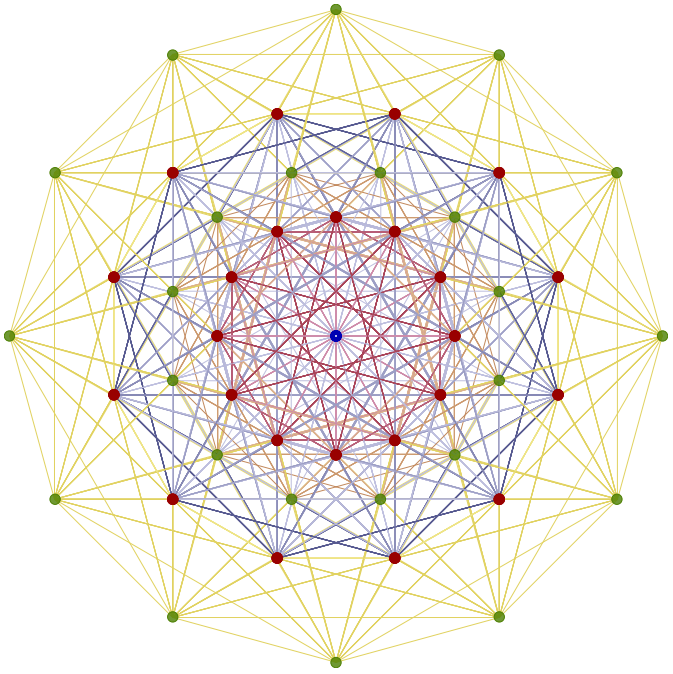
Physics Inspired Introduction To Lie Groups and Lie Algebra

Lecture Notes

Based on Summer Course by IISER-K Alumni



Sagnik Seth

Dept of Physical Sciences
IISER Kolkata

Contents

1 Grouping things together...

Symmetry is one of the many things which both mathematicians and physicists crave to understand. And *Group Theory* is a mathematically formal way of learning about these symmetries. The basic idea is to 'cluster' the symmetries into some 'groups' and then do all kind of nasty things to them. For that, first let us define the main hero of this act: a group.

Definition 1 (Group):
A group g is a ordered pair $(G, *)$ where G is a set and $* : G \times G \to G$ is a binary operation satisfying:

- **Associativity:** $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3 \ \forall \ g_1, g_2, g_3 \in G$
- **Identity:** There exists a unique $e \in G$ such that $\forall \ g \in G, e * g = g * e = g$
- **Existence of Inverse:** For every $g \in G$, there exists g^{-1} such that $g * g^{-1} = g^{-1} * g = e$
- **Closure:** $g * h \in G \ \forall \ g, h \in G$

A few points to note:

- We sometimes (almost everytime) omit $*$ when the context is clear and just write gh for $g * h$ where $g, h \in G$.
- Technically $(G, *)$ is called a group but when context is clear, the just simply refer to G as the group.
- A group G is called *Abelian* if the elements comute, that is, $\forall \ g_1, g_2 \in G \ g_1 g_2 = g_2 g_1$

Let us see some examples of groups, all of which can be checked to satisfy the properties specified in the definition:

1. $(\mathbb{R}\backslash\{0\}, \times), (\mathbb{R}, +)$: the real numbers under multiplication[1] and addition form a group.
2. $\mathrm{GL}(n, \mathbb{R}), \mathrm{GL}(n, \mathbb{C})$: the set of all invertible $n \times n$ matrices over $\mathbb{R}$ or $\mathbb{C}$ field, form a general linear group under matrix multiplication.
3. $\mathrm{SL}(n, \mathbb{R}), \mathrm{SL}(n, \mathbb{C})$: the set of all invertible $n \times n$ matrices with determinant 1, over $\mathbb{R}$ or $\mathbb{C}$ field, form a special linear group under matrix multiplication.
4. $\mathrm{O}(n), \mathrm{SO}(n)$: set of all orthogonal $n \times n$ matrices and orthogonal matrices with determinant 1 form orthogonal and special orthogonal group.
5. S_n: the set of all permutations of n objects form a group. Permutation means arranging the same objects in some way, so basically it can be thought of as a bijection of a set onto itself. We represent these maps by π such that $\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ and

$$\pi \equiv \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

The above representation means that the first row, after the arrangement (acting on by map pi), changes to the second row. As an example, let us consider:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix}$$

