A highlight on Basic Notions of Groups in Abstract Algebra

Neha Sharma[1], Sudhir Narale[2]
[1, 2] Department- Dean Academics
[1, 2] Dr.D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune

Abstract- *This paper is the study of algebraic systems in an abstract way. We are already familiar with a number of algebraic systems from our earlier studies. For example, in number systems such as the integers Z = (….-3,-2,-1, 0, 1, 2, 3…), the rational numbers* $Q = \frac{m}{n}$ *; m; n € Z, the real numbers R, or the complex numbers C = (x +iy; x; y € R) (where* $i^2 = -1$*) there are algebraic operations such as addition, subtraction, and multiplication.*

This paper studies general algebraic systems in an axiomatic framework, so that the theorems one proves apply in the widest possible setting. The most commonly arising algebraic systems are groups, rings and flelds will be briefly discussed in this paper.

Keywords- Abstract Algebra, Algebric Structure, Group, Associativity , Identity, Inverse, Cummutavity

I. INTRODUCTION

"Algebra is generous; she often gives more than is asked of her." – D'Alembert

Abstract algebra is the subject area of mathematics that studies algebraic structures, such as groups, rings, fields, modules, vector spaces, and algebras. The phrase abstract algebra was coined at the turn of the 20th century to distinguish this area from what was normally referred to as algebra, the study of the rules for manipulating formulae and algebraic expressions involving unknowns and real or complex numbers , often now called elementary algebra .

In mathematics, a group is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element. The operation satisfies four conditions called the group axioms, namely closure, associativity, identity and invertibility. One of the most familiar examples of a group is the set of integers together with the addition operation, but the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, applies much more widely. It allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

Groups share a fundamental kinship with the notion of symmetry. For example, a symmetry group encodes symmetry features of a geometrical object: the group consists of the set of transformations that leave the object unchanged and the operation of combining two such transformations by performing one after the other. Lie groups are the symmetry groups used in the Standard Model of particle physics; Poincaré groups, which are also Lie groups, can express the physical symmetry underlying special relativity; and point groups are used to help understand symmetry phenomena in molecular chemistry

The concept of a group arose from the study of polynomial equations, starting with Évariste Galois in the 1830s. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—an active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups. In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely, both from a point of view of representation theory (that is, through the representations of the group) and of computational group theory. A theory has been developed for finite groups, which culminated with the classification of finite simple groups, completed in 2004. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become a particularly active area in group theory.

II. DEFINITION

A group is a set, G, together with an operation • (called the group law of G) that combines any two elements a and b to form another element, denoted a • b or ab. To qualify as a group, the set and operation, (G, •), must satisfy four requirements known as the group axioms:

i. **Closure:** For all a, b in G, the result of the operation, a • b, is also in G.
ii. **Associativity:** For all a, b and c in G, (a • b) • c = a • (b • c).
iii. Identity element:

There exists an element e in G such that, for every element a in G, the equation e • a = a • e = a holds. Such an element is unique, and thus one speaks of the identity element.

iv. Inverse element:

For each a in G, there exists an element b in G, commonly denoted a−1 (or −a, if the operation is denoted "+"), such that a • b = b • a = e, where e is the identity element.

Another Definition

A group is a non-empty set G with an associative binary operation ∗ with the following property:

1) (Identity element) There exists an element e ∈ G such that for all a ∈ G, e ∗ a = a ∗ e = a. (Why is it called “e”? This comes from German “Einheit”.)

2) (Inverse element) For every a ∈ G there exists b ∈ G such that a ∗ b = b ∗ a = e. We often write (G, ∗) to mean that G is a group with operation ∗.

• If F is a field, like Q, R, C, then (F, +) is a group but (F, ·) is not.Furthermore (F/{0}, ·) is a group. Also, if V is a vector space over F , then (V, +) is a group.We can conclude (Z, +) is a group, but that (N, +) is not.

Here is a possibly new example: let G = {1, −1, i, −i}, and let ∗ be multiplication. Then G is a group, and we can write its multiplication table as follow (Cayley table):

Table 1.

	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

Associativity holds because we know that multiplication of complex numbers is associative. We can find the identity element and an inverse of each element.Also closure property holds here.

Theorem 2.1 Let * be an associative binary operation on a non-empty set G. Then G has at most one element e satisfying the property that for all a ∈ G, e ∗ a = a ∗ e = a.

