MA3102

Algebra I

Autumn 2021

Satvik Saha
19MS154

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

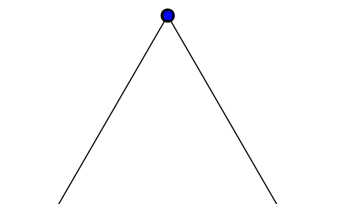
Contents

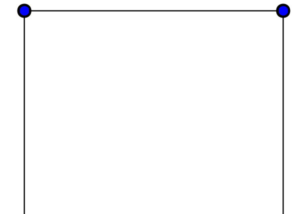
1 Symmetries

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.

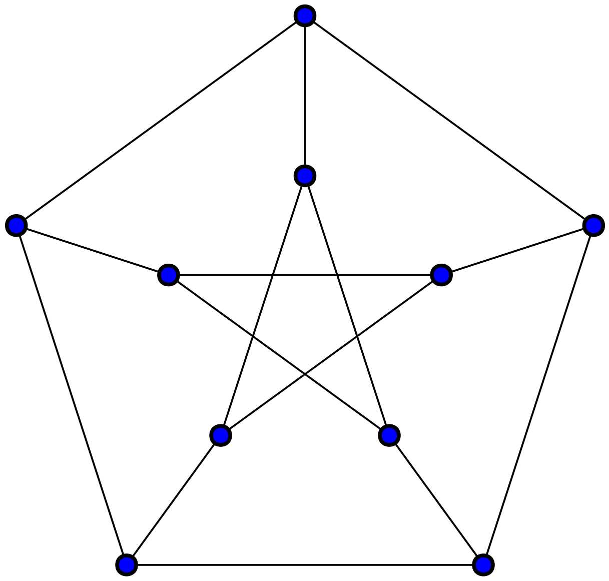
It can be further shown (algebraically) that every member of $O_2(\mathbb{R})$ is of the form

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

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.

2 Groups

2.1 Basic definitions

Definition 2.1. A group is a set G equipped with a binary operation, 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 2.1. *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 2.2. *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 2.3. *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 2.4 (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. □

2.2 Subgroups

Definition 2.2. Let G be a group, and let $H \subseteq G$. We call H a subgroup of G if

1. $e \in H$.
2. For all $x, y \in H$, $xy \in H$.
3. For all $x \in H$, $x^{-1} \in H$.

Note that this is enough to guarantee that H is a group under the same group operation as G.

Example. Consider the group $\mathbb{C} \setminus \{0\}$ of non-zero complex numbers under multiplication. The non-zero reals $\mathbb{R} \setminus \{0\}$ form a subgroup of this group.

Theorem 2.5. *Let $\mathbb{Z}$ be the group of integers under addition. Then, every subgroup of $\mathbb{Z}$ is of the form $\{0\}$ or $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.*

Remark. The same argument shows that every subgroup of a cyclic group is cyclic.

Proof. Let $H \subseteq \mathbb{Z}$ be a subgroup. If $H = \{0\}$, we are done. Otherwise, H contains some positive integers; this is clear since H must contain some non-zero integers, whose inverses have the opposite sign. Let $n \in H$ be the smallest positive integer; we immediately have $n\mathbb{Z} \subseteq H$. Now let $m \in H$ be any other element. Now, use Euclid's Division Lemma to write $m = nq + r$, where $0 \leq r < n$. Now, note that $n \in H$ implies that $nq \in H$, hence the quantity $r = m - nq \in H$. The minimality of n forces $r = 0$, hence $m = nq$. This gives $H \subseteq n\mathbb{Z}$. □

Corollary 2.5.1. *If a and b are coprime integers, there exist integers m and n such that $am + bn = 1$.*

Proof. If a and b are coprime, they share no common factors greater than 1. Note that $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of the integers, and hence there is exists a unique positive integer d such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Since $a, b \in a\mathbb{Z} + b\mathbb{Z}$, we have $a, b \in d\mathbb{Z}$ so there exist r_1, r_2 such that $a = dr_1$, $b = dr_2$. This means that d is a common factor of a and b, forcing $d = 1$, i.e. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Since $1 \in \mathbb{Z}$, $1 \in a\mathbb{Z} + b\mathbb{Z}$, hence there exists a combination $am + bn = 1$. □

Corollary 2.5.2. *The unique positive integer d such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ is the greatest common divisor of a and b.*

