GROUP THEORY : THE JOURNEY CONTINUES (PART I)

VIPUL NAIK

ABSTRACT. Group theory is an important topic in most undergraduate math curricula, and forms the basis for higher studies both in math and in areas where math is applied. This is the sequel to an earlier written article, titled `Group Theory:A First Journey` where we began our journey into groups. In this article, we take that journey further, and cover all the terrain typically covered in any first course on group theory. It is tacitly assumed that the reader has read and mastered thoroughly the contents of `Group Theory:A First Journey`.

1. THE JOURNEY CONTINUES

1.1. **What makes this so important.** In `Group Theory:A First Journey` we saw what made the study of groups so exciting and important. So far, we have acquired a fairly thorough understanding of why groups are defined the way they are. We are now in a position to reap the benefits of this appreciation and explore the inner terrain of groups.

Due to size and logical breakup considerations, the text of this journey (`Group Theory:The Journey Continues`) has been split into three parts. We are currently reading `Part I`.

1.2. **Prerequisites.** This is a firm step in the journey into the landscape of groups – but it is still a very small step into a vast expanse that remains largely mysterious and unexplored.

At the end of this journey, we shall have sufficient strength and maturity in the subject to take up a further study of the subject from any angle.

By this time, we can (having successfully mastered `Group Theory:A First Journey`): [1]

- **Define a group** in more than one way
- **Define and understand the concept of subgroup**
- **Define homomorphism and isomorphism**

We also learnt the *importance* of groups, the *concrete versus abstract* distinction, and the *subtleties* involved in defining subgroups.

1.3. **The explicit promise.** At the end of `Part I`, the learner should be familiar with:

- The concept of **group action** and **orbits**.
- The idea of subgroups acting on groups, and the associated concept of **cosets**.
- The notion of **normal subgroups** and the proof that the kernel of a homomorphism is always a normal subgroup.
- A formalism for expressing **subgroup properties**. In particular, the notion of **characteristic subgroup** and some ideas about how normality and characteristicity behave.
- The concept of **product of subgroups** and **subgroup generated**, as well as **intersection of subgroups**.

Perhaps much more importantly, going through this journey shall give us journeyers a great degree of confidence and maturity in exploring almost anything pertaining to algebra with a sharp eye.

These aims may seem particularly ambitious for our journey – but they will be met with minimal effort. That is because :

> **Mantra.** *The hard part was understanding the core,*
> *Now its just layering more and more*

And in `Group Theory:A First Journey`, we already did most of the hard part.

---

[1]Anybody who cannot do the things specified below is advised to first read (or revise) `Group Theory:A First Journey` before embarking on this journey.

1.4. **Easy but demanding.** Yes, the contents here are quite easy, but in other senses, it is a fairly demanding journey. It requires patience, the ability to jot down, to remember, and to correlate existing ideas. This article is best tackled with an effective **learning strategy**. At the very least, such a strategy requires paper and pencil.

The learning strategy that I myself followed while preparing this journey, and hence, the one that might most suit others journeying along the path, is that using the principles of **property theory**. Learn more on this in my series on property theory.

I have also designed the journey in such a way that even those who start out on the journey without any prior knowledge of property theory will, by the end of the journey, get an intuitive feel of how to apply the property theoretic paradigm, at least in the limited context of groups and algebra.

For more about how to go through this journey, refer the article on the website describing the details of mathematical journeys.

2. Groups acting on sets

2.1. **Equivalence relation.** Before beginning on this, let us recall the notion of equivalence relations.

Definition. An **equivalence relation**(defined) on a set is a relation that is reflexive, symmetric and transitive. If S is the set and R is the relation on it, then R is:

- **reflexive**(defined) : Every element is related to itself, or aRa for every $a \in S$.
- **symmetric**(defined) : If aRb then bRa.
- **transitive**(defined) : If aRb and bRc then aRc.

This is an equivalence because it represents an equality of sorts. For instance, if f is some function from S to another set, then the relation R defined by $aRb \iff f(a) = f(b)$, is an equivalence relation. We can define an equivalence relation on the set of complex numbers by saying – "two complex numbers are equivalent if they have the same modulus". Or we can define a relation on the set of nonzero real numbers by saying – "two nonzero real numbers are equivalent if they have the same sign."

Every equivalence relation partitions the set into **equivalence classes**. The equivalence class of an element a is the set of elements that are related to a, or, in other words, equivalent to a. What we observe is that :

- The equivalence class of a contains a, and is hence nonempty. (This follows from reflexivity).
- The equivalence class of a is also the equivalence class of any element in this equivalence class. (This follows from symmetry and transitivity).

From this, it is clear that two distinct equivalence classes cannot contain a common element.

Equivalence relations thus partition, or stratify, the set. An equivalence relation can be thought of as a **resemblance**.

2.2. **Permutation representations and orbits.** In `Group Theory:A First Journey` we had defined a group action on a set as some rule that, for each element of the group, gave a permutation on the set, such that the composite of two group elements gave the composites of their permutations and the identity element gave the identity permutation.

Formally :

Definition. A **group action**(recalled) of a group $(G, *)$ on a set S is a map $. : G \times S \to S$ such that :

$$
\begin{aligned}
g_1.(g_2.s) &= (g_1 * g_2).s \\
e.s &= s
\end{aligned}
$$

For every element in the group we get a function $S \to S$, and the inverse of an element gives an inverse map. Thus, the function given by every element is a permutation. It was also seen that this gives a **homomorphism** from G to the symmetric group (group of all permutations) on the set S. Conversely, any homomorphism from G to the symmetric group on the set S gives a group action. This enables us to redefine a group action as :

> A group action of a group on a set is a homomorphism from the group to the symmetric group on the set.

For, suppose $\rho : G \to Sym(S)$ is the homomorphism. Then we simply define the action of $g \in G$ on $s \in S$ by the action of $\rho(g)$ on s.

So far, we have concentrated on what happens to the group action when we fix an element in the group. We can also ask : what happens when we fix an element in the set? That is, suppose we fix an element $s \in S$. Then for each $g \in G$, we have a map $g \mapsto g.s$, and we would like to study this map.

Let us now define a relation. An element $t \in S$ is said to be **accessible** from s if there is a $g \in G$ such that $g.s = t$. Loosely speaking, we can reach t from s via an element of G. **Accessibility** defines a relation on S, that is, given any two elements, we can ask whether the second is accessible from the first.

We observe that :

- Every element is accessible from itself. This follows from the presence of the **identity element**. Thus, accessibility is a **reflexive relation**.
- Accessibility is **transitive**. This follows from the way we define a group action. For, suppose $t = g.s$ and $u = h.t$ where $g, h \in G$. Then $u = h.(g.s)$ and hence we get $u = (h * g).s$.
- Accessibility is **symmetric**. This relies on the further fact of **invertibility**. If $g.s = t$, then we have $g^{-1}.t = g^{-1}.(g.s) = s$.

By convention, we ignore both the action symbol . and the group multiplication symbol $*$ and write our expressions in the form $g_1 g_2 s$ instead. This is valid because of the rule $(g_1 * g_2).s = g_1.(g_2.s)$ making the bracketing irrelevant.

Intuitively, we can understand the above as follows. The group offers a way to go from one element of the set to the other. Now, if we can go from one element to another, and from that to yet another, we can compose the two routes and go from the starting element to the final element. We can always reach any element from itself. Most importantly, as a group gives *reversible transformations*, we can always go back the way we came.

The upshot of this is that when a group acts on a set, the relation of accessibility is an **equivalence relation**. We can picture the various equivalence classes under these equivalence relations like islands such that any two points in the same island are accessible to each other but any two points in different islands are not.

The equivalence class of an element in the set under a group action is termed its **orbit**(defined). The orbit of an element is the orbit containing it, or, equivalently, the set of all elements that can be accessed from it.

<div align="center">CONCEPT TESTERS</div>

(1) In `Group Theory:A First Journey`, we had defined a **monoid**(recalled) as a set with an associative binary operation having a neutral element. The definition of group action given above does not use the inverse operation, and hence, we can generalize it to monoids.

Define a **monoid action**(first used) in the same way as a group action, replacing the group by a monoid. Given a monoid action, what can be said about the relation of accessibility? Is it reflexive? Symmetric? Transitive?

(2) Given a group G acting on a set S, define the **orbit**(defined) of a subset T of S as the set of all elements in S that are accessible from some element in T. Prove that the orbit of T is the union of the orbits of all the elements in T.

<div align="center">POINTS TO PONDER</div>

- If you think of $\mathbb{R}^2$ as a space and the group of rotations about the origin acting on it, what do the orbits of points look like? That is, given a point, what are the other points that can be accessed via it from rotations? Draw a picture of the plane partitioned into the various orbits.

  In the above situation, what is the orbit of a straight line through the origin?

- Diagrams of the above sort are what people typically refer to when they talk of a *visual feel* of orbits. This is because orbits under continuous group actions look like the kind of closed trajectories we got in the last problem. Can you think of a finite group acting on $\mathbb{R}^2$ under which the orbit of a single point looks like a collection of finitely many points?

2.3. **Sizes of orbits.** Given any element in the set, we get a map from the group to its orbit, the map taking each element of the group to its image on the element in the set. For instance, if $s \in S$ is fixed, we get a map $g \mapsto g.s$ and the image of this map is precisely the orbit of s.

Thus, given any element of the set, we can get a surjective map from the group to its orbit. The choice of the map depends on the choice of the element we pick.

Suppose we are given that a point $s \in S$ is such that

$$g_1.s = g_2.s \implies g_1 = g_2$$

In other words, different elements of the group take s to different elements of the set.

In that case, the map from G to the orbit of S is bijective. Thus, such orbits will have cardinality same as the cardinality of the group.

A group action such that the above condition holds for *every* point in the set is termed a **semiregular group action**(defined).

<center>CONCEPT TESTERS</center>

(1) Consider a group action of $(G, *)$ on S. Suppose $s \in S$ satisfies the above condition, namely that:

$$g_1.s = g_2.s \implies g_1 = g_2$$

Prove that, if t is in the orbit of s, then t also satisfies the above condition. That is :

$$g_1.t = g_2.t \implies g_1 = g_2$$

Remember not to assume finiteness of G.

