Notes on GE4 (Marked portion (unit 1) of the syllabus) by SB (Subhasundar Bandyopadhyay)
Algebra-II

Books followed: 1. Algebra (Abstract and Linear) - Prof S.K. Mapa
2. Higher Algebra - Ghosh and Chakravorty

Definition of Group: Let G be a non-empty set and '0' be a binary operation on G. Then G is said to be a group with respect to the binary operation '0' or (G, 0) is said to be a group if

(i) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$ (Associative Property)

(ii) there exists an element $e \in G$ such that
$a \circ e = e \circ a = a$ for all $a \in G$ (Existence of identity element)

(iii) for each $a \in G$, there exists an element $b \in G$ such that $a \circ b = b \circ a = e$ (Existence of inverse element)

Note: 1. Let G be a non-empty set. A binary operation '0' on G is a mapping $0 : G \times G \to G$. Example '+' is a binary operation on Real numbers, $0(a, b)$ is denoted by $a \circ b$.

2. Sometimes it is written as $a \circ b \in G$ for all $a, b \in G$ for "0" is a binary operation on G.

3. Let (G, 0) be a group. If in addition $a \circ b = b \circ a$ for all $a, b \in G$. Then G is a said to be a commutative or abelian group.

Examples: 1. Let $\mathbb{Z}$ be set of all integers. Then $(\mathbb{Z}, +)$ is a group. It is also an abelian group.

2. Let $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ be the set of all non-zero rational numbers. Then $\mathbb{Q}^*$ is an abelian group with respect to multiplication.

3. If $\mathbb{Q}$ be the set of all rational numbers. Then $(\mathbb{Q}, +)$ is an abelian group.

4. $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups where $\mathbb{R}$ is the set of all real numbers and $\mathbb{C}$ is the set of all complex numbers.

Note: If G is finite set, then (G, 0) is said to be a finite group and if G be infinite then (G, 0) is said to be

infinite group. Examples 1–4 are all examples of infinite groups.

5. Let $G = \{1, -1\}$. Then $(G, \cdot)$ is an abelian group

6. Let $G = \{1, \omega, \omega^2\}$ where ω is the imaginary cube root of unity. Then $(G, \cdot)$ is an abelian group

7. Let $G = \{1, -1, i, -i\}$. Then $(G, \cdot)$ is an abelian group

Note: Examples 5–7 are all examples of finite group

8. Let $G = \{e, a, b, c\}$. We define a binary operation 'o' given by the following table:

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Here (G, o) is an abelian group. This group is Called Klein's 4-group.

Note: A binary operation 'o' on a finite set can be defined by a table as in example 8. This table is called Cayley's table.

Note: The elements of G, in Example 5, are the roots of $x^2 = 1$, in Example 6, are the roots of $x^3 = 1$, and in Example 7 are the roots of $x^4 = 1$. In general, the roots of $x^n = 1$, for some positive integer n, are called the nth roots of unity. They are n in numbers. They are given by $1, \alpha, \ldots, \alpha^{n-1}$ where $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$

If we take $G = \{1, \alpha, \ldots \alpha^{n-1}\}$. Then $(G, \cdot)$ is an abelian group. It is called the group of nth roots of unity.

9. Let $M_{2\times 2}(\mathbb{R}) = \{A : A \text{ is a } 2\times 2 \text{ real matrix}\}$

Then $M_{2\times 2}(\mathbb{R})$ is an abelian group with respect to matrix addition.

10. Let $G = \{A : A \text{ is a } 3\times 3 \text{ real non-singular matrix}\}$
Then G forms a group with respect to matrix multiplication.

Some Elementary properties using definition of group:

Result 1 : A group (G, o) contains only one identity element

Proof: Let e_1, e_2 be two identity elements in the group
Then $e_1 o a = a o e_1 = a$ for all $a \in G$ —— (1)
and $e_2 o a = a o e_2 = a$ for all $a \in G$. —— (2)

Now $e_1 o e_2 = e_2$ by (1)

and $e_1 o e_2 = e_1$ by (2)

So, $e_1 = e_2$ and this proves that the identity element is unique.

