INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH MOHALI

ज्ञानान्वेषणम्

IN PURSUIT OF KNOWLEDGE

A Study of Group Theoretic Concepts with Visualization of Symmetry Applications

Author: Daksh Arora

Under the Supervision of Prof. Amit Kulshrestha

August 2025

Contents

Abstract

This internship project was carried out under the supervision of Prof. Amit Kulshrestha. The focus was on exploring concepts in Group Theory, and some topics of Abstract Algebra were studied too in the latter part of the internship. A complementary component involved visualising group actions through 3D animations made in Blender via Blender Python API(bpy), which can be used for any arbitrary object made in Blender to show any rotation via quaternion rotations.

1 Introduction

This project was followed by a course on symmetry undertaken by me the preceding semester, also taught by Prof. Amit Kulshrestha. This project provided insight into the topics taught in that course and offered opportunities to learn new topics relevant to Group Theory. This project explored topics such as Isomorphisms, Homomorphisms, Products of Groups, Quotient Groups, Finite Rotation Groups, Sylow Theorems, finitely generated abelian groups, and Automorphisms, some of which were already introduced in the symmetry course and further explored.

To reinforce further understanding, exercises from Groups and Symmetries by M.A. Armstrong were solved. Towards the latter part of the project, topics from Abstract Algebra, such as Rings, Principal Ideals, Integral Domains, and Modules, were also briefly covered.

In addition to theoretical work, this project also has a visualization component to visualize symmetry groups. Animations were created to illustrate rotational symmetries, which are implemented using quaternion rotations. The developed script can be applied to any object modeled in Blender. This connection between algebraic theory and virtual visualization provides a bridge that links abstract mathematical structures with geometric representations through Group Actions.

2 Project Phases

2.1 Revisiting Concepts of Symmetry

2.1.1 Group Axioms

Definition 1

A group $(G, \cdot)$ is a set G together with group operation on G which satisfies these 4 axioms:

- G is closed under the $\cdot$ operation
- The operation is associative, i.e. $(xy)z = x(yz)$
- There exists a neutral element, e such that $xe = ex = x$
- For each element in $a \in G$, $\exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$

There are several examples of Groups and they are useful in various fields. Below are some examples of Groups

Examples:

- The set of integers $\mathbb{Z}$ under addition
- The residue class $\mod n - \{0\}$ under multiplication
- The dihedral group $D\_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ where the group operation is defined by $r^4 = e, sr^n s = (r^n)^{-1}$

Exercise highlights :

Question 2.5

A function from the plane to itself which preserves the distance between any two points is called an isometry. Prove that an isometry must be a bijection and check that the collection of all isometries of the plane forms a group under composition of functions.

Answer: Take $f : \mathbb{R}^2 \to \mathbb{R}^2$ to be isometry of $\mathbb{R}^2$. Thus, f has the following property

$$||f(x) - f(y)|| = ||x - y|| \quad \forall\ x, y \in \mathbb{R}^2$$

First we will prove bijection of any isometric function f.

$\implies$ Assume for some $x, y \in \mathbb{R}^2$, $f(x) = f(y)$. Then,

$$\|f(x) - f(y)\| = \|x - y\| = 0$$

which means that $x = y$
$\Longleftarrow$ Similarly, take some $x, y \in \mathbb{R}^2$ such that $x = y$. Then,

$$\|x - y\| = \|f(x) - f(y)\| = 0$$

which means that $f(x) = f(y)$
$\therefore f$ is a bijection
Now, take some f, g, h which are isometries of $\mathbb{R}^2$

- For $x, y \in \mathbb{R}^2$

  $$\|(f \circ g)(x) - (f \circ g)(y)\| = \|f(g(x)) - f(g(y))\| = \|g(x) - g(y)\| = \|x - y\|$$

  Isometries are closed under composition

- For $x, y \in \mathbb{R}^2$

  $$\|((f \circ g) \circ h)(x) - ((f \circ g) \circ h)(y)\| = \|(f \circ (g \circ h))(x) = (f \circ (g \circ h))(x)\|$$

  Isometries are associative

- $f(x) = x$ is an isometry which acts as a neutral element

- We know that f is bijective, therefore there must exist some isometry f^{-1} such that $f^-1(f(x)) = x$. Now,

  $$\|f^{-1}(f(x)) - f^{-1}(f(y))\| = \|x - y\| = \|f(x) - f(y)\|$$

  So, f^{-1} is also an isometry

$\therefore$ All the isometry of $\mathbb{R}^2$ form a Group under composition

Question 3.9

Let p be a prime number and let x be an integer which satisfies $1 \leq x \leq p - 1$. Show that none of $x, 2x, ..., (p-1)x$ is a multiple of p. Deduce the existence of an integer z such that $1 \leq z \leq p - 1$ and $xz \mod p = 1$.

Answer: According to Euclid's lemma, if $p \mid ab$, then p must divide at least a or b. So consider a number of nx. We know that p is prime, so x cannot divide p. Therefore if $p \mid nx$, we know that $p \nmid x \quad \because 1 \leq x \leq p - 1$. So $p \mid n$. Now take $n \in \{1, 2..., p - 1\}$. For this set, $1 \leq n \leq p - 1$, therefore $p \nmid n$.
$\therefore p \nmid nx \quad \forall n$.

From Bézout's lemma, For some integers x and $p \exists a, b \in \mathbb{Z}$ such that

$$ax + bp = gcd(x, p)$$

Since p is a prime, we know that $gcd(x, p) = 1$.

$$\begin{aligned} ax + bp &= 1 \\ \implies ax + bp &\equiv 1 \mod p \\ \implies ax &\equiv 1 \mod p \end{aligned}$$

$\therefore \exists a \in \mathbb{Z}_p$ such that $ax \mod p = 1$

2.1.2 Dihedral Groups and Subgroups

Dihedral groups show us the symmetry of regular polygons. It is denoted by D_n where n is the number of sides of the regular polygon. This symmetry group consists of n-1 different rotations, with increments of $\frac{360}{n}$ each, and reflection along each axis of symmetry. Due to the properties of this symmetry, we can define this group as follows

Definition 2

D_n is a group which contains $2n$ elements.

$D_n = \{ e, r..., r^{n-1}, s, sr..., sr^{n-1} \}$ where the group operation is defined as $r^n = e$, $s^2 = e$ and $srs = r^{n-1}$

Order of an element a can be defined as the positive integer n when $a^n = e$ where e is the neutral element. Here, we get to see that Dihedral groups have order 2 elements and at least one order n element. The reflections $\{ s, sr \ldots, sr^{n-1} \}$ have order 2 and any element in the rotation set $\{ r, r^2 \ldots, r^{n-1} \}$ can have order x if $\exists a \in \mathbb{Z}^+ \mid ax = n$.

Definition 3

A subgroup H of a group G is defined as a subset of G which itself forms a group under the group operation of G

In case of Dihedral groups, we can observe that $H = \{ e, r, r^2 \ldots, r^{n-1} \}$ is a subgroup of D_n.
The group $2\mathbb{Z} = \{ 2x \mid \forall x \in \mathbb{Z} \}$ is a subgroup of $(\mathbb{Z}, +)$.

Definition 4

The elements of a group which when multiplied together form the entire group are called the set of generators of that group. The group is denoted in terms of generators as $\langle x_1, x_2 \ldots, x_n \rangle$ where x_i are generators

The most common example is the set of generators of a cyclic group $\{ e, x \ldots, x^{n-1} \}$ is $\langle x \rangle$ Another example which is very on theme of this section is the Dihedral Group, which is given by $\langle r, s \rangle$

Question 5.7

Let G be an abelian group and let H consist of those elements of G which have finite order. Prove that H is a subgroup of G.

Answer: Consider a subgroup generated by finite elements of $H = \langle e, x_1 \ldots, x_n \rangle$ such that the set of generators are disjoint from each other i.e. there is no i and j with any integer a and b such that $x_i^a = x_j^b$. Any group element of H can then be expressed in the form of $x_1^{m_1} \cdot x_2^{m_2} \cdots x_n^{m_n}$. This group contains identity element as it is of finite order. We can construct inverse of any element a as $a^{-1} = (x_1^{m_1} \cdot x_2^{m_2} \cdots x_n^{m_n})^{-1} = (x_n^{m_n})^{-1} \cdot (x_{n-1}^{m_n-1})^{-1} \ldots (x_1^{m_1})^{-1} = (x_1^{m_1})^{-1} \cdot (x_2^{m_2})^{-1} \ldots (x_n^{m_n})^{-1}$. And since $x_i^{m_i}$ has a finite order, it has an inverse of finite order and $a^{-1} \in H$. H is also commutative which can be trivially shown due to its abelian property, and H is also closed.
$\therefore H$ is a subgroup of G □

Question 5.11

Show that $\mathbb{Q}$ is not cyclic. Even better, prove that $\mathbb{Q}$ cannot be generated by a finite number of elements.

Answer: Assume that $\mathbb{Q}$ is cyclic and generated by $\langle r \rangle$ and express r as $\frac{a}{b}$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and a and b are co-prime.

$$\mathbb{Q} = \{ \frac{ka}{b} \mid k \in \mathbb{Z} \}$$

This implies each element of $\mathbb{Q}$ has a denominator dividing b but $\frac{1}{b+1} \in \mathbb{Q}$. This is a contradiction.
$\therefore \mathbb{Q}$ is not cyclic
Assume that $\mathbb{Q}$ is generated by a finite set of elements $\langle r_1, r_2 \ldots, r_n \rangle$. Take $r_i = \frac{a_i}{b_i}$. Now take $B = lcm(b_i)$. And change r_i to $r_i = \frac{k_i}{B}$. Then $\mathbb{Q} = \langle \frac{k_1}{B}, \frac{k_2}{B} \ldots, \frac{k_n}{B} \rangle = \langle \frac{K}{B} \rangle$ where $K = gcd(k_1, k_2 \ldots, k_n)$. However, this implies that $\mathbb{Q}$ is cyclic, and we know that it isn't cyclic.
$\therefore \mathbb{Q}$ cannot be generated by finite elements. □

2.1.3 Cayley's Theorem/Lagrange's Theorem

A permutation is a bijection of some arbitrary finite set X to itself. The set of all these permutations form a group under composition. Take a permutation from S_5, which is the group of permutations of 5 elements.

$$\alpha = \begin{bmatrix} 12345 \\ 24513 \end{bmatrix}$$

We will be using the notation for some permutation given as $\alpha = (34)(124)$, which is basically a simplified version of the matrix notation. Any permutation can be written as a composition of transpositions. We can show this by considering some permutation $\alpha = (a_1 a_2 \dots a_k)$. Here α can be written in the form of $(a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$. Define a function

$$\lambda : S_n \to \{+1, -1\}$$

where if the number of transpositions of an element in S_n is even, then this function will output $+1$, and if the element has an odd number of transpositions, then it is -1; these are called even permutations and odd permutations, respectively.

Theorem

The even permutations of S_n form a subgroup of order $n!/2$ which is called the alternating group A_n of degree n.

Proof: Consider two even permutations α and β, the product $\alpha\beta \in A_n$ as it will also have even transpositions. α^{-1} can be constructed by reversing the order of transpositions of α so $\alpha^{-1} \in A_n$. e is given by 0 transpositions so it is also even and belongs to A_n. For every α there exists an odd permutation in S_n given by $(12)\alpha$ therefore, A_n contains exactly half elements as S_n which is $n!/2$. □

We will be discussing isomorphisms in detail in a later section; for now, we can define what it means as it is crucial to the following theorems in this section.

Definition 5

Let G_1 and G_2 are groups, then G_1 and G_2 are said to be isomorphic if there exists a function $\lambda : G_1 \to G_2$ which is bijective and satisfies the property $f(x) \cdot_{G_2} f(y) = f(x \cdot_{G_1} y) \quad \forall\, x, y \in G_1$

Isomorphisms are very useful as they tell us that the groups are identical in structure, and equivalent in general. **Examples:**

- $\lambda : \mathbb{R} \to \mathbb{R}^{\text{pos}}$ defined by $\lambda(x) = e^x$. ($\mathbb{R}^{\text{pos}}$ is positive $\mathbb{R}$ under multiplication)
- D_3 and S_3 are isometric

Cayley's Theorem

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof: Each element g in G gives a permutation $f_g : G \to G$ defined by $f_g(x) = gx$. This is injective since $f_g(x) = f_g(y) \implies gx = gy \implies g^{-1}gx = g^{-1}gy \implies x = y$. It is also surjective as for any $z \in G \quad f_g(g^{-1}z) = gg^{-1}z = z$. Therefore, f_g is bijective. Define G' as a subgroup of S_G where the group operation in S_G is given by

$$f_g \circ f_h(x) = ghx = f_{gh}(x)$$

for all $x \in G$. Therefore, the product of two elements in G' lies in G'. The identity and inverse of any element also exist in G', so G' is a subgroup of S_G. The correspondence between G and G' defined by $g \to f_g$ is certainly bijective. And it sends multiplication of G to G' as $gh \to f_{gh} = f_g f_h$. Therefore, G and G' are isomorphic.
Now, since G is finite, we can number the elements in G as $1, 2 \ldots, n$. Then a permutation in G induces a permutation on the numbers 1 to n. This gives an isomorphism from S_G to S_n. This means that G' is isomorphic to some subgroup G'' of S_n. And we know that G is isomorphic to G'. So $G \cong G'$

$\therefore$ Any finite group is a subgroup of S_n

This theorem is really strong and has alot of consequences further. We can define any group G in terms of a subgroup of S_n.

Definition 6

Consider a subgroup H of a group G. The set $X = \{\, gH \mid g \in G \,\}$ is the set of left cosets of H where $gH = \{\, gh \mid h \in H \,\}$

We claim that if $g_1H \bigcap g_2H \neq \phi$ then $g_1H = g_2H$. We will prove this claim in the following theorem and show all the consequences of this being true.

Lagrange's Theorem

Consider a subgroup H of the group G. Then $|H|$ divides $|G|$.

Proof: Assume that $g_1H \bigcap g_2H \neq \phi$ and $\exists\, h \in g_1H, g_2H$. Here

$$h' = g_1h_1 = g_2h_2 \implies g_1 = g_2h_2h_1^{-1} = g_2h_3$$

This means that $g_1 \in g_2H$. Take an element from g_1H, lets say $g_1h_i = (g_2h_3)h_i = g_2(h_3h_i)$. So $g_1H \subset g_2H$. We can make a similar argument for g_2H and find that $g_2H \subset g_1H$. So, $g_1H = g_2H$. Our main proof is done here, now we just have to show the consequences of this restriction.
The cosets of H need to divide G as each coset has $|H|$ elements and cannot overlap.
$\therefore |H|$ divides $|G| \quad \square$

Corollary: The order of an element g divides $|G|$

Corollary: Groups of prime order are cyclic as $x \in G - \{\, e \,\}$ can have only have a prime order

Corollary: If $x \in G$ then $x^{|G|} = e$

2.1.4 Products, Cauchy's theorem and Conjugacy

Definition 7

A direct product of groups is defined by $G \times H$ where the elements are of the form (g, h) and the group operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2)$

We observe that $G \times H = H \times G$ so order at which groups are written doesn't matter here.