(2) Suppose a group has a semiregular action on a set. Prove that the cardinality of every orbit under this action equals the cardinality of the group. Hence, prove that if the set is finite, the cardinality of the group divides the cardinality of the set.

3. SUBGROUPS ACTING ON GROUPS

3.1. Subgroup actions and right cosets. Given a group acting on a set, the group action can be restricted to any subgroup, giving an action of the subgroup on the set. That is, if G acts on S, and H is a subgroup of G, then we can define an action of H on S simply by making each element of H act on S the same way as it acts when treated as an element of G. It is readily seen that this defines a group action of H on S.

Suppose we consider the group acting on itself by left multiplication. That is, we consider the action $G \times G \to G$ defined by left multiplication. This was introduced in `Group Theory:A First Journey` as the **left regular action** or the **left regular representation** of the group on itself.

Now, we can restrict this action to a subgroup of the group. That is, if $H \leq G$ is a subgroup, we are interested in defining the action $H \times G \to G$ by multiplication. Thus, here G is the set on which H is acting, and the action of $h \in H$ on $g \in G$ is given by $h.g = h * g$ with multiplication in G.

We now make some basic observations :

- The action of H as a group on G as a set, defined as above, is a group action.
- Thus, it has orbits. The orbit of x contains precisely those elements of G that can be written as hx where $h \in H$. These orbits are termed the **right cosets** of H and the right coset of H containing an element x is denoted by Hx. The word *right* is used because the coset element is put on the right.
- The orbit containing the identity element is H itself.
- The group action satisfies the condition of semiregularity. This is a direct consequence of the cancellation property in groups. (Refer section 2.3).
- Thus, there is a bijection between the subgroup and every right coset of it. In particular, the subgroup has the same cardinality as each right coset that it has.

<center>CONCEPT TESTERS</center>

(1) Every group has two subgroups – the **trivial subgroup**, comprising only the identity element, and the **improper subgroup**, which is the whole group. How will the right cosets of the trivial subgroup look? How will the right cosets of the improper subgroup look?

3.2. In proper detail. A lot of new ideas have been introduced above, so the first question that comes up is – can we have some examples, please? However, we shall refrain from the temptation at the moment, and *concentrate on a better understanding of the definition*, through structural variation.

In `Group Theory:A First Journey` we had often, to get a better understanding of why groups are the way they are, considered more generic structures. A similar approach is suitable here.

Groups are a bit like a well constructed puzzle. In a well constructed puzzle, *every* piece is crucial in some way, and no piece can be removed without rendering the puzzle either wrong or trivial. In the same way, *every* facet of the definition of groups is critical in some way, and we can understand this best only by trying to remove that facet.

First of all, instead of a group and a subgroup, we can begin with a semigroup S and look at a subsemigroup that becomes a group under the induced multiplication. Call this subgroup H. Then we have a map $H \times S \to S$ by left multiplication. We still have the following :

- The map is a group action.
- Thus, the subgroup has right cosets, and the right coset corresponding to the identity element of the subgroup is the whole subgroup.

However, the semiregularity condition fails because it is now no longer necessary that if $g_1 s = g_2 s$ then $g_1 = g_2$. The condition will, of course, hold if s is right cancellative. Thus we have :

- A subgroup of a general semigroup defines a group action on the semigroup. This group action partitions the semigroup into right cosets of the subgroup.
- Those elements of the semigroup that are right cancellative have cosets of the same size as the subgroup.
- If the semigroup is right cancellative, then all the cosets have the same size as the subgroup, and the action is semiregular.

<div align="center">Concept Testers</div>

(1) Suppose $(S, *)$ is a **magma** (a set with a binary operation) and G is a subset closed under multiplication such that G is a group under the induced operation. Which of the following conditions is sufficient to ensure that the multiplication map $G \times S \to S$ is a group action?
   - Every element of G is left associative.
   - Every element of G is middle associative.
   - Every element of G is right associative.

3.3. **Left cosets.** We return to groups for the moment.

The **right coset** of an element is the set of all elements accessible to it by multiplication on the left. That is, if $H \leq G$ are groups and $x \in G$ then the right coset Hx is defined as the set of all elements of the form hx where $h \in H$.

We can analogously define **left coset** xH as the set of all elements of the form xh where $h \in H$. It is also easy to see that this definition gives a partitioning of the group into equivalence classes, and that, further, each equivalence class is in bijection with the subgroup. Let us see whether the left cosets can be viewed in terms of an *action*.

We had defined a group action as a map from the Cartesian product of the group and the set to the set. We had placed the group on the left *because we were thinking of group elements as functions* and it is conventional to make *functions act on the left*. However, we can also make functions act on the right.

We define a right action a group on a set as follows :[2]

Definition. A **right group action**(defined) of a group G on a set S is a map $. : S \times G \to S$ such that :

$$
\begin{aligned}
s.(g_1 * g_2) &= (s.g_1).g_2 \\
s.e &= e
\end{aligned}
$$

In a left action, we defined the action of $(g_1 * g_2)$ on an element to be the action of g_2 followed by the action of g_1 (that was because we wrote things on the left). But now, in the right action, the action of $(g_1 * g_2)$ is given by *first* acting g_1 and then acting g_2 on the result. This difference in order is the main point of difference between the left action and the right action.

It is now fairly easy to see that every group has a **right regular action** or **right regular representation** on itself, simply by right multiplication. Restricting this right regular action to a subgroup gives a right action of the subgroup on the group. Thus if $H \leq G$ then the right action of H on G is the multiplication map $G \times H \to G$.

The points left to be checked are detailed below :

<div align="center">Concept Testers</div>

(1) Prove that the notion of orbits and all the observations made about them continue to hold even in the case of right actions.
(2) Show that left cosets are the orbits under the right action of the subgroup on the group.

---

[2]By default, the term action refers to left action, as was defined earlier.

3.4. **Left and right.** This subsection is a little more involved than most, and so it may not be easy to absorb in the first pass. Most of the material in the subsection is not referred to later in the text, except one important fact – "the bijection between left cosets and right cosets of a subgroup".

We shall here knit together plenty of ideas :

- The concept of opposite magma
- The notion of antihomomorphism
- The notion of involutive structures
- Left right duality

First, recall that a homomorphism of groups is a map that preserves the binary operation. In a similar way we define homomorphisms of magmas and semigroups. An **antihomomorphism**(recalled) is a map that reverses the order of the binary operation. Thus, if $(S, *)$ and $(T, .)$ are magmas, then an antihomomorphism from S to T is a map $\phi : S \to T$ such that :

$$\phi(x * y) = \phi(y).\phi(x) \ \forall \ x, y \in S$$

We can now define an **antiisomorphism** as a bijective antihomomorphism, **antiendomorphism** as an antihomomorphism from the magma to itself, and **antiautomorphism** as a bijective antiendomorphism.

In `Group Theory:A First Journey`, we had alluded to the concept of the **opposite magma** to a given magma (here, the order of the binary operation was reversed). We can also define the opposite magma to a magma as the structure such that the identity map defines an antihomomorphism of the structures.

We then have :

- An antihomorphism from one magma to another is a homomorphism if viewed as a map from the opposite magma.
- A magma that is equipped with an antiautomorphism must be isomorphic to its opposite magma.

We had also touched upon the concept of an **involutive semigroup**. An involutive semigroup can be described as a semigroup equipped with an involutive antiautomorphism. Thus, any involutive semigroup automatically becomes isomorphic to its opposite semigroup. Groups have a natural involution – the inverse map, and thus a group is naturally isomorphic to its opposite group.

The upshot is that under this involution the left/right behaviour of groups changes. Since a subgroup is its own inverse, it does not get affected by inversion. However, the inversion map takes the **right coset** Hx to the **left coset** $x^{-1}H$. In particular, the inversion map establishes a **bijection between the collection of left cosets and the collection of right cosets**.

The collection of cosets is sometimes called the **coset space** of the subgroup. As the left coset space and the right coset space can be naturally identified, we do not always make it clear whether we are talking of the left coset space or the right coset space.

CONCEPT TESTERS

(1) Consider a finite magma that is both left cancellative and right cancellative, and a subset that comprises middle associative elements and is a group under the induced multiplication operation. Prove that the number of left cosets of this subgroup equals the number of right cosets, using cardinality arguments.

(2) Consider a magma equipped with an involution (that is, with an involutive antiautomorphism). Suppose there is a subgroup comprising middle associative elements that is closed under the involution. Prove that the number of left cosets of the subgroup equals the number of right cosets, by establishing an explicit bijection.

3.5. **Where we are placed.** In the previous section, we discussed the general action of a group on a set. In this section, we looked at the special case where the group in question was a *subgroup* and the set on which it was acting was the whole group. This made us confront the concept of right cosets.

We then saw that, by interchanging the role of left and right, we were able to define a right group action. The basic difference between a left group action and a right group action is that in a left group action, the action of the product is the composite of first applying the right multiplier and then the left multiplier. In a right group action, the action of the product is the composite of first applying the left multiplier and then the right multiplier.

By considering the right action of a subgroup on the group, we came across the notion of left cosets.

However, there is a natural bijection between the left cosets and right cosets, given by the involutive antiisomorphism of the group : the map $x \mapsto x^{-1}$. Thus, statements that can be made about the *left* group action on the space of its *right* cosets have analogs concerning the *right* group action on the space of *left* cosets.

A crucial fact we had observed was that the action of a subgroup on a group is semiregular, and hence, there is a bijection between the subgroup and its cosets. In the coming section, this fact shall be exploited to draw conclusions about the orders (cardinalities) of groups and subgroups.

4. ORDER INFORMATION

4.1. Lagrange's Theorem.
The **order**(defined) of a group is defined as the cardinality of its underlying set.

The **index**(defined) of a subgroup is the number of left (or right) cosets that the subgroup has. (The two numbers are equal by the canonical bijection established above). Because all the cosets have the same cardinality, we have, in the case of the group having finite cardinality :

Order (cardinality) of a subgroup × Index of the subgroup = Order of the group

Note that the index is a *relative* property of the subgroup with respect to the group. The index of a subgroup H of a group G is sometimes denoted as $G : H$.

The above result is often called **Lagrange's Theorem** and is stated as:

For a finite group, the order of a subgroup must divide the order of the group.

