GROUP THEORY : A FIRST JOURNEY

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 article is a lightweight, hands on treatment of group theory from a refreshing perspective. The central theme is that of properties. However, prior knowledge or understanding of property theory is not a prerequisite to understanding the article. It is suitable for beginning college students or for others with a hobby interest in group theory. Its insights may also be valuable to more advanced students.

1. THE PROMISE – A GREAT JOURNEY

1.1. **It is a crucial journey.** Group theory is one of the first topics taught in undergraduate math curricula, and is the first plunge of college students into the realm of abstract algebra in particular, and possibly college mathematics in general. Groups are a great excuse to introduce a diverse range of concepts that are crucial to the language and toolkit of the whole of mathematics.

This means that the journey into the theory of groups is potentially a very enriching one. But it is also frightening because of the unfamiliarity of the approaches, language and notation used. This is particularly so if groups are the first exposure we get to algebra in this abstract setting.

This article proposes to guide us through that first journey, and promises to take us to a much richer understanding of mathematics as a whole and group theory in particular.

1.2. **Prerequisites.** The **prerequisites** for the article are:
- Basic familiarity with the concept of sets, functions, and binary operations. Lack of familiarity makes the journey more difficult to follow though it may still be accessible.
- Reasonable comfort with the use of symbols to denote sets, elements and operations.
- An ability to manipulate algebraic expressions based on fixed rules.
- An ability to carry out logical reasoning in the mind and on paper, and follow reasoning carried out by others.

All these competencies need to be developed only up to high school level. Thus, the **intended audience** for the article are students who have finished high school, or students who are in high school and are motivated to learn group theory.

1.3. **The explicit promise.** Here is the **explicit promise** of the journey. At the end of this journey, the learner should be able to:
- **Define a group** in more than one way
- **Define and understand the concept of subgroup**
- **Define homomorphism and isomorphism**

The article begins with the following philosophical appreciations:
- An appreciation of the **importance of groups**, and why they are defined the way they are.
- An appreciation of the *subtleties* in the way **subgroups are defined**.
- An appreciation of the distinction between the *abstract structure* and *concrete role* of a group via its **group actions** and **representations**.

The following are topics that this article does *not* contain, but for which it prepares an adequate foundation. These topics will be covered in the sequel article :
- The detailed study of homomorphisms – in particular, the notions of **kernel**, **fibers** and **normal subgroups**.
- The detailed study of **subgroup properties**.

Date: January 6, 2006.

- The detailed study of various kinds of groups – **Abelian**, **cyclic**, **symmetric**, **dihedral** and **alternating**.

1.4. **It is lightweight and hands on.** Group theory tends to appear difficult to students for a variety of reasons. One of them is the sheer variation in the structure of groups, and in the number of different concepts associated with groups. The other is the unimaginative way of teaching them.

This article treats group by emphasizing, at every stage, the **systems** constructed and their **properties**. Emphasis is on those properties that are **simple but crucial** in characterizing structures, as opposed to those that are difficult. The *raison d'etre* [1] of group properties is emphasized.

1.5. **Definition centric approach.**

Let's just find out what these groups mean,
And from that everything we can glean

This is a *foundational* journey – it lays the groundwork by providing the definitions and meanings of many terms that will be used in future journeys. So, naturally, I focus a lot on *knowing the definitions* and developing an *understanding* and an *appreciation* for them.

The main tool I use for enhancing definition understanding is that of *creative variation*. The various components of the definition are varied somewhat, and the new definition is analyzed. How does this term differ from the old one? What does it have in common? This process will help us, by the end of the journey, to have an idea about *why* groups are defined the way they are.

By conventional measures, this journey may appear very abstract – too few examples, very few applications, very little stimulus to the visual and kinesthetic senses, very little juice and spice. However, there is a *reason*. The purpose of this journey is to bring across the definition and *help in the development of a definition based intuition.* So I have deliberately not appealed to examples, problems, real world applications and historical motivations in this journey.

The later journeys will contain more of these, but we first need to get to appreciate the definition *for what it is*!

More on this can be found in the details I have put up in the detailed description of mathematical journeys.

1.6. **Get the most from this journey.** The text of this article is so simple that it can make good bed time reading, or casual web browsing. That is, however, *not* the best way to make use of it. This article represents a cleaned up version of my personal journey. Simply reading is only an act of dreaming. To derive the maximum benefit, it is necessary to *undertake* the journey.

The journey is best undertaken with a paper and pencil in hand, as well as with the willingness to read and reread. Remember – every word here has layers of meaning, layers of significance, and the journey is complete only when we understand why I took each step the way I did. The longer we agonize over each step, the better we can appreciate the beauty of it.

A brief note on the POINTS TO PONDER and CONCEPT TESTERS. The POINTS TO PONDER are meant to be pondered and dwelt upon – they are meant to improve our philosophical understanding of the purpose and significance of our journey. In many of them, there is no satisfactory *solution.*

On the other hand, all the CONCEPT TESTERS have clear cut solutions. Moreover, it should be possible and easy to solve them strictly based on the material done so far. Typically, they require us to rethink proofs that have already been covered in the text, but this time we need to be a little more careful of the underlying assumptions behind what we are doing. If there is any problem in these that we feel shaky in solving, that means that a review of the previous material is in order. However, each of the CONCEPT TESTERS has been put for a very specific purpose, that sometimes unfolds much later in the journey, or perhaps in a much later journey.

We also must avoid the temptation of skipping any of the POINTS TO PONDER or the CONCEPT TESTERS. New terminology introduced in the CONCEPT TESTERS is liable to be used later in the main text, and allusions to these problems may be made.

Again, for more details on how the journeys are designed and how to make best use of them, refer to the detailed description of the mathematical journeys on the website. Okay, now, let's begin!

---

[1] Reason for existence

2. Basic definitions

2.1. What is a group? This is the first, natural and most important step to understanding group theory. Nonetheless, a lot of group theory can be done without formally understanding what a group is![2]

We begin by understanding the concept of a binary operation.

Definition. A **binary operation**(defined) on a set is a map from the Cartesian product of the set with itself (or the set of all ordered pairs over that set) to it.

Thus, a binary operation on a set S is a map $S \times S \to S$. The binary operation is typically denoted by an **infix operator symbol**[3] such as . or $*$, so the image of (a, b) is denoted as $a.b$ or $a*b$ respectively. This is sometimes also termed the **product** of a and b, when the binary operation is termed **multiplication**. However, we must bear in mind that this multiplication can be defined in any manner whatsoever and need not resemble in any manner the multiplication of real numbers we are so used to.

In particular, it is not in general true that $a * b = b * a$. A binary operation satisfying this property is said to be **commutative**(defined). We *do not assume anywhere in this text that the operations we define are commutative.*

The conventional definition of a group, that we shall use quite often, is :

Definition. A **group**(defined) is a **set with a binary operation** satisfying the properties of **associativity**(first used), **neutral element**(first used), and **inverse elements**(first used).

These properties can be expressed as follows (when S is the set and $*$ is the binary operation) :

$$
\begin{aligned}
\text{Associativity} &\equiv a * (b * c) = (a * b) * c \ \forall \ a, b, c \in S \\
\text{Neutral element} &\equiv \exists \ e \text{ such that } a * e = e * a = a \ \forall \ a \in S \\
\text{Inverse element} &\equiv \forall \ a, \ \exists \ b \text{ such that } a * b = b * a = e
\end{aligned}
$$

Points to Ponder

- What is the *significance* of each condition? This is answered in the next section.
- Are any of the conditions redundant? That is, can any of the conditions be removed from the definition without changing the meaning of the word **group**? This is again answered in the next section, but the answer is scattered across it.