Examples:

- $\mathbb{Z}_3 \times \mathbb{Z}_2$ has 6 elements which are $(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)$

Theorem

$\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic if and only if the highest common factor of m and n is 1.

Proof: Let k be the order of $(1, 1)$. Adding $(1, 1)$ to itself k times gives $(0, 0)$.

$$(k \text{ mod } n, k \text{ mod } m) = (0, 0)$$

This means that both m and n are factors of k. If the highest common factor is 1 then mn must be a factor of k, and therefore $k = mn$. So, in this case $(1, 1)$ generates $\mathbb{Z}_n \times \mathbb{Z}_m$.

Now consider d be the highest common factor of m and n and d is greater than 1. Let $m' = m/d$ and $n' = n/d$. For some element (x, y) we have

$$\begin{aligned} m'dn'(x, y) &= (m'dn'x \text{ mod } n, m'dn'y \text{ mod } m) \\ &= (mn'x \text{ mod } n, m'ny \text{ mod } m) \\ &= (0, 0) \end{aligned}$$

so the order of (x,y) is at most $m'dn'$. Therefore, $\mathbb{Z}_n \times \mathbb{Z}_m$ does contain any element of order mn and cannot be cyclic.

Cauchy's theorem

If p is a prime divisor of the order of a finite group G, then G contains an element of order p.

Proof: We need an element $x \in G$ whose order is p. Consider the set X of all ordered strings $\mathbf{x} = (x_1x_2 \dots x_p)$ of elements of G for which

$$x_1x_2 \dots x_p = e$$

We have to find a string which has all the coordinates equal but which is not equal to $(e, e \ldots, e)$. If $\mathbf{x}$ is to lie in X we can choose the elements $x_1, x_2 \ldots x_{p-1}$ arbitrarily and take $x_p = (x_1 x_2 \ldots x_{p-1})^{-1}$. Therefore the size of X is $|G|^{p-1}$, which is a multiple of p. Let $\mathcal{R}$ be the subset of $X \times X$ defined as folows. An ordered pair (x,y) belongs to $\mathcal{R}$ if y can be obtained by cyclically permuting the coordinates of x. In other words y is one of

$$\begin{gathered}(x_1, x_2 \ldots x_p)\\(x_p, x_1 \ldots x_{p-1})\\\vdots\\(x_2, x_3 \ldots x_p, x_1)\end{gathered}$$

Note that all these permutations do belong to X. $\mathcal{R}$ is an equivalence relation and it contains distinct equivalence classes $\mathcal{R}(x)$ which partition X, so adding the sizes of these classes gives us X. If every class other than $\mathcal{R}(e)$ contains p elements then the size of X will be congruent to 1 modulo p, contradicting our calculation. So, there must exist a string other than e which has less than p elements.
So two of the permutations are equal lets say

$$(x_{r+1}, \ldots, x_p, x_1, \ldots x_r) = (x_{s+1}, \ldots, x_p, x_1, \ldots x_r)$$

Assume $r > s$ and cycle back $p - r$ times to give

$$(x_1, x_2, \ldots, x_p) = (x_{k+1}, \ldots, x_p, x_1, \ldots, x_k)$$

where $k = p - r + s$. Equating corresponding coordinates we observe that $x_i = x_{k+i \bmod p}$, and consequently

$$x_1 = x_{k+1} = x_{2k+1} = \cdots = x_{(p-1)k+1}$$

where the suffices are read mod p. Suppose $ak + 1$ and $bk + 1$ are congruent modulo p. Then p divides $(b - a)k$, which is impossible because p is prime and both $b - a$ and k are less than p. Therefore the numbers

$$1, k+1, 2k+1, \ldots, (p-1)k+1$$

are all different when read mod p. As there are p of them reading them mod p just gives 1,2...p jumbled up. We conclude that $x_1 = x_2 = \cdots = x_p$, which gives us $x_1^p = e$ as required. □

Definition 8

For a fixed element $g \in G$ the function from G to G is given by $x \rightarrow gxg^{-1}$ is an isomorphism called conjugation by g.

This preserves the algebraic nature of G as $g(xy)g^{-1} = (gxg)^{-1}(gyg^{-1})$. Two elements of S_n are said to have the same cycle structure if when they are decomposed as products of disjoint cyclic permutations they both have the same number of 2-cycles, the same number of 3-cycles, and so on. We claim that conjugation preserves cycle structure. If θ, ϕ S_n have the same cycle structure, write out the cycle decomposition of ϕ underneath that of θ, taking the constituent cycles in order of decreasing length. In both cases include the integers left fixed by the permutation as cycles of length 1. Let g be the element of S_n which sends each integer mentioned in θ to the integer vertically below it in ϕ. Then $g\theta g^{-1} = \phi$ because moving an integer up from ϕ to θ, pushing it along one position in θ, then dropping it back down to ϕ is the same as moving along one position in ϕ. Therefore, permutations which have the same cycle structure are conjugate in S_n. Conversely, conjugate permutations have the same cycle structure.

Theorem

The center is a subgroup of G and is made up of the conjugacy classes which contain just one element.

Proof: The center of a group is defined as

$$Z(G) = \{\, x \in G \mid \; xg = gx, \; \forall g \in G \,\}$$

If $x, y \in Z(G)$ and $g \in G$, then

$$\begin{aligned} gxy^{-1} &= xgy^{-1} \\ &= x(yg^{-1})^{-1} \\ &= x(g^{-1}y)^{-1} \\ &= xy^{-1}g \end{aligned}$$

Therefore, $xy^{-1} \in Z(G)$. Since $xg = gx$, we get to see that $gxg^{-1} = x$ only so the conjugacy class of x is the singleton element $\{\, x \,\}$

Question

If H and K are subgroups of G for which $HK = G$, if they have only the identity element in common, and if every element of H commutes with every element of K, then G is isomorphic to $H \times K$.

Answer: Define a map

$$\varphi : H \times K \to G, \quad \varphi(h, k) = hk.$$

Since $HK = G$, every $g \in G$ can be expressed as a product hk with $h \in H$, $k \in K$.
For $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$\varphi((h_1, k_1)(h_2, k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2.$$

Since every element of H commutes with every element of K,

$$h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi(h_1, k_1)\varphi(h_2, k_2).$$

Thus φ is a homomorphism.

Suppose $\varphi(h, k) = e$. Then $hk = e \implies h = k^{-1} \in H \cap K = \{e\}$. Hence $h = k = e$. By assumption $HK = G$, so every element of G is in the image of φ.

Therefore φ is an isomorphism, and hence $G \cong H \times K$ $\square$.

Question

A group of order 6 is either isomorphic to $\mathbb{Z}_6$ or isomorphic to D_3

Answer: Let G be a group of order 6. By Lagrange's Theorem, the possible orders of elements in G are $1, 2, 3$, or 6.
Case 1: G has an element of order 6. Then G is cyclic, so $G \cong \mathbb{Z}_6$.
Case 2: G does not have an element of order 6. By Cauchy's theorem, G has an element a of order 3 and an element b of order 2. Then $\langle a\rangle \cap \langle b\rangle = \{e\}$, and $G = \langle a, b\rangle$. Moreover, $bab = a^{-1}$ (since b conjugates a to its inverse).
Thus G has the presentation

$$G = \langle a, b \mid a^3 = b^2 = e,\, bab = a^{-1}\rangle,$$

which is the standard presentation of the dihedral group D_3.
Hence, $G \cong D_3$.

2.1.5 Group Actions

Group actions are useful as they show great applications of Groups in alot of different ways.

Definition 9

Let G be a group and X be a set. An **action** of G on X is a homomorphism map

$$\diamond : G \times X \to X$$

that maps (g, x) to $g \diamond x$ such that

- $1 \diamond x = x \ \forall x \in X$.
- $g \diamond (h \diamond x) = gh \diamond x$ for all $x \in X$ and all $g, h \in G$.

Examples:

- D_4 act on the set of a square's vertices by rotating and reflecting them
- Any group G acts on itself by left multiplication, where an element g sends an element to the product gx

- S_n acts on the set of numbers $\{1, 2, \ldots, n\}$ by permuting them.
- The group of invertible matrices $GL_n(\mathbb{R})$ acts on vectors in $\mathbb{R}^n$ by matrix multiplication

Definition 10

Given an action of G on X and a point $x \in X$, the set of all images $g \diamond x$, as g varies through G, is called the **orbit** of x and written $\text{orbit}(x) = \{ g \diamond x \mid g \in G \}$

The stabilizer of x is defined as the set of elements in G which fix x. It is denoted by $\text{stab}(x) = \{ g \in G \mid g \diamond x = x \}$

Consider elements $x, y \in X$. We claim that if $\text{orbit}(x) \bigcap \text{orbit}(y) \neq \phi$ then $\text{orbit}(x) = \text{orbit}(y)$.
Take $z \in \text{orbit}(x) \bigcap \text{orbit(y)}$. Then

$$z = g_1 \diamond x = g_2 \diamond y$$

For some $g_1, g_2 \in G$

$$g_2^{-1} \diamond (g_1 \diamond x) = g_2^{-1} \diamond (g_2 \diamond y) = g_2^{-1} g_2 \diamond y = y$$

Hence, $y \in$ orbit(x). Thus, orbit(y) $\subset$ orbit(x). A similar argument shows orbit(x) $\subset$ orbit(y). So, orbit(x) = orbit(y) □
Examples:

- Number the 4 vertices of a square as $\{1, 2, 3, 4\}$. Here $\text{orbit}(1) = \{1, 2, 3, 4\}$, and $\text{stab}(1) = \{ id, \text{reflection along diagonal 1-3} \}$
- In $GL_2(\mathbb{R})$ acting on 2D vectors in $\mathbb{R}^2$. Here the orbits are $\text{orbit}(0) = \{0\}$ and $\text{orbit(v)} = \mathbb{R}^2 \backslash \{0\}$, and $\text{stab}(0) = GL_2(\mathbb{R})$ and $\text{stab(v)} =$ the subgroup of all matrices that have **v** as an eigenvector with an eigenvalue of 1

Orbit-Stabilizer Theorem

For each $x \in X$, the correspondence $g(x) \rightarrow g$ stab(x) is a bijection between orbit(x) and the set of left cosets of stab(x)

Proof: The correspondence is clearly surjective, It is injective because if g stab(x) = g' stab(x), then $g = g'h$ for some element $h \in$ stab(x) and therefore $g \diamond x = g'h \diamond x = g'(h \diamond x) = g' \diamond x$.
Put another way, the Orbit-Stabilizer theorem says that cardinality of the orbit of x is equal to the index of the stabilizer of x in G.

Corollary: If G is finite, the size of each orbit is a divisor of the order of G
Write X^g for the subset of X consisting of those points which are left fixed by the element of g in G

The Counting Theorem

The numbers of distinct orbits is

$$\frac{1}{|G|}\sum_{g\in G}|X^g|$$

in other words, the average number of points left fixed by an element of G

Proof: Count the collection of those ordered pairs (g,x) from $G\times X$ for which $g\diamond x = x$. The number of such pairs is

$$\sum_{g\in G}|X^g|$$

It is also equal to

$$\sum_{x\in X}|\text{stab(x)}|$$

Let $X_1, X_2, \ldots, X_k$ be the distinct orbits and rewrite the above term as

$$\sum_{i=1}^{k}\sum_{x\in X_i}|\text{stab(x)}|$$

Points in the same orbit have conjugate stabilizers, so if a is some chosen point of X_i. we have

$$\sum_{x\in X_i}|\text{stab(x)}| = |X_i|\cdot|\text{stab}(a)|$$

$$= \text{orbit(a)}\cdot\text{stab(a)}$$

which is just $|G|$ by the Orbit-Stabilizer theorem. Therefore,

$$k = \frac{1}{|G|}\sum_{g\in G}X^g \quad \square$$

2.1.6 Finite Rotational Groups

The special orthogonal group SO_3 is identified with the group of rotations of $\mathbb{R}^3$. We will enquire about this group and see what possibilities are there for some finite subgroup of SO_3

Theorem

A finite subgroup of O_2 is either cyclic of dihedral

Proof: Take $G \lneqq O_2$ where G is non-trivial.

Case 1:$G \in SO_2$

Each element of G represents a rotation of the plane. We write A_θ for the matrix representing anticlockwise rotation through θ about the origin, and choose $A_\varphi \in G$ so that φ is positive and as small as possible. Given $A_\theta \in G$, we can divide θ by φ and produce $\theta = k\varphi + \psi$ where $k \in \mathbb{Z}$ and $0 \leq \psi < \varphi$. Then

$$A_\theta = A_{k\varphi+\psi} = (A_\varphi)^k A_\psi \quad \text{and} \quad A_\psi = (A_\varphi)^{-k} A_\theta$$

Since A_θ and A_φ both lie in G, A_ψ is also in G. This gives $\psi = 0$ by contradiction. Therefore, G is generated by A_φ and is cyclic.
Case 2:$G \not\subset SO_2$
We set $H = G \cap SO_2$, then $H \leq G$ which has index 2, and H is also cyclic since $H \leq SO_2$. Choose a generator A for H and an element B from $G \backslash H \not\subset$. As B is a reflection, we have $B^2 = I$. If $A = I$, then G consists of I and B and is a cyclic group. Otherwise, the order of A is an integer $n > 1$. The elements of G are

$$I, A, \ldots, A^{n-1}, B, AB, \ldots, A^{n-1}B$$

and they satisfy $A^n = I, B^2 = I$ and $A^{-1}B = BA$. So G is the dihedral group D_n.

Theorem

A finite subgroup of SO_3 is isomorphic either to a cyclic group, a dihedral group, or the rotational symmetry group of one of the regular solids.

Proof: Let G be a finite subgroup of SO_3. Then any $g \in G$ represents rotation of $\mathbb{R}^3$ about some axis. The two points where the axis of a rotation g meets the unit sphere are called poles of g.