Another way of putting it is that groups have the **Lagrange property**(explained) with respect to subgroups – the order of a subgroup divides the order of the group. In general, a structure is said to have the Lagrange property if the order of any substructure must divide the order of the structure.

4.2. Very specific to groups.
Lagrange's Theorem is the first theorem that gives powerful information about the **subgroup structure** of groups. Further, this theorem has already made use of some very special structural properties of groups – the fact that every substructure has cosets, and the fact that they have equal cardinality. The somewhat more general context in which these two things hold is when we consider subgroups of right cancellative (or left cancellative) semigroups. Thus, we have the following generalization:

Given a left cancellative (or right cancellative) finite semigroup, the order of any subgroup (subsemigroup which is a group under the induced operation) must divide the order of the semigroup.

And a somewhat bigger generalization is :

Given a right cancellative finite magma, and a subgroup whose elements are all left associative (or are all middle associative), the order of the subgroup must divide the order of the magma.

While the overall structure need not be a group, it is very necessary that the substructure must be a group, for us to be able to apply the concept of group actions and obtain equivalence classes as orbits. Thus, the **Lagrange property** can be extended at best to **subgroups of certain magmas** and it is unlikely that it can be generalized to scenarios where the substructure itself is not a group.

However, if we put additional structure *on top of the group structure*, the Lagrange property will continue to hold. Thus, the Lagrange property holds for Abelian groups, vector spaces, rings, modules, fields, and many other algebraic structures that have an underlying group structure.

CONCEPT TESTERS
(1) Write out the proof of the generalization given above.

4.3. A storehouse of ideas opens up.
My friend Shreevatsa read in his high school textbook that "every group of prime order is Abelian" [3] but that the result is "beyond the scope of this book". At the time, he had very little idea of groups – his knowledge of groups was far less than what we had after completing `Group Theory:A First Journey`. But his curiosity was aroused when he saw this result and he decided to try it out with the few tools at his disposal.

He proceeded as follows : he picked a non identity element in the group, say x, and looked at the elements x, x^2 and so on. As the group is finite, eventually there will be two powers of x which are equal,

---

[3]a group is Abelian if any two elements of it commute – more on this in section 6.

so that $x^k = x^{k+r}$ for some $k, r \geq 1$. But this gives us $x^r = e$. This indicates that given any element x, there is some finite (minimum) $r > 0$ such that $x^r = e$.

He then observed that the set $\{e, x, x^2 \ldots x^{r-1}\}$ forms a subgroup of the original group. In fact, the product of any two powers of x is again a power of x, but the exponent can be reduced modulo r. Thus, $x^k x^l = x^{k+l}$ and if $k + l \geq r$ we replace $k + l$ by its remainder modulo r.

The **order** of this subgroup is thus the smallest power of x that is the identity. Groups that can be generated by a single element in the above fashion are termed **monogenic groups**(defined) or **cyclic groups**(defined). The single element is termed a **generator**(defined) for the group. Note that every element is a generator for the smallest subgroup containing it, which is a cyclic group. The **order of an element**(defined) is defined as the order of the cyclic subgroup it generates.

Coming back to Shreevatsa's problem, he at this stage reinvented the wheel by deducing Lagrange's theorem via the cosets argument and hence concluded that the order of any non identity element must be a factor of the order of the group. At this stage, he had observed that :

- The order of any non identity element must divide the order of the group.
- The order of a non identity element cannot be 1.

He thus concluded that if the order of the group is prime, the order of any non identity element *must be* the same as the order of the group. This indicates that for any non identity element, the cyclic subgroup generated by it must be the whole group. In particular, it means that : "every group of prime order is a cyclic group of prime order".

But cyclic groups are clearly Abelian, because powers of an element always commute, by associativity. Thus, the statement "every group of prime order is Abelian" has been proved.

Some important ideas that came up in the course of this proof were :

- In a finite group, every element has finite order.
- The cyclic group generated by any element is Abelian.

Both these observations are very crucial. In the next few subsections, we explore these in greater detail and reveal their significance.

4.4. Subgroup criterion for finite orders.
In `Group Theory:A First Journey` we had remarked that it is not true that a subset of a group that is closed under multiplication is a subgroup. An example for infinite groups is the set $(\mathbb{Z}, +)$ (that is, the additive group of integers) and the subset $(\mathbb{N}, +)$ which is a subsemigroup but has no additive identity and no element of it is invertible.

When the multiplicatively closed subset in question is **finite and nonempty**, then in fact it must be a subgroup.

Taken any element in the multiplicatively closed subset, say x. Then, consider the sequence $\{x, x^2, x^3 \ldots\}$. This sequence must contain two equal elements, and thus, by dividing, we get that x has finite order. In other words, there is an r such that $x^r = e$. Further, that also means that $x^{r-1} = x^{-1}$.

Thus, we have shown that :

- Every element in the subset has finite order, because the set is finite.
- Hence, every element in the subset has an inverse.
- Further, because the subset is nonempty, taking any element with finite order gives that the identity element must lie in the subset.

In fact, we can weaken the hypotheses somewhat and say that any multiplicatively closed nonempty subset where every element has finite order must be a subgroup. This suggests that, if every element in the group itself has finite order, then every multiplicatively closed subset is a subgroup.

- An element with finite order is termed a **torsion element**(defined). Any multiplicatively closed subset comprising only torsion elements must be a subgroup. In particular, any finite multiplicatively closed subset must be a subgroup.
- A **torsion group**(defined) is a group where every element has finite order. Any multiplicatively closed subset of a torsion group is a subgroup. As every finite group is torsion, every multiplicatively closed subset of a finite group is a subgroup.

Concept Testers

(1) Prove that any nonempty multiplicatively closed subset of a group that is not a subgroup must contain a subsemigroup that is isomorphic to $(\mathbb{N}, +)$.

4.5. In greater generality. It is time for us to step back and look at the concept of cyclic subgroup in greater generality.

Suppose that, instead of a group, we look at a semigroup $(S, *)$. Then, in the semigroup, we can define

$$x^n := x * x \ldots x$$

when n is a positive integer. The definition is valid because the operation $*$ is associative. Further, it is also clear that in any semigroup, we get :

$$x^{m+n} = x^m * x^n$$

This follows from the fact that both sides are just x multiplied by itself $(m + n)$ times.

In fact, associativity is a very strong condition and there may be magmas (sets with binary operation) that are not associative, but where powers are still defined. The key ingredient needed to define powers is precisely that for any expression of the form $x * x \ldots x$, the bracketing is irrelevant. This is what we call power associativity. A magma is said to be **power associative**(defined) if every expression of the form $x * x \ldots x$ gives the same value irrespective of the bracketing.. In other words, *powers* of an element associate. Clearly, every semigroup is power associative.

In any power associative magma, we can talk of the submagma generated by taking the positive powers of an element. This submagma will be a **commutative subsemigroup**.

There are now two possibilities :

- All the x^n are distinct, as n varies over $\mathbb{N}$.
- Some x^k and x^l are equal.

In the first case, we can establish a bijective correspondence between n and x^n, thus giving an isomorphism between the commutative subsemigroup generated by x, and $(\mathbb{N}, +)$.

In the second case, if we consider the smallest k for which x^k gets repeated, and the smallest l at which the repetition occurs, then the sequence of powers of x is **eventually periodic** with the repeating block going from x^k to x^{l-1}. The semigroup that we get has only $l - 1$ distinct elements in it.

This is all we can say in a general power associative magma. However, if we assume the magma to be left or right cancellative, then we get :

$$x^{k-1} = x^{l-1} \text{ if } k > 1$$

This violates the minimality of k. Thus we conclude that $k = 1$. In other words, the sequence of powers of x is **periodic**.

A little more analysis of this situation reveals that, in this case, we actually get a **subgroup** – the cyclic subgroup of order $l - 1$. However, the multiplicative identity of the subgroup may not be a multiplicative identity in the whole magma.

4.6. Where we have reached. In this section, we began with the **Lagrange property** and used that, along with the behaviour of subgroups generated by a single element, to conclude that "every group of prime order is cyclic" and hence Abelian.

We then explored the more general case of a semigroup, and even a power associative magma, and the subsemigroup (commutative) generated by a single element. We observed that there are two possibilities for the sequence of positive powers :

- It is like $\mathbb{N}$ under addition.
- It becomes eventually periodic.

In case the **generator** is cancellative, the sequence of positive powers can be eventually periodic only if it is periodic. In other words, there is some power of x that is again equal to x.

More exploration along these lines shall be carried on in `Part II`. For the moment we take on the study of **conjugations** and **normal subgroups**, which form the very backbone of group theory.

5. Conjugacy classes and normal subgroups

5.1. Grander steps. Having laboured so far, we are now close to being able to appreciate the vast and beautiful sceneries in the landscape of groups. Till this point, we have been pedantic and fussy about practically every step, insisting on writing it in general form. This has been necessary in order to understand and appreciate how very easy groups are, compared to other structures.

However, the coming steps are of the kind that are best considered only for groups. Even these steps do generalize, but the generalizations require more energy and effort and are not as natural as the development in the case of groups.

We shall also try to understand how the working mathematician (not a group theory expert) perceives groups, and how we can recall and remember the key ideas associated with groups. Admittedly, the journey into groups is extremely fascinating but we all cannot afford to tread every path in this journey. So, we shall try to get a little flavour of each path that we cannot traverse in its entirety.

5.2. **Conjugations.** A **conjugation**(defined) in a group G by an element g in the group is defined as the map $x \mapsto gxg^{-1}$. We sometimes say that we are conjugating x by g. At times, conjugation is also referred to as a **transform**(defined), so that we say that x is being transformed by g.

Conjugations are crucial to group structure in at least two distinct ways. Typically, these two distinct ways are not cleanly separated, because one follows from the other. However, it is conceptually easier to understand if we accept that these two roles played by conjugations are quite different. Moreover, when we study less nice structures such as rings, the two roles become visibly different.

The first crucial fact is :

> Every conjugation is an automorphism.

Proof. We first prove that a conjugation is a homomorphism. That is, if $\phi(x) = gxg^{-1}$ we must show that
$$\phi(xy) = \phi(x)\phi(y)$$
Showing this is sufficient, because, as discussed in `Group Theory:A First Journey`, any map that preserves the multiplicative structure between groups must preserve the inverse map as well as the identity.

