Abstract Algebra - MATH 310

Orbital Stabilizer Theorem and Representation of Group Action

Authers

Makary Fayez - 202001417
Haitham Taha - 202000512
Hesham Elsaman - 202000640

Project Report

Spring 2023

Disclaimer

This report shall be considered a summary of the topic from the book **A First Course in Abstract Algebra - 8th ed. by John B. Fraleigh and Neal E. Brand**

Contents

Introduction

Abstract algebra, as a fundamental branch of mathematics, explores the intricate structures and symmetries within mathematical objects. Within this field, the Orbit-Stabilizer Theorem holds paramount significance, providing valuable insights into the relationship between group actions, orbits, and stabilizers.

The Orbit-Stabilizer Theorem stands as a cornerstone result in group theory, playing a crucial role in understanding the behavior of groups on sets. By considering the actions of a group on a set, the theorem unveils the partitioning of the set into distinct orbits, representing equivalence classes of elements under group transformations. Stabilizers, on the other hand, correspond to subgroups that leave certain elements fixed or invariant.

This theorem finds applications in various areas of mathematics and beyond. For instance, it plays a pivotal role in the study of permutations and their symmetries in combinatorics. By analyzing the behavior of permutations on a set, the Orbit-Stabilizer Theorem allows us to determine the number of distinct arrangements or patterns that can be obtained through group actions.

Additionally, the Orbit-Stabilizer Theorem finds relevance in the field of coding theory, where it aids in understanding the properties of error-correcting codes. By considering group actions on code words, the theorem reveals the structure of stabilizer subgroups, which provide insights into the error detection and correction capabilities of the codes.

In this report, we aim to delve into the Orbit-Stabilizer Theorem, exploring its theoretical foundations, properties, and applications. Through rigorous analysis, we will investigate the interplay between group sizes, orbits, and stabilizers, emphasizing the importance of this theorem in uncovering the symmetries and transformations within abstract algebraic structures.

Relations & Partitions

2.1 Relations

Definition A relation between sets A and B is a subset Ψ of $A \times B$. $a\Psi b$ indicates that an element $(a, b) \in \Psi$(i.e. a is related to b)

2.2 Partitions & Equivalence Relations

Definition A Partition of a set S is a collection of nonempty sets of S such that every element of S is in exactly one of the subsets. The subsets are called the cells of a partition.

Example Consider the set $\mathbb{Z}$ of all integers. We define a relation $\sim$ on $\mathbb{Z}$ as follows: for any two integers $a, b \in \mathbb{Z}$, we say that $a \sim b$, if the remainder of a divided by 3, is the same as the remainder of b divided by 3.
Equivalence Class [0]: This class contains integers that are multiples of 3.
$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.
Equivalence Class [1]: This class contains integers whose remainder when divided by 3 is 1.
$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.
Equivalence Class [2]: This class contains integers whose remainder when divided by 3 is 2.
$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Definition An equivalence relation Ψ on a set S is one that satisfies these three properties for all $x, y \in$ S

- (Reflexive) $x\Psi x$
- (Symmetric) if $x\Psi y$, then $y\Psi x$
- (Transitive) if $x\Psi y$ and $y\Psi z$ then $x\Psi z$

Theorem (Equivalence Relations and Partitions) Let S be a non-empty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition on S, where

$$\bar{a}=\{x \in S | x \sim a\}$$

Conversely, each partition of S gives rise to equivalence relation $\sim$ on S where a $\sim$ b and only if a and b are in the same cell of the partition.

Proof

Equivalence relation $\iff$ the set admits partition

We must show that the different cells $\bar{a} = \{x \in S | x \sim a\}$ for $a \in S$ do give a partition of S, so that every element of S is in some cell and so that if $a \in \bar{b}$, then $\bar{a} = \bar{b}$.

Let $a \in S$. Then $a \in \bar{a}$ by the reflexive condition, so a is at least in one cell. Suppose now that $a \in \bar{b}$. We need to show $\bar{a} = \bar{b}$ as sets. This will show that a cannot be in more than one cell.
$\Rightarrow$ we show that $\bar{a} \subseteq \bar{b}$. Let $x \in \bar{a}$. Then $x \sim a$. But $a \in \bar{b}$. Then, by the transitive condition, $x \sim b$, so $x \in \bar{b}$. Thus $\bar{a} \subseteq \bar{b}$.
$\Leftarrow$ Now, we need to show that $\bar{b} \subseteq \bar{a}$. Let $y \in \bar{b}$. Then, $y \sim b$. But $a \in \bar{b}$, so $a \sim b$, by the symmetric condition, $b \sim a$. Then by transitive condition $y \sim a$, so $y \in a$. Hence $\bar{b} \subseteq \bar{a}$. So, $\bar{b} = \bar{a}$

Dihedral Group

3.1 Introduction to the Dihedral Group

Definition: Let $n \geq 3$. The dihedral group D_n is defined as the set of all one-to-one functions $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ that map onto $\mathbb{Z}_n$ and satisfy the following property: for any two vertices i and j in the n-sided polygon P_n, the line segment connecting i and j is an edge in P_n if and only if the line segment connecting $\phi(i)$ and $\phi(j)$ is an edge in P_n.