2.2. Analysis of the definition. The definition of group given above matches the format : "a [name] is a [contextual specifier] provided that [meaning]". Here the name is **group** and the contextual specifier is **set with binary operation**. This means that given any set with a binary operation, we can ask : *is this a group?*

A little care is necessary here. Given a **set** without the binary operation, it is meaningless to ask whether or not it is a group. The binary operation is an *intrinsic part of the group structure.* [4] Often this fact is emphasized by writing the group as $(S, *)$ where S is the underlying set and $*$ is the binary operation.

Thus, the property of *being a group* makes sense only in the context of sets with binary operations. However, by abuse of language, the group is often treated as being the same as its underlying set, so that we can use words like "subset of the group", "element of the group".

On the other hand, the definition of the term also makes it clear that the **structure of the group** is dependent only on the way the set and its binary operation are defined. That is, the binary operation on the set **encodes all information about the group**.

---

[2]Groups were first defined formally by Felix Klein's assistant von Dyck, although the concept of a group was used to great effect by Galois and Abel. (In fact, even some of Gauss's work reflects that groups were at the back of his mind.) As students of group theory, we shall resist the temptation of working without a definition.

[3]infix means that the symbol is put between the two operands, in contrast with prefix (before) and postfix (after). The concept of infix makes sense only for binary operators.

[4]the correct formulation of the question might be : given a set, can it be given a group structure? The answer in this case is yes, but there are many possible group structures that can be given to it.

2.3. **Any set and any binary operation.** A binary operation on a set is a map from the Cartesian product of the set with itself, to itself. Thus, to specify a binary operation, all we need to do is : for every a and b in the set, define the value of $a * b$.

There is clearly a very large number of ways of doing this, and most of them are unlikely to be of use. Nonetheless, sets with binary operations form an interesting universe with which to start, and over which to prescribe properties.

Definition. A **magma**(defined) is a set with a binary operation.[5]

A group is thus a very special kind of magma – it is associative, it has a neutral element, and it has inverse elements. The imposition of these properties *severely restricts* the nature of the binary operation that can be defined.

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

- Did we ever see **addition tables** and **multiplication tables** for multiplying numbers? The concept can be extended to any finite magma. Given a finite magma $(S, *)$ (That is, a magma whose set has finite cardinality) consider a table whose rows correspond to the elements of S and whose columns have the elements of S, and in each cell, fill in the product of the row element and the column entry. Does every multiplication table give a magma?
- Suppose the ordering of the elements in the rows and columns is the same. Then what kind of multiplication table would a magma have if it were to be a group? More generally, what are the constraints on the multiplication table corresponding to each of the properties that we can talk of for a binary operation?

2.4. **Why groups?** The meaning of a group has been given above, and everything that can be said about groups stems from that definition. Thus, the deeper the inspection of the definition, the better the insight into groups.

Historically, however, groups did not arise via this abstract definition. The *raison d'etre* for the existence of groups is that they represent **reversible transformations**. The analogy goes as follows :

- There is some space on which the group acts.
- Every element of the group gives a reversible transformation on that space.
- The product of two elements gives a transformation which is the composite of the transformations given by the elements individually. This explains why the group operation is associative.
- The neutral element gives the transformation that changes nothing.
- The inverse of an element gives the reverse transformation.

We can turn this around. Given any structure with a collection of reversible transformations, such that composing any two transformations (doing one after the other) in the collection also gave a transformation in the collection, the collection of transformations forms a group. In some sense, the very purpose of groups is to be the collections of transformations of certain spaces.

Historically, this is how groups came into being, and the abstract definition that we have seen above came much later in an attempt to systematize our knowledge state.

A slight word of caution here. When a group acts on a space, it is possible that two different elements of the group act in the same way. It is also possible that certain transformations of the space are never achieved via elements of the group. These aspects shall be explored later.

2.5. **Where we are placed.** What we've had so far is simply a tantalizing glimpse of the *what* and the *why* of the existence of groups. The journey has not yet begun. Our understanding of groups is fuzzy at best. What are the kinds of groups? What is the structure that groups could have?

The route to better understanding of all these aspects is, once again, the definition. It does not matter if, at this stage, we have *no example of a group* in mind. The definition is a noble mantra that we should keep chanting till we understand it inside out. Examples shall emerge naturally.

<div align="center">3. The definition and properties of a group</div>

3.1. **A basic idea.** So far as possible, we shall try to explore in the *most general scenario* possible. This is a natural thing to do keeping in mind that the more general our scenario, the wider the applicability of the results. But there is a more fundamental reason. When we look at a more general scenario, it becomes clear to us precisely what properties of the system are in use, and what properties are irrelevant.

---

[5]Earlier, the word **groupoid** was in use, but the term groupoid is also used more commonly in another context. The term **magma** has not become part of common parlance but has started coming into use.

3.2. **Neutral element.** To repeat, a group is a "magma with associativity, neutral element and inverse elements". We now want to understand more clearly what a neutral element is.

An element in a magma is said to be **neutral**(defined) if multiplying any element by it on the left or on the right leaves that element unchanged. That is, if $(S, *)$ is a magma and $e \in S$, e is said to be neutral if:

$$a * e = e * a = a \ \forall \ a \in S$$

The property of being neutral is a conjunction[6] of two properties :

$$e \text{ is left neutral} \equiv e * a = a \ \forall \ a \in S$$
$$e \text{ is right neutral} \equiv a * e = a \ \forall \ a \in S$$

The property of an element being **neutral** is thus the property of its being **left neutral** as well as being **right neutral**.

In the case of groups, neutral elements are also termed **identity elements**.

Now we come to an important first result of group theory:

Claim. The identity element (neutral element) of a group is unique.

Proof. let e_1 and e_2 be two identities. Then their product must equal both of them and hence they must be equal. That is, $e_1 = e_1 * e_2 = e_2$ and hence $e_1 = e_2$. $\qquad \square$

This is so simple that it is often ignored as being trivial and of no consequence. However, trying to understand *why* these properties hold is essential to being able to justify the axioms.

In this proof, no property of the group structure is used. This suggests that the more general statement is true : given any magma, there can be at most one neutral element.

Let us look at the proof of this : let a and b be neutral elements in a magma $(S, *)$. Then $a * b = a$ as b is neutral and $a * b = b$ as a is neutral. Thus, $a = b$.

A look at this proof suggests that what we really need is for the element on the right to be right neutral and for the element on the left to be left neutral. This suggests that a more general version still is :

Claim. If a magma has a left neutral element and a right neutral element, then they are equal, and hence, that becomes a neutral element.

In all cases, the proof remains the same, but this statement is so much more revealing! In particular, it shows that the property of there being at most one neutral element has nothing to do with the binary operation giving a group!

CONCEPT TESTERS

(1) Prove that if a magma has more than one left neutral element, then it cannot have a neutral element.
(2) Prove that if a magma has more than one right neutral element, then it cannot have a neutral element.
(3) The **opposite magma**(defined) to a given magma is defined as follows : the order of the operands is interchanged. For instance, if $(S, *)$ is a magma, then the opposite magma is $(S, .)$ where $a.b$ is defined as $b * a$. Prove that a left neutral element becomes right neutral in the opposite magma, and a right neutral element becomes left neutral in the opposite magma. Thus, show that every neutral element remains a neutral element in the opposite magma.

POINTS TO PONDER

- Can the above statements be explained graphically in terms of the multiplication table of the magma?
- How are the multiplication table of a magma and that of the opposite magma related?