[1] Note that under multiplication, no inverse exist for zero, so we exclude 0

The red elements are how the objects are initially there, blue are how the objects change place after permutation. Note that, under the map π, $1 \to 7, 7 \to 3, 3 \to 5, 5 \to 1$ and also $4 \to 6, 6 \to 4$ while 2 is mapped to 2 itself. This hints writing the thing in a cyclic structure, like $(1\ 7\ 3\ 5)(2)(4\ 6)$. We say $1, 7, 3, 5$ form a *4-cycle* while $4, 6$ form a *2-cycle*.

1.1 Symmetries of the Equilateral Triangle

This is one of the typical examples which is always mentioned in any group theory introduction, so as a reverence to the old-age custom, we include it too. To describe this, we will consider three actions on the triangle:

- Leave it alone
- Rotate it by some angle
- Flip (reflect) it about some axis.

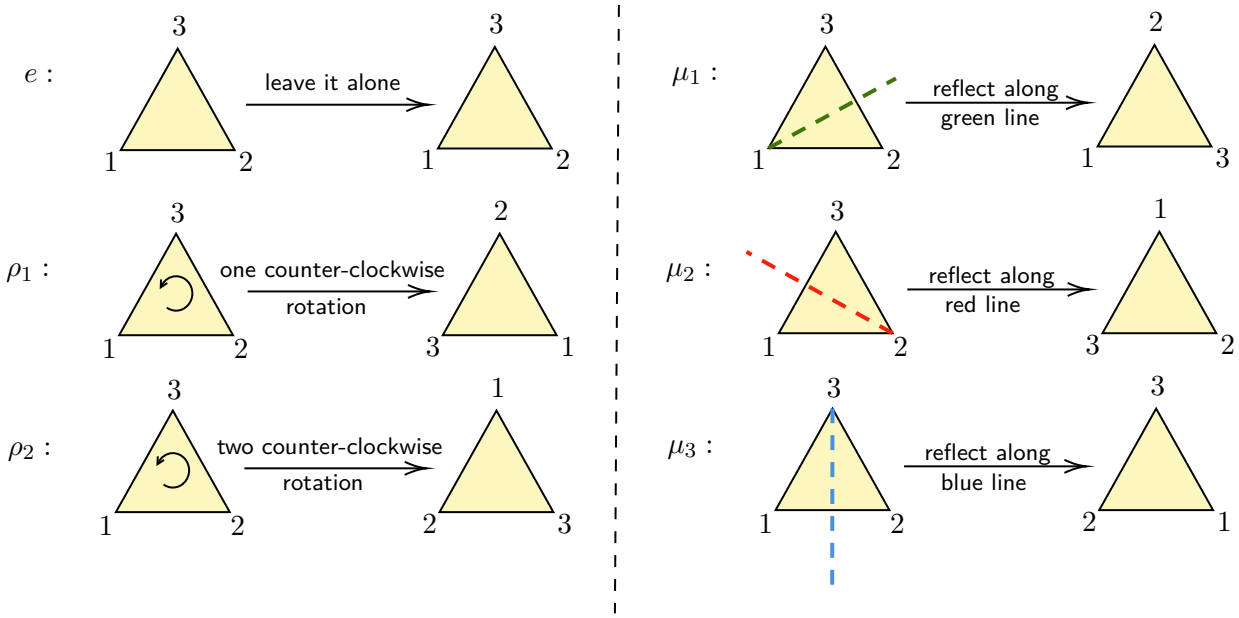


Figure 1: Diagram showing the different actions of reflection and rotations to the equilateral triangle.

Okay, so these six actions form a group for the symmetries of an equilateral triangle. To check that, we can try to form the multiplication table for these operations, which is a table demonstrating the result of the composition of the elements with each other. The table looks like something like this:

$*$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e						
ρ_1						
ρ_2						
μ_1						
μ_2						
μ_3						

Now, note the following things: First, the first row and first column will be filled as it is, since acting with identity does not change anything. Second, $\rho_1^2 \equiv \rho_2$ (since it is how we defined it).