The left hand side becomes :

$$
\begin{aligned}
\phi(xy) &= g(xy)g^{-1} \\
\implies \phi(xy) &= gx(g^{-1}g)yg^{-1} \\
\implies \phi(xy) &= (gxg^{-1})(gyg^{-1}) \\
\implies \phi(xy) &= \phi(x)\phi(y)
\end{aligned}
$$

For the sake of clarity, we can also verify that

$$
\begin{aligned}
\phi(e) &= geg^{-1} \\
\implies \phi(e) &= gg^{-1} \\
\implies \phi(e) &= e
\end{aligned}
$$

And that :

$$
\begin{aligned}
\phi(x^{-1}) &= gx^{-1}g^{-1} \\
\implies \phi(x^{-1}) &= (g^{-1})^{-1}x^{-1}g^{-1} \\
\implies \phi(x^{-1}) &= (gxg^{-1})^{-1} \text{ (Here we use the reversal law for products)} \\
\implies \phi(x^{-1}) &= (\phi(x))^{-1}
\end{aligned}
$$

We have so far succeeded in showing that the map $x \mapsto gxg^{-1}$ is a homomorphism. We must show that it has an inverse homomorphism as well, to be able to claim that it is an automorphism. The inverse map here is the map $x \mapsto g^{-1}xg$. If we denote this as ρ, we have :

$$
\begin{aligned}
\rho(\phi(x)) &= g^{-1}(gxg^{-1})g &= x \\
\phi(\rho(x)) &= g(g^{-1}xg)g^{-1} &= x
\end{aligned}
$$

$\square$

A conjugation is also called an **inner automorphism**(defined) because it can be expressed by an **algebraic formula** using elements *inside* the group.

As we can see, the proof uses heavily all the three aspects of group structure – namely the existence of identity element, the associativity and the existence of inverse elements.

<div align="center">Concept Testers</div>

(1) Consider a monoid S with identity element e. Prove that, if $xy = e$, the map $s \mapsto ysx$ is a semigroup homomorphism from S to itself, though not necessarily a monoid homomorphism.

(2) In the above problem, prove that if $xy = yx = e$, the map $s \mapsto ysx$ is an automorphism of the monoidal structure. Thus, the elements possessing both left and right inverses in a monoid give rise to monoid automorphisms.

<center>POINTS TO PONDER</center>

- Suppose $(S, *)$ is a magma with a neutral element e. What conditions must x and y satisfy so that the map $s \mapsto ysx$ is a magma homomorphism? What conditions must they satisfy so that it is a homomorphism preserving the neutral element? What conditions must they satisfy so that it is an automorphism?
- Can we come up with other formulas that are always guaranteed to give rise to a homomorphism for any group? The answer is in fact *no* – something we shall explore later.

5.3. **The inner automorphism group.** Every element of the group defines an inner automorphism. This inner automorphism is a bijection from the group to itself. Further, if we consider two elements of the group, the inner automorphism induced by their composite is the composite of the inner automorphisms induced by them individually.

That is, if c_g is the map $x \mapsto gxg^{-1}$, we have :

$$
\begin{aligned}
c_{gh}(x) &= ghx(gh)^{-1} \\
\implies c_{gh}(x) &= ghxh^{-1}g^{-1} \\
\implies c_{gh}(x) &= g(hxh^{-1})g^{-1} \\
\implies c_{gh}(x) &= c_g(c_h(x)) \\
\implies c_{gh} &= c_g.c_h
\end{aligned}
$$

This means that the map $g \mapsto c_g$ is a homomorphism from G to the symmetric group on G, or, in other words, defines an action of the group on itself. This is the group action on itself by conjugation. It differs from the group action on itself by left multiplication in the sense that here, the permutation induced by any fixed element of the group is an *automorphism*.

The image of G under this map is the set of all automorphisms of G that are inner, that is, the **inner automorphism group**(defined) of G. The inner automorphism group forms a subgroup of the automorphism group (the group of all automorphisms) of G which in turn forms a subgroup of the symmetric group on G (that is, the group of all permutations on G as a set). We thus have :

<center>Inner automorphism group $\leq$ Automorphism group $\leq$ Symmetric group</center>

Another way of looking at this is that the property of being an inner automorphism is stronger than the property of being an automorphism, because only those automorphisms that can be expressed in a particular way are inner. The property of being an automorphism, in turn, is stronger than the property of being an arbitrary permutation, because only those permutations that preserve the group structure are deemed to be automorphisms.

5.4. **Conjugacy as an equivalence relation.** Every group acts on itself via conjugation. Under this group action, there are **orbits**. These orbits are termed **conjugacy classes**.

When a group acts on a set, it also naturally acts on the set of all subsets of any given cardinality. For instance, suppose G acts on a set S, and we look at the set of all subsets of S of cardinality k. Since the action of any element of G is a permutation, the images of the elements in any subset are distinct, and hence, give rise to another subset of the same cardinality. Thus, the group acts on a subset of cardinality k, giving another subset of cardinality k.

Clearly, the identity maps every subset to itself, and the composite of two group elements acts as the composite of their actions, so this satisfies the axioms of a groups action.

Thus, the group action on the set of its *elements* by inner automorphisms also gives rise to the group action on the set of its *subsets* by the same inner automorphisms. The image of a subset under the inner automorphism is the set of all elements obtained as images of the *elements* of the subset under that inner automorphism.

5.5. Conjugate subgroups. The conjugation map is an automorphism, and hence, conjugation by any element must take everything to something similar. In particular, conjugation takes a subgroup of the group to a subgroup.

Two subgroups H and K of a group G are said to be **conjugate** in G provided that there is an $x \in G$ such that $xHx^{-1} = K$. Here xHx^{-1} is the set of all elements of the form xhx^{-1} where $h \in H$.

<div align="center">POINTS TO PONDER</div>

- Is it possible that a subgroup of a group be conjugate to a proper subgroup of itself?

5.6. A philosophical view of conjugations. We are typically interested in meaningfully studying only those aspects of structure that are **isomorphism invariant**. Any aspect of group structure that is isomorphism invariant must at the very least be automorphism invariant.

Thus, we might ask : "why look only at inner automorphisms in so much detail, when we should actually be looking for invariance under all automorphisms?" There are a number of deep reasons for this. The first, of course, is that inner automorphisms are far tamer and easier to handle than arbitrary automorphisms. Secondly, they can be expressed by explicit formulas, which in itself adds to their utility.

Yet another reason is linked to normal subgroups, which shall unfold in section 7.

The most important reason is that inner automorphisms extend to the way that groups *act* or *manifest themselves*. This point, again, will become clear only after some time.

5.7. Where we are placed. We have seen conjugations in the following role :

- Algebraic formulas that are guaranteed to give rise to automorphisms. These are called inner automorphisms. Moreover, the inverse of a conjugation is also a conjugation.
- A way for the group to act on itself as automorphisms. That is, a homomorphism from the group to its automorphism group. The automorphisms that are realized as images of elements of the group are precisely the inner automorphisms.

As mentioned in the previous subsection, there are plenty of reasons why inner automorphisms are studied in a lot of detail, as compared to other automorphisms.

In the next two sections, we shall see how conjugations are a measure of *failure of commutativity*, and introduce ourselves to the concept of **normal subgroups**.

<div align="center">6. COMMUTATIVITY AND ABELIAN GROUPS</div>

6.1. Commutativity as a property of binary operations. Let us recall the way we have proceeded so far, to get a good understanding of the subject of group theory. We began by considering a magma, viz a set with a binary operation, and looking at various properties that we could impose upon the binary operation. Among the properties that we considered were associativity, the existence of neutral elements and the existence of left (and right) inverses. These formed the focus of our study because they were precisely the properties corresponding to the definition of group.

We had also introduced, at the time, the notion of a **commutative binary operation**, but had not discussed it in detail.

Definition. A binary operation $*$ on a set S is said to be **commutative**(defined) if we have :

$$a * b = b * a \ \forall \ a, b \in S$$

We're now going to learn more about commutativity.

6.2. Commutativity along with associativity. The operation of addition on the set of natural numbers $\mathbb{N}$ is both commutative and associative, that is :

$$
\begin{aligned}
a + b &= b + a \ \forall \ a, b \in \mathbb{N} \\
a + (b + c) &= (a + b) + c \ \forall \ a, b, c \in \mathbb{N}
\end{aligned}
$$

In `Group Theory:A First Journey` we had observed that as a consequence of associativity, the parenthesization (or bracketing) in any expression can be dropped. If the operation is commutative as well, then the *order of the terms* also becomes irrelevant. Thus, we have :

$$a + (b + c) = (a + b) + c = (b + c) + a = b + (c + a) \ldots$$

As a result, the only thing that matters in our expression is how many times each letter occurs.

A set with a binary operation that is both commutative and associative is termed an **Abelian semi-group**(defined). If the operation also gives a group structure, it is termed an **Abelian group**(defined). Thus, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are examples of Abelian groups, while $(\mathbb{N}, +)$ is an Abelian semigroup which is not an Abelian group.

The following conventions are typical for Abelian groups :

- The binary operation is denoted by $+$.
- The neutral element is denoted by 0.
- The inverse of x is denoted by $-x$. Expressions such as ab^{-1} are written as $a - b$.
- The nth power of x is denoted as nx.

The reason why we follow these conventions shall become clearer when we study the general concept of modules over commutative rings.

<div align="center">Concept Testers</div>

(1) Suppose $(S, +)$ is a commutative magma (that is, a set with commutative binary operation $+$). Prove that S is isomorphic to its opposite magma.
(2) Prove that the set of left associative elements of S is precisely the same as the set of right associative elements of S, where $(S, +)$ is a commutative magma. Is it also the same as the set of middle associative elements?
(3) Suppose $(S, *)$ is a magma. An element in S is said to be **central**(defined) if it commutes with every element in S, that is, $a \in S$ is central if and only if $a * x = x * a \ \forall \ x \in S$. The **center**(defined) or **commutative center**(defined) is the set of all central elements. Prove that if the magma has a neutral element, then that is central.
(4) Prove that the intersection of the commutative center and associative center of a magma is a submagma.
(5) Prove that in a semigroup, the commutative center forms a subsemigroup, and in a monoid, it forms a submonoid.
(6) It is clear that if, in a monoid, a central element has a left inverse, it also has a right inverse and they are equal. Prove that the inverse of an invertible central element in a monoid is also an invertible central element.
(7) Thus, show that the (commutative) center of any group is a subgroup thereof.