Result 2 In a group (G, o), each element has only one inverse

Proof: Let $a \in G$ and a', a'' be two inverses of a.

Then $a' o a = a o a' = e$

and $a'' o a = a o a'' = e$, e is the identity element in G.

Now, $a' o (a o a'') = (a' o a) o a''$, since o is associative.

But, $a' o (a o a'') = a' o e = a'$ and $(a' o a) o a'' = e o a'' = a''$

So, $a' = a''$ and this proves that the inverse of a is unique.

Note 1: The unique inverse of a is denoted by $\vec{a}^{-1}$. Therefore for a in G, $a o \vec{a}^{-1} = \vec{a}^{-1} o a = e$ holds (e is the identity element in G)

Note 2. In $(\mathbb{R}, +)$, 0 is the identity element. For each $a \in \mathbb{R}$, $-a$ is the inverse of a

Note 3. In the group $(G, \cdot)$ where $G = \{1, \omega, \omega^2\}$, 1 is the identity element. $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$ and $1^{-1} = 1$

Note 3. Identity element has self inverse, i.e, $\vec{e}^{-1} = e$.

Result 3 In a group (G, o)

(i) $a o b = a o c \Rightarrow b = c$ (Left Cancellation Law)

(ii) $b o a = c o a \Rightarrow b = c$ (Right Cancellation Law)

for all $a, b, c \in G$.

Proof: (i) Since $a \in G$, $\vec{a}^1 \in G$

$$a o b = a o c$$

$$\Rightarrow \vec{a}^1 o (a o b) = \vec{a}^1 o (a o c)$$

$$\Rightarrow (\vec{a}^1 o a) o b = (\vec{a}^1 o a) o c, \text{ since } o \text{ is associative}$$

$$\Rightarrow e o b = e o c, \text{ } e \text{ being the identity element in } G.$$

$$\Rightarrow b = c$$

(ii) $$b o a = c o a$$

$$\Rightarrow (b o a) o \vec{a}^1 = (c o a) o \vec{a}^1$$

$$\Rightarrow b o (a o \vec{a}^1) = c o (a o \vec{a}^1), \text{ since } o \text{ is associative}$$

$$\Rightarrow b o e = c o e, \text{ } e \text{ being the identity element in } G$$

$$\Rightarrow b = c$$

Result 4 In a group (G, o), for all a, b in G, each of the equation $a o x = b$ and $y o a = b$ has a unique solution in G.

Proof: Since $a, b \in G$, $\vec{a}^1 o b \in G$.

Now $a o (\vec{a}^1 o b) = (a o \vec{a}^1) o b$ (since o is associative

$= e o b$, e is the identity element in G.

$= b$

This shows that $\vec{a}^1 o b$ is a solution of the equation $a o x = b$

We shall prove that this solution is unique. Let there be two solutions x_1 and x_2 in G of the equation $a o x = b$. Then $a o x_1 = b$ and $a o x_2 = b$. This implies $a o x_1 = a o x_2$

or, $x_1 = x_2$ (by left cancellation law)

So, $a o x = b$ has a unique solution $\vec{a}^1 o b$.

Similarly, $b o \vec{a} \in G$ and $(b o \vec{a}^1) o a = b o (\vec{a}^1 o a)$ (since o is associative

$= b o e$, e is the identity in G.

So, $b o \vec{a}^1$ is a solution of $y o a = b$ $= b$

Let there be two solutions y_1 and y_2 of $y o a = b$. Then we get $y_1 o a = b$ and $y_2 o a = b \Rightarrow y_1 o a = y_2 o a \Rightarrow y_1 = y_2$ (by right cancellation law)

So, $y o a = b$ has a unique solution $b o \vec{a}^1$.