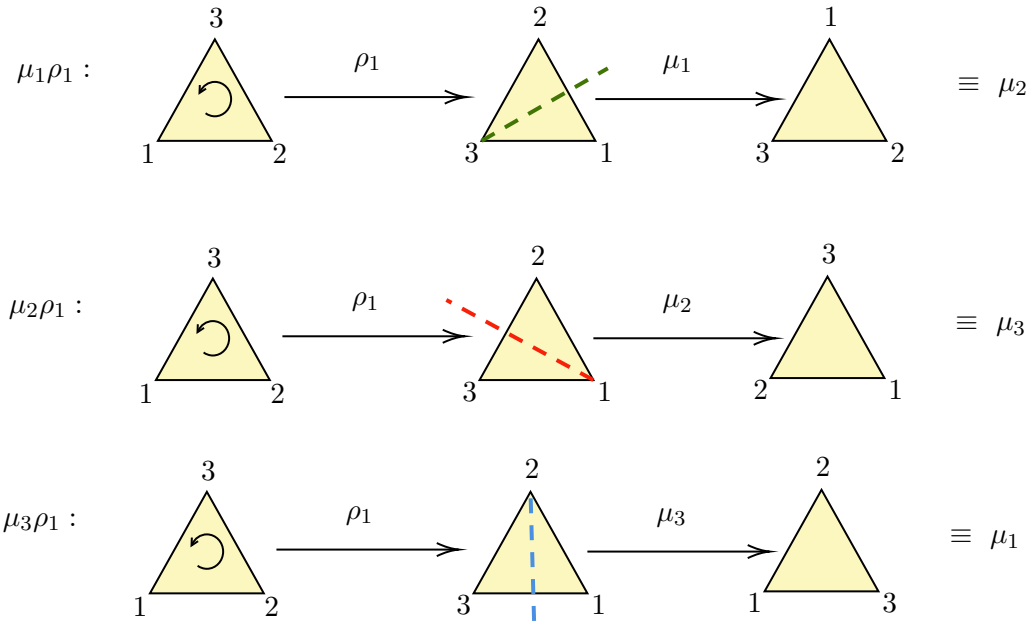
Also, note that rotations will commute with themselves and one anti-clockwise rotation is rotation by $120°$, so accordingly $\rho_1 \equiv 120°$, $\rho_2 \equiv 240°$ and hence $\rho_2\rho_1 = \rho_1\rho_2 \equiv 360° \equiv e, \rho_2^2 \equiv 480° \equiv 120° \equiv \rho_1$.

Also, reflecting along the same line twice will result in the initial configuration, so $\mu_i^2 \equiv e \ \forall \ i$ Let us now fill the table with these information:

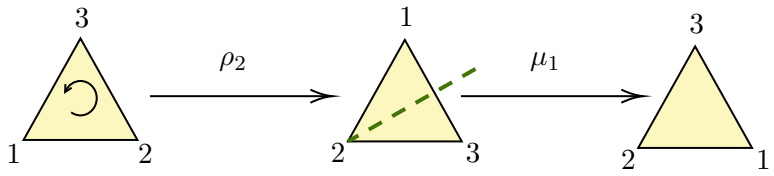
$*$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e			
ρ_2	ρ_2	e	ρ_1			
μ_1	μ_1			e		
μ_2	μ_2				e	
μ_3	μ_3					e

Now there are the non-intuitive actions left, combining rotation with reflections and reflections with reflections. Let us see these actions. We have to be careful with the following :

- ab means b is acted first and then a.
- When taking reflections, we should take them along the axes specified initially, not based on the current position of the index. So, μ_2 does not mean taking reflection along the axis passing through the vertex with '2' on it. μ_2 is taking reflection from the bottom-right vertex of the triangle, irrespective of what index is there on the vertex.

