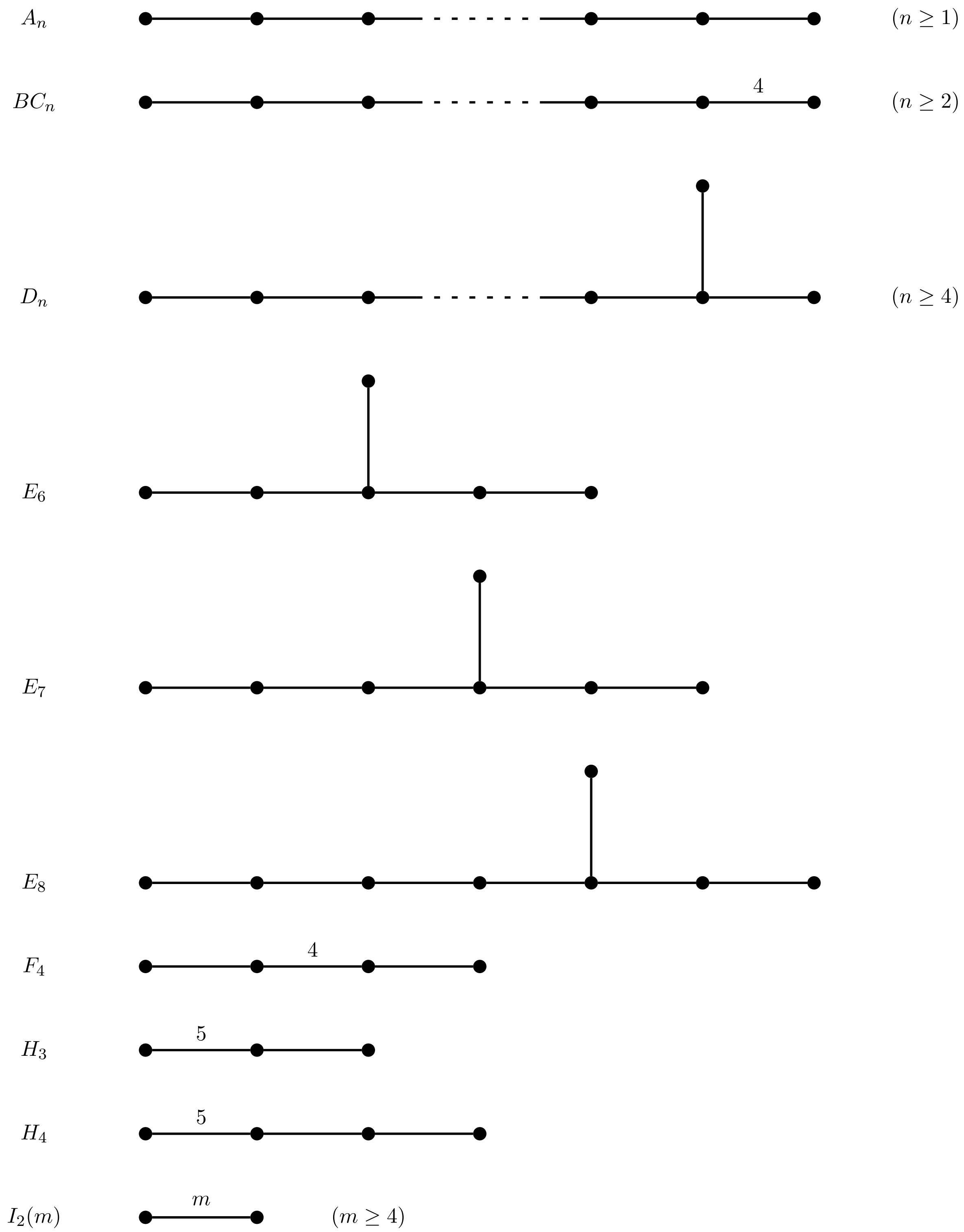
to the group presentation:

$$\left\langle r_1, r_2, r_3 \;\middle|\; r_1^2 = r_2^2 = r_3^2 = e,\ (r_1 r_2)^4 = (r_2 r_3)^3 = (r_1 r_3)^2 = e \right\rangle$$

For brevity the 3 labels will often be excluded.

