MA3102

Algebra I

Autumn 2021

Satvik Saha
19MS154

*Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.*

Contents

1 Groups and Symmetries **1**
1.1 Symmetries of plane figures 1
1.2 Symmetries of the Euclidean plane 2
1.3 Symmetries of the Petersen graph 2
1.4 Basic definitions 3

1 Groups and Symmetries

1.1 Symmetries of plane figures

A symmetry of a plane figure can be thought of as a rigid motion which *preserves its structure*, i.e. sends it to itself.

For example, consider an equilateral triangle; there is the identity symmetry (which does nothing), two rotations by $2\pi/3$ and $2\pi/3$, and three reflections. This gives us a total of 6 symmetries. Coincidentally, the plane symmetries of an equilateral triangle are precisely the set of $3! = 6$ permutations of its vertices.

The same cannot be said of a square; there are $4! = 24$ of its vertices, but only 8 of them are rigid motions. Here, we see 4 rotations and 4 reflections.

In general, a regular n-gon has $2n$ plane symmetries, of which n are rotations and n are reflections. This can be seen by noting that a symmetry of an n-gon is completely determined by its action on an edge; once the final positions of the first two vertices is determined, the rest are forced. There are n positions for the first vertex, which leaves only 2 positions for the second vertex. One of these choices results in a rotation (since it preserves the cyclicity of the vertices) and the other a reflection (since it reverses the cyclicity of the vertices).

Note that these symmetries can be *composed*, i.e. applied in succession. For example, a rotation by $2\pi/n$ can be applied repeatedly to obtain every possible rotational symmetry. Similarly, we can perform rotations and reflections in succession, and we always end up with another symmetry. This composition is associative, there is an identity symmetry, and each symmetry has an inverse. The collection of such symmetries forms a *group*.

The group of plane symmetries of a regular n-gon is called the *dihedral group*, denoted as D_{2n}.

1.2 Symmetries of the Euclidean plane

Consider the class of isometries of the plane, i.e. all bijections $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that $\|f(\boldsymbol{v}) - f(\boldsymbol{w})\| = \|\boldsymbol{v} - \boldsymbol{w}\|$. These constitute symmetries of the Euclidean plane $\mathbb{R}^2$. The three basic forms of such symmetries are rotations, reflections, and translations; it can be shown that every symmetry of $\mathbb{R}^2$ is a combination of at most three reflections. Another representation for each symmetry is

$$f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{v}_0,$$

where $A \in O_2(\mathbb{R})$ is an orthogonal matrix, accounting for the rotational and reflectional part of the transformation.

To show this, set $\boldsymbol{v}_0 = f(\boldsymbol{0})$ and define $g = f - \boldsymbol{v}_0$. Thus, $g(\boldsymbol{0}) = \boldsymbol{0}$, and g is also an isometry. Not that for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^2$, we can write

$$\begin{aligned}
\|g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 &= \|g(\boldsymbol{v})\|^2 + \|g(\boldsymbol{w})\|^2 - 2\langle g(\boldsymbol{v}), g(\boldsymbol{w})\rangle, \\
\|\boldsymbol{v} - \boldsymbol{w}\|^2 &= \|\boldsymbol{v}\|^2 + \|\boldsymbol{w}\|^2 - 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle.
\end{aligned}$$

On the other hand, $\|g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 = \|\boldsymbol{v} - \boldsymbol{w}\|^2$, and $\|g(\boldsymbol{v})\|^2 = \|\boldsymbol{v}\|^2$, $\|g(\boldsymbol{w})\|^2 = \|\boldsymbol{w}\|^2$. This gives $\langle g(\boldsymbol{v}), g(\boldsymbol{w})\rangle = \langle \boldsymbol{v}, \boldsymbol{w}\rangle$, i.e. g preserves the inner product.

We claim that $g(\alpha\boldsymbol{v}) = \alpha g(\boldsymbol{v})$ for all $\alpha \in \mathbb{R}$, $\boldsymbol{v} \in \mathbb{R}^2$. Note that $\|g(\alpha\boldsymbol{v})\| = \|\alpha\boldsymbol{v}\| = \|\alpha g(\boldsymbol{v})\|$. Now,

$$\begin{aligned}
\|g(\alpha\boldsymbol{v}) - \alpha g(\boldsymbol{v})\|^2 &= \|g(\alpha\boldsymbol{v})\|^2 + \|\alpha g(\boldsymbol{v})\|^2 - 2\langle g(\alpha\boldsymbol{v}), \alpha g(\boldsymbol{v})\rangle \\
&= \alpha^2 v^2 + \alpha^2 v^2 - 2\alpha\langle \alpha\boldsymbol{v}, \boldsymbol{v}\rangle \\
&= 2\alpha^2 v^2 - 2\alpha^2 v^2 \\
&= 0.
\end{aligned}$$

This proves that $g(\alpha\boldsymbol{v}) = \alpha g(\boldsymbol{v})$.

Next, we claim that $g(\boldsymbol{v} + \boldsymbol{w}) = g(\boldsymbol{v}) + g(\boldsymbol{w})$ for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^2$. Write

$$\begin{aligned}
\|g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 &= \|g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v})\|^2 + \|g(\boldsymbol{w})\|^2 - 2\langle g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v}), g(\boldsymbol{w})\rangle \\
&= \|\boldsymbol{v} + \boldsymbol{w} - \boldsymbol{v}\|^2 + \|\boldsymbol{w}\|^2 - 2\langle \boldsymbol{v} + \boldsymbol{w}, \boldsymbol{w}\rangle + 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle \\
&= w^2 + w^2 - 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle - 2w^2 + 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle \\
&= 0.
\end{aligned}$$

This proves that $g(\boldsymbol{v} + \boldsymbol{w}) = g(\boldsymbol{v}) + g(\boldsymbol{w})$. Thus, g is a linear map.