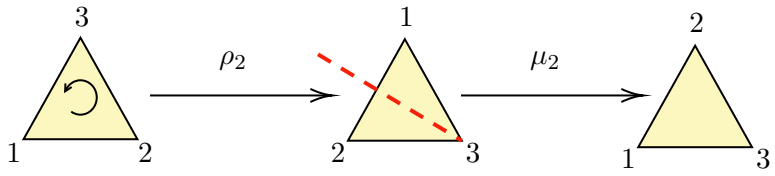


$\mu_1\rho_2$:



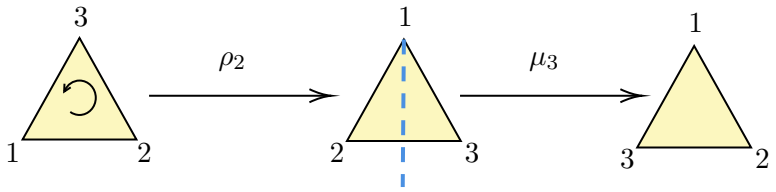
$\equiv \mu_3$

$\mu_2\rho_2$:



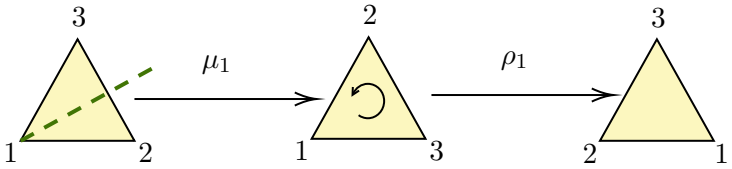
$\equiv \mu_1$

$\mu_3\rho_2$:



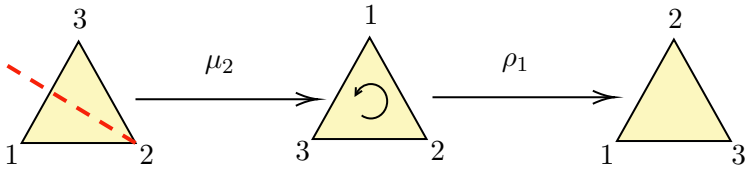
$\equiv \mu_2$

$\rho_1\mu_1$:



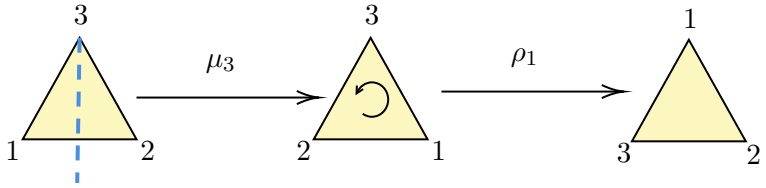
$\equiv \mu_3$

$\rho_1\mu_2$:

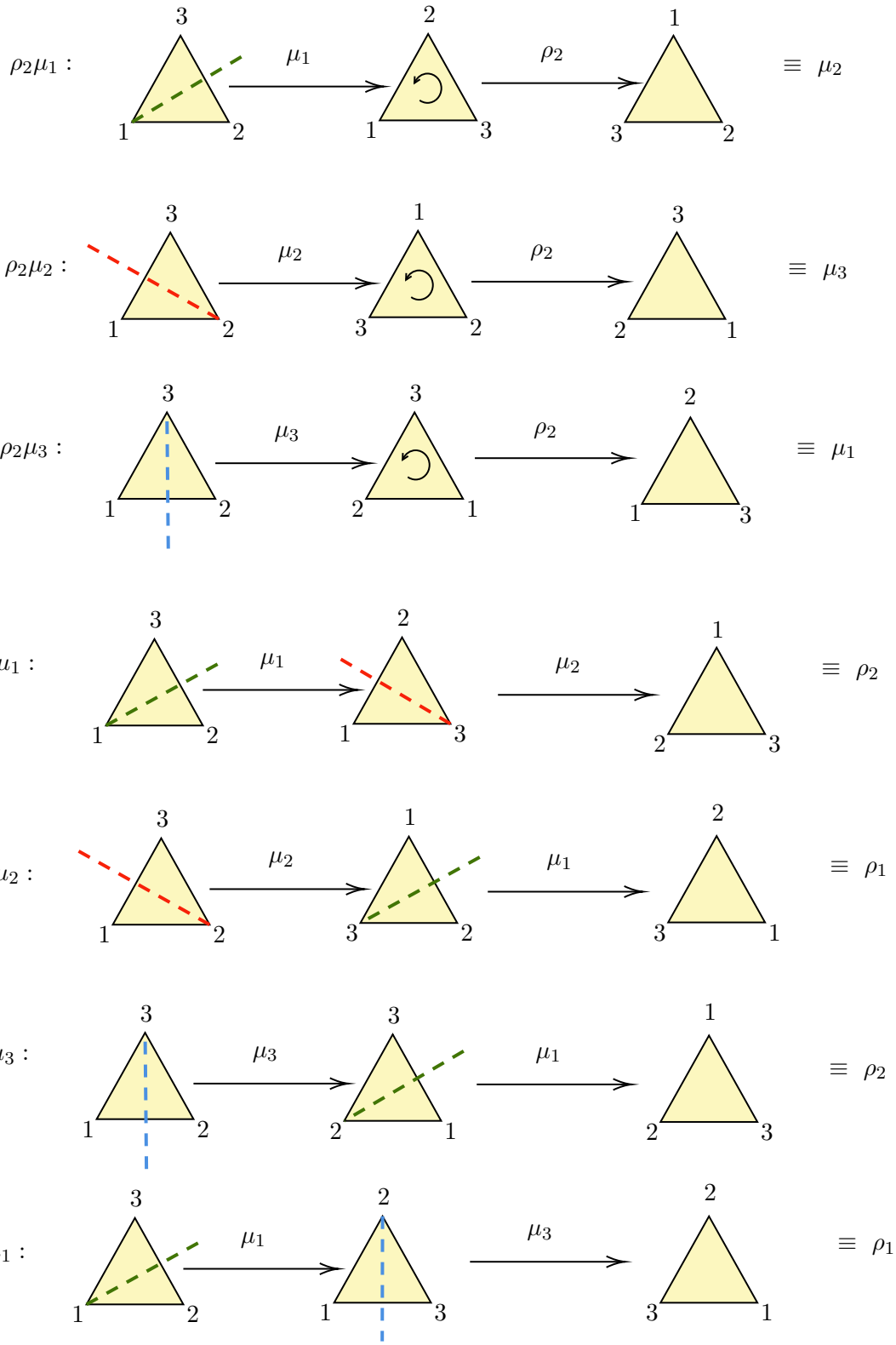


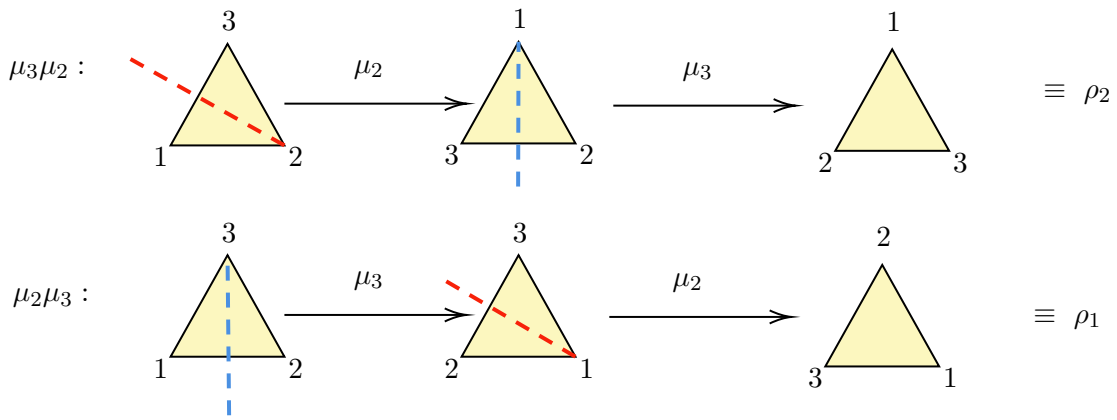
$\equiv \mu_1$

$\rho_1\mu_3$:



$\equiv \mu_2$


$\rho_2\mu_1$:
μ_1
ρ_2
$\equiv \mu_2$
$\rho_2\mu_2$:
μ_2
ρ_2
$\equiv \mu_3$
$\rho_2\mu_3$:
μ_3
ρ_2
$\equiv \mu_1$
$\mu_2\mu_1$:
μ_1
μ_2
$\equiv \rho_2$
$\mu_1\mu_2$:
μ_2
μ_1
$\equiv \rho_1$
$\mu_1\mu_3$:
μ_3
μ_1
$\equiv \rho_2$
$\mu_3\mu_1$:
μ_1
μ_3
$\equiv \rho_1$



So, from the above diagrams, we can fill in the rest of the table. The final multiplication table thus becomes:

$*$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e

Table 1: Final multiplication table for the symmetries of an equilateral triangle

We can now check the group properties from this table. By the way, the group of symmetries of the equilateral triangle is denoted by D_3[1].