---

[6]conjunction is a formal term for AND

3.3. **Associativity as a property of magmas.** Associativity is a property that can be discussed in the context of binary operations. That is, given any binary operation, we may ask the question : *is this associative?*

Prima facie, [7] associativity says that given three elements in sequence, the manner in which we bracket them does not affect the value of the result. That is, we have, for every a, b and c in $(S, *)$:

$$a * (b * c) = (a * b) * c$$

From this, it can in fact be deduced that given any sequence of elements $a_1, a_2 \ldots a_n$ in $(S, *)$, the order of bracketing the elements is immaterial – any two bracketings give the some result. For instance, if a_1, a_2, a_3 and a_4 are elements of $(S, *)$ where $*$ is associative, then :

$$a_1 * (a_2 * (a_3 * a_4)) = a_1 * ((a_2 * a_3) * a_4) = (a_1 * (a_2 * a_3)) * a_4 = ((a_1 * a_2) * a_3) * a_4 = (a_1 * a_2) * (a_3 * a_4)$$

In the above, *each* equality can be deduced by applying associativity. In the more general case of n terms, the proof that all bracketings give the same answer relies on showing that any bracketing can be converted to any other bracketing by repeated application of associativity.

This means that the bracketing can be dropped when referring to products of a sequence of elements with regard to an associative operation.

Associativity places a fairly strong restriction on the structure of the magma.

Definition. A set with an associative binary operation (that is, an associative magma) is termed a **semigroup**(defined). A semigroup with a neutral element is termed a **monoid**(defined).

In semigroups and monoids, and more specifically, in groups, it is customary to drop the $*$ symbol as well as the bracketing and to simply refer to the product $a * b$ as ab. Thus, the product $a * (b * c)$ which is the same as $(a * b) * c$ can be simply written as abc.

However, this notation must not be used unless it has been established that the binary operation is associative, and we shall refrain from using it for the next few sections.

<center>CONCEPT TESTERS</center>

(1) An element of a magma is termed **left associative**(defined) if any expression with it on the left associates. That is, $m \in S$ is left associative for a magma $(S, *)$ if, for every a and b in S, we have :

$$m * (a * b) = (m * a) * b$$

Prove that the product of two left associative elements in the magma is left associative.

(2) Define **middle associative** and **right associative** analogously to left associative. Prove that the product of two right associative elements is right associative, and that the product of two middle associative elements is middle associative.

(3) Define the **associative center**(defined) of a magma as the set of elements that are left associative, middle associative and right associative. Prove that the associative center is closed under multiplication (that is, the product of two elements in it is also in it). Also, prove that if the magma has a neutral element, then that lies in the associative center.

(4) Prove that given a magma, the set of left associative elements of the magma is equal to the set of right associative elements in the opposite magma, and the set of right associative elements of the magma is equal to the set of left associative elements in the opposite magma. What can be said about the set of middle associative elements?

(5) Thus, show that the opposite magma to a semigroup is a semigroup, and the opposite magma to a monoid is a monoid.

<center>POINTS TO PONDER</center>

- The above proofs seem to rely simply on manipulation. Is there some *conceptual* explanation of their truth? Or perhaps, is there some conceptual explanation of why the manipulation goes through?
- Sometimes, for operations which are not associative, we define a direction of associativity – for instance, we interpret $a_1 * a_2 * a_3 \ldots a_n$ as meaning $a_1 * (a_2 * (a_3 * \ldots a_n) \ldots)$. If we assume the default bracketing to be to the right, then we say that the operation is **associated to the right**, otherwise we say that the operation is **associated to the left**. Are there some operations that

---

[7]at first glance

are not associative, that are convenient to associate to the right, and are there some operations that are convenient to associate to the left? It might be interesting to check out the associativity rules used in the programming language `C`.

3.4. **Inverse elements.** Given a magma $(S, *)$ with a neutral element e, such that $a * b = e$, we say that a is a **left inverse**(defined) of b and that b is a **right inverse**(defined) of a. If $a * b = b * a = e$ then a and b are simply said to be **inverses**(defined) of each other.

An element that possesses a left inverse is said to be **left invertible**(defined) and an element that possess a right inverse is said to be **right invertible**(defined) An element that possesses an inverse is called **invertible**(defined).

The idea of an inverse element is to *cancel the action* of the original element. Thus, the left inverse cancels the action when multiplied on the left, and the right inverse cancels the action when multiplied on the right.

The problem with inverse elements in general is that the left inverse and right inverse can cancel each other only if they are allowed to meet face to face. This means that if a is buried deep inside an expression, then we have to somehow bring a^{-1} next to a before we can cancel them. **Associativity** plays a crucial role in accomplishing this, which is why most results pertaining to inverse elements rely on associativity or some variant thereof.

An important introductory property is :

Claim. If an element of a group has two inverses, then they are equal.

Proof. Let b and c be two inverses of a. Then we have :

$$\begin{aligned}
b * (a * c) &= (b * a) * c \text{ by associativity} \\
\implies b * e &= e * c \text{ by inverse property} \\
\implies b &= c \text{ by neutral element property}
\end{aligned}$$

Thus, every element has a unique inverse. $\square$

Thus, while the concept of inverse element makes sense in any magma with a neutral element, the "uniqueness of inverse" requires the magma to be associative. The property can be rephrased somewhat to say :

Claim. Given a monoid, every element can have at most one inverse.

Again, in the same way as we did for neutral elements, we observe that the proof goes through even if b is a left inverse and c is a right inverse. Thus, we can rephrase this by saying that :

Claim. Given a monoid and an element in it, every left inverse of that element equals every right inverse of that element.

The upshot of all this is that in groups, the inverse element of an element is unique, and we thus have a map from the group to itself, taking each element to its inverse. The inverse of an element x is denoted by x^{-1}. Two interesting properties of this are :

$$\left(x^{-1}\right)^{-1} = x \text{ (Involutive law)}$$
$$(x * y)^{-1} = y^{-1} * x^{-1} \text{ (Reversal law)}$$

The first property states that the inverse operator, when applied twice, gets an element back to itself. The second says that the inverse of a product is the product of the inverses but in reverse order. This rule is sometimes termed the **reversal law**(defined).

A couple of observations here :

- The involutive nature of the inverse operation can be generalized to saying that if an element has a left inverse, it is a right inverse of its left inverse.
- Also, the reversal law can be generalized : if $x_1, x_2 \ldots x_n$ all have right inverses $y_1, y_2 \ldots y_n$, then so does $x_1 * x_2 \ldots x_n$ and its right inverse is the product $y_n * y_{n-1} \ldots y_1$.

CONCEPT TESTERS

(1) Prove that if an element in a monoid has more than one left (right) inverse, then it cannot have a right (left) inverse.

(2) Given a monoid where *every* element has a left inverse, prove every element has a right inverse and that they are equal. This means that the axiomatization of a group can be weakened somewhat by assuming only that every element has a left inverse.

(3) Call an element m of a magma $(S, *)$ with neutral element e **middle associative**(recalled) if for all a and b in S, we have

$$a * (m * b) = (a * m) * b$$

Prove that if m has a left inverse and a right inverse, then they are equal.

(4) An **involutive semigroup**(defined) is a semigroup $(S, *)$ with an operation $'$ from S to S such that :

$$\begin{aligned} (a')' &= a \ \forall \ a \in S \\ (a * b)' &= b' * a' \ \forall \ a, b \in S \end{aligned}$$

The operation $'$ is termed the involution. (The involution is part of the structure). Prove that every group can naturally be given the structure of an involutive semigroup.

(5) Prove that every commutative semigroup can be given the structure of an involutive semigroup.

(6) Prove that the reversal law is valid for involutive semigroups, that is :

$$(a_1 * a_2 \ldots a_n)' = a_n' * a_{n-1}' \ldots a_1'$$

POINTS TO PONDER

- Can we define a notion of inverse elements without invoking neutral elements?
- What can be said about the relation between an involutive semigroup and its opposite semigroup?
- The set of matrices under multiplication is an involutive semigroup, even though it is neither a group nor is it commutative. What is the involution here (it is a very standard operation)?