Proof. If e' is an element of G with $e' * a = a * e' = a$ for all a ∈ G, then

$e' * e = e$ and $e' * e = e'$

by the defining properties of e and e, whence $e = e'$.

In particular, a group (G, ∗) has exactly one element e that acts as an identity element, and it is called the identity element of G. Furthermore, the inverses of each element also unique.

Theorem 2.2 Let (G, ∗) be a group, a ∈ G. Then there exists a unique element b ∈ G such that b ∗ a = a ∗ b = e.

. By the inverse element axiom, such an element b exists. Let c ∈ G such that c ∗ a = a ∗ c = e. Then

c = c ∗ e = c ∗ (a ∗ b) = (c ∗ a) ∗ b = e ∗ b = b,

by associativity and by the property of identity e.

This unique inverse element of a is denoted as a^{-1}.When the operation ∗ is +, then the inverse is written as −a.

We also introduce another bit of notation: for a ∈ G, a^0 is the identity element, if n is a positive integer, then a^n is the shorthand for a ∗ a ∗ · · · ∗ a, where a is written n times. Clearly if n > 0, then $a^n = a^{n-1} * a = a * a^{n-1}$.When the operation ∗ is +, then a ∗ a ∗ · · · ∗ a (with a being written n times) is usually denoted as na.

Group of symmetry:

Two figures in the plane are said to be congruent if one can be changed into the other using a combination of rotations, reflections, and translations. Every figure is congruent to itself. However, some figures are congruent to themselves in more than one way, and these more congruences are called symmetries. A square has eight symmetries. These are:

The elements of the symmetry group of the square (D4). Vertices are denoted by color or number.

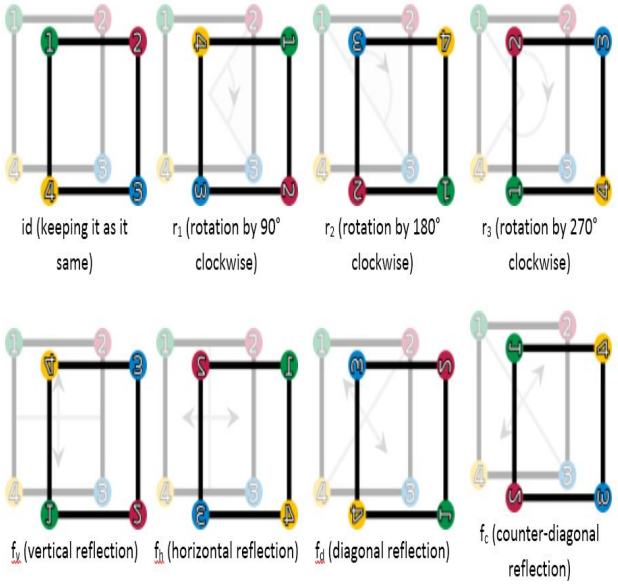

Figure 1.

- the identity operation leaving everything unchanged, denoted id;
- rotations of the square around its center by 90° clockwise, 180° clockwise and 270° clockwise, denoted by r_1, r_2 and r_3, respectively;
- reflections about the vertical and horizontal middle line (f_h and f_v), or through the two diagonals (f_d and f_c).

These symmetries are represented by functions or transformations. Each of these functions sends a point in the square to the corresponding point under the symmetry. For example, r_1 sends a point to its rotation 90° clockwise around the square's center, and f_h sends a point to its reflection across the square's vertical middle line. Composing two of these symmetry functions gives another symmetry function. These symmetries determine a group called the dihedral group of degree 4 and denoted D_4. The underlying set of the group is the above set of symmetry functions, and the group operation is function composition. Two symmetries are combined by composing them as functions, that is, applying the first one to the square, and the second one to the result of the first application. The result of performing first a and then b is written symbolically from right to left as b • a.

The group as in the above discussion is denoted by S_X and is called the permutation group of X or symmetric group of X.

- Definition 2.1: Order of group G

The total number of elements of a group G is called the order of G.It is denoted as |G|. We call group G finite if it has only finitely many elements; otherwise it is infinite.

- Definition 2.2: Order of element

Let G be a group and a ∈ G. If there is a positive integer n such that $a^n = e$, then the smallest such positive integer n is the order of a. If no such n exists, we say that a has infinite order. The order of a is denoted |a|.