- show the graph is well defined up isometryish

- disjoint unions of graphs correspond to products of groups
- bilinear form of a coxeter group
- if positive definite, the coxeter group is finite
- classify positive-definite forms
- all of which can be seen as reflection groups of regular polyhedra. some of which will be described in the previous section?



5 Uniform polytopes

uniform polytopes

6 Tits' word problem

words

7 Euclidean Reflection Groups

7.1 Structure of Euclidean Reflection Groups

This section follows AB8, cite in final version
Let W be an affine reflection group, naturally acting on the Euclidean space V, with fixed set of affine hyperplanes $\mathcal{H}$. We fix an arbitrary chamber C as our fundamental chamber, S be the set of reflection with respect to its walls. For an n-dimensional Euclidean space V, we have the isomorphism $\mathrm{AO}(V) \cong V \rtimes \mathrm{O}(V)$. Every element $\mathrm{AO}(V)$ represents the composition of an orthogonal linear map with a transition τ_v sending x to $x+v$. Note W can be taken as a subgroup of $\mathrm{AO}(V)$.

Theorem 7.1.1. 1. The hyperplanes $H \in \mathcal{H}$ fall into finitely many classes under parallelism;

2. Let $\overline{W}$ be the image of W under the projection $\eta : \mathrm{AO}(V) \twoheadrightarrow \mathrm{O}(V)$, then $\overline{W}$ is finite.

Proof. (1) Let $\Phi := \{\pm e_H : H \in \mathcal{H}\}$, where e_H is the unit vector normal to H. We will show $\angle(e_1, e_2)$ can take finitely many values. Let $H_1, H_2 \in \mathcal{H}$ normal to e_1, e_2. If they are parallel, then $\angle(e_1, e_2) = \pi$. So we may assume they intersect and take $x \in H_1 \cap H_2$. Since W is transitive on chambers, and by the fact that chambers D, D' is separated by wall H' if and only if wD, wD' is separated by wH', we can choose $w \in W$ with $wx \in \overline{C}$. Then $\overline{C}$ intersects with wH_1 and wH_2, with vectors $\bar{w}e_1, \bar{w}e_2$ normal to them, where $\bar{w} = \eta(w)$. $\angle(e_1, e_2) = \angle(\bar{w}e_1, \bar{w}e_2)$ since $\bar{w}$ is an isometry. C has finitely many walls so there are only finitely many possibilities for angles between two vectors in Φ, hence it is finite as we are in a finite-dimensional space.
(2) Note Φ we defined is stable under action of $\overline{W}$ and reflection with respect to the hyperplanes they are perpendicular to generates $\overline{W}$. We show the natural homomorphism $\sigma : W \to S(\Phi)$ is injective. Suppose $w \in \ker(\sigma)$, w fixes all vectors of Φ. But then $V_0 = \mathrm{Span}(\Phi)$ is also fixed by w. Write the vector space V as $V_0 \oplus V_1$ for V_1 some subspace of V. Then since every reflection s_e fixes every point of V_1, so does w. We then conclude w is identity hence $\overline{W}$ is finite. $\square$

Definition 7.1.2. We say W is essential if intersection of hyperplanes H $s_H \in \overline{W}$ is a singleton.

Definition 7.1.3. A Coxeter group is irreducible if its Coxeter diagram is connected.

For a general affine reflection group, we can reduce it to essential, irreducible cases. If it is irreducible, then there are sets of hyperplanes $\mathcal{H}_i$, each hyperplane in $\mathcal{H}_i$ is orthogonal to the ones in other $\mathcal{H}_j$'s. We can decompose the space into direct sum $V_1 \oplus \cdots \oplus V_n$, where each V_i corresponds to $\mathcal{H}_i$, and the corresponding reflection group W_i is irreducible in V_i. If W_i is not essential, we can quotient the intersection of all hyperplanes out to get an essential one.