3.5. **Where we are placed now.** Groups are a very special kind of magma. In particular, they have three properties :

- The property of **associativity** – a magma with this property is called a semigroup. Associativity is powerful because it helps us remove brackets and club terms together in different ways.
- The property of the existence of a **neutral element** – we saw that this property makes sense for a general magma, and further, that some results can be deduced in the general case on it.
- The property of the existence of **inverse elements** – we saw that, particularly in the presence of associativity, inverse elements have a powerful effect in terms of *cancelling the action*.

What we have seen in th past few subsections is that it is often more fruitful to *analyze these properties in a more general context* rather than simply considering them for groups. This helps us understand *just why* the properties seem to click. For instance, the uniqueness of neutral elements can be proved in the general context of a magma, while the uniqueness of inverses requires associativity.

This not only makes proofs easier, but also helps us to appreciate the importance of groups as well as move towards more general structures.

Another way of looking at this is that after having strained in each step to see just *what property is being used to prove what* we realize how easy groups are – they have all the properties, and we can use those properties freely and without fear. Thus, we are no longer worried about some constraining factors that bothered us earlier in the journeys. But as we begin with groups, there are new aspects that we need to keep in mind, aspects that did not bother us when we were fighting with the basic issues.

4. SUBGROUPS – AND A NEED TO REDEFINE GROUPS

4.1. **Subgroups.** Given a structure, we can talk of its substructures – parts of the structure which are also structures. A **subgroup**(first used) of a group is a subset which is also a group. We need to, however, be a little careful here.

When we say a *subset which is also a group*, we mean that it has a group structure that it *inherits naturally* from the original group. Formally:

Definition. Given a group, a **subgroup**(defined) of the group is a subset of its underlying set, that is closed under the binary operation, such that the binary operation, restricted to the subset, gives it a group structure.

8

This group structure is obtained simply by restricting the binary operation to that subset. Now come the following problems :

- Suppose there is a subset to which the binary operation can be restricted. Is it necessary that this subset will have a neutral element and inverse elements?
- Suppose it has a neutral element and inverse elements. Will the neutral element for this, and the inverse elements in this, be the same as in the bigger group?

The answer to the first question is no (however, it is yes if we restrict our attention to finite subsets) and the answer to the second question is yes. However, the *yes* in the answer to the second question is dependent very specifically on the group structure. (We shall come to the proof at a later stage).

4.2. **What do we define as group structure?** The content of the last section showed that once the binary operation of the group is fixed, both the neutral element and the inverse map are uniquely fixed. This suggests that a group may be defined at the outset by specifying the binary operation, the constant which is the neutral element, and the unary operation which is the inverse map. We can thus redefine a group as follows :

Alternative Definition. A **group**(defined) is a set with a constant (called a **neutral element**), a unary operation (called the **inverse map**) and a binary operation (called **multiplication** or **composition**) satisfying the properties of associativity, neutrality and inverses. If $(G, e, ^{-1}, *)$ is th group with set G, identity element e, inverse operation $^{-1}$ and multiplication $*$, we have :

$$
\begin{aligned}
\text{Associativity} &\equiv a * (b * c) = (a * b) * c \ \forall \ a, b, c \in G \\
\text{Neutral element} &\equiv a * e = e * a = a \ \forall \ a \in G \\
\text{Inverse element} &\equiv a * a^{-1} = a^{-1} * a = e \ \forall \ a \in G
\end{aligned}
$$

This definition has several advantages. First of all, it defines all the operations upfront rather than covertly. More importantly, all the properties now read as identities with all **variables quantified universally**. This observation is extremely crucial and is one of the main benefits of this way of axiomatizing. It generalizes to an extremely powerful concept – that of **universal algebra**(first used).

With this, we obtain the following definition of subgroup:

Alternative Definition. Given a group (a set with a binary operation, a unary operation and a constant satisfying the three identities above) a **subgroup**(defined) is a subset that is closed under all three operations. *Because the identities were universal*, it immediately follows that the subgroup is a group in its own right with these operations defined on it.

4.3. **Why they become the same for groups.** We gave two definitions of groups, and saw that they gave rise to the same structures. We also gave two definitions of subgroups. However, it is not yet clear whether those two definitions are equivalent. The first definition only insists that there *exists a group structure* on the subset when the binary operation is restricted to it. The second definition requires that this group structure have the same identity element and the same inverse map.

So, to show that the definitions are equivalent, we need to establish the following claim:

Claim. Given a subset of the group which is closed with respect to the binary operation, such that that binary operation induces a group structure on it, that subset is in fact a subgroup.

Proof. What we need to check is that the neutral element and the inverse elements are the same. To establish that the neutral element remains the same, we need to show that if, for the given subset, there is an element f such that $a * f = f * a = a$ for all a in the subset, then $f = e$ where e is the neutral element of the bigger group.

The rough idea is to start with the equation :

$$
a * f = a * e
$$

and to *cancel a* from the equation. The question is : how can we validly cancel a? To cancel a, we need to put something that will remove a. That something is a^{-1}.

Formally, we multiply both sides on the *left* with a^{-1}, to get :

$$\begin{aligned} a^{-1} * (a * f) &= a^{-1} * (a * e) \\ \implies (a^{-1} * a) * f &= (a^{-1} * a)e \\ \implies e * f &= e * e \\ \implies f &= e \end{aligned}$$

$\square$

4.4. Cancellation: a gleaning from the proof. A careful look at the above proof shows that the property of f and e being neutral was not used, so that in fact groups have the **cancellation property** by which, for all elements a, b and c:

$$a * b = a * c \implies b = c$$
$$b * a = c * a \implies b = c$$

We now make the following observations :

- An element of a magma is **left cancellative**(defined) if it can always be cancelled on the left. It is **right cancellative**(defined) if it can always be cancelled on the right. An element is **cancellative**(defined) if it is both left cancellative and right cancellative.
- A magma is said to be **left cancellative**(defined) if all its elements are left cancellative, and **right cancellative**(defined) if all its elements are right cancellative. It is **cancellative**(defined) if it is both left cancellative and right cancellative.
- In a monoid, every element with a left inverse is left cancellative and every element with a right inverse is right cancellative.
- In particular, in a group, every element is cancellative. Thus, a group is a cancellative magma.
- Given a magma with a left (right) cancellative element, there is at most one right (left) neutral element.
- If a subset of a magma (with a right neutral element) contains a left cancellative element, and that subset has an element that is right neutral for all its elements, then that must be the right neutral element of the magma.
- Thus, given a left (right) cancellative magma with a right (left) neutral element, any submagma (multiplicatively closed set) with a right (left) neutral element must have the same right (left) neutral element as the magma.
- Thus, given a left (right) cancellative magma with neutral element, any submagma with a neutral element must have the same neutral element.
- Piecing together all these facts, we conclude that in a group, every submagma (that is, multiplicatively closed subset) with a neutral element must have the same neutral element.

The above chain of reasoning may seem far more complicated than what we did. In fact, we have subconsciously gone through all these steps even as we wrote the short and elegant proof. Putting it down in this way makes it clear that there is such a large number of properties in between. Firstly, it introduces a new concept – that of cancellative elements.

The approach here can best be characterized by saying :

> Rather than saying – "we can always cancel in a group" we instead define the property of being cancellative and rephrase by saying – "a group is cancellative". That is, we introduce a *new* property and study it in its own right rather than simply accepting it as a fact of life for groups. This opens the way to the study of new structures.

The idea of ceaseless parsing of the definition, to break it into a chain of properties, is not merely intellectually rewarding, but also helps us uncover the *deep philosophical reasons* behind the great truths.

Concept Testers

(1) Prove that a left cancellative element in a magma with a neutral element, has at most one right inverse. Show that this is a generalization of the statement that in a monoid, an element with left inverse can have at most one right inverse.

(2) The **square**(defined) of an element in a magma is its product with itself. An **idempotent**(defined) is an element that equals its own square. Prove that every left (right) neutral element in a magma is an idempotent.

(3) If a magma has a left neutral element, and a right cancellative idempotent, then prove that they must be equal.