We will come back to this table again and again! Well, notice one thing, all elements of the group occur exactly once in each row or column of the multiplication table. This leads to a pretty nice observation that each row and column of the multiplication table is a permutation of the group elements.

Fun Fact:
Consider a finite group G with h elements. For any $g_k \in G$ the sequence $\{g_i g_k\}_{i=1}^{h}$ contains each group element exactly once.

Proof. For any g_i, there exists an element $g_r = g_i g_k^{-1}$ since $g_k^{-1} \in G$ and elements of G satisfy closure property. Then we have $g_i = g_r g_k$ and then g_i must appear in the sequence atleast once, since $r \leq h$. Now, this happens for all $i = 1, \ldots, h$ and there are only h terms in the sequence. Thus, each element can occur atmost once.

[1]The symmetries of a regular polygon are known as dihedral groups. This group is usually denoted D_n for the symmetries of a regular n-gon. It so happens that the dihedral group of degree 3 (the group of symmetries of an equilateral triangle) is 'isomorphic' to the symmetric group, denoted by, $D_3 \cong S_3$

1.2 Subgroup

So we saw what a group is. Now, let us see what a subgroup is [1]. A subset $H \subseteq G$ is called a *subgroup* if it is a group in its own right, where the binary operation is the same operation as in G but restricted to $H \times H$, that is, $*\big|_{H\times H}$

Lemma 1:
If $H \subseteq G, H \neq \emptyset$ and if $h_1 h_2^{-1} \in H \ \forall \ h_1, h_2 \in H$, then H is a subgroup of G

Proof. Note that the restricted binary operation is still associative. Now, $h_1 = h_2 \implies h_1 h_1^{-1} = e$ and hence $e \in H$ (existence of identity). Then take $h_1 = e, h_2 = h \in H \implies eh^{-1} = h^{-1} \in H$ (existence of inverse). Now, take $h_1 = h', h_2 = h^{-1}$ for $h', h \in H$, then $h' \left(h^{-1}\right)^{-1} = h'h \in H$ (closure property). Thus, H follows all properties of a group and hence is a subgroup of G.

Using the lemma above, we can say that the special linear group is a subgroup of the general linear group. Obviously, $\mathrm{SL}(n, \mathbb{R}) \subseteq \mathrm{GL}(n, \mathbb{R})$. For the other part, note that, $A, B \in \mathrm{SL}(n, \mathbb{R}) \implies \det(A) = \det(B) = 1$. Now, $\det(AB^{-1}) = \det\{A\} \det\{B^{-1}\} = \det\{A\} \frac{1}{\det\{B\}} = 1 \implies AB^{-1} \in \mathrm{SL}(n, \mathbb{R})$, hence proved.

1.2.1 Cyclic Subgroups

Consider a group G and let $g \in G$. Then the *cyclic subgroup* of G generated by g, is given by the set $\langle g \rangle = \{g^k | k \in \mathbb{Z}\} \subseteq G$[2]. Note that the cyclic subgroup is element-specific. Let us see an example using the symmetry group of the equilateral triangle.

So, $G \equiv \{e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ is the group of symmetries of the equilateral triangle. Now,

- $\langle e \rangle = \{e\}$ (since powers of identity is always identity)
- $\langle \rho_1 \rangle = \{\rho_1, \rho_1^2 = \rho_2, \rho_1^3 = e, \ldots \text{repetitions}\} \equiv \{\rho_1, \rho_2, e\}$
- Similarly, $\langle \mu_1 \rangle = \{\mu_1, e\}$
- and so on...

For a finite group, the cyclic subgroup must have some repitition and hence there exists $m, n \in \mathbb{N}$ such that $g^m \equiv g^{m+n}$ and hence $g^n = e$. If there always exist this kind of n, then the set $\{n \in \mathbb{N} | g^n = e\} \neq \emptyset$ has a minimum element and this is called the *order* of g. If no such finite n exist (which happens mostly when infinite groups are considered), then order is taken to be infinite.

For finite groups, we have $g^m g^n = g^{(m+n) \bmod r}$ where r is the order of g. This mimics the group of integers under addition modulo r, denoted by $\mathbb{Z}/r\mathbb{Z}$.