<div align="center">Points to Ponder</div>

- Look carefully at the proof of the Concept Tester above, showing that the intersection of the commutative center and associative center is a submagma. What kinds of associativity have we used in the proof? Left, middle or right?

6.3. **Significance of Abelianness.** Commutativity and associativity together make the structure quite simple. Terms can be brought together in any manner. Thus, $a + b + b + a$ is the same as $2a + 2b$ and this is the same as $2(a + b)$.

We had earlier seen that many important properties pertaining to inverse elements required the use of associativity. The crux was that when multiplying by the inverse of an element to cancel its action, we needed to re parenthesize the expression. This reparanthesization required the use of associativity.

With the additional property of commutativity, we can make sure that an element and its inverse sitting far from each other in an expression can cancel each other's action.

<div align="center">Concept Testers</div>

(1) Prove that in an Abelian group, the map $x \mapsto nx$ is a group endomorphism where $n \in \mathbb{Z}$. More generally, prove this for a commutative magma.
(2) Prove that if ϕ and ψ are two homomorphisms from a magma $(S, .)$ to a commutative magma $(T, *)$ prove that $x \mapsto \phi(x) * \psi(x)$ is also a homomorphism. Show that the previous problem is a special case of this.
(3) Prove that a group is Abelian if and only if the map $x \mapsto x^2$ is an endomorphism.
(4) Prove that a group is Abelian if and only if the map $x \mapsto x^{-1}$ is an endomorphism.

<div align="center">Points to Ponder</div>

- The second Concept Tester above gives an important intrinsic characterization of Abelian groups – by saying that the pointwise product of two homomorphisms from a group to an Abelian group is also a homomorphism. Can we use this to give a group structure to the set of all homomorphisms from a group to an Abelian group?

  This is discussed in more detail in `Ring Theory : A First Journey`.

- Let us look again at the proof of the statement that a group is Abelian if and only if the map $x \mapsto x^2$ is an endomorphism. What property of groups have we used in the proof? Can the result be extended to more general structures?
- Let ϕ be an endomorphism of a finite group G. Let α be the ratio of the number of elements in G taken to their inverses, to the total cardinality of G. We have shown above that if $\alpha = 1$, then G is Abelian. Is there some threshold value α_0, such that if $\alpha \geq \alpha_0$, then G is Abelian?

6.4. **Conjugation map in view of commutativity.** The basic result we have is :

Claim. Two elements commute if and only if the conjugation map by any one of them fixes the other.

Proof. Let the group be G and the elements be a and b. Then :

$$
\begin{aligned}
ab &= ba \\
\Longleftrightarrow a &= bab^{-1} \text{ (multiplying by } b^{-1} \text{ on the right)} \\
\Longleftrightarrow aba^{-1} &= b \text{ (multiplying the original by } a^{-1} \text{ on the right)}
\end{aligned}
$$

Note that when performing manipulations with groups, we need to specify not just the value by which we are multiplying, but also whether we perform the multiplication on the left or on the right. $\square$

Though the above proof is very elementary, the idea behind the proof is very important. We shall later encounter it when we study normal subgroups, and product of subgroups.

Some consequences of this are :

- In an Abelian group, the conjugation map by any element is the identity map.
- In a general group, the conjugation map by any element fixes every element in the center.
- In a general group, the conjugation map by any element in the center fixes every element.

We had earlier remarked that the group can be considered to act on itself by conjugation and under this action, there are orbits. Each such orbit is termed a **conjugacy class**(defined). In other words, the conjugacy class of x is the set of all elements of the form gxg^{-1} where $g \in G$ (that is, all elements accessible from G via conjugations). If an element in the group is central, then its orbit is itself – that is, its conjugacy class comprises only the element itself.

A subset of a group is called **self conjugate**(defined) if it is a union of conjugacy classes, that is, a union of orbits under the group action by conjugation. This indicates that the conjugation map by any element in the subgroup leaves the subset invariant. Clearly, *any* subset of the center is self conjugate, because every singleton subset in it is an orbit.

A **self conjugate subgroup**(defined) or **normal subgroup**(defined) is defined as a subgroup that is also a self conjugate subset. Normal subgroups play a pivotal role in group theory. This shall unfold in the next section (section 7).

CONCEPT TESTERS

(1) Prove that the inner automorphism group of a group is the trivial group if and only if the group is Abelian.
(2) A **nontrivial automorphism**(defined) is an automorphism other than the identity map. Prove that $(\mathbb{Z}, +)$ (that is, the group of integers under addition) has precisely one nontrivial automorphism, and that this is not inner.

6.5. **Where we are placed.** In this section, we looked at Abelianness of groups and commutativity of elements and related these with the conjugation map. The study of which elements of the group commute with each other helps us understand the group structure very well. Currently, we are not sufficiently well equipped to undertake that part of the journey, so we must prepare ourselves better.

In the next section, we shall look at **normal subgroups** in many different ways, and study them from every angle. Though our study may appear detailed, there are many facets of normality that we do not touch upon at this early stage in the journey. We shall explore some of them later in the journey, and in `Part II`, while others shall be left for the next journey – `Group Theory:We Delve Deep`.

7. NORMAL SUBGROUPS

7.1. **As ideals – kernels of homomorphisms.** The **kernel**(defined) of a **group homomorphism**(recalled) is the inverse image of the identity element under the homomorphism. That is, if $\phi : G \to H$ is a group homomorphism, the set

$$\{x \mid x \in G, \phi(x) = e\}$$

is termed the kernel of ϕ and is written as $\ker \phi$.

In `Group Theory:A First Journey`, we had seen, in one of the CONCEPT TESTERS, that the kernel of any group homomorphism $\phi : G \to H$ is a subgroup of G. The proof was as follows :

- $\phi(e) = e$, so this subset contains the identity of G.
- $\phi(x) = e$ and $\phi(y) = e$ so $\phi(xy) = \phi(x)\phi(y) = e$, so this subset is closed under multiplication.
- $\phi(x) = e$ implies that $\phi(x^{-1}) = (\phi(x))^{-1} = e$, so the subset is closed under inverses.

The fact that we used crucially in the proof was that the identity element, in itself, is a subgroup, and is hence closed under the operations of neutral element, inverse and multiplication. That is why its pre-image must also be closed under these operations.

In other words :

Upshot. Any formula that is guaranteed to take the identity element to the identity element must leave the inverse image of the identity element invariant.

We know that the identity element is invariant under conjugation by any element in the group. That is, given any g, $geg^{-1} = g$ (this is essentially the same as saying that $ge = eg$). This would lead us to suspect, from the above statement, that the inverse image of the identity element is a normal subgroup. And indeed:

Claim. The kernel of any group homomorphism is a normal subgroup of the group on the left.

Proof. Let $\phi : G \to H$ be a homomorphism of groups, and let N be the inverse image of the identity. We have already shown that N is a subgroup of G. To show that it is normal in G, we need to prove that the conjugation map by any element in G leaves N invariant.

Let $g \in G$. Consider $c_g : x \mapsto gxg^{-1}$. Suppose $x \in N$. Then we have :

$$
\begin{aligned}
x &\in N \\
\phi(x) &= e \\
\implies \phi(g)\phi(x)\phi(g^{-1}) &= \phi(g)\phi(g^{-1}) \\
\implies \phi(gxg^{-1}) &= e \\
\implies c_g(x) &\in N
\end{aligned}
$$

Hence, N is a normal, or self conjugate, subgroup. $\square$

Notice that so far, all we have shown is:

$$\text{Kernel of a group homomorphism} \implies \text{normal}$$

We have *not* shown that every normal subgroup can be expressed as the kernel of a group homomorphism. That result shall have to wait till `Part II`.

In symbols, we write $N \trianglelefteq G$ to denote that N is a normal subgroup of G (when N is simply a subgroup, we write $N \leq G$).

CONCEPT TESTERS

(1) Prove that every homomorphism on groups can be expressed as a surjective homomorphism followed by an injective homomorphism. (Hint : Look at the image of the homomorphism as a subgroup of the group on the right).
(2) Prove that if a subgroup of a group is the kernel of a homomorphism, then it is the kernel of a surjective homomorphism.
(3) What is the kernel of an injective homomorphism? Is it a normal subgroup?
(4) The **trivial homomorphism**(defined) is the homomorphism from a group to the trivial group that takes every element to the identity element. What is the kernel of the trivial homomorphism? Is it a normal subgroup?
(5) Suppose H_1 and H_2 are subgroups of G. Then consider the inclusion map $H_1 \to G$. What is the inverse image of H_2 under this map?

POINTS TO PONDER

- Is it true that every normal subgroup can be realized as the kernel of some homomorphism? Equivalently, is it true that every normal subgroup can be realized as the kernel of some surjective homomorphism?
- What are the various possibilities for the image group under such a surjective homomorphism?

7.2. As subgroups with the same left and right cosets. Normality is equivalent to the condition that the left cosets are the same as the right cosets:

Claim. If N is a subgroup of G, N is normal in G if and only if $Nx = xN$ for every $x \in G$.

Proof. Suppose N is normal. Consider an element in Nx. This can be written as nx where $n \in N$.
We would like to write it in the form xn' where $n' \in N$. Let us compute n'.

$$
\begin{aligned}
nx &= xn' \\
\implies x^{-1}(nx) &= x^{-1}(xn') \\
\implies x^{-1}nx &= n'
\end{aligned}
$$

The second step is multiplication by x^{-1} on the left to cancel out the x in the right hand side.
It is clear that, because N in normal, $n' \in N$, and hence, nx can be written as an element of xN.
To prove the converse, suppose every element of the form nx can be written as an element of the form xn' for some n'. Then, as shown above, $n' = x^{-1}nx$. This means that for every x in G and every n in N the conjugate of n by x^{-1} lies in N. This shows that N is normal. $\square$

Thus we have shown that:

$$\text{Normal} = \text{Left and right cosets coincide}$$

In some sense, N commutes with the element x. The approach used in this proof is simply a kind of generalization of the earlier observation : "two elements commute if and only if conjugation by one element fixes the other." Here, the corresponding statement is : "a subgroup and an element commute if and only if conjugation by the element fixes the subgroup."