(4) Prove that, in a monoid, the only idempotent with a left (right) inverse is the neutral element.

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

- Given a finite subset of a group that is closed under the multiplication, that subset must be a subgroup. How will we prove this? How do we make use of finiteness.

  This, and many other related ideas, are discussed in `Group Theory:The Journey Continues`.

4.5. The subgroup criterion. To check whether a given subset is a subgroup, we need to check that it is closed under three operations – the binary operation of multiplication, the unary operation of inversion, and the constant operation, namely the identity element. The **subgroup criterion** gives a *single expression* with respect to which we can check closure.

The subgroup criterion is as follows :

Theorem 1 (Subgroup Criterion). *A nonempty subset of a group is a subgroup iff it is closed under the map* $(x, y) \mapsto xy^{-1}$.

Proof. Clearly, any subgroup must be closed under the map $(x, y) \mapsto xy^{-1}$. We need to prove the converse : any subset that satisfies the condition is a subgroup.

We verify this in three stages :

- **It contains the neutral element** : take any x in the subset (as it is nonempty). Then $e = xx^{-1}$ lies in the subset.
- **It is closed under the inversion map** : take any y in the subset. Then $y^{-1} = ey^{-1}$ lies in the subset.
- **It is closed under products** : take any x and y in the subset. Then y^{-1} also lies in the subset, and hence so does $x(y^{-1})^{-1} = xy$.

$\square$

The main use of the above observation lies in making the proof that a given subset is a subgroup somewhat shorter, because now we have a single condition to check instead of three. Note that we still have to check that the subset is not empty.

4.6. Where we are placed now. We now have with us two definitions of the group (introduced in sections 2.1 and 4.2) and we have seen the merits of each. While the first definition is convenient for many purposes, it is the second one (where all the three operations are defined explicitly) that makes groups so well behaved.

We also saw that we need to exercise some care while defining the concept of a subgroup.

When we study more algebraic structures such as rings, modules and fields, and the corresponding notions of subrings, submodules and subfields, then we shall have to confront similar issues, and in many of these cases, there will be no easy answers as was the case with groups. This makes it all the more clear that groups are a well behaved, well disciplined structure.

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

(1) Consider the set $\{0, 1\}$ with operation $*$ such that $0 * 0 = 0 * 1 = 1 * 0 = 0$ and $1 * 1 = 1$. Prove that this is a monoid under the induced operation but not a group.

(2) Show that, for the above monoid, the subset $\{0\}$ is a subsemigroup with a neutral element.

(3) Thus prove that the following statement is not true : "If a monoid has a subset which is a monoid under the induced binary operation, then that is a submonoid (in the sense that it has the same neutral element)."

<div align="center">5. EXAMPLES AND IDEAS</div>

5.1. Exercising restraint. The *ability to refrain from specific visualization* is often as necessary as the *ability to indulge in specific visualization*. This is a little like reading – most people vocalize what they read in their mind as they read. This ability to vocalize is at times useful, but is often a hindrance to reading speed. Refraining from subvocalization is thus important to improve reading speed. In much the same way, refraining from specific visualization is important at times for proper comprehension.

Our approach, in the case of groups, will be to understand *how examples of groups arise* in the concrete mathematical world. For this purpose, we shall first need to take our discussion of groups as collections of reversible transformations, a little further.

5.2. **A group as a collection of transformations.** The idea : "give a system, and give it some structure, and look at all the transformations of the system that preserve the structure". Clearly, the identity transformation, that is, the transformation that preserves everything, will preserve the specific structure. Further, if two transformations preserve the structure, so does their composite. Finally, if a transformation preserves some structure, so does its inverse.

The beauty is that *every group* can be viewed in this way. However, given a group, there may be multiple ways of viewing it in this way. Each such way gives an **action**(first used) of the group. This action is sometimes also termed a **representation**(first used) of the group.

A loose analogy with people would be appropriate. What a person *is* is what she is made up of – her physical, mental and emotional self. The way she *appears* to the outside world is via her *actions*. For instance, she may act as a mother, a sister, an engineer, or a tourist. The way she acts depends, of course, on what she *is*, but does not provide complete information of it.

Figuring out what people *are* requires us to understand their inner nature. However, this is not directly possible. We need to collect information about the ways they act in various situations, and use this **detective work** to piece together and find out what they are.

In the case of groups, we are a little luckier, for we do have a clear structural understanding of what groups are. Nonetheless, a lot of questions as well as answers regarding their structure arise from an analysis of the way they act.

We are now in a position to look at a few ways in which groups act.

5.3. **Permutation representations – groups acting on sets.** Here, the system is a set, and the group acts by *permuting* the elements of the set. That is, each element of the group induces a bijection from the set to itself, such that the composite of two elements induces the composite of the corresponding bijections. The neutral element induces the identity bijection.

Formally:

Definition. An **action**(defined) of a group $(G, *)$ on a set S is a map $G \times S \to S$ denoted by the letter . (that is, the image of (g, s) is written as $g.s$) provided that :

$$e.s = s \text{ where } e \text{ is the neutral element of } G$$
$$g_1.(g_2.s) = (g_1 * g_2).s$$

By abuse of notation, we leave out the group multiplication operation as well as the ., so that we write things like $g_1 g_2 s$ instead. This makes sense precisely because our action is a group action.

It is very important to note that from these assumptions, it follows that the inverse of an element induces the inverse of the corresponding map. This follows from the fact that, for every s, we have $g^{-1}gs = es = s$, and $gg^{-1}s = es = s$.

This means that given every element in the group, the corresponding map $S \to S$ is invertible. In other words, for every element in the group, the induced map $S \to S$ is a bijection, or, in other words, a permutation.

A group action is also sometimes termed a **permutation representation**(defined) of the group.

5.4. **Monoids acting on sets.** The definition of action does not make much use of the group structure. In fact, the definition can be used *mutatis mutandis*[8] to define an action by an arbitrary magma with a neutral element. In particular, we could consider a **monoid action**(defined).

However, replacing the group by a monoid does result in significant changes in the way the action *behaves*. Even animals can act, but they sure act very differently from humans! Similarly, even monoids can act, but group actions are very special.

In particular, it is *no longer true* that every element in the monoid induces a permutation on the set on which it is acting, because of the *failure of existence of inverses*. However, we can salvage the following:

- Those elements with left inverses must give rise to injective maps.
- Those elements with right inverses must give rise to surjective maps.
- Those elements with inverses must give rise to bijective maps.

CONCEPT TESTERS

(1) Provide an explicit definition of a monoid action.
(2) Prove the three assertions made above.

---

[8]without any change, as it is

- What happens if, instead of a semigroup, we consider a general magma acting on a set, governed by the same definition? What role does associativity (or the lack of it) play in the way the action pans out?

5.5. A little background on permutations. Before going into the next section, it might do well to recall a few facts about permutations.

A **permutation** is a bijective map from a set to itself. Permutations are typically denoted by small Greek letters such as σ or ϕ. Given two permutations σ_1 and σ_2, their composite $\sigma_1.\sigma_2$ is defined as the composite as functions – so that $(\sigma_1.\sigma_2)(x) = \sigma_1(\sigma_2(x))$.

The **identity permutation** is the identity function on the set. The **inverse** of a permutation is another permutation such that the composite both ways is the identity permutation.

The set of permutations on a given set, with **composition** as the binary operation, gives a **group structure** where the neutral element is the identity permutation and the inverse of an element is the inverse permutation. This group is termed the **symmetric group** on the set S and is sometimes symbolically denoted as Sym_S.

(1) Show that the symmetric group acting on a set defines a group action.

- How can we write a permutation? There are many ways of doing this – the **two line method** writes the elements in two lines, with the image of each element under the element. How can we compose two permutations written using the two line method? How can we write the inverse of a permutation written in the two line method, again in the two line method.