1.2.2 Centre of a Group

Definition 2 (Centre):
If G is a group, then the centre of the group denoted by $Z(G)$ is given by:

$$Z(G) = \{a \in G | ab = ba \ \forall \ b \in G\}$$

[1] Think about it, it is natural that smaller groups are always formed within a bigger group
[2] We can check that this set is indeed a subgroup.

Basically, we are looking for the set of all elements which commute with every other element in the group. Let us see an example for $\mathbb{Z}_4$, the group of integers under addition modulo 4. The multiplication table is given by:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Then we can check that $Z(\mathbb{Z}_4) = \{0, 1, 2, 3\} = \mathbb{Z}_4$. Note that G itself was abelian and hence the centre of the group is the entire group itself. We can also check that $Z(D_3) = \{e\}$. So we saw the centre of a group being the entire set as well as just the identity. Can we have something in between?

It turns out that $Z(D_4) = \{e, \rho_2\}$ where D_4 is the group of symmetries of the square and ρ_2 being the action of rotation by 180° anti-clockwise.

Lemma 2:
The centre of a group $Z(G)$ is a subgroup of the group G.

Proof. We will use lemma 1 for this. Let us take $a, b \in Z(G)$ and let $k \in G$ be any arbitrary element. Then, from the definition of centre of group,

$$ak = ka \implies a = kak^{-1} \qquad bk = kb \implies b = kbk^{-1} \implies b^{-1} = kb^{-1}k^{-1}$$

Then we have:

$$(ab^{-1})k = (kak^{-1})(kb^{-1}k^{-1})k = kak^{-1}kb^{-1}k^{-1}k = kaeb^{-1}e = k(ab^{-1}) \implies ab^{-1} \in Z(G)$$

1.3 Cyclic Group

Definition 3 (Cyclic Group):
A group G is called *cyclic* if there exists $g \in G$ such that $\langle g \rangle = G$. The element g is called the generator of the group.

For example, if we consider $\mathbb{Z}_6$ (integers under addition modulo 6), then:

$$\begin{aligned} 1^1 &\equiv 1 = 1 \\ 1^2 &\equiv 1 + 1 = 2 \\ 1^3 &\equiv 1 + 1 + 1 = 3 \\ 1^4 &\equiv 1 + 1 + 1 + 1 = 4 \\ 1^5 &\equiv 1 + 1 + 1 + 1 + 1 = 5 \\ 1^6 &\equiv 1 + 1 + 1 + 1 + 1 + 1 = 6 \equiv 0 \end{aligned}$$

After that repititions start occurring, however, note that, we have obtained all the elements of the group. Hence we can say $\langle 1 \rangle = \mathbb{Z}_6$ and hence 1 is a generator of the cyclic group $\mathbb{Z}_6$. Similarly, we can check that $\langle 5 \rangle = \mathbb{Z}_6$[1]

Fun Fact:
For any integer $n > 1$, $\mathbb{Z}_n = \langle 1 \rangle = \langle n - 1 \rangle$

We will now see a nice relation between cyclic and abelian groups. It turns out, every cyclic group is abelian.

[1] A group can have multiple generators.

Lemma 3:
Every cyclic group is an abelian group but converse is not true.

Proof. Let G be a cyclic group. Then $G = \langle a \rangle = \{a^k | k \in \mathbb{Z}\}$ for some $a \in G$. Let us take $g_1, g_2 \in G \implies \exists\ m, n \in \mathbb{Z}$ s.t. $g_1 = a^m, g_2 = a^n$. Then we have:

$$g_1 g_2 = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = g_2 g_1$$

For the converse, let us take the group of integers under multiplication modulo 12, $U(12) = \{1, 5, 7, 11\}$. We can check that the multiplication table is:

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Since the table is symmetric, the group is abelian. However, note that:

$$\begin{aligned}\langle 1 \rangle &= \{1\} \\ \langle 5 \rangle &= \{5, 1\} \\ \langle 7 \rangle &= \{7, 1\} \\ \langle 11 \rangle &= \{11, 1\}\end{aligned}$$

Thus, this is not a cyclic group, since none of the elements generate the entire group and hence, converse of the lemma does not hold true.