These poles are the only points fixed by rotation of the unit sphere. Let X

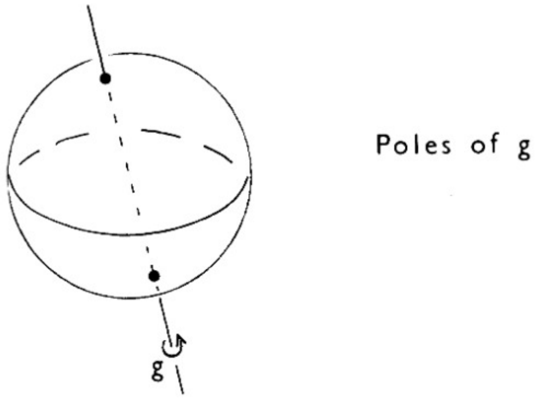

Figure 1: Source: MA Armstrong Groups & Symmetries Fig 19.1

denote the set of all poles of all elements of $G - \{\, e \,\}$. Take $x \in X$ and $g \in G$. Let x be a pole of the element $h \in G$. Then $(ghg^{-1})(g(x)) - g(h(x)) = g(x)$

which shows that $g(x)$ is a pole of ghg^{-1} and hence $g(x) \in X$. Therefore, this is an action of G on X. We will now apply the Counting Theorem and show restrictions on the possible points of X. Let N denote the number of distinct orbits, choose a pole from each orbit and call these poles $x_1, x_2, \dots x_N$. Every element $G - \{ e \}$ fixes precisely two poles, while id fixes them all, so we have the following equation

$$\begin{aligned}
&N = \frac{1}{|G|}\{\, 2|G| - 1 + |X|\,\} \\
&N = \frac{1}{|G|}\{\, 2|G| - 1 + \sum_{i=1}^{N} |G(x_i)|\,\} \\
&2(1 - \frac{1}{|G|}) = N - \frac{1}{|G|}\sum_{i=1}^{N} |G(x_i)| \\
&= N - \sum_{i=1}^{N} \frac{1}{|G(x_i)|} = \sum_{i=1}^{N}(1 - \frac{1}{|G_{x_i}|})
\end{aligned}$$

Here, G_x is stabilizer of x and $G(x)$ is orbit of x Assuming G is non trivial, LHS is greater than or equal to 1 and less than 2. But each stabilizer G_x has order of atleast 2 so

$$\frac{1}{2} \leq 1 - \frac{1}{|G_{x_i}|} < 1$$

for $1 \leq i \leq N$. So, $N = 2$ or $N = 3$

If $N = 2$ then we get $2 = |G(x_1)| + |G(x_2)|$ and there can only be two poles. That means there is only one axis, say L and every element of G is a rotation about this axis. The plane passing through origin and perpendicular to L is rotated on itself by G. Therefore $G \cong G' \leq SO_2$. So G is cyclic.

If $N = 3$, write x_1, x_2, x_3 as x, y, z, then

$$\begin{aligned}
&2\Big(1 - \frac{1}{|G|}\Big) = 3 - \Big(\frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|}\Big) \\
&1 + \frac{2}{|G|} = \frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|}
\end{aligned}$$

The sum on RHS is greater than 1, so there are total 4 possibilities

Case (a) $|G_x| = |G_y| = 2, |G_z| = n \qquad$ where $n \geqslant 2$

If $|G_x| = |G_y| = |G_z| = 2$ then G is a group of order 4 in which every element other than identity has order 2. Therefore, G is isomorphic to Klein's group/D_2. Let g_z generate G_z and remember that g is an isometry. The poles x and $g_z(x)$ are equidistant from z, similar for y. So $-z$ much be the other point in $G(z)$ and we have $g(x) = -x, g(y) = -y$. Therefore, the axes through x, y and z are

perpendicular to one another, and the three orbits are $\{\pm x\}, \{\pm y\}, \{\pm z\}$.
If $|G_x| = |G_y| = 2$ and $|G_z| = n \geq 3$ then G is a group of order $2n$. The axis through z is fixed by every rotation in G_z, so G_z is cyclic. The points $x, g(x), \ldots, g^{n-1}(x)$ are all distinct. We can see this by considering $g^r(x) = g^s(x)$ where $r > s$, then $g^{r-s} = x$. But z and $-z$ are the only poles which are left fixed by g^{r-s} and x cannot be $-z$, as $|G_x| = 2$ whereas $|G_{-z}| = |G_z| = n \geq 3$. Because g is an isometry,

$$\|x - g(x)\| = \|g(x) - g^2(x)\| = \cdots = \|g^{n-1}(x) - x\|$$

Therefore, $x, g(x), \ldots, g^{n-1}(x)$ are the vertices of a regular n-gon P. Since G consists of $2n$ elements, each of which preserves P, G is dihedral.

Case (b) $|G_x| = 2, |G_y| = |G_z| = 3$
The order of G is 12. The orbit of z has 4 points. Choose one, say u which satisfies $0 < \|z - u\| < 2$ and choose a generator g for G_x. Then $u, g(u)$ and $g^2(u)$ are all distinct. Since g is an isometry, these are equidistant from z and lie at the corners of an equilateral triangle. Therefore, $z, u, g(u), g^2(u)$ are the vertices of a regular tetrahedron which is sent to itself by every rotation in G. So G is the rotational symmetries of a tetrahedron

Case (c) $|G_x| = 2, |G_y| = 3, |G_z| = 4$
The order of G is 24. There are six points in orbit of z. Choose one, say u and let g generate G_z. Then $u, g(u), g^2(u), g^3(u)$ are distinct, equidistant from z and lie at the corners of a square. Therefore, $z, -z, u, g(u), g^2(u), g^3(u)$ are the vertices of a regular octahedron and G is its rotational symmetry group. Since rotational symmetry of an octahedron and a cube are isomorphic, this is also the rotational symmetry of a cube.

Case (d) $|G_x| = 2, |G_y| = 3, |G_z| = 5$
The order of G is 60. There are 12 points in the orbit of z. Choose two, u and v which satisfy

$$0, \|z - u\| < \|z - v\| < 2$$

u and v exist since if we take g as the minimal rotation of G_z then $u, g(u), g^2(u), g^3(u), g^4(u)$ are all distinct, equidistant from z and lie at the corners of a regular pentagon similarly for v, so $-z$ is the only 12^{th} position left. Now, we also see that $u \in G(u) = G(z)$. As $-u$ lies at a distance of 2 from u, it must be one of the points $v, g(v), g^2(v), g^3(v)$, or $g^4(v)$. Looking out from u, we see eleven points and five which are closest to u must be equidistant from u. These are $z, g(u), g^3(v), g^2(v)$ and $g^4(u)$, therefore

$$\|u - z\| = \|u - g(u)\| = \|u - g^2(v)\|$$

We can now check that our twelve points lie in the vertices of a regular icosahedron, and G is the rotational symmetry group of this icosahedron. □

2.2 Further Concepts in Abstract Algebra

2.2.1 Quotient Groups and Isomorphisms

Definition 9

A H subgroup is called a normal subgroup of G if H is the union of conjugacy classes of G

Normal groups have an interesting property, that is, their left cosets form a natural group.

Theorem

If H is a normal subgroup of G, the set of all left cosets of H in G forms a group under this multiplication.

Proof: The product of two left cosets is again a left coset because

$$(xH)(yH) = xyH$$

for any two elements $x, y \in G$. Accepting this for the moment, associativity follows from associativity in G, the coset $eH = H$ acts as an identity and $x^{-1}G$ is the inverse of xH for each $x \in G$. So, this is a group □
If H is a normal subgroup of G we write $H \trianglelefteq G$. The group of left cosets of H in G is called the quotient group of G by H and denoted by G/H. **Examples:**

- The conjugacy classes $\{\, e \,\}$ and $\{\, (12)(34), (13)(24), (14)(23) \,\}$ make up a normal subgroup J of A_4. There are three left cosets $J, (123)J, (132)J$ and the quotient group A_4/J is isomorphic to $\mathbb{Z}_3$
- Every subgroup of an abelian group is a normal subgroup because the conjugacy classes are just the elements of the group.

Theorem

The subgroup H of G is normal if and only if $xH = Hx$ for all $x \in G$.

Proof: $\Longrightarrow$ Suppose H is normal. Given $x \in G, h \in H$, we know that the conjugates xhx^{-1} and $x^{-1}hx$ must belong to H. Therefore,

$$xh = (xhx^{-1})x \in Hx$$

and we have $xH \subset Hx$. We can use a similar argument to show that $Hx \subset xH$. So, $Hx = xH$.
$\Longleftarrow$ Assume $xH = Hx$ for all $x \in G$. If $h \in H, x \in G$ the conjugate xhx^{-1} belongs to

$$(xH)x^{-1} = (Hx)x^{-1} = H$$

and therefore H must be normal in G.

Definition

Let G_1 and G_2 be groups. A homomorphism is a function $\varphi : G_1 \to G_2$ which satisfies the property $\varphi(x) \cdot_{G_2} \varphi(y) = \varphi(x \cdot_{G_1} y) \quad \forall\, x, y \in G_1$

If a homomorphism is bijective, then it is called an isomorphism. The kernel K of a homomorphism φ is defined to be the set of elements of G_1 which map to the identity element of G_2.
Notice that if H is a normal subgroup of G the function $\varphi : G \to G/H$ defined by $\varphi(x) = xH$ is a homomorphism because

$$\varphi(xy) = xyH = (xH)(yH) = \varphi(x)\varphi(y)$$

for all $x, y \in G$. THe image of this homomorphism is G/H and its kernel is precisely H.

First Isomorphism Theorem

The kernel K of a homomorphism $\varphi : G \to G'$ is a normal subgroup of G, and the correspondence $xK \to \varphi(x)$ is an isomorphism from the quotient group G/K to the image of φ.

Proof: Suppose $x, y \in K$, then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e$, showing that $xy^{-1} \in K$. Certainly K is non-empty because $e \in K$, hence K is a subgroup of G. If $x \in K$ and $g \in G$, then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e.$$

Therefore, gxg^{-1} belongs to K and the subgroup K is normal in G.

Second Isomorphism Theorem

Suppose H, J are subgroups of G with J normal in G. Then HJ is a subgroup of G, $H \bigcap J$ is a normal subgroup of H, and the quotient groups $HJ/J, H/H \bigcap J$ are isomorphic.

Proof: (i) HJ is a subgroup of G. Since $J \trianglelefteq G$, we have $HJ = JH$. For $h_1 j_1, h_2 j_2 \in HJ$,

$$(h_1 j_1)(h_2 j_2)^{-1} \;=\; h_1 j_1 j_2^{-1} h_2^{-1} \;=\; h_1 (j_1 j_2^{-1} j^{-1})(j h_2^{-1})$$

where we use normality of J to write $h_2^{-1} j_1 h_2 = j \in J$. Thus the product lies in HJ, so $HJ \leq G$.

(ii) $H \cap J \trianglelefteq H$. Let $h \in H$ and $x \in H \cap J$. Because $J \trianglelefteq G$, we have $hxh^{-1} \in J$; and clearly $hxh^{-1} \in H$. Hence $hxh^{-1} \in H \cap J$, proving $H \cap J \trianglelefteq H$.

(iii) Isomorphism $H/(H \cap J) \cong (HJ)/J$. Define

$$\varphi : H \longrightarrow (HJ)/J, \qquad \varphi(h) = hJ.$$

This is a homomorphism: $\varphi(h_1h_2) = h_1h_2J = (h_1J)(h_2J)$. Its image is all of $(HJ)/J$, since any coset in $(HJ)/J$ has the form $(hj)J = hJ$ with $h \in H$, $j \in J$. The kernel is

$$\ker\varphi = \{h \in H : hJ = J\} = \{h \in H : h \in J\} = H \cap J.$$

By the First Isomorphism Theorem,

$$H/(H \cap J) \;\cong\; \operatorname{Im}\varphi \;=\; (HJ)/J. \quad \square$$

Third Isomorphism Theorem

Let H, J be a normal subgroups of G and suppose H is contained in J. Then J/H is a normal subgroup of G/H and the quotient group $(G/H)/(J/H)$ is isomorphic to G/J

Proof: The funetion $\varphi : G/H - +G/J$ defined by $\varphi(xH) = xJ$ is a homomorphism and is surjetive. A coset xH belongs to the kernel of φ precisely when $xJ = J$; in other words, when $x \in J$. Therefore, the kernel of φ is J/H and the result follows from the First Isomorphism Theorem

2.2.2 Sylow's Theorem

There are 3 Sylow's Theorems, which correlate the order of a group with the subgroup of that group. Let G be a finite group whose order is divisible by the prime number p. Suppose p^m is the highest power of p which is a factor of G and set $k = |G|/p^m$.

Theorem 1

The group G contains at least one subgroup of order p^m.

Theorem 2

Any two subgroups of G of order p^m are conjugate.

Theorem 3

The number of subgroups of G of order p^m is congruent to 1 modulo p and is a factor of k.

Proof of Theorem 1: Let X denote the collection of all subsets of G which have p^m elements, and let G act on X by left translation, so that the group element $g \in G$ sends the subset $A \in X$ to gA. The size of X is the binomial coefficient $\binom{|G|}{p^m}$, which is not divisible by p. Hence, there must be an orbit orbit(A) whose size is not a multiple of p.

We have

$$|G| = |\operatorname{orbit}(A)| \cdot |\operatorname{stab}(A)| \qquad (*)$$

consequently $|\operatorname{stab}(A)|$ is divisible by p^m. Now $\operatorname{stab}(A)$ is the stabilizer of A, so if $a \in A$ and $g \in \operatorname{stab}(A)$, then $ga \in A$. This means that the whole right coset $\operatorname{stab}(A)\, a$ is contained in A whenever $a \in A$, and $|\operatorname{stab}(A)|$ cannot exceed p^m. Therefore, $\operatorname{stab}(A)$ is a subgroup of G which has order p^m □.

Proof for Theorem 2 and Theorem 3: Let $H_1, \ldots, H_t$ denote the subgroups of G which have order p^m, and let H_1 act on the set $\{H_1, \ldots, H_t\}$ by conjugation so that $h \in H_1$ sends H_j to hH_jh^{-1}. If K_j is the stabilizer of H_j, then

$$K_j = H_1 \cap H_j.$$

We can prove this as follows, $K_j = \{\, h \in H_1 \mid hH_jh^{-1} = H_j \,\}$ and therefore $K_j \subset H_1$ and $H_1 \cap H_j \subset K_j$. We must show that K_j is contained in H_j. Certainly $K_jH_j = H_jK_j$, so K_jH_j is a subgroup fo G.In addition, J_j sits inside K_jH_j as a normal subgroup and the Second Isomorphism Theorem gives

$$K_jH_j/H_j \cong K_j/K_j \cap H_j$$

The order of K_jH_j is therefore $|K_j| \cdot |H_j|/|K_j \cap H_j|$, which is a power of p. But the largest available power of p is $p^m = |H_j|$, hence $K_jH_j = H_j$, and we have $K_j \subset H_j$ as required.