Theorem 7.1.4. Assume W is essential and irreducible in n-dimensional vector space V, then one of the following is true:

1. W is finite, C has n walls;

2. W is infinite, C has $n+1$ walls, and vectors perpendicular to any n walls form a basis. $\overline{C}$ is compact.

Proof. □

Definition 7.1.5. A Euclidean reflection group is an infinite, irreducible, affine reflection group.

For the rest of this section, let W be a Euclidean reflection group. Let T be the kernel of the projection above restricted on W, then we have a short exact sequence

$$1 \to T \to W \to \overline{W} \to 1$$

By possibly taking quotient of the vector space V, we may assume that the intersection

$$V_0 = \bigcap_{s_H \in \overline{W}} H$$

does not have positive dimension. In this case:

Proposition 7.1.6. There exists point $x \in V$ such that its group of stabilizers W_x is isomorphic to $\overline{W}$. In particular, $W \cong T \rtimes W_x$.

Proof. By Theorem 7.1.1, let $\overline{\mathcal{H}}$ be the set of linear hyperplanes parallel to some affine planes of $\mathcal{H}$. $\overline{W}$ is generated by reflection about these hyperplanes. Choose n hyperplanes $H_1, \ldots, H_n$ from $\mathcal{H}$, each parallel to a distinct linear hyperplane of these walls and take their intersection, which is a single point x [Why? Consider this as a system of linear equations]. Linear parts of $s_{H_1}, \ldots s_{H_n}$ generates $\overline{W}$ and since translations have no fixed points, W_x bijects to $\overline{W}$. □

By Proposition 7.1.6, with possibly shifting we can assume 0 is a special point and hence $W \cong T \rtimes W_0 \cong T \rtimes \overline{W}$. We can then identify T by

$$L := \{v \in V : \tau_v \in W\}$$

as an additive group.
We then have $W \cong L \rtimes \overline{W} \leq V \rtimes \mathrm{O}(V) \cong \mathrm{AO}(V)$ We next show L is a lattice i.e. L is in the form of $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ for $\{e_i\}_{1 \leq i \leq n}$ a basis of V

Lemma 7.1.7. Non-identity elements of L are bounded away from 0, i.e. L is a discrete subgroup of V as a topological group.

Proof. Pick $x \in C$ of the fundamental chamber. Since W is simply transitive on chambers, so is L. Let

$$U = \{v \in V : x + v \in C\}$$

U is a neighbourhood of 0 since C is open. Thus $U \cap L = \{0\}$, L is bounded away from 0. □

The next lemma is from theory of topological groups:

Lemma 7.1.8. If L is a discrete subgroup of the additive group of a finite-dimensional $\mathbb{R}$-vector space, then $L = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ for some linearly independent vectors $e_1, \ldots, e_r$.

Proof. We prove by induction on $\dim V$. Assume $L \neq 0$, by discreteness, choose $e \in L$ of minimal length δ. $L \cap \mathbb{R}e$ must contain e. Operation of L is the vector addition so $\mathbb{Z}e \subseteq L \cap \mathbb{R}e$. If $(L \cap \mathbb{R}e) \backslash \mathbb{Z}e$ is nonempty, then we would have a contradiction with minimality of length of e. So $L \cap \mathbb{R}e = \mathbb{Z}e$.
For any element $v \in L \backslash \mathbb{Z}e$, we can find $w \in \mathbb{R}e$ such that distance fo v to $\mathbb{R}e$ equals $d(v, w)$. Let $u \in \mathbb{Z}e$ be of minimal distance to v. Then $d(v, w) \geq |d(v, u) - d(w, v)| \geq |\delta - \delta/2| = \delta/2$ by triangle inequality.
Now we consider the quotient group $L/\mathbb{Z}e$ as the subgroup of additive group of the quotient space $V/\mathbb{R}e$. Since we have the canonical isomorphism $(\mathbb{R}e)^\perp \to V/\mathbb{R}e$, define a map $V \to (\mathbb{R}e)^\perp$ by $v \mapsto v^\perp$. Given any two cosets $[v], [w] \in V/\mathbb{R}e$, define $d([v], [w]) = ||v^\perp - w^\perp||$, which clearly a metric. The above is actually showing $L/\mathbb{Z}e$ is a discrete subgroup of $V/\mathbb{R}e$. The lemma follows from induction. □

We are now left to show the set of linearly independent vectors given in Lemma 7.1.8 is a basis of V.