5.6. Currying and uncurrying. We look again at the map $G \times S \to S$. We had observed that for every element of G, this gives a map $S \to S$.

More generally, suppose we have a map from $A \times B \to C$ where A, B and C are sets. Then for each element of A we get a map $B \to C$. This means that we get a map $A \to (B \to C)$. Further the two maps convey exactly the same information.

This observation forms the backbone of a lot of **functional programming** and the process of converting between the two forms is known as **currying** and **uncurrying**.

In the case of groups acting on sets, the map $G \times S \to S$ gives an associated map $G \to (S \to S)$ and we now try to comment on this nature of this map. The first thing to observe is that the map cannot be surjective, that is, every function from S to S cannot be obtained as the image of an element of G. This is because the image of any element of G must give a *bijective* map from S to S. Thus, the image of G under this map is a subset of the symmetric group on S, or Sym_S.

Further, the map $G \to Sym(S)$ has a special property, namely that the action of the product of two elements in G is the composite of their actions. If we let ρ denote this map, then we can say that :

$$\rho(g_1 g_2) = \rho(g_1).\rho(g_2)$$

The product on the left is in G (by the binary operation defined for G), and the product on the right is in $Sym(S)$ (by the natural group structure on it). In other words, the map from G to $Sym(S)$ *preserves some kind of group structure*. Such maps are called **group homomorphisms**, and we shall study more about them soon.

(1) Prove that given any group the multiplication action $G \times G \to G$ defines an action of G on itself as a set. This is termed the **left regular action** or the **left regular representation** of G. What crucial nature of the group operation is used in showing that for each $g \in G$, the induced map $G \to G$ is a permutation?
(2) A **quasigroup** is a set with a binary operation, say $(S, *)$, such that given any a and b in S the equation $a * x = b$ has a unique solution in S and the equation $y * a = b$ has a unique solution in S. If the quasigroup has a neutral element, then it is termed an **algebra loop**.

Prove that if S is a quasigroup, then the map $x \mapsto s * x$ for some $s \in S$ is a permutation.
(3) Prove that a quasigroup is a cancellative magma.

- A **Latin square** is an $n \times n$ matrix such that every row is a permutation of the numbers 1 to n, and every column is a permutation of the numbers 1 to n. Given any magma whose multiplication table is a Latin square, is it necessary that it be a quasigroup?
- The condition of being a quasigroup is a fairly strong one – the only thing missing is associativity. Is every associative quasigroup a group, or is some additional condition required to ensure group structure? If so, what additional condition must be added?

5.7. **The combinatorics of finite sets.** In enumerative combinatorics (as studied in high school under the label "permutations and combinations"), we saw that the number of permutations on a set of cardinality n is $n!$ which is $\prod_{k=1}^{n} k$.

Now, we know that the *set* of all permutations on a set of cardinality n is not merely a set, but has a natural composition law, which equips it with a group structure. In other words, we have an *example of a group*, and we know that the cardinality of the group is $n!$ if the group is acting on n elements. This group is denoted by Sym_n or sometimes S_n. and is talked of as the **symmetric group** on n elements.

Group theory has thus helped us perceive structure in the collection of permutations where earlier, we only had numbers. A natural next question would be : what can we say about the subgroups of this group? The subgroups would, in this case, be subsets which contain the identity element, and are closed under composition and inversion.

For instance, suppose we take the set of integers $\{1, 2 \ldots n\}$. The permutations of this set form the group S_n, or the symmetric group on n elements. Suppose we look at those permutations that arise by *cyclically* permuting the numbers, that is, the permutation that takes each number x to $x + k$ modulo n, where k is a fixed number. For instance, we could have the permutation that takes 1 to 3, 2 to 4, and so on, but takes $n - 1$ to 1 and n to 2. This corresponds to a cyclic shift by 2.

Thus, for every $k \in \mathbb{Z}^9$ (that is, for every integer k), we have an associated permutation on the set: the **cyclic shift** by k. We observe that :

- Given k_1 and k_2, the cyclic shift induced by $k_1 + k_2$ is the composite of the cyclic shifts induced by k_1 and k_2.
- The cyclic shift induced by 0 is the identity map.

This suggests that these cyclic shifts define a map from the set of integers to the symmetric group on n elements. That is, we have a map $\rho : \mathbb{Z} \to S_n$. Further, we have :

$$\rho(0) = e_{S_n}$$
$$\rho(k_1 + k_2) = \rho(k_1)\rho(k_2)$$

The first of these means that the cyclic shift by 0 gives the identity permutation (which is obvious). The second says that performing a cyclic shift by $k_1 + k_2$ has the same effect as first performing a cyclic shift by k_2 and them performing a cyclic shift by k_1.

This is reminiscent of an action. In fact, it *is* an action if we consider $\mathbb{Z}$ to be a group under addition, that is, we take $(\mathbb{Z}, +)$ as our group. The identity element in this case is 0, the inverse of an element is its negative, and the composite of two elements is their sum in $\mathbb{Z}$.

Thus, we have an action of the group of integers on a finite set of n elements, and also a map from the group of integers to the symmetric group on n letters. We note a few points about this map :

- Two elements k and l in $\mathbb{Z}$ induce the same cyclic shift permutation (that is, map to the same element in S_n) iff[10] $k - l$ is a multiple of n.
- The image of $\mathbb{Z}$ under the map ρ, that is, the elements of S_n that can be realized as cyclic shift permutations, form a subgroup of S_n. This subgroup has n elements, namely, the cyclic shift permutations corresponding to $0, 1 \ldots (n-1)$.

We shall return to this observation a little later on, to understand it in greater detail.

5.8. **Transformations in space.** The examples of groups discussed here are intended primarily to enrich our appreciation of groups and their importance. It is not crucial to understand all of them.

The **plane** is a set of points and groups can be made to act on this set of points. However, in addition to being a set, the plane also carries with it some structure, and we may impose restrictions on what structure our maps must preserve. The stronger the structure, the fewer the transformations that preserve it.

---

[9]$\mathbb{Z}$ denotes the set of integers

[10]iff means if and only if

An **automorphism** of a structure is a transformation that preserves the structure. Thus, we are interested in studying the automorphism groups of planes under various kinds of structures.

Sometimes, specifying the underlying structure being preserved may be quite difficult, but we can still give some criteria for symmetry. For instance, we may consider bijective maps from the plane to itself that take:

- **Continuous curves to continuous curves** : The structure preserved here is quite weak. For instance, a straight line need not even go to a straight line. The shapes and sizes of figures could get largely distorted. Such maps must preserve the *topology*.
- **Smooth curves to smooth curves** : Suppose we call a curve smooth if a tangent can be drawn at every point on it. Then we are interested in maps that take smooth curves to smooth curves. Roughly, such a map must preserve the *differential structure* of the plane upto first order.
- **Straight lines to straight lines** : Transformations that preserve collinearity are termed **collineations**. All collineations arise as **affine transformations** and belong to the **affine group** of order 2 over $\mathbb{R}$.
- **Straight lines to straight lines and angles to equal angles**: Such transformations are termed **similarities**.
- **Straight lines to straight lines and lengths to equal lengths** : Such transformations are termed **isometries** and give rise to the **orthogonal group**.

It is clear that there are many levels of structure associated with the plane. Some depend on the topological structure, some on the differential structure, and some on the algebraic structure. Each notion of structure gives an associated automorphism group.

5.9. **Where this leaves us.** As has been emphasized, the role of groups is to *act* – on various structures, whether they be sets, or spaces with some properties. The nature of the group captures the structure, and conversely, knowledge about the structure improves our knowledge of the group. However, the information that the structure and the (automorphism) group give about each other is incomplete.