Now continuing our argument, $K_1 = H_1$ and the orbit of H_1 has just one element, namely H_1 itself. If $j \neq 1$, the order of K_j is a smaller power of p than p^m, so the size of every other orbit is a multiple of p. Adding up the sizes of the orbits shows that t is congruent to 1 modulo p.
Now let the whole group G act on $\{H_1, \ldots, H_t\}$ by conjugation. In order to prove Theorem 2, we must verify that this G-action is transitive. Each G-orbit is made up of various H_1-orbits. The G-orbit of H_1 certainly contains H_1, and therefore its size is congruent to 1 modulo p.

Suppose now that H_r is not in the G-orbit of H_1, and let H_r act on $\{H_1, \ldots, H_t\}$ by conjugation. The G-orbit of H_1 is now partitioned into H_t-orbits and the size of each of these is a multiple of p as the exceptional orbit $\{H_t\}$ is not present. This leads us to conclude that $|\operatorname{orbit}(H_1)|$ is congruent to 0 modulo p, which does not agree with our previous calculation. Therefore the G-orbit of H_1 must be all of $\{H_1, \ldots, H_t\}$ as required.

Since the size of an orbit is always a factor of the order of the group involved, we now know that t divides kp^m. But p does not divide t, so t must be a factor of k. □

Question

Show that a group of order 126 must contain a normal subgroup of order 7. Prove that a group of order 1000 cannot be a simple group.

Answer: Decomposing 126 into primes gives us $2 \times 3^2 \times 7$. There must be n number of $7-$Sylow subgroups present, say H_i. According to Sylow's

Second and Third Theorem, $n \mid 18$ and $n \equiv 1 \mod 7$. n can be a factor of 18, therefore it can be 1,2,3,6,9,18. The only number possible here that belongs to 1 mod 7 class is 1. Therefore, $n = 1$, since the Sylow Subgroups are closed under conjugation, we have that $gH_ig^{-1} = H_j$, but there is only 1 $7-$Sylow subgroup, so $H_i = H_j$. Therefore, a group of order 126 contains a normal subgroup of order 7.

Decomposing 1000 into primes gives us $2^3 \times 5^3$. There must be n number of $5-$Sylow groups, say K_i. As argued above, if we consider a $5-$Sylow subgroup, the number of such Sylow subgroups, say m, needs to divide 8 and be congruent to $1 \mod 5$. The only such m is 1, therefore, there exists one normal subgroup, and this group cannot be simple.

Question

If p is not congruent to 1 modulo q, show that every group of order pq is cyclic.

Answer: Here $p > q$ and p, q are primes.

Let G be a group with cardinality pq. Consider the number of $p-$Sylow Subgroups, say n_p, then $n_p = 1$ or q. If $n_p = q$, then $q \equiv 1 \mod p$, which is not possible as $p > q$ and q is a prime(not 1). So $n_p = 1$. Now consider $q-$Sylow Subgroups, say n_q, then if $n_q = p$, then $p \equiv 1 \mod q$, but this contradicts our given condition, so $n_q = 1$. So the Sylow groups H($p-$Sylow Subgroup) and K($q-$Sylow Subgroup) are both normal, and $G \cong H \times K$, which is cyclic.

Question

Suppose H is a Sylow subgroup of G and let J be a subgroup of G which contains H. If H is normal in J, and if J is normal in G, prove that H is normal in G.

H is normal in J, so we have that for any $j \in J$ we have that $jHj^{-1} \cong H$. Take any $g \in G$, $gHg^{-1} \subset J$. Since H is a Sylow subgroup of G, it must be a Sylow subgroup of J as well. And since H is normal in J, there is no other Sylow subgroup present in J with the same order as $|H|$. So, $gHg^{-1} = H$ and $H \triangleleft G$.

2.2.3 Finitely Generated Abelian Groups

A group if finitely generated if it has a finite set of generators.

Structure Theorem of Abelian Groups

Any finitely generated abelian group is isomorphic to a direct product of cyclic groups

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \times \mathbb{Z}^s$$

in which m_i is a factor of m_{i+1} for $1 \leq i \leq k-1$

Take x to be generated by the minimal set $x_1, x_2, \dots, x_r$ where the only relation between these elements is the trivial one obtained by raising each element to a multiple of its order. So the expression for $g \in G$ is unique with respect to the generators and the correspondence

$$g \to (n_1, \dots, n_r)$$

is an isomorphism between G and $\mathbb{Z}^r$, where n_i is the exponent of x_i element. Among all relations between all possible minimal sets of generators, there will be a smallest positive exponent, say m_1. Suppose m_1 is the exponent of x_1 in the relation

$$e = x_1^{m_1} x_2^{n_2} \dots x_r^{n_r}$$

between the generators $x_1, \dots, x_r$. We claim that m_1 is a factor of n_2. If $n_2 = qm_1 + u$ where $0 \leq u < m_1$, then

$$\begin{aligned} e &= x_1^{m_1} x_2^{am_1+u} x_3^{n_3} \dots x_r^{n_r} \\ &= (x_1 x_2^q)^{m_1} x_2^u x_3^{n_3} \dots x_r^{n_r} \end{aligned}$$

Since $x_1 x_2^q, x_2 \dots x_r$ is also a minimal set of generators this contradicts our choice of m_1 unless $u = 0$. Hence, $n_2 = qm_1$ as required. Similarly we can show m_1 is a factor of $n_3, \dots, n_r$ and we set $n_i = q_i m_1$ for $3 \leq i \leq r$.
Now change the set of generators to $z_1, x_2, \dots, x_r$ where $z_1 = x_1 x_2^q x_3^{q_3} \dots x_r^{q_r}$ and the relation becomes $e = z_1^{m_1}$.
Let $H = \langle z_1 \rangle$ and let G_1 be the subgroup generated by $x_2, \dots, x_r$. It is easy to see $HG_1 = G$ and $H \cap G_1 = \{ e \}$. Therefore $G \cong H \times G_1 \cong \mathbb{Z}_{m_1} \times G_1$. Now carrying out similar procedure for G_1, we can get to possibilities, $G_1 \cong \mathbb{Z}_{m_2} \times G_2$ or $G_1 \cong Z^{r-1}$. In the prior condition, m_2 occurs as the exponent of, say y_2 in the relation

$$e = y_2^{m_2} y_3^{n_3} \dots y_r^{n_r}$$

between the minimal set of generators $y_2, \dots, y_r$. Since $z_1, y_2, \dots, y_r$ generate G and since

$$e = z^{m_1} y_2^{m_2} y_3^{n_3} \dots y_r^{n_r}$$

we see that m_1 is a factor of m_2. Therefore, we can apply this step inductively and obtain the result stated in the theorem. □
We will be proving a general case of this in Section 2.2.7 for Modules over PID

Uniqueness of Abelian Groups

Let $G_1 = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \times \mathbb{Z}^s$ where $m_1 \mid m_2 \mid \cdots \mid m_k$, and $G_2 = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^t$, where $n_1 \mid n_2 \mid \cdots \mid n_t$. If G_1 and G_2 are isomorphic then $s = t, k = l$ and $m_i = n_i$ for $1 \leq i \leq k$

Proof: Let $T(G)$ denote the torsion subgroup of an abelian group G. It is characteristic, hence preserved by isomorphisms. From $G_1 \cong G_2$ we obtain

$$T(G_1) \cong T(G_2) \quad \text{and} \quad G_1/T(G_1) \cong G_2/T(G_2).$$

Since $T(G_1) = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ and $G_1/T(G_1) \cong \mathbb{Z}^s$ (and similarly for G_2), it follows that the free ranks coincide:

$$\mathbb{Z}^s \cong \mathbb{Z}^t \quad \Rightarrow \quad s = t.$$

Thus it remains to show $k = \ell$ and $m_i = n_i$.

We use the following standard fact if

$$H = \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_r}$$

is finite abelian, then for any positive integer q the number of solutions of $x^q = e$ in H equals

$$N_H(q) = \prod_{i=1}^{r} \gcd(a_i, q).$$

Indeed, in each cyclic factor $\mathbb{Z}_{a_i}$ the equation $x^q = e$ has exactly $\gcd(a_i, q)$ solutions; independence across direct sums gives the product.

Let $H_1 = T(G_1) = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ and $H_2 = T(G_2) = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_\ell}$. Since $G_1 \cong G_2$, we have $H_1 \cong H_2$, hence $N_{H_1}(q) = N_{H_2}(q)$ for all q.

Take $q = m_1$. Using the divisibility chains $m_1 \mid m_i$ and $n_1 \mid n_j$, we get

$$N_{H_1}(m_1) = \prod_{i=1}^{k} \gcd(m_i, m_1) = \prod_{i=1}^{k} m_1 = m_1^k,$$

and

$$N_{H_2}(m_1) = \prod_{j=1}^{\ell} \gcd(n_j, m_1) \leq m_1^{\ell}.$$

The condition that $N_{H_1}(m_1) = N_{H_2}(m_1)$ forces $k \leq \ell$ and, $\gcd(n_j, m_1) = m_1$ for at least k indices j (otherwise $N_{H_1}(m_1)$ would be $< m_1^k$). By symmetry, exchanging the roles of (m_i) and (n_j) and taking $q = n_1$ yields $\ell \leq k$ and $\gcd(m_i, n_1) = n_1$ for at least ℓ indices i. Consequently

$$k = \ell \quad \text{and} \quad m_1 \mid n_j \text{ for all } j, \quad n_1 \mid m_i \text{ for all } i.$$

In particular $m_1 \mid n_1$ and $n_1 \mid m_1$, hence $m_1 = n_1$.

Let $r = k = \ell$. Consider the subgroups

$$K_1 = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \leq H_1, \qquad L_1 = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r} \leq H_2,$$

and write $m_1 = n_1$ from Step 2. Mod out the common first factor:

$$\overline{H}_1 := H_1/\mathbb{Z}_{m_1} \;\cong\; \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}, \qquad \overline{H}_2 := H_2/\mathbb{Z}_{n_1} \;\cong\; \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}.$$

Since $H_1 \cong H_2$ and the summands $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{n_1}$ coincide, we have $\overline{H}_1 \cong \overline{H}_2$. Repeating the argument of Step 2 with $q = m_2$ (and symmetry with $q = n_2$) gives $m_2 = n_2$. Proceeding inductively, we obtain

$$m_i = n_i \quad \text{for all } 1 \leq i \leq r.$$

Thus we get $s = t$, $k = \ell$, and $m_i = n_i$ for $1 \leq i \leq k$, as claimed. □

2.2.4 Automorphisms

An **automorphism** of a group G is an isomorphism from G to G. The set of all automorphisms forms a group under composition of functions which is called the **automorphism group** of G written $\text{Aut}(G)$ **Examples:**

- An automorphism θ of $\mathbb{Z}$ must send 1 to an integer which generated $\mathbb{Z}$. therefore $\theta(1) = \pm 1$. If $\theta(1) = 1$, we have the identity automorphism. Otherwise, $\theta(1) = -1$ and θ sends each integer n to $-n$. We see immediately that $\text{Aut}(\mathbb{Z}\ )$ is isomorphic to $\mathbb{Z}_2$

- Suppose G is $\mathbb{Z}_2 \times \mathbb{Z}_2$. An automorphism permutes the three non-identity elements, and one easily checks that any such permutation, when completed by sending e to e, is an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is isomorphic to S_3

Conjugation by a fixed element g of G gives a particular type of automorphism $x \to gxg^{-1}$ called an inner automorphism. The inner automorphisms form a normal subgroup $\text{Inn}(G)$ of $\text{Aut}(G)$. If G is abelian, only the identity automorphism is an inner automorphism

Theorem

$\text{Inn}(G)$ is isomorphic to the quotient group $G/Z(G)$

Proof: The function from G to $\text{Aut}(G)$ which sends each g to the inner automorphism $x \to gxg^{-1}$ is a homomorphism. Its image consists of the inner automorphisms, and its kernel is

$$\{\, g \in G \mid x = gxg^{-1}, \forall x \in G \,\}$$

$$= \{\, g \in G \mid xg = gx, \forall x \in G \,\}$$

$$= Z(G)$$

Now the result will follow from First Isomorphism Theorem □

Definition

A semi-direct product $H \times_\varphi J$of groups H and J along with the homomorphism $\varphi : H \to J$is defined as

$$(x, y)(x', y') = (x.\varphi(y)(x'), y.y')$$

Associativity follows from

$$\begin{aligned}(x, y)(x', y')](x'', y'') &= (x.\varphi(y)(x'), y.y')(x'', y'') \\ &= (x.\varphi(y)(x').\varphi(y.y')(x''), y.y'.y'') \\ &= (x.\varphi(y)(x'.\varphi(y')(x'')), y.y', y'') \\ &\qquad \text{because } \varphi \text{ is a homomorphism} \\ &= (x, y)(x'.\varphi(y')(x''), y'.y'') \\ &= (x, y)[(x', y')(x'', y'')\end{aligned}$$

The function $(x, y) \to y$ is a homomorphism from $H \times_\varphi J$ onto J whose kernel $\{\, \{\, x, e_J \,\} \mid x \in H \,\}$ is isomorphic to H. So we have a copy of H in $H \times_\varphi J$ as a normal subgroup

Theorem

Let H, J be subgroups of G. If H is a normal subgroup, $HJ = G$ and $H \cap J = \{\, e \,\}$ then G is isomorphic to the semidirect product $H \times_\varphi J$ where $\varphi : J \to \mathrm{Aut}(H)$ is the homomorphism defined by $\varphi(y)(x) = yxy^{-1}$ for all $x \in H, y \in J$

Proof: Define $\psi : H \times_\varphi J \to G$ by $\psi(x, y) = xy$. Then ψ is a homomorphism because

$$\begin{aligned}\psi[(x, y)(x', y')] &= \psi(x.\varphi(y)(x'), y.y') \\ &= \psi(xyx'y^{-1}, y.y^{-1}) \\ &= xyx'y^{-1}yy' \\ &= xyx'y' \\ &= \psi(x, y)\psi(x', y')\end{aligned}$$

The image of ψ is all of G because $G = HJ$, so that every element of G may be written in the form xy. If (x, y) lies in the kernel of ψ, then $xy = e$ giving $x = y^{-1}$. Therefore, x and y both belong to $H \cap J = \{\, e \,\}$ and (x, y) is the identity element of $H \times_\varphi J$. So, ψ is an isomorphism.