Now let $g(\boldsymbol{e}_1) = \boldsymbol{a}$ and $g(\boldsymbol{e}_2) = \boldsymbol{b}$. Clearly, $\|\boldsymbol{a}\| = \|\boldsymbol{b}\| = 1$. For arbitrary $\boldsymbol{v} \in \mathbb{R}^2$, we immediately get $g(\boldsymbol{v}) = v_x\boldsymbol{a} + v_y\boldsymbol{b}$, so by arranging $\boldsymbol{a}$ and $\boldsymbol{b}$ as the columns of a 2×2 matrix A, we have $g(\boldsymbol{v}) = A\boldsymbol{v}$. We clearly have $A^\top A = \mathbb{I}_2$ from $\boldsymbol{a}^\top\boldsymbol{a} = \boldsymbol{b}^\top\boldsymbol{b} = 1$, and $\langle \boldsymbol{a}, \boldsymbol{b}\rangle = \langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle = 0$. Thus, $A \in O_2(\mathbb{R})$. Substituting this back into f, we have

$$f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{v}_0$$

as desired.

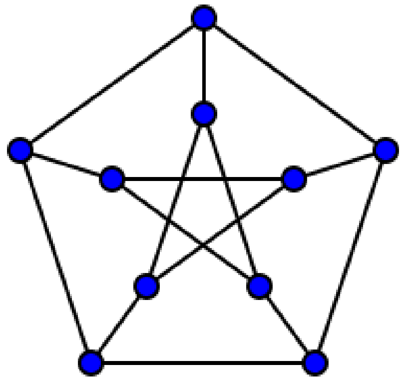
It can be further shown (algebraically) that every member of $O_2(\mathbb{R})$ is of the form

$$\begin{bmatrix} \cos\theta & \mp\sin\theta \\ \sin\theta & \pm\cos\theta \end{bmatrix}.$$

1.3 Symmetries of the Petersen graph

Consider a graph $G(V, E)$. A symmetry of G is a bijection $f\colon V \to V$ on the set of vertices, which preserves the edges. In other words, it preserves the adjacency function. Thus, it can be shown that the degree of each vertex will be preserved by a symmetry.

The following graph is called the Petersen graph, with 10 vertices and 15 edges.



We can show that this graph has 120 symmetries. This can be done by looking at all 2 element subsets of $\{1, 2, 3, 4, 5\}$, of which there are 10. Place these subsets as the vertices of a new graph, and connect two such sets with an edge if they *are disjoint*. The resulting graph can be shown to be identical to the Petersen graph. It is immediately clear that any permutation of the set $\{1, 2, 3, 4, 5\}$ produces a relabelling of the vertices, which nevertheless preserves the Petersen graph. This gives us at least $5! = 120$ symmetries.

To show that there are at most 120 symmetries, note that every vertex has exactly 3 neighbours. Thus, when sending a vertex V to its image, we have 10 choices, but we have 3 choices for the first neighbour V_1, 2 for the second neighbour V_2. and 1 for the third neighbour V_3. Finally, choose a neighbour of V_3, say V_4 and place it in on of the 2 remaining positions. It can be shown that this completely determines the symmetry; each remaining vertex has a complete characterization in terms of the ones already fixed. Thus, we have an upper bound of $10 \times 3 \times 2 \times 1 \times 2 = 120$ symmetries.

1.4 Basic definitions

Definition 1.1. A group is a set G with a binary operation of composition, satisfying the following properties.

1. *Associativity*: For all $x, y, z \in G$, $x(yz) = (xy)z$.
2. *Existence of an identity element*: There exists $e \in G$ such that for all $x \in G$, $ex = e = xe$.
3. *Existence of inverse elements*: For every $x \in G$, there exists some $y \in G$ such that $xy = e = yx$. We denote $y = x^{-1}$.

Example. The integers $\mathbb{Z}$ form a group under addition.

Example. The set $\{-1, +1\}$ forms a group under multiplication.

Example. The symmetries of a tetrahedron form a group under composition of symmetries.

Lemma 1.1. *The identity element in a group is unique.*

Proof. Let G be a group, and suppose that $e, e' \in G$ satisfy

$$ex = x = xe, \qquad e'x = x = xe'$$

for all $x \in G$. Thus, we specifically have

$$ee' = e' = e'e, \qquad e'e = e = ee',$$

hence $e = e'$. □

Lemma 1.2. *The inverse of an element in a group is unique.*

Proof. Let G be a group, and let $x \in G$. Suppose that $y, y' \in G$ satisfy

$$xy = e = yx, \qquad xy' = e = y'x.$$

Thus

$$y = ye = y(xy') = (yx)y' = ey' = y'.$$ □

Lemma 1.3. *The inverse of the inverse of an element in a group is the element itself.*

Proof. Let G be a group, and let $x \in G$. Set $w = (x^{-1})^{-1}$. We have

$$x^{-1}x = e = xx^{-1}, \qquad wx^{-1} = e = x^{-1}w.$$

Thus,

$$w = we = w(x^{-1}x) = (wx^{-1})x = ex = x.$$ □

Lemma 1.4 (Cancellation Law)**.** *Let G be a group, and let $x, a, b \in G$ such that $xa = xb$. Then, $a = b$. Analogously, if $ax = bx$, then $a = b$.*

Proof. Simply multiply by x^{-1} as appropriate. □