1.3.1 Infinite Cyclic Groups

Let us consider the infinite group $(\mathbb{Z}, +)$[1]. Then, note that $\mathbb{Z} = \langle 1 \rangle$, that is, $\mathbb{Z}$ is cyclic group. And, order of every element is infinite, apart from 0.

Lemma 4:
If G is an infinite cyclic group generated by $a \in G$, then order of g is infinite for all $g \in G, g \neq e$.

Proof. We have $G = \{a^k | k \in \mathbb{Z}\}$. Consider $e \neq g \in G$, then $g = a^m$ for some $m \in \mathbb{Z} \backslash \{0\}$. Now, for any $l \in \mathbb{Z}$, $g^l = (a^m)^l = a^{ml}$. For order to be finite, $g^l = e \implies a^{ml} = e \implies ml = 0$ but $m \neq 0$ forces l to be zero. Thus, no positive powers exist such that $g^l = e$ and hence, the order of the group is infinite.

Lemma 5:
Let G be an infinite cyclic group. If $a \neq e \in G$ and a has infinite order, then $\forall\ u, v \in \mathbb{Z}, a^u = a^v \Leftrightarrow u = v$. If G is finite and order of a is n, then $a^u = a^v \Leftrightarrow n | (u - v)$

Proof. ($\implies$)For infinite case: Let $a^u = a^v \implies a^u (a^v)^{-1} = e \implies a^u a^{-v} = e \implies a^{u-v} = e$. Since order of a is infinite, $a^{u-v} = e$ iff $u - v = 0 \implies u = v$.

For finite case: $a^{u-v} = e \implies (u - v) = 0 \bmod n$

($\impliedby$) $u = v \implies a^u = a^v$ lol 😂

[1] This can be thought of as group of integers under addition modulo 1

1.4 Cosets

For this, let us focus on something related to lemma 1. Consider a relation $\sim_L \subseteq G \times G$ such that for $a, b \in G, a \sim_L b \iff a^{-1}b \in H$. We show the following:

Proposition 1:
Let G be a group and let H be a subgroup of G. Define the relations $\sim_L$ and $\sim_R$ such that $a \sim_L b \iff a^{-1}b \in H$ and $a \sim_R b \iff ab^{-1} \in H$. Then, $\sim_L$ and $\sim_R$ are an equivalence relations on G.

Proof. For $\sim_L$:

- $a \in G \implies a^{-1}a = e \in H \implies a \sim_L a$ (reflexive)
- $a \sim_L b \implies a, b \in Ga^{-1}b \in H \implies (a^{-1}b)^{[}-1] \in H \implies b^{-1}a \in Hb \sim_L a$ (symmetric)
- $a \sim_L b, b \sim_L c \implies a^{-1}b \in H, b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ (transitive)

Similarly we can show for $\sim_R$ Whenever we define any equivalence relation, we at once go into the equivalence classes (since these form a partition of the set). We will now see how the equivalence classes look for these relations.

Lemma 6:
The equivalence class of an element $a \in G$ under the relation $\sim_L$ is given by $[a] = \{ah \mid h \in H\}$

Proof. Let $x \in [a]$, then $x \sim_L a$. Then, by symmetricity, $a \sim_L x \implies a^{-1}x \in H$. Hence $a^{-1}x = h$ for some $h \in H$.

From this, we have $x = ah$ which implies that $x \in \{ah \mid h \in H\} \implies [a] \subseteq \{ah \mid h \in H\}$. Now, let us prove the opposite way:

Let $x \in \{ah \mid h \in H\} \implies x = ah$ for some $h \in H$. This implies that $a^{-1}x = h \in H \implies x \sim_L a \implies x \in [a]$. Thus, $\{ah \mid h \in H\} \subseteq [a]$. From these two things, we can say:

$$[a] = \{ah \mid h \in H\}$$

Similarly, for $\sim_R$, we will have $[b] = \{hb \mid h \in H\}$. This will lead us to the definition of cosets.

Definition 4 (Cosets):
Let G be a group and H be a subgroup of G. Let $a \in G$, then the *left coset* of G is given by $aH = \{ah \mid h \in H\}$ and the *right coset* of G is given by $Ha = \{ha \mid h \in H\}$

2 When Groups said, "represent us!"