2.2.5 Euclidean Groups and Wallpaper Patterns

The isometries of a plane form a group under composition of functions called the Euclidean Group E_2. A function $g : \mathbb{R}^2 \to \mathbb{R}^2$ belongs to E_2 if

$$\|g(\mathbf{x}) - g(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$$

We will show that a general element of E_2 is either a *rotation about the origin followed by translation*, or a *reflection in a line passing the origin followed by translation.* The translations make a subgroup T of E_2. This can be checked by considering any two elements $\tau_1, \tau_2 \in T$ defined as $\tau_1(\mathbf{x}) = \mathbf{u} + \mathbf{x}$,$\tau_2(\mathbf{x}) = \mathbf{v} + \mathbf{x}\ \forall \mathbf{x} \in \mathbb{R}^2$

$$\begin{aligned} \tau_1 \tau_2^{-1} &= \tau_1((-\mathbf{v}) + \mathbf{x}) \\ &= \mathbf{u} + ((-\mathbf{v}) + \mathbf{x}) \\ &= (\mathbf{u} - \mathbf{v}) + \mathbf{x} \end{aligned}$$

So $\tau_1 \tau_2^{-1}$ is translation by **u- v** and therefore belongs to T. If $g = \tau f$ and if f is a rotation, then g is called a *direct isometry.* If f is a reflection, g is said to be *opposite isometry.* Suppose $f \in O$,$\tau \in T$ and $\tau(\mathbf{0} = \mathbf{v})$. Then for each $\mathbf{x} \in \mathbb{R}^2$ we have

$$\begin{aligned} f\tau f^{-1}(\mathbf{x}) &= f(\mathbf{v} + f^{-1}(\mathbf{x})) \\ &= f(\mathbf{v}) + f(f^{-1}(\mathbf{x})) \qquad \text{because } f \text{ is linear} \\ &= f(\mathbf{v}) + \mathbf{x} \end{aligned}$$

Therefore, the conjugate $f\tau f^{-1}$ is translation by vector $f(\mathbf{v})$. Since the elements of T and O together generate E_2, we see that T is a normal subgroup of E_2. If $g = \tau f$, $h = \tau_1 f_!$ where $\tau, \tau_1 \in T$ and $f, f_1 \in O$, then

$$gh = \tau f \tau_1 f_1 = (\tau f \tau_{\cdot} f^{-1})(f f_1)$$

expresses gh as an orthogonal transformation followed by a translation. Put another way, the correspondence $g \to (\tau, f)$ is an isomorphism between E_2 and $T \times_\varphi O$ where $\varphi : O \to Aut(T)$ is conjugation. If $\mathbf{v} = \tau(0)$ and M is the orthogonal matrix which represents f in the standard basis for $\mathbb{R}^2$ then

$$g(\mathbf{x}) = \mathbf{v} f_M(\mathbf{x}) = \mathbf{v} + \mathbf{x} M^t$$

for all $x \in \mathbb{R}^2$. Conversely, given $\mathbf{v} \in \mathbb{R}^{\nvDash}, M \in O_2$, the equation above is an isometry of the plane. We may therefore think of each isometry as an *ordered pair* $(\mathbf{v}, M)$.

Theorem

Every direct isometry is a translation or a rotation. Every opposite isometry is a reflection or a glide reflection

Proof: Let ($\mathbf{v}$, $\boldsymbol{A}$) be a direct isometry where $0 \leq \theta \leq 2\pi$. When $\theta = 0$ we have the translation ($\mathbf{v}$,$\boldsymbol{I}$). Otherwise

$$\det(I - A) = \det \begin{bmatrix} 1 - \cos\theta & \sin\theta \\ -\sin\theta & 1 - \cos\theta \end{bmatrix} = 2 - 2\cos\theta$$

is positive. So, $I - A$ is invertible and the equation

$$\mathbf{c} - f_A(\mathbf{c}) = f_{I-A}(\mathbf{c}) = \mathbf{v}$$

has a unique solution for c. The given isometry is the rotation $(\mathbf{c} - f_A(\mathbf{c}), A)$ about this point $\mathbf{c}$.

Each opposite isometry can be seen as $(\mathbf{v}, B)$ where $0 \leq \varphi < 2\pi$. If $f_B(\mathbf{v}) = -\mathbf{v}$ then we have a reflection on the line m for which $\mathbf{a} = \mathbf{v}/2$. When $f_B(\mathbf{v}) \neq -\mathbf{v}$ then we can set $\mathbf{w} = \mathbf{v} - f_B(\mathbf{v})$ and see that

$$\begin{aligned} f_B(\mathbf{w}) &= f_B(\mathbf{v} - f_B(\mathbf{v})) \\ &= f_B(\mathbf{v}) - f_B^2(\mathbf{v}) \\ &= f_B(\mathbf{v}) - \mathbf{v} = -\mathbf{w} \end{aligned}$$

Taking components of $\mathbf{v}$ along $\mathbf{w}$ gives us the vector $(\mathbf{v}, \mathbf{w}/\|\mathbf{w}\|^2)$ and our isometry becomes the glide reflection (2$\mathbf{a}$+$\mathbf{b}$, B) where $2\mathbf{a} = (\mathbf{v}, \mathbf{w}/\|\mathbf{w}\|^2)\mathbf{w}, \mathbf{b} = \mathbf{v} - 2\mathbf{a}$ □

The groups which arise from symmetry groups of two dimensional repeating patterns are called ***wallpaper patterns***.

Define $\pi : E_2 \rightarrow O_2$ by $\pi(\mathbf{v}.M) = M$. We can easily see that π is a homomorphism. IF G is a subgroup of E_2, we write H for $G \cap T$ and J for $\pi(G)$, calling H the translation subgroup of G and J the point group of G

Theorem

Let L be the orbit of the origin under action of H on $\mathbb{R}^2$. Select a non-zero vector $\mathbf{a}$ of minimum length in L, then choose a second vector $\mathbf{b}$ from L which is skew to $\mathbf{a}$ and whose length is as small as possible. The set $\mathbf{L}$ is the lattice spanned by $\mathbf{a}$ and $\mathbf{b}$, i.e. L is span($\mathbf{a}$,$\mathbf{b}$)

Proof: The correspondence $(\mathbf{v}, I) \rightarrow \mathbf{v}$ is an isomorphism between T and the additive group $\mathbb{R}^2$ which sends H to L. Therefore, L is a subgroup of $\mathbb{R}^2$ and every point $m\mathbf{a} + n\mathbf{b} \in L$. Using these points, we can divide the plane into parallelograms. Choose an $x \in L$ but not in the lattice. Choose a parallelogram which contains $\mathbf{x}$ and a corner $\mathbf{c}$ which is as close to $\mathbf{x}$ as possible. The vector **x-c** is not the zero vector, it is not equal to $\mathbf{a}$ or $\mathbf{b}$ and its length is less than $\|\mathbf{b}\|$. But $\mathbf{x} - \mathbf{c} \in L$, since $\mathbf{x}$ and $\mathbf{c}$ are in L. So we cannot have $\|\mathbf{x} - \mathbf{c}\| < \|\mathbf{a}\|$ since $\mathbf{a}$ is supposed to be of minimum length in L. On the other hand, if $\|\mathbf{a}\| \leq \|\mathbf{x} - \mathbf{c}\| < \|\mathbf{b}\|$ then $\mathbf{x} - \mathbf{c}$ must be skew to $\mathbf{a}$ and contradicts our choice of $\mathbf{b}$. Therefore, no such point $\mathbf{x}$ can exist and $L = \text{span}(\mathbf{a}, \mathbf{b})$□

We can classify lattices into 5 different types according to the shape of the parallelogram determined by $\mathbf{a}$ and $\mathbf{b}$.

1. *Oblique:* $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$
2. *Rectangular:*$\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| = \|\mathbf{a}+\mathbf{b}\|$
3. *Centered Rectangular:*$\|\mathbf{a}\| < \|\mathbf{b}\| = \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$
4. *Square:*$\|\mathbf{a}\| = \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| = \|\mathbf{a}+\mathbf{b}\|$
5. *Hexagonal*$\|\mathbf{a}\| = \|\mathbf{b}\| = \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$

The point group J acts on the lattice L.

Proof: J is a subgroup of O_2 which acts on the plane in a usual way. If $M \in J$ an if $x \in L$, we need to show that $f_M(\mathbf{x}) \in L$. Suppose $\pi(g) = M$ where $g = (\mathbf{v}, M)$ and let $\tau = (\mathbf{x}, I)$. Since H is the kernel of the homomorphism $\pi : G \to J$, it is a normal subgroup of G, and therefore $g\tau g^{-1}$ lies in H. But,

$$\begin{aligned} g\tau g^{-1} &= (\mathbf{v}, M)(\mathbf{x}, I)(-f_M^{-1}(\mathbf{v}), M^{-1}) \\ &= (\mathbf{v}, M)(\mathbf{x} - f_M^{-1}(\mathbf{v}), M^{-1}) \\ &= (\mathbf{v} + f_M(\mathbf{x} - f_M^{-1}(\mathbf{v})), MM^{-1}) \\ &= (\mathbf{v} + f_M(\mathbf{x}) - \mathbf{v}, I) \\ &= (f_M(\mathbf{x}), I) \end{aligned}$$

So, $f_M(\mathbf{x})$ is a point of the lattice L.

Theorem

The order of a rotation in a wallpaper group is only 2,3,4 or 6

Proof: Every rotation in G has a finite order because the point group is finite. If we have a rotation of order q, then the rotation matrix is

$$A = \begin{bmatrix} \cos\frac{2\pi}{q} & -\sin\frac{2\pi}{q} \\ \sin\frac{2\pi}{q} & \cos\frac{2\pi}{q} \end{bmatrix}$$

where $A \in J$. Now J acts on L, so $f_A(\mathbf{a})$ lies in L. Suppose q is greater than 6. Then $\frac{2\pi}{q} < 60°$ and $f_A(\mathbf{a}) - \mathbf{a}$ is a vector in L which is shorter than $\mathbf{a}$. This contradicts our initial choice for $\mathbf{a}$. If $q - 5$, the angle between $f_A^2(\mathbf{a})$ and $-\mathbf{a}$ is $36°$. Now, $f_A^2(\mathbf{a}) + \mathbf{a} \in L$ and is shorter than $\mathbf{a}$ which is again a contradiction.$\square$

There are 17 different wallpaper groups. We will now prove this fact and classify these groups. We will first describe the notation which we will be using during this proof. Each wallpaper group is represented by p,c,m,g and the integers

1,2,3,4,6. The letter p refers to the lattice and stands for the word *primitive*. A primitive lattice is made up of primitive cells which are cells which are basic parallelograms not containing any interior lattice points. In the centred rectangular case, we take a non-primitive cell and its center as a basic building block and use the letter c to denote the resulting centered lattice. Here m denotes reflection and g denotes glide reflection and the numbers indicate the order of rotation. Rotation of order 2 are called half turns. Below are the images for 17 wallpaper groups

Case(a) The lattice is *oblique*. Then the only orthogonal transforming preserving L are the identity and rotation by π about the origin. Therefore, the point group of G is a subgroup of $\{\pm I\}$.

(p1) Consider J to only have I, then G is generated by two independent translations. It has elements $(m\mathbf{a}+n\mathbf{b}, I)$.

(p2) Here, take $J = \{\pm I\}$. So, G contains a *half turn* and we can take the fixed point of this half turn as origin so that $(\mathbf{0}, -I) \in G$. The two cosets H and $H(\mathbf{0}, -I)$ together form a union which is a subgroup of E_2. The elements of G which are not translations are in $H(\mathbf{0}, -I)$ and we have that

$$(m\mathbf{a}+n\mathbf{b}, I)(\mathbf{0}, -I) = (m\mathbf{a}+n\mathbf{b}, -I)$$

where $m, n \in \mathbb{Z}$. This means that all half turns are about the points $\frac{1}{2}m\mathbf{a}+\frac{1}{2}n\mathbf{b}$

Case(b) The lattice is *rectangular*. This means there are 4 orthogonal transformations which preserve L, which are I, a half turn about $\mathbf{0}$, reflection in x-axis and reflection in y-axis. So, the point group of G is subgroup of $\{I, -I, B_0, B_\pi\}$.

(pm) J is $\{I, B_0\}$ and G contains a *reflection* along a horizontal axis

(pg) Suppose J is $\{I, B_0\}$, but there are no reflections in G. The G has a glide reflection whose line is horizontal and it passes through origin. If we applied glide reflection twice, it gives a translation, hence our glide has the form $(\frac{1}{2}k\mathbf{a}, B_0)$ for some integer k. If k is even then we have $(-\frac{1}{2}k\mathbf{a}, I)$ is a translation in G and the reflection $(\mathbf{0}, B_0)$ is equivalent to $(-\frac{1}{2}k\mathbf{a}, I)(\frac{1}{2}k\mathbf{a}, B_0)$ and this belongs to G contradicting our initial assumption. So, k is odd. Now $(\frac{1}{2}\mathbf{a}, B_0) = (-\frac{1}{2}(k-1)\mathbf{a}, I)(\frac{1}{2}k\mathbf{a}, B_0)$ lies in G. The non-translation elements of G have the form $(m\mathbf{a}+n\mathbf{b}, I)(\frac{1}{2}\mathbf{a}, B_0) = ((m+\frac{1}{2})\mathbf{a}+n\mathbf{b}, B_0)$ where $m, n \in \mathbb{Z}$. These are glides along horizontal lines which pass through lattice points or lie midway between lattice points. The length of each glide is an odd multiple of $\frac{1}{2}\mathbf{a}$.

Now, we assume that the point group is all of $\{I, -I, B_0, B_\pi\}$ for all the next groups here. There are three possibilities either both, just one or neither of B_0, B_π can be realized by reflections in G.

(p2mm) Here G contains a reflection about horizontal axis and a reflection about the vertical axis

(p2mg) Suppose G contains a reflection in a horizontal mirror but doesn't contain a reflection in the vertical mirror. Then B_π must be realized in G by a vertical glide reflection. Taking the origin as the point of intersection between horizontal mirror and vertical glide line, and the restrictions of pg,

allow us to assume that $(\mathbf{0}, B_0$ and $(\frac{1}{2}\mathbf{b}, B_\pi)$ belong to G. Here also, the product $(\frac{1}{2}\mathbf{b}, B_\pi)(\mathbf{0}, B_0) = (\frac{1}{2}\mathbf{b}, -I)$ is the half turn about $\frac{1}{4}\mathbf{b}$. The right cosets $H, H(\mathbf{0}, B_0), H(\frac{1}{2}\mathbf{b}, B_\pi), H(\frac{1}{2}\mathbf{b}, -I)$ together form the group G. A typical element of the second coset here has the form $(m\mathbf{a}+n\mathbf{b}, I)(\mathbf{0}, B_0) = (m\mathbf{a}+n\mathbf{b}, B_0)$ where m and n are integers. When $m = 0$ then this isometry is a reflection in the horizontal mirror which either passes through lattice points or lies midway between them. If m is not zero, the mirrors change to glide lines and translation part of the glide is $m\mathbf{a}$. The third coset contains the elements $(m\mathbf{a}+(n+\frac{1}{2})\mathbf{b}, B_\pi)$ which are all vertical glides whose lines pass through lattice points or lie midway between them. Finally $H(\frac{1}{2}\mathbf{b}, -I)$ consists of the half turns centered at the points $\frac{1}{2}m\mathbf{a} + \frac{1}{2}(n + \frac{1}{2})\mathbf{b}$. Interchanging horizontal and vertical here leads to a group isomorphic to p2mg.
(p2gg) Here there are no reflections in G.

