UNIVERSITY OF ANBAR

COLLEGE OF EDUCATION FOR PURE SCIENCES

DEPARTMENT OF MATHEMATICS

GROUP THEORY- GROUP -2-

SECOND CLASS

Dr. Majid Mohammed Abed

2019-2020

The First Lecture

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, but in 1824, N. H. Abel (1802–1829) proved that there is no such formula giving 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. His fundamental idea involved his invention of the idea of *group*. Since Galois's time, groups have arisen in many other areas of mathematics.

function is a*G* on a set

Binary Operation

Definition. A binary operation $*$ on a nonempty set A is a function from $A \times A$ to A.

Definition . A binary operation $*$ on A is associative if $\forall a, b, c \in A$, $(a * b) * c = a * (b * c)$. A binary operation $*$ on A is commutative if $\forall a, b \in A$, $a * b = b * a$.

Definition . If $*$ is a binary operation on A, an element $e \in A$ is an identity element of A w.r.t $*$ if $\forall a \in A$, $a * e = e * a = a$.

Example . The element 1 is an identity element for Z, Q and R w.r.t. multiplication. 0 is an identity element for Z, Q and R w.r.t. addition.

Definition . Let $*$ be a binary operation on A with identity e, and let $a \in A$. We say that a is invertible w.r.t. $*$ if there exists $b \in A$ such that $a * b = b * a = e$. If f exists, we say that b is an inverse of a w.r.t. $*$ and write $b = a^{-1}$. Note, inverses may or may not exist.

Example . Every $x \in Z$ has inverse w.r.t. addition because $\forall x \in Z$, $x + (-x) = (-x) + x = 0$. However, very few elements in Z have multiplicative inverses.

Example . Let $*$ be a binary operation on Z defined by $\forall a, b \in Z$, $a * b = a + 3b - 1$.

(a) Prove that the operation is binary.

(b) Determine whether the operation is associative and/or commutative. Prove your answers.

(c) Determine whether the operation has identities.

(d) Discuss inverses.

Example. Let $*$ be a binary operation on the power set P(A) defined by $\forall X, Y \in P(A)$, $X * Y = X \cap Y$. (a) Prove that the operation is binary. (b) Determine whether the operation is associative and/or commutative. Prove your answers. (c) Determine whether the operation has identities.

(d) Discuss inverses.

Example . Let $*$ be a binary operation on F(A) defined by $\forall f, g \in F(A)$, $f * g = f \circ g$. (a) Prove that the operation is binary. (b) Determine whether the operation is associative and/or commutative. Prove your answers.

(c) Determine whether the operation has identities. (d) Discuss inverses

Remark .

An additive group is a set G equipped with an operation (+) and an identity element 0 □ G such that

(i) a + (b + c) = (a + b) + c for every a, b, c □ G;

(ii) 0 + a = a for all a □ G;

(iii) For every a □ G, there is −a □ G with (−a) + a = 0.

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

Definition A group *G* is called abelian if it satisfies the following:

***x* ∗ *y* = *y* ∗ *x* holds for every *x* , *y* ∈ *G*.**

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.

References

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

[2] Joseph J.Rotman, Advanced Modren Algebra, 2003.

[3] John B. Fraleigh, A First Course in Abstract Algebra, Seventh Edition, 2002 [4] Joseph A. Gallian, Contemporary Abstract Algebra, 2010.