Lemma 7.1.9. In the context of Lemma 7.1.8, r=n.

Proof. Since $\overline{W}$ is generated by n reflections $\square$

7.2 Some Model Theory of Euclidean Reflection Groups

This section follows MPS22, cite in final version

Definition 7.2.1. We say a structure $\mathcal{N}$ is interpretable in $\mathcal{M}$ if:

1. The underlying set A is $\{\overline{x} \in M^k : \mathcal{M} \models \phi(\overline{x})\}$ for some formula ϕ.
2. For every function symbols $f(\overline{x})$ of $\mathcal{N}$, there is a formula ϕ such that $\mathcal{M} \models \phi(\overline{x}, \overline{y})$ if and only if $\mathcal{N} \models f(\overline{x}) = \overline{y}$.

Definition 7.2.2. We say the theory of a group G is decidable if there is an algorithm such that for all sentences ϕ, it can decide whether ϕ is true in G.

For a definition of sentence and algorithm, see Cite appendix

Proposition 7.2.3. Euclidean reflection group G is definable in the abelian group $\mathbb{Z}$ with finitely many parameters.

This result follows from the following two lemmas:

Lemma 7.2.4. Let $G \cong \mathbb{Z}^d \rtimes_\sigma Q$ where $1 \leq d < \omega$, Q is some finite group, and $\theta : Q \to \mathrm{Aut}(\mathbb{Z}^d)$ a group homomorphism. G is interpretable in the structure $\mathcal{M} = (\mathbb{Z}^d, +, \pi_x)_{x \in Q}$ with finitely many parameters, where $+$ is the normal vector addition and $\pi_x := \sigma(x)$

Proof. We enumerate $\{\pi_x : x \in Q\}$ as $t_0, \ldots, t_{n-1}$ and $t_i := (i, 0, \ldots, 0)$ a d-tuple. Let $G = (\mathbb{Z}^d \times Q, \cdot)$. We represent the universe of G by a tuple (a, t_i) where $a \in M$ and $0 \leq i < n$. We need to define the group operation $(a_i, t_i) \cdot (a_j, t_j) = (a_i +_{\mathbb{Z}^d} t_i(a_j), t_i \cdot_Q t_j)$ in $\mathcal{M}$. $t_i \cdot_Q t_j$ is definable since Q in finite, we can enumerate all possible product of all elements in Q. $a_i +_{\mathbb{Z}^d} t_i(a_j)$ is definable since $+$ is a built-in function symbol of $\mathcal{M}$ and t_i is same with π_x for some x. Again this claim follows from enumerating all possibilities of t_i's. $\square$

Lemma 7.2.5. $(\mathbb{Z}^d, +, \pi_x)_{x \in Q}$ is interpretable in $(\mathbb{Z}, +, 0)$ with finitely many parameters.

Proof. Since there are finitely many π_x's, it suffices to show we can define π_x in $(\mathbb{Z}, +, 0)$ for some $x \in Q$. π_x is an automorphism of $\mathbb{Z}^d$, which is an $d \times d$ invertible matrix A over $\mathbb{Z}$. $\pi_x(\overline{b}) = A\overline{b}$ is simply a matrix multiplication so clearly definable over A. $\square$

Theorem 7.2.6. Let W be a Euclidean reflection group. Then $Th(W)$ is decidable.

Proof. W is interpretable in the structure $(\mathbb{Z}, +, 0)$ with finitely parameters by Proposition 7.2.3. But all these parameters are integers, so it is interpretable in the structure $(\mathbb{Z}, +, 0, 1)$ with no parameters. We then can translate every sentence in W back to a sentence of $(\mathbb{Z}, +, 0, 1)$. Since the Presburger arithmetic $(\mathbb{Z}, +, <, 0, 1)$ is decidable, as a definable structure in its reduct, $Th(W)$ is also decidable. $\square$

A Model Theory Preliminaries

We fix our language $\mathcal{L} = (e, \cdot)$ to be the language of groups.

