INTRODUCTION TO GROUP THEORY

BY

Prof Dr. Muna Abbas Ahmed

University of Baghdad\College of Science for Women\Department of Mathematics

Chapter One

1. Binary operation
2. Groups
3. Subgroups
5. Product of groups

Chapter two

1. Normal subgroup
2. Quotient groups
3. Left Coset and right Coset

Chapter three

Isomorphism theorems of groups

Chapter four

1. Internal direct product of groups
2. External direct product of groups

المحاضرة الاولى

Basic Definitions

Generalizations of the quadratic formula for finding the roots of cubic and quartic polynomials were discovered in the early 1500s. Over the next three centuries, many tried to find analogous formulas for the roots of higher-degree polynomials. Still, in 1824, N. H. Abel (1802–1829) proved that no formula gives the roots of the general polynomial of degree 5. In 1831, E. Galois (1811– 1832) completely solved this problem by finding precisely which polynomials, of arbitrary degree, admit such a formula for their roots. This fundamental idea involved his invention of the idea of *group*. Since Galois's time, groups have arisen in many other areas of mathematics.

Definition (1): A binary operation on a set G is a function

$$*: G \times G \to G.$$

Definition (2): A group is a set G with an operation $*$ and a special element $e \in G$ (sometimes denoted by 1), called the identity, such that:

(i) The associative law holds: for every $a, b, c \in G$,

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

(ii) $e * a = a$ for all $a \in G$;

(iii) For every $a \in G$, there is $a^{I} \in G$ with $a^{I} * a = e$.

Remark (3):

An additive group is a set G together with an operation (+) and an identity element $0 \in G$ such that

(i) $a + (b + c) = (a + b) + c$ for every $a, b, c \in G$;

(ii) $0 + a = a$ for all $a \in G$;

(iii) For every $a \in G$, there is $-a \in G$ with $(-a) + a = 0$.

Note that the inverse of a, in additive notation, is written -a instead of a^{-1}.

Definition (4): A group G is called abelian if it satisfies the following:

$x * y = y * x$ holds for every $x , y \in G$.

Remark (5):

This term honours N. H. Abel who proved a theorem, in 1827, equivalent to there being a formula for the roots of a polynomial if its Galois group is commutative. This theorem is virtually forgotten today because it was superseded by a theorem of Galois around 1830.

Definition (6): If G is a group and $a \in G$, then the unique element $a^{-1} \in G$ such that $a^{-1} * a = e$ is called the inverse of a, and it is denoted by a^{-1}.

Here are three more properties hold in all groups.

Lemma (7): If G be a group, then the following statement are holds:

(i) The cancellation laws hold: if a, b, x $\in$ G, and either x * a = x * b or a * x = b * x, then a = b.
(ii) $(a^{-1})^{-1} = a$, for all a $\in$ G.
(iii) If a, b$\in$G, then:

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

More generally, for all n $\geq$ 2,

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a^{2-1} * a^{1-1}.$$

Proof:

(i) $a = e * a = (x^{-1} * x) * a = x^{-1} * (x * a)$

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

In similar proof, when x is on the right.

From now on, we will usually denote the product a b in a group by ab (we have already abbreviated α β to αβ in symmetric groups), and we will denote the identity by 1 instead of by e. When a group is abelian, however, we will often use additive notation. Here is the definition of group written in additive notation.

Some Examples:

In this lecture, we give some examples about groups, such as $(Z,+)$, $(Q\setminus\{0\},.)$, S_n with the composition operator and Boolean group.

Examples:

(i) $(Z,+)$; The set of all integers is an additive abelian group with identity $e = 0$, and with the inverse of an integer n being $-n$. Similarly, one can see that $(Q,+)$ and $(R,+)$ are additive abelian groups, where Q is the set of rational numbers and R is the set of real numbers.

(ii) $(Q\setminus\{0\}, .)$; The set of all nonzero rational numbers, is an abelian group, where (.) is the ordinary multiplication, the number 1 is the identity, and the inverse of r is $1/r$. Similarly, $(R\setminus\{0\},.)$ is a multiplicative abelian group.

(iii) Let X be a set. Recall that if A and B are subsets of X, then their symmetric difference is $A\Delta B=(A-B)\cup(B-A)$. The Boolean group P (X) is the family of all the subsets of X with addition given by symmetric difference.

(iv) Consider S_n, the set of all permutations of $X = \{1, 2, \ldots, n\}$. It is form a group with the composition operation.

Remark: Let G be a group, let a, b G, and let m and n be (not necessarily positive) integers.

(i) If a and b commute, then $(ab)^n = a^n b^n$.

(ii) $(a^n)^m = a^{mn}$.

(iii) $a^m a^n = a^{m+n}$.

References

1. D. M. Burton, Abstract and linear algebra, 1972.

2. Joseph J. Rotman, Advanced Modern Algebra, 2003.

3. John B. Fraleigh, A First Course in Abstract Algebra, Seventh Edition, 2002.

4. Joseph A. Gallian, Contemporary Abstract Algebra, 2010.