However, groups have been studied as entities in their own right because we are interested in understanding what they *intrinsically* are. The action of a group is simply a **manifestation** of it and is not the group itself. The same group may have many manifestations, or, more technically, **representations**. The abstract study helps us to understand the structure underneath these representations.

This brings us to the question of what it means for two groups to be the *same*, and how the structures on different groups can be related. This forms the content of the next section.

6. STRUCTURE PRESERVING MAPS

6.1. **Isomorphisms.** In the discussion of symmetric groups, we had implicitly assumed that the symmetric group on any two sets of the same cardinality is essentially same. This notion of being *essentially same* is precisely the notion of **isomorphism**(first used). In the language of isomorphisms, we say that the symmetric groups on any two sets of the same cardinality are isomorphic.

Roughly an isomorphism is an identification of two objects as being the same thing. In the case of groups, an isomorphism between two groups is a bijective map between their corresponding sets that preserves the binary operation.

Definition. If G_1 and G_2 are two groups, then an **isomorphism**(defined) is a bijective map $\phi : G_1 \to G_2$ such that:

$$\phi(gh) = \phi(g)\phi(h)$$

Here, the multiplication on the left is in G_1 and the multiplication on the right is in G_2.

This notion of isomorphism corresponds to the definition of a group given in section 2.1, where a group was treated simply as a set with a binary operation. In section 4.2 we had looked at an alternative way of defining groups : by specifying upfront the binary operation, the inverse map and the constant. Corresponding to this, the notion of isomorphism may be expressed as follows :

Alternative Definition. An **isomorphism**(defined) between groups G_1 and G_2 is a bijective map $\phi : G_1 \to G_2$ such that :

$$\begin{aligned}
\phi(gh) &= \phi(g)\phi(h) \\
\phi(e_{G_1}) &= e_{G_2} \\
\phi(g^{-1}) &= (\phi(g))^{-1}
\end{aligned}$$

In fact, the two notions of isomorphism are precisely the same. This stems from the fact that the binary operation on the group *uniquely determines* the inverse map and the identity element. (This was the content of sections 3.2 and 3.4).

Two important points :

- The inverse of an isomorphism is an isomorphism.
- The composite of two isomorphisms is an isomorphism.

These facts are intuitively obvious when we think of isomorphisms as *structure preserving maps*.

Given a group, we can also consider isomorphisms from the group to itself. That is, we can consider permutations of the group that preserve the group structure. Such isomorphisms are termed **automorphisms** of the group. Earlier we had discussed that given any structure, the automorphisms of that structure form a group. Thus, given a group, the automorphisms of that group give another group!

CONCEPT TESTERS

(1) Using the fact that the composite of two isomorphisms is an isomorphism and the inverse of two isomorphisms is an isomorphism, prove that the automorphisms of a group form a group with the binary operation being composition.
(2) Show that the automorphism group of a group is a subgroup of the symmetric group operating on its underlying set.

POINTS TO PONDER

- The notion of isomorphism can be defined for other algebraic structures as well. Define the notion of isomorphism for a pair of magmas, for a pair of semigroups, and for a pair of monoids.
- In the case of algebraic structure, the "bijective" nature of isomorphisms forces them to have inverses. However, this is not true for all structures. The hackneyed example from elementary calculus is of a differentiable function $x \mapsto x^3$ that is bijective but fails to have a differentiable inverse. How does this example tie in with concepts of "isomorphism"?

6.2. **Homomorphisms.** The notion of homomorphism has been alluded to while discussing a group action. A homomorphism from one group to another is a map (not necessarily bijective) that preserves the composition. Thus, the definition is almost same as that of isomorphism, but it drops bijectivity.

Definition. Given two groups G_1 and G_2, a homomorphism is a map $\phi : G_1 \to G_2$ such that :

$$\phi(gh) = \phi(g)\phi(h)$$

The left multiplication is in G_1 and the right multiplication is in G_2.

Again, this definition is in the spirit of the definition of a group given in section 2.1. If we instead follow the definition of a group given in section 4.2, then the corresponding notion of homomorphism is:

Definition. Given two groups G_1 and G_2, a homomorphism is a map $\phi : G_1 \to G_2$ such that:

$$\begin{aligned}
\phi(gh) &= \phi(g)\phi(h) \ \forall \ g, h \in G_1 \\
\phi(e_{G_1}) &= e_{G_2} \\
\phi(g^{-1}) &= (\phi(g))^{-1} \ \forall \ g \in G_1
\end{aligned}$$

Yet again, these two definitions encode the same concept! In this new light, we may redefine an isomorphism as a **bijective homomorphism**.

We now prove the following :

Claim. The image of a group under a homomorphism is a subgroup of the codomain with the restriction map being a homomorphism.

In symbols, suppose $\phi : G_1 \to G_2$ is a homomorphism. Let H be the subset of G_2 comprising those elements that arise as images of elements of G_1. Then the claim is that H is in fact a subgroup of G_2 and the map ϕ is a homomorphism when treated as a map from G_1 to H.

Proof. The proof requires us to show that the product of two elements in H is also in H, the inverse element of an element in H is in H, and the identity element is in H. Each of these follows directly from the way homomorphisms are defined.

In symbols, let $p, q \in H$. Then there are $g, h \in G_1$ such that $\phi(g) = p$ and $\phi(h) = q$. This gives us that $pq = \phi(g)\phi(h) = \phi(gh)$ and hence that $pq \in H$.

In a similar way we can prove that the neutral element is in H and the inverse of an element in H is in H. The condition of the map $\phi : G_1 \to H$ being a homomorphism now follows directly. $\square$

Concept Testers

(1) Prove that the two definitions of homomorphism are equivalent. (We are now fairly practised at this – we proved that the two definitions of group are equivalent, the two definitions of subgroup are equivalent, and the two definitions of isomorphism are equivalent).
(2) Given a homomorphism $\phi : G_1 \to G_2$, prove that the set of elements in G_1 that map to the identity of G_2 form a subgroup of G_1. That is the set $\{x | \phi(x) = e_{G_2}\}$ is a subgroup of G_1.
(3) Prove that there is a group consisting of only one element, and that any two such groups are isomorphic. Such a group is called a **trivial group**. Prove that, for any group, there is a unique set map from that group to the trivial group and that such a set map is a homomorphism.
(4) Prove that the symmetric group on 1 element (S_1) is the trivial group.

Points to Ponder

- What was the *philosophical reason* that the proof of the second Concept Tester went through? What facts were used in the proof?
- Can *every subgroup* be obtained as the pre-image of the identity element in a group homomorphism? The answer is in fact *no* – subgroups with this property are termed **normal subgroups**. More about this is to be found in Group Theory:The Journey Continues.

6.3. **Subgroups as injective homomorphisms.** Given a set and a subset, there is a natural **inclusion map** from the subset to the set – the map taking each element of the subset to the same element in the set. This map is **injective**.

In case of a subgroup of a group, the natural inclusion map gives rise to an **injective homomorphism**.

That is, if H is a subgroup of G, then the map $\phi : H \to G$ defined by $\phi(h) = h \; \forall \; h \in H$ is a homomorphism. This follows directly from the definitions.

We can now turn this around. We can say that a subgroup is a group along with an injective homomorphism to the given group. Thus, we call H a subgroup of G if there is an injective homomorphism from H to G. Of course, H may not physically be a subset of G, but there will be a subgroup of G with which H can be identified, so that subgroups can, for all practical purposes, be treated as injective homomorphisms.[11]

Concept Testers

(1) Prove that in a homomorphism, the image of a subgroup is a subgroup. (Here, the image of a set is the set of images of all its elements).
(2) Prove that in a homomorphism, the pre-image of a subgroup (of the codomain) is a subgroup (of the domain).
(3) Prove that a subgroup of a subgroup is a subgroup.
(4) Suppose H and K are subgroups of G such that H is a subset of K. Prove that H is a subgroup of K.
(5) Suppose H and K are subgroups of G. Prove that $H \cap K$ is a subgroup of both H and K, and also of G.
(6) Prove that the intersection of a family of subgroups of a given group (possibly infinite) is a subgroup of each member of that family and also of the whole group.
(7) Prove that every group has the **trivial group** as a subgroup (namely, the identity element itself). This is often called the **trivial subgroup**. Further, prove that every group has itself as a subgroup. This is called the **improper subgroup**. Any subgroup of the group that is neither the trivial subgroup nor the whole group itself, is called a **proper nontrivial subgroup**.