Concept Testers

(1) Prove that a subgroup of index 2 in a group must be a normal subgroup. Establish an explicit homomorphism from this group to another group, whose kernel is the given subgroup of index 2.

7.3. As inner automorphism invariant subgroups. In the last subsection, we defined a normal subgroup as the kernel of a homomorphism, and proved that a necessary and sufficient condition for a subgroup to be normal is that it be a union of conjugacy classes, or equivalently, that any inner automorphism take elements within the subgroup to elements within the subgroup.

I would like to emphasize that this latter definition constitutes a *different characterization* of normal subgroups compared to the characterization as a kernel of a homomorphism, and the two characterizations being the same is simply a consequence of the orderliness of group theory. Let us look at the statement again :

A subgroup is said to be normal if any inner automorphism of the group takes elements of the subgroup to elements of the subgroup.

Another way of putting this is as follows :

A subgroup is said to be normal if it is invariant under all inner automorphisms of the group.

Here, we say that a subset is invariant under a function from the set to itself if its image lies inside it.
Actually, we can say something more. If we look at the restriction of an inner automorphism to the subgroup, we get a set map from the subgroup to itself (because it is invariant under the inner automorphism). From this, we can in fact deduce that the restriction is an **endomorphism** of the subgroup.
A more generalized version of this is the claim :

Claim. If a subgroup is invariant under an endomorphism, the restriction of the endomorphism to the subgroup defines an endomorphism from the subgroup to itself.

For instance, if H is a subgroup of G and there is an automorphism σ of G such that $\sigma(h) \in H$ whenever $h \in H$. Then the restriction of σ to H defines a map $H \to H$. This map is again an endomorphism.
But, if the original map is an **automorphism**, there is no reason to suppose that the restriction map is also an automorphism. That is, it may be possible that an automorphism of G restricts to an endomorphism of H that is not an automorphism of H.

Claim. If a subgroup is invariant under an injective endomorphism, the restriction of the endomorphism to the subgroup defines an injective endomorphism from the subgroup to itself.

Claim. It is possible that a subgroup is invariant under an automorphism but that the restriction of the automorphism to the subgroup is not an automorphism of the subgroup.

But now comes the twist :

Claim. If a subgroup is invariant under an automorphism and also under the inverse of that automorphism, then the restriction of the automorphism to the subgroup must be an automorphism on the subgroup.

Now we return to the definition of **normal subgroup**. A normal subgroup was defined as a subgroup that is invariant under all inner automorphisms. But we know that the *inverse of an inner automorphism is an inner automorphism*. This means that, by the above claim, the restriction of any inner automorphism to a subgroup is an automorphism of the subgroup. This allows us to redefine a normal subgroup thus :

> A normal subgroup is a subgroup such that the restriction of any inner automorphism of the group to the subgroup is an automorphism of the subgroup.

<div align="center">CONCEPT TESTERS</div>

(1) Prove all the claims above. Be very careful about what aspects of the group theoretic definition are being used.
(2) Prove that the map $x \mapsto 2x$ is an automorphism of $(\mathbb{Q}, +)$ but that its restriction to $\mathbb{Z}$ is not an automorphism of $\mathbb{Z}$.
(3) Prove that if a finite subgroup of a group is invariant under an automorphism of the group, then the restriction to the subgroup must be an automorphism of the subgroup.

7.4. **A mapping system formulation.** Normality is a **subgroup property**. That is, given a group and a subgroup, we can ask the question : *is the subgroup normal?* The normality depends not just on the structure of the group or of the subgroup, but on the *way the subgroup is placed in the group*.

In particular that means that it is meaningless to talk of anything like a normal *group*. Normality is *relative*.

Now, given any group, and any subgroup, we can, for every function on the group, try to restrict that function to the subgroup. This restriction gives a map from the subgroup to the group. If the subgroup is *invariant* under the function, then the restriction gives a map from the subgroup to itself. We can then ask questions like : how do properties associated with the function on the group affect properties associated with the function on the subgroup?

In this language, we define normality as :

$$\text{Normal } \equiv^{\text{(Function restriction)}} \text{Inner automorphism} \to \text{Set map}$$

Translated into words, normality is the property of a subgroup whereby every inner automorphism (as a function on the whole group) restricts to a set map (as a function on the subgroup).

We had seen that we can replace Set maps on the right by endomorphisms, because the restriction of any endomorphism, if a well defined set map, is an endomorphism. Thus, we can rewrite it as :

$$\text{Normal } \equiv^{\text{(Function restriction)}} \text{Inner automorphism} \to \text{Endomorphism}$$

Because the property of being an inner automorphism is closed under inversion (that is, the inverse of an inner automorphism is inner), we can further rewrite this as :

$$\text{Normal } \equiv^{\text{(Function restriction)}} \text{Inner automorphism} \to \text{Automorphism}$$

So far, with every step, we have made the right side stronger and stronger, without changing the meaning of normality. Is it possible to go further, and make the right side Inner Automorphisms? The answer is *no*. In fact, automorphisms is the best we can hope for.

<div align="center">POINTS TO PONDER</div>

• The above statement – "automorphisms is the best we can hope for" is vaguely formulated. Can we make a precise formulation of this, in a manner that it is clear how to mathematically approach the problem? (The proof relies on a construction that is far ahead of us at the moment, but the formulation of the problem is pure logic).

7.5. Characteristicity. Normal subgroups are subgroups that remain preserved under certain symmetries of the whole group. This suggests that any symmetry invariant way of defining a subgroup will give us a normal subgroup.

To this end, let us try to define a notion of subgroup that is invariant under *all* symmetries. We define the following :

Definition. A **characteristic subgroup**(defined) of a group is a subgroup with the property that every automorphism of the group restricts to an automorphism of the subgroup.

This is also sometimes termed an **invariant subgroup**(defined) or an **automorphism invariant subgroup**(defined) Given any automorphism of the group, it takes an element of the subgroup to some element of the subgroup. Using the claims in section 7.3, we conclude that the restriction to the subgroup is, in fact, an automorphism of the subgroup.

Some important points about characteristicity :

- Characteristicity is a **subgroup property**. That is, the property of being a characteristic subgroup depends, not just on the bigger group or on the subgroup, but on the *way the subgroup is placed in the bigger group*.
- Characteristicity can be expressed as a property in the mapping system as :

$$\text{Characteristic } \equiv^{\text{(Function restriction)}} \text{Automorphism} \to \text{Automorphism}$$

  It can also be expressed as :

$$\text{Characteristic } \equiv^{\text{(Function restriction)}} \text{Automorphism} \to \text{Set map}$$

- A property π is transitive if the following holds : if H is a subgroup of K with property π in K and K is a subgroup of G with property π in G, then H has property π in G.
  Characteristicity is transitive, which is evident from the mapping system representation of characteristicity (because the left and right sides are the same). That is, "every characteristic subgroup of a characteristic subgroup is a characteristic subgroup".
- A characteristic subgroup of a normal subgroup is normal.

In the next subsection, we expound on the last two statements.

Concept Testers

(1) Prove that the trivial and improper subgroup are characteristic.
(2) Using the mapping system formulation, show that any characteristic subgroup is normal.
(3) Prove that the center of a group (that is, the set of elements that commute with every element of the group) is a characteristic subgroup of the group.

Points to Ponder

- Given a group, any procedure that selects a unique subgroup in an intrinsic group theoretic manner must yield a characteristic subgroup. Why is that so?

7.6. Characteristic and normal. We now give proofs of the above statements. We begin by proving :

Claim. Characteristicity is transitive. That is, a characteristic subgroup of a characteristic subgroup is characteristic.

Proof. Let us fix some names (for convenience). Let H be a characteristic subgroup of K and K be a characteristic subgroup of G. We need to show that H is a characteristic subgroup of G.

That is, we need to show that H, as a subgroup of G, satisfies :

$$\text{Characteristic } \equiv^{\text{(Function restriction)}} \text{Automorphism} \to \text{Automorphism}$$

So, we need to show that, starting with any automorphism of G, the restriction of that automorphism to H is well defined.

We know that the restriction to K is well defined, so, any automorphism of G restricts to an automorphism of K. But as H is a characteristic subgroup of K any automorphism of K restricts to an automorphism of H. But the restriction of the restriction of a function, is simply the restriction, so we conclude that the restriction of any automorphism of G, to H, is an automorphism of H.

$\square$

No property of automorphisms as such was used in the above proof. This suggests a somewhat more general formulation :

Claim. Suppose a subgroup property π can be expressed as $\alpha \to \alpha$ with respect to function restrictions. Then, π is transitive. That is, if H has property π as a subgroup of K and K has property π as a subgroup of G then H has property π as a subgroup of G.

<center>CONCEPT TESTERS</center>

(1) Prove the property mentioned above – that "a characteristic subgroup of a normal subgroup is normal". Try to express the proof using a mapping system formulation, and obtain a generalized version.

(2) Why can the above proof not be used to show that every normal subgroup of a normal subgroup is normal?

(3) A **central factor**(defined) of a group is a subgroup with the property that every inner automorphism of the group restricts to an inner automorphism of the subgroup. Prove that every normal subgroup of a central factor is normal.

<center>POINTS TO PONDER</center>

- When we say "every characteristic subgroup of a normal subgroup is normal" or "every characteristic subgroup of a characteristic subgroup is characteristic" we are essentially making assertions of the form : "every subgroup with property π in a subgroup with property σ has property θ". Can we think of this as saying something like π multiplied with σ implies θ? How can this notion be made precise? Such questions are in the realm of **property theory**.

- We had earlier seen that a subgroup of index 2 in a group is always a normal subgroup. Can the fact be proved using the mapping system formulation of normality? Is it necessary that a subgroup of index 2 must always be characteristic?

7.7. Where this leaves us. In this section, we have introduced ourselves to a very important concept – that of a **normal subgroup**. A normal subgroup has been described as a union of conjugacy classes, as an inner automorphism invariant group, and as a subgroup with the same left and right cosets. We have also seen that the kernel of any homomorphism must be a normal subgroup.

In fact, the converse also holds – every normal subgroup occurs as the kernel of a homomorphism, and in some sense, the kernel tells us all we need to know about the homomorphism when it is surjective. This is by no means immediate, though it is not hard to prove. We defer the proof for later (it is there in `Part II`). The construction involved is that of the **quotient group**.