Proof. Let d be the greatest common divisor of a and b. Write $a = a'd$, $b = b'd$, and note that a' and b' are coprime. Thus, pick m and n such that $a'm + b'n = 1$. This gives $d = am + bn$, so $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. Now, consider an arbitrary combination $ap + bq \in a\mathbb{Z} + b\mathbb{Z}$; simply write $ap + bq = (a'p + b'q)d \in d\mathbb{Z}$, hence $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$. □

Theorem 2.6. *Let $\mathbb{C}^\times$ be the group of non-zero complex numbers under multiplication. Then, every finite subgroup of $\mathbb{C}^\times$ is of the form $H_n = \{z^k : k \in \mathbb{N}\}$ for some n^{th} root of unity z.*

Proof. Let $H \subset \mathbb{C}^\times$ be a finite subgroup. Note that we demand $1 \in H$. If this is the only element of H, we are done, otherwise choose a different $z \in H$. Now, if $|z| \neq 1$, note that there are infinitely many elements $z, z^2, z^3, \dots$ which must belong to H, which is a contradiction; note that these generated elements are distinct as they have different magnitudes. Thus we demand $|z| = 1$, so write $e^{2\pi ix}$.

Examine the elements $1, z, z^2, \dots, z^n, \dots \in H$ for all $n \in \mathbb{N}$. Since H is finite, some pair of these must be equal. This means that $z^a = z^b$ for some $a < b$, so cancellation gives $z^{b-a} = 1$. Thus, z is a root of unity, which means that $z = e^{2\pi ik/n}$ for some $n \in \mathbb{N}$, $0 < k < n$.

We have shown that every non-identity element in H is a root of unity. Thus, pick $w = e^{2\pi ix} \in H$ such that $0 < x < 1$ and x is minimal. Furthermore, set $x = k/n$, $0 < k < n$ with k and n coprime. We claim that H consists solely of the n^{th} roots of unity. The fact that H contains all powers of w, hence all n^{th} roots of unity is clear. Conversely, pick arbitrary $z = e^{2\pi iy} \in H$, $z \neq 1, w$; since z is a root of unity, write $y = k'/n'$ where $0 < k' < n'$, k' and n' are coprime. The minimality of x gives $x < y$, hence $y - x = (k'n - kn')/nn' > 0$. Set $p = k'n$, $q = kn'$, and using $p > q$ write $p = aq + r$ where $0 \leq r < q$. Then,

$$z = e^{2\pi ip/nn'} = e^{2\pi i(aq+r)/nn'} = e^{2\pi iaq/nn'} e^{2\pi ir/nn'} = w^a e^{2\pi ir/nn'}.$$

Thus, $zw^{-a} = e^{2\pi ir/nn'} \in H$. However, note that $r/nn' < q/nn' = x$; the minimality of x forces $r = 0$. This gives $z = w^a$, proving the result. □

2.3 Cyclic groups

Definition 2.3. A group G is called cyclic if there exists an element $g \in G$ such that every element of G is a power of g. We say that G is generated by the element g, or $G = \langle g \rangle$.

Example. The additive group of integers $\mathbb{Z}$ is cyclic.

Example. The additive group of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group.

Example. Let G be a cyclic group generated by g such that all the powers g^n are distinct. Clearly, G is infinite. Now, note that we can enumerate the elements of G as follows.

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

We can construct a bijection $\varphi\colon G \to \mathbb{Z}$, $g^n \mapsto n$. This preserves the group operation, since $g^m g^n = g^{m+n} \mapsto m + n$, so $\varphi(g^m g^n) = \varphi(g^m) + \varphi(g^n)$. Thus, the groups G and $\mathbb{Z}$ are essentially the same.

Example. Let G be a cyclic group generated by g such that the powers $g^m = g^n$, $m > n$. This immediately gives $g^{m-n} = e$. Let k be the smallest natural number such that $g^k = e$; we claim that $G = \{e, g, \dots, g^{k-1}\}$. To see this, note that every element of G is of the form g^p. Use the Division Lemma to write $p = kq + r$ where $0 \leq r < k$, hence $g^p = g^{kq+r} = (g^k)^q g^r = g^r$. Also, the elements $e, g, \dots, g^{k-1}$ are distinct, by the minimality of k.