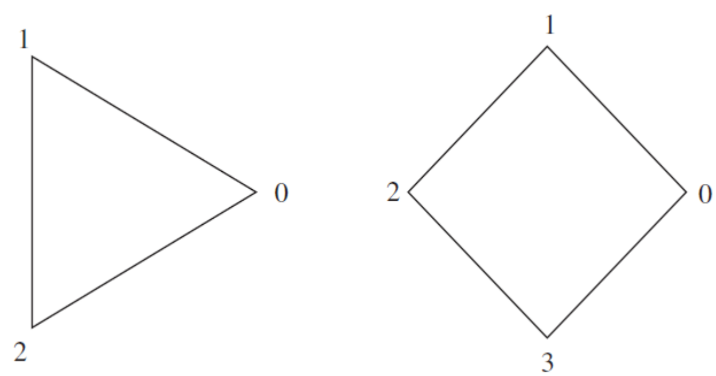

Figure 3.1: P_3 & P_4

Theorem For any $n \geq 3$, $\langle D_n, \circ \rangle$ is a group.

Proof We first show that function composition is an operation on D_n. Let ϕ, $\theta \in D_n$ and suppose that the line between vertices i and j is an edge in P_n. Since $\theta \in D_n$, the line between $\theta(i)$ and $\theta(j)$ is an edge of P_n. Because $\phi \in D_n$, and the line between $\theta(i)$ and $\theta(j)$ is an edge, the line between $\phi(\theta(i)) = \phi \circ \theta(i) and \phi(\theta(j)) = \phi \circ \theta(j)$ is an edge of P_n. The operation of function composition already meets the associativity requirement, the function $\iota(k) = k$ acts as the identity, and finally, the fact that the mapping is one-to-one and onto P_n forces it to admit to being reversible, thus ensuring the existence of the inverse mapping. Therefore, $\langle D_n, \circ \rangle$ is a group.

Example Let $n \geq 3$ and $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ be given by rotating the n-gon P_n by $\frac{2\pi}{n}$, which just rotate each vertex to the next one. That is,

$$\rho(k) = k +_n 1$$

for each $k \in \mathbb{Z}_n$, as can be visualized in Fig.3.2. The function ρ matches edges to edges and it is one-to-one and onto. So $\rho \in D_n$.

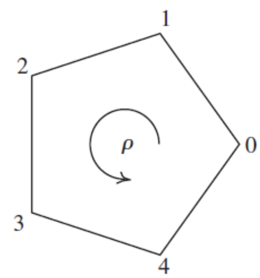

Figure 3.2: D_3 & D_4

3.2 Special Dihedral Group - D_4

The following is the product table of the members of the D_4 group.

$\circ$	ι	ρ	ρ^2	ρ^3	μ	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$
ι	ι	ρ	ρ^2	ρ^3	μ	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$
ρ	ρ	ρ^2	ρ^3	ι	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$	μ
ρ^2	ρ^2	ρ^3	ι	ρ	$\mu\rho^2$	$\mu\rho^3$	μ	$\mu\rho$
ρ^3	ρ^3	ι	ρ	ρ^2	$\mu\rho^3$	μ	$\mu\rho$	$\mu\rho^2$
μ	μ	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$	ι	ρ	ρ^2	ρ^3
$\mu\rho$	$\mu\rho$	$\mu\rho^2$	$\mu\rho^3$	μ	ρ	ρ^2	ρ^3	ι
$\mu\rho^2$	$\mu\rho^2$	$\mu\rho^3$	μ	$\mu\rho$	ρ^2	ρ^3	ι	ρ
$\mu\rho^3$	$\mu\rho^3$	μ	$\mu\rho$	$\mu\rho^2$	ρ^3	ι	ρ	ρ^2

Table 3.1: Product Table for the Elements of D_4

3.3 Code Illustration

The code is written in Python using the library Manim.

Miko.py

```python
from manim import *
from manim import MathTex


class RotateSquare(Scene):
    def construct(self):



        square = Square(side_length=4, color=GRAY, fill_opacity=0.6)
        label_bottom_left = MathTex("\\texttt{1}").next_to(square.get_vertices()[0], DOWN+LEFT)
        label_bottom_right = MathTex("\\texttt{2}").next_to(square.get_vertices()[1], DOWN+RIGHT)
        label_top_right = MathTex("\\texttt{3}").next_to(square.get_vertices()[2], UP+RIGHT)
        label_top_left = MathTex("\\texttt{4}").next_to(square.get_vertices()[3], UP+LEFT)




        intro_words = Text("""
                    This video will illustrate the Actions
                    of the Dihedral group on a Square
        """)
        intro_words.to_edge(UP)

        intro = Text("""
                    Miko: hye!!
        """)
```

Figure 3.3: Manim Code.