In order to understand normality better, we understood another property – that of being **characteristic**, that is, **automorphism invariant**. The property of being characteristic is stronger than that of being normal.

To understand the relationship between characteristicity and normality, we used a mapping system formulation for both properties, and worked via that formulation. We saw that many of our proofs became exercises in logic and the ideas behind the proofs got more clearly illuminated.

This way of approaching subgroup properties, from the viewpoint of mapping system formulations, and trying to formulate results as relationships between properties, lies at the heart of **property theory**. Refer the appendix for a somewhat more detailed review. More on this is to be found in my article on property theory.

<center>8. SUBGROUP STRUCTURE</center>

8.1. A little warm up. As the above discussion on normal and characteristic subgroups makes clear, the term **subgroup** carries with it not just the abstract group structure of the subgroup, but also the manner in which it is embedded in the bigger group.

Some facts that we had seen about subgroups in `Group Theory:A First Journey`.

- A subgroup of a subgroup is a subgroup.
- The intersection of a family of subgroups is a subgroup of each of them, and hence of the whole group.
- If one subgroup is a subset of another subgroup, then it is a subgroup of that.

An interesting consequence of these is that given any subset we can look at the smallest subgroup containing that subset, that is also the intersection of all subgroups containing that subset. This is explored in more detail in section 8.3.

8.2. **Some facts on normal and characteristic subgroups.** Recall that normality has been defined as follows :

$$\text{Normal} \equiv^{\text{(Function restriction)}} \text{Inner automorphism} \to \text{Set map}$$

That is, a subgroup is said to be normal in a group if given any inner automorphism of the group, the inner automorphism takes the subgroup to within itself.

We now try to prove the statement :

The intersection of a family of normal subgroups is a normal subgroup.

Proof. The intersection is clearly a subgroup. Thus, we only need to show that the restriction satisfies the property :

$$\text{Normal} \equiv^{\text{(Function restriction)}} \text{Inner automorphism} \to \text{Set map}$$

In other words, we need to show that any inner automorphism of the group must take elements in the intersection to themselves.

Suppose we look at some element in the intersection of the family of subgroups. Look at its image under an inner automorphism. This image must lie in each of the subgroups (because each of them is normal) and hence also lies in the intersection. So we are done. □

Let us look at the above proof and try to comprehend *what made it click*. The crucial argument was purely set theoretic – if a collection of subsets is invariant under a particular function, so is their intersection. The particular nature of the function – "inner automorphism", played no role in the proof. This suggests that we can state more generally :

Any subgroup property π defined as :

$$\pi \equiv^{\text{(Function restriction)}} \alpha \to \text{Set map}$$

satisfies the following : the intersection of a family of subgroups, each having property π in the whole group, also has property π in the whole group.

Here, α could be any property of functions from the group to itself.

The proof is exactly the same as that for normal subgroups. Note that now "inner automorphisms" can be replaced by any property α. In particular, we can set α to be all automorphisms, in which case we have the statement :

The intersection of an arbitrary family of characteristic subgroups of a group is a characteristic subgroup of the group.

More generally, properties that can be written in the above form, as $\alpha \to$ Set map, are termed **invariance properties**. Thus, a slicker way of saying the above is :

Any invariance property of subgroups (such as normality, characteristicity) is closed under arbitrary intersections.

There are plenty of statements about normality that do not generalize to arbitrary invariance properties. For instance :

A normal subgroup of a group is a normal subgroup of any subgroup of the group containing it.

Proof. Let us fix some names, for convenience of explanation. Let G be the subgroup, H be the normal subgroup (in symbols, $H \trianglelefteq G$), and K be a subgroup of G containing H. Then we want to show that H is normal in K. That is, we want to show that given any inner automorphism of K, it takes elements of H to elements of H.

We *cannot proceed further* by treating inner automorphisms as a black box. We need to use what inner automorphisms are. An inner automorphism is a conjugation by some element in the group. In particular, an inner automorphism in K is a conjugation by some element in K.

We know that a conjugation by an element in K is also a conjugation by an element in G (because elements of K are elements of G). Thus, if H is invariant under conjugations by elements in G, it is also invariant under conjugations by elements in K.

Thus, we have shown that H is normal in K. □

Roughly speaking, the main fact about inner automorphisms that we have used in the above proof is that any inner automorphism of a subgroup (in the above proof, K) *extends to* an inner automorphism of the group (in the above case, G). Look at the POINTS TO PONDER for further exploration.

The Concept Testers given below are more of exercises in logic than in group theory. However, the results that they give rise to are very fundamental to our understanding the properties of normality and characteristicity. To get the most out of them, it is best to revisit the solutions and try to understand *what makes them click*.

Concept Testers

(1) If H is a normal subgroup of G and K is an arbitrary subgroup of G, prove that $H \cap K$ is a normal subgroup of K.
(2) Suppose $H_1 \trianglelefteq K_1 \leq G$ and $H_2 \trianglelefteq K_2 \leq G$. Prove that $H_1 \cap H_2$ is a normal subgroup of $K_1 \cap K_2$.
(3) Prove that if $\phi : H \to G$ is a surjective map from a group H to a group G that is also a homomorphism, then the image of a normal subgroup of H is a normal subgroup of G.
(4) Prove that if $\phi : H \to G$ is a homomorphism of groups, then the pre-image of any normal subgroup of G is a normal subgroup of H.

   If H is a subgroup of G and ϕ is an inclusion map, show that this establishes that "any normal subgroup is a normal subgroup of any subgroup containing it".

Points to Ponder

- What aspects of normality did we use in each of these proofs? Which of these statements can be generalized to characteristicity?
- The key attribute of inner automorphisms that we are using in our proofs is that they can be transferred across homomorphisms, and in particular, extended from subgroups. This raises some interesting automorphism properties :
   - The property of being an automorphism that can be lifted to an automorphism of any bigger group containing it.
   - The property of being an automorphism that gives rise to an automorphism for every surjective homomorphism to another group.
   - The property of being an automorphism that gives rise to an automorphism for every homomorphism to another group.

   Inner automorphisms satisfy all these properties? Why? What attribute of inner automorphisms is used in proving each of these?

8.3. **Subgroup generated, and some results.** We had defined earlier, the **subgroup generated by a subset** as the smallest subgroup that contains it, or, equivalently, as the intersection of all subgroups that contains it. If a subset is already a subgroup, it is the same as the subgroup it generates.

Here is a description of the subgroup generated by a subset :

Claim. The subgroup generated in the subset (that is, the smallest subgroup containing the subset) is precisely the set of all elements that can be written as finite products of elements in the subset, and their inverses.

Proof. This rests on two observations:
- The set of all elements that can be written as finite products of elements in the subset and their inverses forms a subgroup.
- Any subgroup containing the subset must contain all elements that can be written as finite products of elements in the subset and their inverses.

$\square$

We now use this to show that :

Claim. The subgroup generated by the union of a family of normal subgroups is normal.

Proof. Take an arbitrary element in the subgroup generated. This can be written as a finite product with each element being in one of the normal subgroups (if its inverse lies in the normal subgroup, so does it). Let us say the given element is written as

$$g = g_1 g_2 \ldots g_n$$

Let ϕ be the conjugation map by an element of the group. Then, using the fact that a conjugation is an endomorphism, we can write :

$$\phi(g) = \phi(g_1)\phi(g_2)\ldots\phi(g_n)$$

Each $\phi(g_i)$ lies in the normal subgroup in which g_i does, and so, lies in the union of the normal subgroups. Thus, their product lies in the subgroups generated, and hence, the subgroup generated is invariant under any conjugation. □

The above proof establishes the more general fact:

Claim. The subgroup generated by any self conjugate subset is a self conjugate subgroup (that is, normal subgroup).

<div align="center">CONCEPT TESTERS</div>

(1) Prove that, if α is a property of endomorphisms, then the subgroup generated by a subset that is invariant under every endomorphism of type α, is also invariant under every endomorphism of type α.
(2) Prove that the subgroup generated by a family of characteristic subgroups is a characteristic subgroup.

8.4. Product of subgroups.

Definition. The product of two subsets of a group is defined as the set of all elements that can be written as a product of an element in the first set with an element in the second set.

Thus, if S and T are subsets of G, then their product ST is defined as:

$$ST := \{st | s \in S, t \in T\}$$

When S contains the identity of the group $T \subseteq ST$, and when T contains the identity of the group, $S \subseteq ST$.

Definition. The inverse of a subset of a group is defined as the set of inverses of its elements. Thus, if S is a subset, its inverse S^{-1} is defined as:

$$S^{-1} := \{s^{-1} | s \in S\}$$

A subset S is said to be **symmetric**(defined) if $S = S^{-1}$.

From the identity :

$$(st)^{-1} = t^{-1}s^{-1}$$

We obtain that :

$$(ST)^{-1} = T^{-1}S^{-1}$$

This gives an important result :

Claim. If S and T are symmetric subsets, then $(ST)^{-1} = TS$. In particular, ST is symmetric if and only if $ST = TS$.

We now prove the important result :

Claim. If H and K are two subgroups of G, then $HK = KH$ if and only if HK is a subgroup. In that case, it is also the smallest subgroup containing both H and K.

Proof. Suppose HK is a group. Then H, K and HK are all symmetric subsets (as H and K are anyway subgroups). Thus, by the above observation, $HK = KH$.

Conversely, suppose $HK = KH$. It is already clear that $e \in HK$ (as $e \in H$ and $e \in K$). Moreover, by the above observation, HK is symmetric, so it is closed under inverses. Thus, all we need to do is show that the product of two elements in HK is in HK.

Let $a, b \in HK$. Then we can write $a = h_1 k_1$ where $h_1 \in H$ and $k_1 \in K$. Also, since $b \in KH$, we can write $b = k_2 h_2$ where $k_2 \in K$ and $h_2 \in H$. This gives us $ab = h_1(k_1 k_2)h_2$.

The problem is that we have an element of H times an element of K times an element of H. If we can somehow get the two elements of H together then we will be done. For this, look at the product $(k_1 k_2)h_2$. This lies in KH. Hence it lies in HK, so we can rewrite it as $h_3 k_3$ where $h_3 \in H$ and $k_3 \in H$. This gives us $ab = h_1(h_3 k_3) = (h_1 h_3)k_3$, so that $ab \in HK$.