Using a construction similar to that in the previous example, we can show that the groups G and $\mathbb{Z}/k\mathbb{Z}$ are essentially the same.

Lemma 2.7. *Let G be a cyclic group of n elements. Then, it has $\phi(n)$ generators, where ϕ is Euler's Totient function denoting the number of positive integers less than and coprime to n.*

Proof. Write $G = \{e, g, \dots, g^{n-1}\}$. We claim that g^m generates G if and only if m and n are coprime.

First, suppose that m and n are coprime; choose integers a and b such that $am + bn = 1$. Thus, we have $g = g^{am+bn} = g^{am}g^{bn} = g^{am}$, which means that $g^k = g^{amk}$ in general.

Next, suppose that g^m generates G. Further suppose that $d > 1$ is a common divisor of m and n, and write $m = m'd$, $n = n'd$. Note that since g^m generates G, so does g^d since $g^m = (g^d)^{m'}$. We claim that the subgroup generated by g^d has $n' < n$ elements, and hence cannot generate G, i.e. $\langle g^d \rangle = \{e, g^d, \dots, g^{(n'-1)d}\}$. Clearly, given any power g^{kd}, we can write $kd = nq + r$ for $0 \leq r < n$; since d divides both kd and nq, it must also divide r, hence $r = r'd$. Since $0 \leq r < n$, we must have $0 \leq r' < n'$, which means that $g^{kd} = g^{nq+r} = g^{r'd} \in \{e, g^d, \dots, g^{(n'-1)d}\}$. This proves the result. □

2.4 Cosets and Lagrange's Theorem

Definition 2.4. Let G be a group, and let H be a subgroup of G. A left coset of H is the set

$$gH = \{gh : h \in H\}$$

for some $g \in G$.

Lemma 2.8. *All left cosets of H contain the same number of elements.*

Proof. Consider the bijection

$$f\colon H \to gH, \qquad h \mapsto gh.$$

This map is injective by cancellation, and surjective by construction. Thus, all cosets of H contain exactly the same number of elements as in H. □

Lemma 2.9. *The left cosets of H partition the group G.*

Remark. Two left cosets are either equal, or disjoint.

Proof. Define the equivalence relation $\sim_H$, where $a \sim b$ if and only if $a = bh$ for some $h \in H$. Clearly, this is reflexive ($e \in H$), symmetric ($h^{-1} \in H$) and transitive ($h_1 h_1 \in H$ when $h_1, h_2 \in H$). Thus, this is an equivalence relation, and its equivalence classes partition the group G. However, we see that the equivalence class $[g]$ is precisely the left coset gH. □

Definition 2.5. The index of H in G, denoted by $[G : H]$, is the number of left cosets of H in G.

Theorem 2.10 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. The order of H divides the order of G. In fact,*

$$|G| = [G : H]|H|.$$

Proof. This follows directly from the previous two lemmas. Each coset of H contains $|H|$ many elements, are disjoint, and cover the entire group G. □

Corollary 2.10.1. *Let G be a finite group of n elements. Then, $g^n = e$ for any $g \in G$.*

Proof. Consider the cyclic subgroup $H = \langle g \rangle$ of G, and suppose that it has m elements. Then, $g^m = e$. However, Lagrange's Theorem says that m divides n, so $g^n = e$. □

Theorem 2.11. *The set of integers between 1 and n which are coprime to n form a multiplicative group modulo n.*

Proof. Let $\mathbb{Z}_n^\times$ be the set of these integers. Clearly, $1 \in G$ which is our identity. Multiplication modulo n is associative. Finally, let $m \in \mathbb{Z}_n^\times$. Since m and n are coprime, we can find p and q such that $mp + nq = 1$, which means that $mp = 1$ modulo n. Furthermore, p is coprime to n, since any common divisor of p and n must also divide $mp + nq = 1$. Thus, every $m \in \mathbb{Z}_n^\times$ has an inverse, which proves that this is a multiplicative group. □

Corollary 2.11.1 (Euler's Theorem)**.** *Let n be a positive integer, and let $1 \leq a < n$ be coprime to n. Then,*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. This follows directly from the fact that $|\mathbb{Z}_n^\times| = \phi(n)$. □

Corollary 2.11.2 (Fermat's Little Theorem)**.** *Let p be a prime. Then,*

$$a^p \equiv a \pmod{p}.$$