Case (c) The lattice of G is *centered rectangular.* The orthogonal transformations preserving L are the same as in the rectangular case. Therefore, the point group must again be a subgroup of $\{ I, -I, B_0, B_\pi \}$. We discover two new groups.
(cm) Suppose J is $\{ I, B_0 \}$ and that $(\mathbf{v}, B_0$ realizes B_0 in G. This isometry is either a reflection in horizontal mirror or glide along horizontal line. Choose a point on the mirror or glide line as origin, so $2\mathbf{v}$ is a multiple of $\mathbf{a}$, and we see that the vertical direction is determined by the vector (**2b-a**)
(i) If $2\mathbf{v} = k\mathbf{a}$ and k is even, the reflection $(\mathbf{0}, B_0) = (-\frac{1}{2}k\mathbf{a}, I)(\frac{1}{2}k\mathbf{a}, B_0)$ belongs to G. The elements of G which are not translations have the form $(m\mathbf{a} + n\mathbf{b}, B_0) = ((m + \frac{1}{2}n)\mathbf{a} + \frac{1}{2}n(2\mathbf{b} - \mathbf{a}, B_0)$ where $m, n \in \mathbb{Z}$. Taking n to be evene and $m = -\frac{1}{2}n$ produces all the reflections in horizontal mirrors which pass through lattice points. If n is even but $m \neq -\frac{1}{2}n$, these mirrors change to glide lines, the translation part of each glide being a multiple of $\mathbf{a}$. If n is odd then we get glides along lines which lie midway between lattice points. The translation part of each of these glides is an odd multiple of $\frac{1}{2}\mathbf{a}$.
(ii)If k is odd then $(\frac{1}{2}(2\mathbf{b} - \mathbf{a}, B_0) = (-\frac{1}{2}(k+1)\mathbf{a} + \mathbf{b}, I)(\frac{1}{2}k\mathbf{a}, B_0$ lies in G. This is again a reflection and shifting the origin onto its mirror leads back to (i).
Substituting $\{ I, B_\pi \}$ as point group instead of $\{ I, B_0 \}$ leads to a group which is isomorphic to cm.
(c2mm) J is $\{ I, -I, B_0, B_\pi \}$. From above we see that both B_0 and B_π can be realized by reflections in G.

Case (d) The lattice of G is *square.* Then the group of orthogonal transformations which preserves L is the dihedral group of order 8 generated by $A\frac{\pi}{2}$ and B_0. The point group J is a subgroup of this group and to get something new we must include $A\frac{\pi}{2}$
(p4) Here J is generated by $A\frac{\pi}{2}$
(p4mm) Here J is generated by $A\frac{\pi}{2}$ and B_0, and B_0 can be realized by a reflection in G.
(p4gm) Suppose J is generated by $A\frac{\pi}{2}$ and B_0 but B_0 cannot be realized by a reflection. Choose the fixed point of a rotation of order 4 as origin,

so that $(\mathbf{0}, A\frac{\pi}{2})$ belongs to G, and let $(\lambda\mathbf{a} + \mu\mathbf{b}, B_0)$ realize B_0. Squaring $(\lambda\mathbf{a} + \mu\mathbf{b}, B_0)$ gives $(2\lambda\mathbf{a}, I)$, so 2λ is an integer. If 2λ is even the reflection $(\mu\mathbf{b}, B_0) = (-\lambda\mathbf{a}, I)(\lambda\mathbf{a} + \mu\mathbf{b}, B_0)$ lies in G and we have a contradiction. So 2λ must be odd and $(\frac{1}{2}\mathbf{a} + \mu\mathbf{b}, B_0) = ((\frac{1}{2} - \lambda)\mathbf{a}, I)(\lambda\mathbf{a} + \mu\mathbf{b}, B_0)$ is an element of G. Also $(\mathbf{0}, A\frac{\pi}{2})(\frac{1}{2}\mathbf{a} + \mu\mathbf{b}, B_0) = (\frac{1}{2}\mathbf{b} - \mu\mathbf{a}, B\frac{\pi}{2})$ and $(\frac{1}{2}\mathbf{b} - \mu\mathbf{a}, B\frac{\pi}{2})^2 = ((\frac{1}{2} - \mu)(\mathbf{a} + \mathbf{b}), I)$ showing $\frac{1}{2} - \mu$ to be an integer. We conclude that the glide $(\frac{1}{2}\mathbf{a} + \frac{1}{2}\mathbf{b}, B_0) = (\frac{1}{2} - \mu)\mathbf{b}, I)(\frac{1}{2}\mathbf{a} + \mu\mathbf{b}, B_0)$ belongs to G. The right cosets $H(\mathbf{0}, I), H(\mathbf{0}, -I), H(\mathbf{0}, A\frac{\pi}{2}), (\mathbf{0}, A\frac{3\pi}{2}), H(\frac{1}{2}\mathbf{a}+\frac{1}{2}\mathbf{b}, B_0), H(\frac{1}{2}\mathbf{a}+\frac{1}{2}\mathbf{b}, B_{\frac{\pi}{2}}), H(\frac{1}{2}\mathbf{a} + \frac{1}{2}\mathbf{b}, B_\pi), H(\frac{1}{2}\mathbf{a} + \frac{1}{2}\mathbf{b}, B_{\frac{3\pi}{2}})$ make up G. It is easy to recognise their elements geometrically. For example, a typical member of $H(\frac{1}{2}\mathbf{a}+\frac{1}{2}\mathbf{b}, B\frac{\pi}{2})$ has the form $((m+\frac{1}{2})\mathbf{a}+(n+\frac{1}{2})\mathbf{b}, B_{\frac{\pi}{2}}) = (\frac{1}{2}(m+n+1)(\mathbf{a}+\mathbf{b}) + \frac{1}{2}(m-n)(\mathbf{a}-\mathbf{b}), B_{\frac{\pi}{2}}$. Taking $m + n + 1 = 0$ we get all the reflections in mirrors tilted at 45° to the horizontal which pass midway between lattice points. When $m + n + 1$ is non-zero and $m - n$ is even, we have glides along lines of gradient one which pass through lattice points. The coset $H(\mathbf{0}, -I)$ on the other hand contains all the half turns $(m\mathbf{a} + n\mathbf{b}, -I)$ centered at the points $\frac{1}{2}m\mathbf{a} + \frac{1}{2}n\mathbf{b}$.

Case(e) The lattice of G is *hexagonal.* Then the point group must be in the dihedral group of order 12 generated by $A_{\frac{\pi}{3}}$ and B_0. We are led to a new wallpaper group when J contains rotations of order 3 or 6.
(p3) J is generated by $A_{\frac{2\pi}{3}}$
(p3m1) J is generated by $A_{\frac{2\pi}{3}}$ and B_0
(p31m) Suppose J is generated by $A_{\frac{2\pi}{3}}$ and $B_{\frac{\pi}{3}}$. Choose the fixed point of a rotation of order 3 as origin, so that $(\mathbf{0}, A_{\frac{2\pi}{3}})$ belongs to G, and let $(\lambda\mathbf{a}+\mu\mathbf{b}, B_{\frac{\pi}{3}})$ in G. Now $(\lambda\mathbf{a} + \mu\mathbf{b}, B_{\frac{\pi}{3}})^2 = ((\lambda + \mu)(\mathbf{a} + \mathbf{b}), I)$ so $\lambda + \mu$ is an integer. Also, $(\mathbf{0}, A_{\frac{2\pi}{3}})(\lambda\mathbf{a} + \mu\mathbf{b}, B_{\frac{\pi}{3}}) = (\lambda(\mathbf{b} - \mathbf{a}) - \mu\mathbf{a}, B_\pi)$ and $(\lambda(\mathbf{b} - \mathbf{a}) - \mu\mathbf{a}, B_\pi)^2 = (\lambda(2\mathbf{b}-\mathbf{a}), I)$ showing that λ is an integer. Therefore, both λ and μ are integers and the reflection. $(\mathbf{0}, B_{\frac{\pi}{3}} = (-\lambda\mathbf{a} - \mu\mathbf{b}, I)(\lambda\mathbf{a} + \mu\mathbf{b}, B_{\frac{\pi}{3}})$ belongs to G. The elements of G have the form $(m\mathbf{a}+n\mathbf{b}, M)$ where $m, n \in \mathbb{Z}$ and M is one of the matrices $I, A_{\frac{2\pi}{3}}, A_{\frac{3\pi}{3}}, A_{\frac{\pi}{3}}, A_{\frac{5\pi}{3}}, A_\pi$.
(p6) J is generated by $A_{\frac{\pi}{3}}$
(p6mm) J is generated by $A_{\frac{\pi}{3}}$ and B_0.

These 17 groups listed out are all unique. We will show this for each case. We only need to concern ourselves with groups whose point groups are similar, so we begin with a summary of the point groups. Let J denote the point group.

J is trivial $\to G \cong$ p1
$J \cong \mathbb{Z}_2 \to G$ is p2, pm, cm or pg
$J \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ is p2mm, p2mg, c2mm or p2gg
$J \cong \mathbb{Z}_3 \to G \cong$ p3
$J \cong \mathbb{Z}_4 \to G \cong$ p4
$J \cong \mathbb{Z}_6 \to G \cong$ p6
$J \cong D_3 \to G$ is p3ml or p3lm
$J \cong D_4 \to G$ is p4mm or p4gm

$J \cong D_6 \to G \cong$ p6mm

To prove the uniqueness, we will use the properties that isomorphism between wallpaper groups sends translations to translations, rotations to rotations, reflections to reflections, and glides to glides
No two of* p2, pm, pg, cm *are isomorphic

Among these only p2 contains rotations, so it cannot be isomorphic to any others. Of the three remaining groups, pg does not contain reflection, so it is not isomorphic to pm or cm. Let us take a glide in pm and write it as reflection followed by a translation, then both the reflection and the translation belong to pm. But this is not true for cm as it contains glides whose constituent parts do not lie in cm. So, pm and cm are not isomorphic.

No two of* p2mm, p2mg, c2mm or p2gg *are isomorphic

Here p2gg is the only one out of the 4 which does not contain reflection, so it cannot be isomorphic to others. Only p2mm contains constituents of its glides, so it cannot be isomorphic to p2mg or c2mm. In p2mg, product of two reflections is a translation because the mirror are horizontal, however c2mm has horizontal and vertical mirrors and the product of these elements is a half turn. So, p2mg and c2mm are not isomorphic

p3ml *is not isomorphic to* p3lm

p3lm has rotation of 3 which is a product of two reflections but this is not true for p3ml. Therefore, they aren't isomorphic

p4mm *is not isomorphic to* p4gm

p4mm has rotation of order 4 which can be written as a product of two reflections and both of them belong to p4mm. The corresponding statement is not true for p4gm. Therefore, p4mm and p4gm are not isomorphic

2.2.6 An overview of Ring axioms, Principal Ideals and Integral Domains

We will now expand from the Group Axioms to other Algebraic systems. These systems are important as they serve building blocks for what we call Modern Algebra. The abstract concept of a group has its origins in the set of mappings, or permutations, of a set onto itself. In contrast, ring stem from another and more familiar place, the set of integers. While in group, we define our own Group Operations, we see that in a Ring there are two binary operations defined which are familiar to us. The following are the axioms of a Ring.

Ring Axioms

A non-empty set R is said to be an *associative ring* if in R there are defined two operations denoted by $+$ and $\cdot$ respectively, such that for all $a, b, c \in R$

- $a + b \in R$
- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- $\exists\, 0 \mid a + 0 = a = 0 + a$
- $\exists - a \mid (-a) + a = a + (-a) = 0$
- $a \cdot b \in R$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$

Essentially, what we are saying here is that $(R, +)$ forms an abelian group and $\cdot$ is a binary operator similar to multiplication in integers.

Examples

- R is the set of integers; $+$ is addition and $\cdot$ is multiplication of integers. R is a commutative ring with unit element
- R is the set of even integers under the usual operations of addition and multiplication. R is a commutative ring but has no unit element.
- R is the set of integers mod p where p is any number.

An **ideal** I of ring R is a subset of R which has the property that it is closed under addition and for any $r \in R$ and $a \in I$, $r \cdot a \in I$. Consider R is a commutative ring, then $a \in R - \{0\}$ is said to be a **zero-divisor** if there exists $a, b \in R - \{0\}$ such that $ab = 0$, i.e. a and b are non-zero elements which multiply to give 0.

Integral Domain

A commutative ring is an *integral domain* if it has no zero-divisors

The ring of integers, naturally, is an example of an integral domain.

While not related to our goal of understanding the Structure Theorem of Modules over PID, we will prove an interesting lemma.

Lemma

A finite integral domain is a field

Proof: An integral domain is a commutative ring such that $ab = 0$ if and only if at least one of a or b is itself 0. A field can be described as a commutative ring where the non-zero elements of a ring form an abelian group under multiplication. Let D be a finite integral domain. To see that D is a field, we need to show that

1. Produce an element $1 \in D$ such that $a \cdot 1 = a$ for every $a \in D$
2. For every element $a \neq 0 \in D$, there is an element b such that $a \cdot b = 1$

Let $x_1, x_2 ..., x_n$ be all the elements of D, and suppose that $a \neq 0 \in D$. Consider the elements $x_1 a, x_2 a, ..., x_n a$; they are all in D. We claim that they are all distinct. Suppose $x_i a = x_j a$ for $i \neq j$ then $(x_i - x_j)a = 0$ but $a \neq 0$ so this is a contradiction. Thus $x_1 a, x_2 a ..., x_n a$ are n distinct elements lying in D, which has exactly n elements. According to the Pigeon Hole principle, these must account for every element in D.

A **Principal Ideal** is an Ideal which is generated by a single element $a \in R$. Generated by a single element here means that $I = \langle a \rangle = \{\, ra \mid \forall r \in R \,\}$.