The project is uploaded on GitHub, you can find it at Orbit-Stabilizer Theorem.

Conugate Classes & Group Action

4.1 Conjugate Subgroups and Normal Subgroups

Definition: An isomorphism $\phi : G \to G$ of a group G with itself is an automorphism of G. The automorphism $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the inner automorphism of G by g. Performing i_g on x is called conjugation of x by g.

We see that the normal subgroups of a group G are precisely those that are ***invariant*** under all inner automorphisms. A subgroup K of G is a conjugate subgroup of H if $K = i_g[H] = gHg^{-1}$ for some $g \in G$.

4.2 Group Action

The Notion of a Group Action: For any sets A, B, and C, we can view a map $* : A \times B \to C$ as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write $a * b = c$, or simply $ab = c$. In this section, we will be concerned with the case where X is a set, G is a group, and we have a map $* : G \times X \to X$. We shall write $*(g, x)$ as $g * x$ or gx.

Example: Let $G = GL(n, R)$ and X the set of all column vectors in R_n. Then for any matrix $A \in G$ and vector $v \in X$, Av is a vector in X. So multiplying is an operation $* : G \times X \to X$. From linear algebra, we know that if B is also a matrix in G, then $(AB)v = A(Bv)$. Furthermore, for the identity matrix I, $Iv = v$.

G-sets and Orbit-Stabilizer Theorem

5.1 G-sets, the Applications of G-sets, and Isotropy Supgroups

Definition Let X be a set and G a group. An action of G on X is a map $*: G \times X \to X$ such that

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a G-set.

5.1.1 Isotropy Subgroups

Let X be a G-set. Let $x \in X$ and $g \in G$. It will be important to know when $gx = x$. We let

$$Xg = \{x \in X \mid gx = x\} \quad \textit{and} \quad G_x = \{g \in G \mid gx = x\}$$

5.2 Orbit-Stabilizer Theorem

Theorem Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

Proof Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1 x = x$ and $g_2 x = x$. Consequently, $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x$, so $g_1 g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course, $ex = x$, so $e \in G_x$. If $g \in G_x$, then $gx = x$, so $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, and consequently $g^{-1} \in G_x$. Thus G_x is a subgroup of G.

Definition Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup** of x.

5.2.1 Orbits

Theorem Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \equiv x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\equiv$ is an equivalence relation on X.

Proof For each $x \in X$, we have $ex = x$, so $x \equiv x$ and $\equiv$ is *reflexive*. Suppose $x_1 \equiv x_2$, so $gx_1 = x_2$ for some $g \in G$. Then $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1, sox_2 \equiv x_1$, and $\equiv$ is *symmetric*. Finally, if $x_1 \equiv x_2$ and $x_2 \equiv x_3$, then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \equiv x_3$ and $\equiv$ is *transitive*.

Definition Let X be a G-set. Each cell in the partition of the equivalence relation described in the previous theorem is an *Orbit* in X under G. If $x \in X$, the cell containing x is the *Orbit* of x. We let this cell be G_x.

The relationship between the orbits in X and the group structure of G lies at the heart of many applications. The following theorem gives this relationship. Recall that for a set X, we use $|X|$ for the number of elements in X, and $(G : H)$ is the index of a subgroup H in a group G.

Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : Gx)$. If $|G|$ is finite, then $|G_x|$ is a divisor of $|G|$.

Proof We define a one-to-one map ψ from G_x onto the collection of left cosets of G_x in G. Let $x_1 \in G_x$. Then there exists $g_1 \in G$ such that $g_1x = x_1$. We define $\psi(x_1)$ to be the left coset g_1G_x of G_x. We must show that this map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1x = x_1$. Suppose also that $g_1'x = x_1$. Then, $g_1x = g_1'x$, so $g_1^{-1}(g1x) = g_1^{-1}(g_1'x)$, from which we deduce $x = (g_1^{-1}g_1')x$. Therefore $g_1^{-1}g_1' \in G_x$, so $g_1' \in g_1G_x$, and $g_1G_x = g_1'G_x$. Thus the map ψ is well-defined.

To show the map ψ is one-to-one, suppose $x_1, x_2 \in G_x$, and $\psi(x_1) = \psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1 = g_1x$, $x_2 = g_2x$, and $g_2 \in g_1Gx$. Then $g_2 = g_1g$ for some $g \in G_x$, so $x_2 = g_2x = g_1(gx) = g_1x = x_1$. Thus ψ is one-to-one.

Finally, we show that each left coset of G_x in G is of the form $\psi(x_1)$ for some $x_1 \in G_x$. Let g_1G_x be a left coset. Then if $g_1x = x_1$, we have $g_1G_x = \psi(x_1)$. Thus ψ maps G_x one-to-one onto the collection of left cosets so $|G_x| = (G : G_x)$. If $|G|$ is finite, then the equation $|G| = |Gx|(G : Gx)$ shows that $|Gx| = (G : Gx)$ is a divisor of $|G|$.

References

Fraleigh, J. B. (2020). A First Course in Abstract Algebra.