Linear Algebra and Applications

Sartaj Ul Hasan

Department of Mathematics
Indian Institute of Technology Jammu
Jammu, India - 181221

Email: sartaj.hasan@iitjammu.ac.in

Lecture 11

(Aug 20, 2019)

Finite Groups

- If $(G, *)$ is a group, and the underlying set G is finite, then we call it a finite group. For a finite group $(G, *)$, the number of elements in G is called the **order** of the group, written $|G|$ or $o(G)$.
- Some examples of finite groups:
  1. Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and define $a +_6 b := (a + b)$ mod 6 for all $a, b \in \mathbb{Z}_6$. This operation is known as addition mod 6 (modular addition). Then $(\mathbb{Z}_6, +_6)$ is an abelian group.
  2. We can generalize the above example to any positive integer n. Let $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ and define $a +_n b := (a + b)$ mod n for all $a, b \in \mathbb{Z}_n$. Then $(\mathbb{Z}_n, +_n)$ is an abelian group.

Examples of Finite Groups - continued

3. Let $K_4 = \{e, a, b, c\}$ and let $*$ be an operation on K_4 defined by the following table (such a table is known as a group composition table). Then it can be verified that all the group axioms are satisfied by $(K_4, *)$, known as Klein's four group.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

4. Let $\mathbb{Z}_n^\times :=$ set of positive integers $< n$ and relatively prime to n, for $n \geq 2$, that is, $\mathbb{Z}_n^\times := \{j \ : \ 1 \leq j < n, \gcd(j, n) = 1\}$.

   Define the operation $\times_n$ on $\mathbb{Z}_n^\times$ by $a \times_n b := a \times b \pmod{n}$ for all $a, b \in \mathbb{Z}_n^\times$ (multiplication modulo n).

   Then $(\mathbb{Z}_n^\times, \times_n)$ is a group.

   Note that $(\mathbb{Z}_n^\times, \times_n)$ is a finite group and $|\mathbb{Z}_n^\times| = \phi(n)$, where ϕ is Euler's ϕ function, aka totient function.

Examples of Groups that are NOT abelian

- The set $\mathrm{GL}_n(\mathbb{R})$ of all $n \times n$ invertible matrix over $\mathbb{R}$ forms a group with respect to matrix multiplication, but it is NOT abelian. This group is usually known as **General Linear Group** of order n over $\mathbb{R}$. Also note that this is an example of infinite group which is NOT abelian.

- The set $\mathrm{GL}_n(\mathbb{Z}_p)$ of all $n \times n$ invertible matrix over $\mathbb{Z}_p$ forms a group with respect to matrix multiplication, but it is NOT abelian. This is an example of finite group, which is NOT abelian. List all the elements of $\mathrm{GL}_2(\mathbb{Z}_2)$ and verify!