2.2.7 Modules over PID

Modules can be thought of as a generalization for a vector space, instead of the scalars lying in a field, we assume that they lie in a ring. PID is an abbreviation for Principal Ideal Domain. A ring R is called a PID if R is an integral domain and every ideal I of R is finitely generated.

$R-$module

Let R be any ring, a non-empty set M is said to be an $R-$module if M is an abelian group under an operation $+$ such that for every $r \in R$ and $m \in M$ there exists an element rm such that

- $r(a + b) = ra + rb$
- $r(sa) = (rs)a$
- $(r + s)a = ra + sa$

for all $a, b \in M$ and $r, s \in R$

An additive subgroup A of the $R-$module M is called a submodule of M if whenever $r \in R$ and $a \in A$ then $ra \in A$.
The main goal of this section is to prove structure theorem for finitely generated $R-$modules where R is a Principal Ideal Domain. This theorem when applied

to ring of integers $\mathbb{Z}$, we obtain a proof of Fundamental Theorem for Finitely Generated Abelian Groups which we proved in Section 2.2.3
Some $R-$module M is said to be a Noetherian $R-$module if there are no infinite increasing chains of submodules, i.e., whenever $M_1 \subseteq M_2 \subseteq \ldots$ is an increasing chain of submodules of M, there exists an integer $m \in \mathbb{Z}^+$ such that $\forall k \geq m$, $M_k = M_n$. The ring R is said to be Noetherian if it is Noetherian as a module over itself, as in there are no infinite increasing chains of left ideals in R.

Theorem

Let R be a ring and let M be a $R-$module. Then the following are equivalent.

1. M is a Noetherian $R-$module
2. Every nonempty set of submodules of M contains a maximal element under inclusion
3. Every submodule M is finitely generated

Proof: $\{1 \implies 2\}$ Assume M is Noetherian and let Σ be some nonempty collection of submodules of M. Choose any $M_1 \in \Sigma$. If M_1 is a maximal element of Σ, 2 holds. If M_1 is not maximal, then there exists some $M_2 \in \Sigma$ such that $M_1 \subset M_2$. If M_2 is maximal in Σ, 2 holds. Repeating this argument, we see that if 2 fails, we can produce by the Axiom of Choice an infinite strictly increasing chain of elements of Σ, contrary to 1.

$\{2 \implies 3\}$ Assume 2 holds and let N be some submodule of M. Let Σ be a collection of every finitely generated submodule of N. Since $\{0\} \in \Sigma$, this collection is non-empty. By 2, Σ contains a maximal element, say N'. If $N \neq N'$, take $x \in N - N'$. Since $N' \in \Sigma$, the submodule N' is finitely generated by assumption, hence the submodule generated by N' and x is finitely generated. This contradicts maximality of N', so $N = N'$ is finitely generated.

$\{3 \implies 1\}$ Assume 3 holds and let $M_1 \subseteq M_2 \subseteq \ldots$ be a chain of submodules of M. Let $N = \bigcup_{i=1}^{\infty} M_i$ and see that N is a submodule. By 3, N is finitely generated by $a_1, \ldots a_n$. Since $a_i \in N \quad \forall i, 1 \leq i \leq n$, each a_i lies in one of the submodules in the chain, say M_{j_1}. Let $m = \max\{j_1, \ldots, j_n\}$. Then $a_i \in M_m$ for all i so they module generated is contained in M_m, i.e. $N \subseteq M_m$. This implies $M_m = N = M_k$ for all $k \geq m$ which proves one. □

Corollary: If R is a PID, then every nonempty set of ideals of R has a maximal element and R is a Noetherian ring.
This follows from the fact that R satisfies Condition 3, so it is Noetherian.

Proposition: Let R be an integral domain and let M be a free $R-$module of rank $n < \infty$. Then any $n+1$ elements of M are $R-$linearly dependent. In other words, for any $y_1 \dots y_{n+1} \in M$ there are elements $r_1, \dots, r_{n+1} \in R$ not all zero such that

$$r_1 y_1 + \cdots + r_{n+1} y_{n+1} = 0$$

Proof: Embed R in its quotient field F. Since $M \cong \underbrace{R \oplus R \cdots \oplus R}_{n-times}$ we obtain $M \subseteq \underbrace{F \oplus F \cdots \oplus F}_{n-times}$. The latter is an $n-$dimensional vector space over F so any $n{+}1$ elements of M and $F-$linearly dependent. By clearing denominators of the scalars, we obtain an $R-$linear dependence relation among the $n+1$ elements of M.

Theorem

Let R be a PID and M be a free $R-$module of finite rank n and N is a submodule of M. Then

- N is free of rank $m, m \leq n$ and
- there exists a basis $y_1, \dots y_n$ of M so that $a_1 y_1, \dots a_m y_m$ is a basis of N where $a_1, \dots, a_m$ are non zero elements of R with the divisibility relations $a_1 \mid a_2 \mid \cdots \mid a_m$. Since R is a PID, this ideal must be principal, say it is generated by $a_\varphi \in R$. Let $\Sigma = \{\, \varphi(N) \mid \varphi \in \mathrm{Hom}_R(M, R) \,\}$, this is the collection of all principal ideals in R obtained from the homomorphism. By Corollary above, Σ has at least one maximal element

Proof: The theorem is trivial for $N = \{\, 0 \,\}$, so we take a non-trivial case. For some homomorphism φ of M into R, the image $\varphi(N)$ of N is a submodule of R, and an ideal in R, which must be generated by a single element, say a_φ as R is PID. Take $\Sigma = \{\, \langle a_\varphi \mid \varphi \in \mathrm{Hom}_R(M, R) \,\}$ to be the collection of principal ideals obtained from these homomorphisms. Σ is not empty since $\{\, 0 \,\} \in \Sigma$ where φ is trivial homomorphism. By the Corollary above, Σ has at least one maximal element, say $v(N) = \langle a_v \rangle$. Let $a_1 = a_v$ for this maximal element, and let $y \in N$ be such that $v(y) = a_1$. We now focus on showing a_1 is nonzero. Let $x_1, \dots x_n$ be a basis of the free module M and let $\pi_i \in \mathrm{Hom}_R(M, R)$ be the natural projection homomorphism onto the i^{th} coordinate with respect to this basis. Since N is nonempty, there is an i such that $\pi_i(N) \neq 0$, so Σ contains a nontrivial element. Since a_1 is the maximal ideal (generating) element here, so $a_1 \neq 0$.

Let d be a generated for the principal ideal generated by a_1 and $\varphi(y)$. Then d divides both a_1 and $\varphi(y)$ and $d = r_1 a_1 + r_2 \varphi(y)$. Consider the homomorphism $\psi : M \to R$ such that$\psi = r_1 v + r_2 \varphi$. Then $\psi(y) = (r_1 v_1 + r_2 \varphi)(y) = r_1 a_1 + r_2 \varphi(y) = d$ so that $d \in \varphi(N)$, so $\langle d \rangle \subseteq \psi(N)$ and $\langle a_1 \rangle \subseteq \langle d \rangle \subseteq \psi(N)$ by maximality of a_1, we have $\langle a_1 \rangle = \langle d \rangle = \psi(N)$. So $\langle a_1 \rangle = \langle d \rangle$ shows that $a_1 \mid \varphi(y)$ since d divides $\varphi(y)$. We now apply this to projection homomorphism π_i, we see that a_1 divides $\pi_i(y)\ \forall i$. Write $a_1 b_i$ for some $b_i \in R$, $1 \leq I \leq n$ and define

$$y_1 = \sum_{i=1}^{n} b_i x_i$$

. We see that $a_1 y_1 = y$. Since $a_1 = v(y) = v(a_1 y_1)$ and $a_1 \neq 0$ in integral domain R. So $v(y_1) = 1$.

Now we see that the element $y_1$is taken as one element in a basis for M and that $a_1 y_1$ can be taken as one element in a basis for N, i.e. $M = Ry_1 \oplus \text{ker } v$ and $M = Ra_1 y_1 \oplus (N \cap \text{ker } v)$. To see the first equality, consider $x \in M$ and write $x = v(x)y_1 + (x - v(x)y_1)$. Since $v(x - v(x)y_1) = v(x) - v(x)v(y_1) = v(x) - v(x) \cdot 1 = 0$. So $x - v(x)y_1 \in \text{ker } v$. This shows that any element of M can be written as a sum of Ry_1 and ker v. To see it is direct sum, take an element $ry_1 \in \text{ker } v$, then $0 = v(ry_1) = rv(y_1) = r$ which shows that $ry_1 = 0$. This proves the first equality. To show second equality, observe that $v(x')$ is divisible by a_1 for every $x' \in N$ by definition of a_1 as a generator. If we write $v(x') = ba_1 \;\; b \in R$, then $x' = v(x')y_1 + (x' - v(x')y_1) = ba_1 y_1 + (x' - ba_1 y_1)$ where $(x' - ba_1 y_1) \in \text{ker } v$ and is an element of N. This shows that $N = Ra_1 y_1 + (N \cap \text{ker } v$. This being a direct sum follows as a special case from the first equality.

We now have all the tools at our disposal to prove this theorem through induction arguments.

For part (1), consider rank m of N. If $m = 0$, then N is a torsion module, hence $N = 0$ since a free module is torsion free, so (1) holds trivially. Now take $m > 0$. Since we showed above that the sum of N is direct, we see that $N \cap \text{ker } v$ has rank $m - 1$. By induction, $N \cap \ker v$ is a free $R-$module of rank $m - 1$. Again by directness of sum of N, we see that adjoining $a_1 y_1$ to some basis of $N \cap \text{ker } v$ gives a basis of N, so N is free of rank m, which proves (1)

For part (2), consider the rank n of M. Applying (1) to the submodule $\ker v$ shows that this submodule is free, and because the sum of M is direct, it is free of rank $n - 1$. By induction assumption applied to module $\ker v$, its submodule $\ker v \cap N$, we see that there is a basis $y_2 \dots y_n$ of $\ker v$ such that $a_2 y_2 \dots a_m y_m$ is a basis of $N \cap \ker v$ for some elements $a_1 \dots a_m \in R$ with $a_2 \mid \cdots \mid a_m$, Since sums of N and M are direct, $y_1 \dots y_n$ is a basis for M and $a_1 y_1 \dots a_m y_m$ is a basis for N. To complete the induction, we show that $a_1 \mid a_2$. Define a homomorphism $\varphi : M \to R$ by defining $\varphi(y_1) = \varphi(y_2) = 1$ and $\varphi(y_i) = 0$ for the rest. Then for this homomorphism φ we have $a_1 = \varphi(a_1 y_1)$ so $\langle a_1 \rangle \subseteq \varphi(N)$. By maximality of $\langle a_1 \rangle$ in Σ, it follows that $\langle a_1 \rangle = \varphi(N)$. Since $a_2 = \varphi(a_2 y_2) \in \varphi(N)$ then we have $a_2 \in \langle a_1 \rangle$, i.e. $a_1 \mid a_2$. This completes the proof of the theorem.

Now we have everything required to prove the Structure Theorem of Modules over PID.

Fundamental Theorem; Invariant Factor Form

Let R be a PID and let M be a finitely generated $R-$module. Then

1. $M \cong R^r \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle$ where $a_1 \mid \cdots \mid a_m$
2. M is torsion free iff M is free
3. $\mathrm{Tor}(M) \cong R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle$

Proof: The module M can be generated by a finite set of elements by assumption, so let $x_1, \ldots, x_n$ be the set of generators of M , W.L.O.G. of minimal cardinality. Let R^n be the free module of rank n with basis $b_1, \ldots, b_n$ and define the homomorphism $\pi : R^n \to M$ by defining $\pi(b_i) = x_i$ for all i, which is automatically subjective since $x_1 \ldots x_n$ generate M. By the First Isomorphism Theorem for modules, we have $R^n/\ker\pi \cong M$. Now, considering R^n and submodule $\ker\pi$ we can choose another basis $y_1 \ldots y_n$ of R^n, so that $a_1y_1 \ldots a_my_m$ is a basis for $\ker\pi$. This implies

$$M \cong R^n/\ker\pi = (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m)$$

. To identify the quotient on the right hand side we use the natural subjective $R-$module homomorphism.

$$Ry_1 \oplus \cdots \oplus Ry_n \to R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle \oplus R^{n-m}$$

that maps $\alpha_i y_i$ to $\alpha_i \mod a_1$ for $1 \leq i \leq m$ and α_i for $m+1 \leq i \leq n$. The kernel of this map is clearly the set of elements where a_i divides α_i for $1 \leq i \leq m$. Hence we obtain

$$M \cong R^{n-m} \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_m\rangle$$

If a is unit in R then $R/\langle a\rangle = 0$, so in this direct sum we may remove any of the initial a_i which are units. This gives the decomposition in (1).

Since $R/\langle a\rangle$ is a torsion $R-$module for any nonzero element $a \in R$, (1) implies M is a torsion free module iff $M \cong R^r$ which is (2). (3) is a consequence from the definition since the annihilator of $R/\langle a\rangle$ is evidently the ideal $\langle a\rangle$.□

Tbe integer r here is called the *free rank* of M and the elements $a_1 \ldots a_m \in R$ are called the invariant factors.

Fundamental Theorem; Elementary Divisor Form

Let R be a PID and let M be a finitely generated $R-$module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of primes in R, i.e.

$$M \cong R^r \oplus R/\langle p_1^{\alpha_1} \rangle \oplus \cdots \oplus R/\langle p_t^{\alpha_t} \rangle$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are positive powers of(not necessarily distinct) primes in R.

Suppose a is a nonzero element of the PID R. Since R is also a Unique Factorization Domain, we can write $a = up_1^{\alpha_1} \ldots p_t^{\alpha_s}$ where p_i are distinct primes in R and u is a unit. This factorization is unique up to units, so the ideals $\langle p_i^{\alpha_i} \rangle$ $1 \leq i \leq s$ are uniquely defined. For $i \neq j$ we have $\langle p_i^{\alpha_i} \rangle + \langle p_j^{\alpha_j} \rangle = R$ since the sum of these two ideals is generated by the gcd of them which is 1 for distinct primes. The intersection of all these ideals is the ideal $\langle a \rangle$ where a is lcm$p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Then the Chinese Remainder Theorem shows

$$R/\langle a \rangle \cong \bigoplus_{i=1}^{s} R/\langle p_i^{\alpha_i} \rangle$$

. Applying this to Invariant Factor Form, we obtain $M \cong R^r \oplus R/\langle p_1^{\alpha_1} \rangle \oplus \cdots \oplus R/\langle p_t^{\alpha_t} \rangle$. □

These two theorems end our proof for Structure Theorem for Modules over PID

2.3 Visualizing Symmetries

Our focus on this project was on visualizing symmetries via animations. While tools like TikZ exist and are excellent in creating mathematical shapes, it has limited uses when it comes to animations. There are several tools that can be used to animate 3D objects. Some coding-based tools we can use are Three.js, p5.js, Manim, and Blender. Tools like Three.js and p5.js are JavaScript libraries that are excellent for creating an interactive environment with an easy-to-use and understand structure for those fluent with JavaScript. Manim is a Python library made by Grant Sanderson(YouTube channel:3blue1brown), which was created to aid in creating math educational videos. Due to its simplicity and the popularity of Grant Sanderson, it is very well known for math visualization; however, it has limited use cases in 3-dimensional objects. Blender is an open-source, free-to-use 3D graphics software tool. It can be used for creating animation films, interactive physics. 2D animations and much more. This project focuses on the blender feature, which is the Blender Python API. This is a Python library integrated along with the software, which can help in automating any tool present within Python.