---

[11] A more accurate way of putting this is that subgroups can be treated as injective homomorphisms upto commuting isomorphism. However, the notion of commuting isomorphism is not being introduced at this stage.

6.4. **Refining these ideas.** In a sense, many notions related to the group can be defined purely based on the way the homomorphism is defined. In fact, an extreme viewpoint would be to think that the only properties related to groups that make sense are those that can be expressed in the language of homomorphisms.

Homomorphisms can be defined for any kind of structure, and the way homomorphisms are defined indicates the kind of structure we are interested in. For instance, we could define homomorphism between ordered sets as maps which preserve the order. We could define homomorphisms between planes as maps which preserve a notion of continuity.

In this context, we use the following general terms :

- An **endomorphism**(defined) is a homomorphism from the object to itself. An endomorphism of a group is thus a homomorphism from the group to itself.
- An **isomorphism**(defined) is a homomorphism whose inverse exists and is also a homomorphism.
- An **automorphism**(defined) is an isomorphism from an object to itself. It is thus both an isomorphism and an endomorphism.

At a somewhat more philosophical level, homomorphisms are maps that preserve some kinds of structure, but are accompanied by some *loss of information*. However, isomorphisms are maps that preserve all levels of structure. Automorphisms are *symmetries* of the structure.

Concept Testers

(1) Prove that the set of endomorphisms of a group form a monoid under the natural composition. Prove that the set of automorphisms form a submonoid of this monoid which is also a group.
(2) The group of automorphisms of a given group acts in a natural way on the group. Prove that this is a group action, and hence show that the automorphism group of a group is a subgroup of the permutation group on its set of elements.
(3) The **order** of a group is the cardinality of its set of elements. A group is said to be **finite** if its order is finite. Using the previous problem, show that the automorphism group of a finite group is finite.
(4) Try a similar approach to show that the set of endomorphisms of a given group is finite.

7. Review of the journey so far

7.1. **Have we reached where we set for?** It is time to look back at the goals we had set our sights on when we began. Each of us might profit from going back to the original aims and assessing how far we have reached in achieving them.

Here is my personal assessment :

- **Define a group** in more than one way : We have seen two ways of defining groups, in sections 2.1 and 4.2. Both of these have their merits – the first one having the merit that it requires us to define only one binary operation, and the second one having the merit that it defines all the operations upfront, as part of the structure.
- **Understand the concept of subgroup** : We understood a subgroup in many terms – as a multiplicatively closed subset with a group structure (this corresponds to the definition in section 2.1) and as a subset closed under the three group operations (this corresponds to the definition in section 4.2). This also brought out an important idea : the notion of substructure depends on what we define as *essential* to the structure and what we define as *incidental* to the structure. We also saw that a subgroup corresponds to an **injective homomorphism**.
- **Define homomorphism and isomorphism** : We understood the general notion of isomorphism of groups, and the general notion of homomorphism of groups, as maps that preserve the multiplicative structure (as per the first definition of groups) or, equivalently, all the three structures, of groups. Isomorphisms have been viewed in three ways – as homomorphisms whose inverse homomorphisms exist, as bijective homomorphisms, and as maps that identify two objects (that is, identify them in a way that makes them the same or indistinguishable).

In addition, I feel that we have learnt to appreciate:

- The **need for groups** and the role that the definition plays : We haven't been able to delve into all the uses of groups. But the fact that groups are storehouses of **symmetries** and **reversible transformations**, more technically termed **automorphisms**, has been brought out. All of this utility stems from the definition. We also saw how changing the definition slightly changes the behaviour as well.

- The *subtleties* in the way we define subgroups. Clearly, this *two alternative definitions* shows that we need to be careful while defining structures. However, groups being such well behaved creatures, the pair of alternative definitions almost always seem to be equivalent (whether for groups, subgroups, or homomorphisms). The full appreciation of the distinctions will come when we find that the definitions *fail to be equivalent* when we move to other common structure such as rings. (We already had a slight flavour of this where we saw a monoid with a subsemigroup that was a monoid but did not have the same neutral element. Locate this!).
- The distinction and complementarity of **abstract structure** and **concrete action**: This has only just begun unfolding. We saw that the presence of inverses in a group makes its action always give permutations. Many more aspects will come out with time, but the principle is clear.

7.2. **The unexpected delights.** On the way to a better understanding of the path we tread, we also got glimpses of other beautiful territories – while at the same time realizing that ours was the most beautiful of all. To understand why groups were defined the way they were, we introduced ourselves to weaker structures such as :

- **Magma** : Set with binary operation
- **Semigroup** : Associative magma
- **Monoid** : Semigroups with a neutral element
- **Quasigroup** : A magma where any element can be taken to any other element by left multiplication in a unique way, and by right multiplication in a unique way
- **Algebra loop** : Quasigroup with a neutral element

We also saw properties such as :

- **Associativity**
- **Commutativity**
- **Neutral elements**
- **Inverse elements** with respect to a neutral element

Then we saw elements that are :

- Left associative, right associative and middle associative
- Left cancellative and right cancellative
- Left neutral and right neutral
- Left invertible and right invertible

And of course, when in the realm of groups, all these become well behaved.

8. Preparations for the further journey

8.1. **We are getting there.** We have now understood the definition of a group, and its basic purpose, quite thoroughly – pending too many examples. It is now fitting to begin a serious study of groups, along with all the examples and all the properties in the finer print. The main tools in our study shall be the tools of careful property oriented analysis and the careful review of definitions.

8.2. **The contexts in which we shall discuss properties.** We shall go on to study various properties of groups. For instance, we may look at the property of a group being **finite**. We may look at the property of a group being **infinite**. Each group property that we study must satisfy the following :

- Given any group, it must either have the property or not have the property.
- The property must be **isomorphism invariant**. In other words, if two groups are isomorphic, either both of them have the property, or neither does.

It is clear that any property that we would naturally come to define for groups must satisfy the above two conditions. As we proceed further along our journey of groups, we shall collect many properties on the way. Some of these properties may be stronger than (in the sense that they may imply) others.

Apart from groups, we may be interested in **subgroup properties**. That is, we are interested in the properties of how a subgroup is embedded in a group. A subgroup property depends not only on the structure of the subgroup, but also on the manner in which it sits inside the group. Subgroup properties must satisfy two conditions :

- Given any group and any subgroup thereof, the subgroup either satisfies the property inside the group, or does not satisfy the property inside the group.

- The subgroup properties are invariant upto **commuting isomorphism** That is, suppose G_1 and G_2 are isomorphic (sometimes written as $G_1 \cong G_2$), and that H_1 is a subgroup of G_1 that goes to H_2, a subgroup of G_2, under this isomorphism. Then H_1 satisfies the property in $G_!$ iff H_2 satisfies the property in G_2.

In addition to group properties and subgroup properties, we may want to study the properties of **elements in groups**, the properties of **equivalence relations in groups**, or the properties of **endomorphisms on groups**. Different properties become important in different contexts.

8.3. **What we shall strive to achieve.** We shall strive to understand :
- What are the various kinds of groups (upto isomorphism)?
- What are the various representations of groups, or in what ways can the groups act?
- Given a group, what do its endomorphisms and automorphisms look like?
- What kinds of subgroups does a group have?

There are a few other questions that we will add to this list as we proceed.

So, happy journey!