Clearly, any subgroup containing H and K must contain HK, so it is the smallest subgroup containing H and K if it is a subgroup. □

<div align="center">22</div>

Essentially, we used the fact that $HK = KH$ to rewrite a product of an element of H and an element of K as a product of an element of K and an element of H. This is similar to the way we use commutativity of elements, except that in this case, we have to *write different elements*. That is, $h_1 k_1$ may not be equal to $k_1 h_1$, but we know that it can be written as some kh with k in K and h in H.

If H and K are two subgroups such that $HK = KH$, then we say that H and K are **mutually permutable** or that they **commute**. This suggests a new subgroup property.

(1) Prove that the set of all subsets of a group, with multiplication defined as above, form a monoid.
(2) If a group G is generated by two subgroups H and K then show that every element of G can be written as a product of the form $h_1 k_1 h_2 k_2 \ldots h_n k_n$ where $h_i \in H$ and $k_i \in K$.

8.5. Quasinormality and modularity.

Definition. A subgroup of a group is said to be **permutable**(defined) or **quasinormal**(defined) if it is mutually permutable with every subgroup of the group.

We prove that :

Claim. Every normal subgroup is quasinormal.

Proof. Let $N \trianglelefteq G$ be a normal subgroup and K be any subgroup. We need to prove that $NK = KN$. Let $a \in NK$. Then $a = nk$ where $n \in N$ and $k \in K$. We need to write a as something in K times something in N.

Now, if n and k commuted with one another, there would be no problem – we could simply write nk as kn. The problem is that n and k do *not* commute. But we still have that N and k commute. That is, the left coset of k and the right coset of k for N are the same. This means that there is a $n' \in N$ such that $nk = kn'$.

Thus, we get $NK = KN$. $\qquad\square$

Thus, the fact that normal subgroups are mutually permutable with other subgroups arises from the fact that normal subgroups commute with every element. It is clear that the condition of a subgroup commuting with every element is significantly stronger than the condition of the subgroup commuting with another subgroup as a whole. However, it is not very easy to find examples of quasinormal subgroups that are not normal.

An important property of groups relating to the product of subgroups is the **modular property of groups**:

If A, B and C are subgroups of G such that $A \leq C$, then :

$$A(B \cap C) = AB \cap C$$

The proof of this is direct.

(1) Prove (carefully) the modular property of groups. Make sure that the argument does not prove that :
$$A(B \cap C) = AB \cap AC$$
Because that is not true!
(2) Let $< A, B >$ denote the smallest subgroup of G containing $A \cup B$. A subgroup $A \leq G$ is said to be a **modular subgroup**[4] if :

$$< A, B \cap C > = < A, B > \cap C$$

whenever C is a subgroup containing A. Prove that every quasinormal (or permutable) subgroup is modular, and hence show that every normal subgroup is modular.
(3) A subgroup A of G is called **distributive** if :

$$< A, B \cap C > = < A, B > \cap < A, C >$$

where B and C could be any subgroups. Prove that any distributive subgroup is modular.
(4) A subgroup of a group is called **universally comparable**(defined) if given any other subgroup of the group, one of them is contained inside the other. Prove that :
   • The trivial and improper subgroup are universally comparable.

---

[4]the term "modular" is used in a completely different sense when talking of modular groups

- Any universally comparable subgroup is characteristic.
- Any universally comparable subgroup is distributive.

Points to Ponder

- We mentioned, above, the properties of being quasinormal, modular, distributive, and universally comparable? Is any of these transitive?
- Which of the above properties is closed under intersections? A subgroup property is closed under intersections, if the intersection of a family of subgroups satisfying the property also satisfies the property. We had earlier seen that any invariance property is closed under intersections.
- Which of the above properties is closed under subgroup generation? A subgroup property is closed under subgroup generation if the subgroup generated by the union of a family of subgroups satisfying the property also satisfies the property. We had seen earlier that if α is an endomorphism property, α invariance is closed under subgroup generation.
- Which of the above properties satisfies the **intermediate subgroup condition**? A subgroup property is said to satisfy the intermediate subgroup condition if whenever a subgroup has the property in the group, it also has the property in any other subgroup of the group containing it. We had seen that normality satisfies the intermediate subgroup condition.
- Based on the results obtained for normality and characteristicity, formulate other generalized properties *of* subgroup properties and check each of the properties introduced above for those.

8.6. **Where we are now.** In this section, we have tried to understand a little more about the **subgroup structure** of groups. We have, in particular, seen how to go about showing that the intersection of normal subgroups is normal, the intersection of characteristic subgroups is characteristic. We saw that a mapping system formulation with a property theoretic emphasis made the ideas behind the proofs clearer.

We also introduced two important ideas – the **subgroup generated** and the **product of two subgroups**. While the subgroup generated by a set may contain products of arbitrary finite length over elements of the set, the product of two subsets is the set of elements that can be written as an element of the first set times an element of the second set.

These, and some more, facets of subgroup structure shall be explored in `Part II` where we shall also study, in great detail, some specific classes of groups, based on the ideas developed so far.

9. Review of the journey so far

9.1. **Did we accomplish our goals?** At the beginning of this journey, I had made an explicit promise. Let's assess whether that promise has been fulfilled.

The components of the promise, and my personal view of how far we have got there:

- The concept of **group action** and **orbits**: Section 2 was largely on this. We looked at group actions, orbits, semiregular group actions, and the equivalence relations defined by group actions. We also tried to get a *feel* for group actions.

  However, the term "group action" as it is frequently used refers to a whole lot of other things beyond what we have done in this section. So we have *not* performed a complete study of group actions.

- The idea of subgroups acting on groups, and the associated concept of **cosets**: In section 3, we introduced the idea of how a subgroup acts naturally on a group, and how we can tap this action to give a lot of information about subgroup structure. In particular, we discussed the Lagrange property in section 4.

  In these two sections, we considered corresponding notions for many variants of groups in terms of structure. These variations were used mainly for illustrative purposes to show us just *what facets of group structure are being used*, but there are a number of practical situations where they do arise.

  What we have *not* done is the action of a group on the coset spaces of its subgroups. This has been reserved for `Part II`, where we will use this action to understand more about normal subgroups.

- The notion of **normal subgroups** and the proof that the kernel of a homomorphism is always a normal subgroup: In fact, we talked of normal subgroups as self conjugate subgroups, inner automorphism invariant subgroups, and also as subgroups that have the same left and right cosets. Using the inner automorphism invariance, we established, in section 7, that the kernel of a homomorphism is always a normal subgroup.

We also took a deeper look at conjugations and inner automorphisms, and related these to the notion of commutativity.

- A formalism for expressing **subgroup properties**. In particular, the notion of **characteristic subgroup** and some ideas about how normality and characteristicity behave.

  We did succeed in establishing the formalism, and were able to use it (quite effectively) to understand the *essence of proofs*. We also made generic statements, such as the statement that any invariance property is closed under intersections.

- The concept of **product of subgroups** and **subgroup generated**, as well as **intersection of subgroups**.

  This has just been touched upon. More in this thread will be done in `Part II`.

9.2. **The unforeseen treats.** As I complete penning this journey, I feel that some things turned out much better than I had dared to promise:

- The fact that variants to the Lagrange property hold for subgroups of structures more general than groups, and the conditions those structures need to satisfy.
- The concept of conjugations and normal subgroups, and the *many facets* to conjugation – as a measure of failure of commutativity, as well as in the sense of being automorphisms that can be *expressed by algebraic formulas*. Normal subgroups were those with the same left/right cosets, which were self conjugate, which were inner automorphism invariant.
- The power of the mapping formalism which really helped us get to the core of proofs of statements like "the intersection of normal subgroups is normal". I enjoy the general style of proving things, and I hope to have transmitted this joy.
- The sheer number of distinct notions involved in product of subsets of subgroups, and the way we again see *normality coming up*.

9.3. **What's next.** The journey `Group Theory:The Journey Continues` picks up from precisely this point in the next part, namely `Part II`.

Appendix A. Subgroup properties encountered so far

A.1. **A recapitulation.** We have, so far in the journey, come across some subgroup properties:

- The property of being the trivial subgroup
- The property of being the improper subgroup
- Normality
- Characteristicity
- Quasinormality

In the Concept Testers and Points To Ponder we encountered some more properties :

- The property of being a central factor
- Modularity
- Distributivity
- Universal comparability

Of these, normality, characteristicity and the property of being a central factor were expressed using a mapping system formulation while other properties were expressed in an *ad hoc* fashion. The mapping system formulation was very helpful in understanding normality and characteristicity properly, and helped us understand the logic behind our proofs. For the remaining properties, no adequate formalism has so far been developed.

The properties of modularity, distributivity and universal comparability are **lattice theoretic properties** expressible in terms of the lattice of subgroups. This shall be explored in more detail in `Part II`.

A.2. **Properties of these properties.**

- Normality and characteristicity are the invariance properties with respect to inner automorphisms and automorphisms respectively. Thus, they are both closed under intersections and subgroup generation.
- Normality satisfies the intermediate subgroup condition. More strongly, the inverse image of a normal subgroup under any homomorphism is a normal subgroup, and the image of a normal subgroup under a surjective homomorphism is a normal subgroup.

- Characteristicity is transitive. Normality is not transitive, but a characteristic subgroup of a normal subgroup is normal.
- The property of being a central factor is not an invariance property. It is, however, transitive. Also, a normal subgroup of a central factor is a normal subgroup.

A.3. **Implication diagram for these.** We have the following implication chains :

$$
\begin{array}{rcccl}
\text{Trivial or improper} & \implies & \text{Universally comparable} & \implies & \text{Characteristic} \\
\text{Universally comparable} & \implies & \text{Distributive} & \implies & \text{Modular} \\
\text{Characteristic} & \implies & \text{Normal} & \implies & \text{Quasinormal} \\
\text{Quasinormal} & \implies & \text{Modular} & & \\
\text{Trivial or improper} & \implies & \text{Central factor} & \implies & \text{Normal}
\end{array}
$$

By the time we complete `Part II`, we will have a much bigger collection of subgroup properties and we shall be able to put them all in proper perspective.