2.3.1 JavaScript Tools

Due to my unfamiliarity with JavaScript, I wasn't able to explore these libraries in-depth. However, we will focus on an overview of p5.js and Three.js. p5.js can be thought of as a digital sketchbook, a simple and accessible point for beginners or people with a non-tech background, such as artists, designers, etc, to create interactive visuals. It prioritizes ease of use and creative expression. For a project on symmetry, p5.js is excellent for visualizing 2D groups. For instance, one could easily draw a regular n-gon and apply the rotations and reflections of the dihedral group D_n, while 3D capabilities are present in p5.js through WebGL, it requires more manual effort. WebGL is a low-level and widely accepted JavaScript API for rendering hardware-accelerated 2D and 3D graphics in a web browser, directly using your computer's GPU. On the other hand, Three.js can be thought of as a gateway into the world of 3D graphics on the web. It helps build immersive 3D worlds, complete with scenes, lighting and cameras.

Here, we will mostly focus on the finite group of SO_3 symmetries. In Three.js, you would define a `Mesh` using `IcosahedronGeometry` and a `Material` , add it to the `Scene` , and then update its `.rotation` property in an `animation loop` . This set of information is called a `scene graph` , which is a tree-like structure containing geometries, materials, lights, and a camera. It is very helpful, especially when it comes to finite groups of SO_3, as there is a `Quaternion` class and methods like `.applyQuaternion()` that make it very straightforward to represent group actions onto 3D objects. The Three.js ecosystem is also very vast. It is useful in various cases, such as 3D data visualisation, physics simulations, and advanced graphics, making it a more industrial-strength tool for dedicated 3D work.

While both libraries render visuals from code, Three.js is more 3D-friendly compared to p5.js, which has more support for 2D visualization. Their working philosophies differ; while p5.js is ideal for creative coding and 2D sketches, Three.js provides a robust framework for building dedicated 3D environments. However, for the specific goal of creating detailed 3D animations of group actions, the learning curve of these libraries and my existing proficiency with Python led to the selection of Blender Python API(BPY), which provided a dedicated 3D environment with powerful, integrated scripting capabilities

2.3.2 Python Tools(Manim)

In this section, we will be focusing on 2 Python libraries in particular, Manim and BPY. Manim is an exceptional tool for creating precise, explanatory animations. The core strength of Manim lies in an easy-to-use, easily understandable, and mathematically accurate approach to visualization. We can define scenes in Python, specifying objects like LaTeX formulas, graphs, and vector fields, and then animate their properties over time. This allows for a level of precision and clarity that is difficult to achieve with traditional animation software. Manim is excellent for visualizing concepts in 2D such as symmetries of a polygon. While it does also show some 3D capabilities, its primary focus remains on 2D and, to some extent, vector fields. Creating and manipulating complex, shaded 3D solids here is less straightforward than in a dedicated 3D modeling environments. Manim has the `Dodecahedron` , `Icosahedron` , `Cube` , `Octahedron` , and `Tetrahedron` classes which create a three-dimensional mathematical object(`Mobject`) representing the respective platonic solids in a `ThreeDScene` , without having to define its vertices and faces manually. However, one major drawback is that due to all the `Polyhedron` defined for visual convenience, they are all *normalized* to appear at a manageable size on the screen. Due to this the proportions of these `Mobjects` are not mathematically equivalent even if they might look the same roughly.

Every Manim animation is contained within a **Scene**. In our Python script, we begin by creating a case that inherits from Manim's base `Scene` class (or `ThreeDScene` for 3D animations). The logic for the animation goes inside a method named `construct(self)` . Running this code, it automatically executes this `construct` method to generate the video detailed in that code block for that scene. The `Scene` can be thought of as a single, continuous shot in a film, The `construct` then would be the script that tells the actors what to do and when. Everything on the screen in a Manim animation is a Mobject. Mobjects are the fundamental building blocks for the scene. These include shapes, text, graphs and 3D shapes etc. The process of building an animation inside the `construct` follows a simple pattern. After defining your Mobjects, you can animate with `self.play()` method. This function takes one or more Animation objects as arguments and renders them over a default duration of 1 second. Some common animations are `Create(my_object)` (draws an object onto the screen), `FadeIn(my_object)` (fades an object into view), `Transform(obj1, obj2)` (morphs one object into another, the `.animate` syntax, `self.wait(duration)` (to pause the animation for a specified number of seconds. Below is a script as an example of what a Manim animation script would look like

```python
from manim import *

class DodecahedronScene(ThreeDScene):
    def construct(self):
        #Set the camera's position
        self.set_camera_orientation(phi=75 * DEGREES, theta=30 *
            DEGREES)

        # Create a Dodecahedron object
        dodec = Dodecahedron(
            edge_config={"color": BLUE, "stroke_width": 3},
        )

        #Add the object to the scene
        self.add(dodec)

        # Animate a rotation of 2*PI (360 degrees) around the Y-axis
        self.play(
            Rotate(dodec, angle=2 * PI, axis=UP),
            run_time=5
        )
        self.wait(1)
```

To turn this script into a video file, we need to run the following command on our terminal `manim -pql my_animation.py DodecahedronScene`

2.3.3 The DNA and RNA of Blender

The `bpy` works as a direct, low-level interface to Blender's core processes and data structures. Every action that can be performed through the GUI has a corresponding `bpy` command. This design principle makes it an amazing tool for precise, data-driven animation. Fundamentally, `bpy` is organized into three modules, `bpy.data` , `bpy.context` and `bpy.ops` .
The `bpy.data` gives direct access to all the raw data within the `.blend` file(.blend is the file extension given to a Blender file). Every element such as objects, meshes, materials, scenes, textures is stored in collections within `bpy.data` . Some collections include

- `bpy.data.objects` : This contains all the objects in the scene. An object can be defined as a container that holds a position, rotation and scale in 3D space. It doesn't contain the geometry itself. For example. `bpy.data.objects['Cube']` would give the object named as "Cube"
- `bpy.data.meshes` : This holds actual geometry data like the vertices, edges and faces. An object in `bpy.data.objects` will have a data property that links to a mesh in `bpy.data.meshes` . This distinction is crucial, as there can be multiple objects that all share and instance the same single mesh data.
- `bpy.data.materials` : Contains all materials, which define the surface appearance of an object(e.g., color, roughness, transparency).
- `bpy.data.scenes` : Contains the scenes of a file. Each scene is a world containing objects and settings.
- `bpy.data.actions` : Holds animation data, such as keyframe information.

Manipulation of data through `bpy.data` is the most direct and efficient way to work. For example, to move an object up by 2 units on the Z-axis, you can write:

```python
import bpy

# Access the object named 'Cube'
cube_obj = bpy.data.objects['Cube']

# Directly modify its location property
cube_obj.location.z += 2.0
```

While on the topic of data structures, it is important to mention how `bpy` gets seamlessly integrated. Those are done by the DNA and RNA architecture of Blender. The term ”**DNA**” stands for **Data-Block Abstraction** and the biological analogy is intentional. Just as DNA contains the fundamental blueprint of a living being, Blender’s DNA system contains blueprint for every piece of data within a `.blend` file.

At core, all data in Blender is defined as a C-struct. A C-struct means a struct(short for structure) in the C programming language which is a composite data type that lets us group together variables of different types under a single name. The DNA system is a clever way to write these C-structs to a file and read them back again. A special block within every `.blend` file called the **SDNA**(Structure DNA), contains a compact representation of every single data structure’s definition used in that file. If we were to create a file in an older version of Blender, the new version reads the old SDNA block, understands the old data layout and can intelligently transfer that data into its newer, updated C-structs. The DNA is raw, untyped, and highly optimized genetic code of a scene.

RNA stands for **Runtime Introspection and Access** and its job is to act as a universal translator, ”transcribing” the raw DNA into a usable format. The RNA system is a C++ layer that wraps the C-based DNA structs. It takes the raw data fields and exposes them as well-defined properties with metadata. This metadata includes name, description, data type, range, and python access path. This architecture means that both the graphical user interface and a Python script are communicating with the exact same RNA properties. When a user drags a slider for an object’s location, the UI is modifying an RNA property. When a script executes `my_object.location.x=5.0`, it modifies the very same RNA property, which in turn changes the same underlying DNA data. Because there is no transition layer, the synchronization is instantaneous, making `bpy` an exceptionally robust and predictable tool for procedural tasks.

Blender’s GUI is context-sensitive, the tools available depend on what is selected, what mode it is in(Object Mode, Edit Mode etc) and which window the mouse is hovering over. `bpy.context` is the API’s way of accessing this state. It provides information about the current state of the application such as:

- `bpy.context.active_object`: The currently active, selected object
- `bpy.context.selected_object`: A list of all selected objects

- `bpy.context.scene` : The current scene
- `bpy.context.mode` : The current interaction mode

While `bpy.data` is for accessing and modifying raw data, `bpy.ops` is for executing **operators**. Operators are functions that replicate the tools and buttons in the Blender UI. For example, to add a new icosahedron to the scene, we would use the operator

```python
import bpy

# Runs the operator to add an icosphere
bpy.ops.mesh.primitive_ico_sphere_add(subdivisions=3, radius=1.0)
```

We can now define a workflow how these components finally work together. We use `bpy.ops` to setup a scene to clear default objects and add a new object(here a platonic solid). We use `bpy.context.active_object` to get a reference to the newly created object. This is needed as `bpy` is a context based language. We define the axes through which we wish to see the rotation, we can here retrieve the vertices data and do the needed mathematical manipulation.

```python
# Get the object's world matrix
world_matrix = obj.matrix_world

# Get the local coordinate of the first vertex
local_coord = mesh.vertices[0].co

# Calculate the world coordinate
world_coord = world_matrix @ local_coord

print(f"Local coordinate: {local_coord}")
print(f"World coordinate: {world_coord}")
```

Above is an example of how to retrieve vertex data. After defining all of this, we can begin applying the action by modifying the object's properties(here rotation) using bpy.data. At the end, we can then create a visual animation, using `keyframe_insert()` method on the object's rotation property at different frames. Here is the code for reference which I got towards the end

```python
import bpy
import math

#Useful functions
def UnitVector(axis):
    v=[]
    for i in list(axis):
        v.append(i**2)
    magnitude=math.sqrt(sum(v))
    v=[]
    for i in axis:
        v.append(i/magnitude)

    return v


def Quaternion(axis,angle):
    w=math.cos(angle/2)

    v=[0,0,0]
    for i in range(3):
      v[i]=math.sin(angle/2)*axis[i]
    return [w]+v

#Add Mesh
#Uncomment which platonic solid is required
#bpy.ops.mesh.primitive_solid_add() #Tetrahedron
#bpy.ops.mesh.primitive_solid_add(source='6') #Cube
#bpy.ops.mesh.primitive_solid_add(source='8') #Octahedron
#bpy.ops.mesh.primitive_solid_add(source='12') #Dodecahedron
#bpy.ops.mesh.primitive_solid_add(source='20') #Icosahedron


#Retrieve mesh
shape=bpy.context.active_object

#Insert Keyframe 1
shape.keyframe_insert("rotation_quaternion",frame=1)

#Define Angle and Axis
#vertice=shape.data.vertices
deg=180
angle = math.radians(deg)
axis = [x,y,z] #axis at which to rotate the object
order=x #Insert symmetry's order

for i in range(order):

    #Quaternion Rotation
    shape.rotation_mode = 'QUATERNION'
    qrot =Quaternion(UnitVector(axis),angle*(i+1))
    shape.rotation_quaternion = qrot

    #Insert Last Keyframe
    shape.keyframe_insert("rotation_quaternion",frame=50*(i+1))
    shape.keyframe_insert("rotation_quaternion",frame=50*(i+1)+10)
'''
Dodecahedron
axis = [0.75576,-0.28868,0.46709] Line segment Order 2
axis = [0.57735,-0.57735,0.57735] Vertice Order 3
axis = [0.3791,-0.016445,0.6982] Face Order 5
'''
```

3 Conclusion

This project offered profound insights into both theoretical and applied aspects of Group Theory. It was also a great tool for demonstrating how the abstraction of problems in mathematics is essential to providing efficient solutions. Revisiting foundational concepts, such as group axioms, subgroups, and permutation groups (Cayley's theorem), strengthened a deep conceptual understanding of how algebraic structures operate. Working through various problems from Armstrong's *Groups and Symmetries* provided valuable insights into the field of Group Theory and made many concepts in the field more familiar. It provided a great way to improve problem-solving skills in mathematics in general; the concepts presented during the proofs and various arguments used became especially insightful. Proof of Sylow's Theorem provided a very tidy and neat concept which really showed the usefulness of Group Actions, and how a concept like that reveals such a universal theorem if applied correctly. Similarly, with the Structure Theorem, simplifying abstract complex problems becomes much easier and doable, which outlines a key concept in mathematics, that is, simplifying the problems to make them more approachable.

The latter half also provided a great opportunity to demonstrate the applications of these abstractions and explore various tools for visualizing such abstract topics, thereby providing assistance in teaching these concepts to those unfamiliar with them. Creating mathematically accurate animations with the softwares strengthened the concepts of Symmetry further and can provide a good way to showcase these concepts to those who might have trouble visualising complex patterns in their minds or through still images.

References

[1] M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, 1988.

[2] I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, 1975.

[3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., Wiley, 2004.

[4] The Manim Community Developers, *Manim: An Open-Source Mathematical Animation Engine*,
Available at: https://www.manim.community/

[5] Three.js Developers, *Three.js Documentation*,
Available at: https://threejs.org/docs/

[6] p5.js Contributors, *p5.js Reference Documentation*,
Available at: https://p5js.org/reference/

[7] Blender Foundation, *Blender Python API Documentation*,
Available at: https://docs.blender.org/api/current/

Acknowledgement of AI Assistance: Grammarly AI was used to ensure no grammatical error occurs and to improve language clarity in this report.