III. THEOREMS

Lemma 3.1 *For any* n ∈ N, $(a^n)^{-1} = (a^{-1})^n$.

Proof. By definition, $(a^n)^{-1}$ is the unique element of G whose product with a^n in any order is e. But by associativity,we have

$$an * (a-1)n = (an-1 * a) * (a-1 * (a-1)n-1)$$
$$= an-1 * (a * (a-1 * (a-1)n-1))$$
$$= an-1 * ((a * a-1) * (a-1)n-1))$$
$$= an-1 * (e * (a-1)n-1))$$
$$= an-1 * (a-1)n-1,$$

which by induction on n equals e (the cases n = 0 and n = 1 are trivial). Similarly, the product of a^n and $(a^{-1})^n$ in the other order is e. This proves that $(a^{-1})^n$ is the inverse of a^n, which proves the lemma.

With this, if n is a negative integer, we write a^n to stand for $(a^{-n})^{-1}$.

Theorem 3.2 (Cancellation) *Let* (G, ∗) *be a group,* a, b, c ∈ G *such that* a ∗ b = a ∗ c.
Then b = c.

Similarly, if b ∗ a = c ∗ a, *then* b = c.

Proof. By the axioms and the notation,

$b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c.$

Similarly we can proove second part.

Exercise * Prove that for every $a \in G$, $(a^{-1})^{-1} = a$.

Exercise * Let $a, b \in G$. Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$.

Exercise * Let G be a group, $a \in G$. Then the left translation or the left multi-plication by a is the function $L_a : G \to G$ defined by $L_a(x) = a * x$. Prove that L_a is a one-to-one and onto function.

Exercise * Let G be a group, $a \in G$. Then the conjugation by a is the function $C_a : G \to G$ defined by $C_a(x) = a*x*a^{-1}$. Prove that C_a is a one-to-one and onto function and that its inverse is C_a-1 .

Lemma 3.3 *If* $a * b = b * a$, *then for all/any one* $n \in Z$, $(a * b)^n = a^n * b^n$.

Proof. If n = 0 or n = 1, this holds trivially. Now let n > 1. By commutativity, $b^m * a = a * b^m$ for all $m \geq 0$. Then by induction on n,

$(a * b)n = (a * b)n-1 * (a * b) = (an-1 * bn-1) * (a * b)$
$= ((an-1 * bn-1) * a) * b = (an-1 * (bn-1 * a)) * b$

$= (an-1 * (a * bn-1)) * b = (an-1 * a) * bn-1) * b$
$= an * (bn-1 * b) = an * bn.$

Thus the lemma holds for all $n \in N$. If $n < 0$, then by the positive case and commutativity, $(a * b)^n = (b * a)^n = ((b * a)^{-n})^{-1} = (b^{-n} * a^{-n})^{-1}$, whence from Exercise 2.6, $(a * b)^n = (a^{-n})^{-1} * (b^{-n})^{-1}$, which is $a^n * b^n$. □

A partial converse also holds (why is this only a partial converse?):

Proposition 3.4 *Let* $a, b \in G$ *such that* $(a * b)^2 = a^2 * b^2$. *Then* $a * b = b * a$.

Proof. By assumption,

$a * b * a * b = (a * b)2 = a * a * b * b,$

so that by cancellation, $b * a = a * b$.

IV. CONCLUSION

The concept of a group arose from the study of polynomial equations, symmetries of polygons starting with Évariste Galois in the 1830s. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—an active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups.

This paper is the revision of abstract algebra. A Journey of conversion of algebraic structure to a Group

when certain properties are satisfied which are closure, associativity, identity, inverse.

REFERENCES

[1] G.Birkhoff, current trends in algebra, Amer.Math.Monthly, 1973,80:760-782 and 1974,81:746

[2] A.Gallian, The search for finite simple group, Math Magazine, 1976,49:163-179

[3] O.J. Schmidt, Abstract theory of groups, W.H.Freeman and Co.,1966 (Translation by F.Holling and I.B.Roberts of the 1916 Russian Edition

[4] G.A.Miller , History of the theory of groups, collected works,3.vol,pp 427-467, pp1-18 and pp 1-15 respectively.University of Illinois Press,1935,1938 and 1946