Definition A.0.1. The set of $\mathcal{L}$-terms is the smallest set $\mathcal{T}$ such that

1. variables $x_i \in \mathcal{T}$ for $i = 0, 1, \dots$;
2. if $t_1, t_2 \in \mathcal{T}$ then $(t_1 \cdot t_2) \in \mathcal{T}$

Definition A.0.2. The set of $\mathcal{L}$-formulas is the smallest set $\mathcal{F}$ such that

1. all atomic formulas $(t_1 = t_2) \in \mathcal{F}$ for $t_1, t_2 \in \mathcal{T}$;
2. $\mathcal{F}$ is closed under $\neg$ ("not"), $\vee$ ("or"), $\wedge$ ("and"), $\to$ ("implies"), $\forall$ ("for all"), $\exists$ ("there exists").

By drawing a truth table or otherwise, it suffices to define the satisfaction of $\wedge$, $\neg$, and quantifiers for $\mathcal{L}$-formulas.

Definition A.0.3. We say a formula ϕ has x as a free variable if x does not appear in any quantifiers of ϕ.

Definition A.0.4. Let ϕ be a formula with free variables $x_1, \dots, x_n$. We inductively define a group $G \models \phi$ as follows.

1. If $\phi(\overline{x})$ is $t_1(\overline{x}) = t_2(\overline{x})$, then $G \models \phi$ if t_1 and t_2 are exactly the same term.
2. If $\phi(\overline{x})$ is $\neg\psi(\overline{x})$, then $G \models \phi(\overline{x})$ if $G \not\models \psi(\overline{x})$.
3. If $\phi(\overline{x})$ is $\psi_1(\overline{x}) \wedge \psi_2(\overline{x})$, then $G \models \phi(\overline{x})$ if $G \models \psi_1(\overline{x})$ and $G \models \psi_2(\overline{x})$.
4. If $\phi(\overline{x})$ is $\forall y \psi(\overline{x}, y)$, then $G \models \phi(\overline{x})$ if for all $a \in G$ $G \models \psi(\overline{x}, a)$.
5. If $\phi(\overline{x})$ is $\exists y \psi(\overline{x}, y)$, then $G \models \phi(\overline{x})$ if there is $a \in G$ $G \models \psi(\overline{x}, a)$.

If $G \models \phi(\overline{a})$ we say $\phi(\overline{a})$ is true in G

Definition A.0.5. We say a formula ϕ is a sentence if it does not have free variables.

To make the term algorithm clear, we recall definitions from computability theory.
We have infinitely many initial configuration of the register $R_1, R_2, \dots$, each is a nonnegative integer.

Definition A.0.6. A register machine program is a finite sequence of instructions $I_1, \dots, I_M$, where each I_j is one of the following:

1. Z(n): set R_n to zero;
2. S(n): increase R_n by one;
3. T(n,m): set R_n to be R_m;
4. J(n,m,s), where $1 \le s \le M$: if $R_n = R_m$, then go to I_s, otherwise go to the next instruction;
5. HALT

and I_m is HALT

Definition A.0.7. Suppose $A \subseteq \mathbb{N}^k$. $f : A \to \mathbb{N}$ is computable if there is a register machine program P such that:

1. If $x \in A$, then P does not halt on input x;
2. If $x \in A$, then P halts on input x with $R_1 = f(x)$.

Definition A.0.8. We say a set $A \subseteq \mathbb{N}^k$ if the function

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

is computable.

We then can say a theory of G is decidable if the set of true sentences in G. We can make "input of ϕ" more precise using Gödel's coding.

Theorem A.0.9. The theory of $\mathbb{Z}$ in the language of $(+, 0, 1, <, \equiv_p)$ where $\equiv_p$ is the relation of "two integers are same modolu p" is complete, admits quantifier elimination hence decidable.

References

[1] J. E. Humphreys. *Reflection groups and Coxeter groups*, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.