

Group theory

In this lecture we give outline and it is not limited about group theory which we must take it in this course

Syllabus :

- 1- Group , definition and examples explain it .
- 2- Some important theories on group and properties of its .
- 3- Important group , symmetric group , group of integer number modulo n (i.e. Z_n) .
- 4- A belian group .
- 5- Cyclic group .
- 6- Subgroups .
- 7- Centre of group .

References :

- 1- Introduction to modern algebra by David Burton .
- 2- Group theory by M.Suzuki .
- 3- A first course in abstract algebra by J.B.Fraleigh .
- 4- نظرية الزمر تأليف د. باسل عطا و د. عادل غسان .

I- Definition (1.1) : Semigroup

Let A be anon-empty set . A binary operation $*$ is a function from the Cartesian product $A \times A$ into A . This means that $*$: $A \times A \rightarrow A$ is a binary operation iff :

- 1- $a*b \in A$ for each $a,b \in A$ (closure condition) .

2- If $a, b, c, d \in A$ such that $a = c$, and $b = d$, then $a * b = c * d$ (well-define condition).

Examples(1.2):

1- $(+, -, \times)$ are binary operations on $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$.

2- $(+, -)$ are not binary operation on odd integer number.

3- $(-)$ is not binary operation on \mathbb{N} (natural number).

Homework :

1- Let $a * b = a + b + 2$ for each $a, b \in \mathbb{Z}$. Is $*$ binary operation on \mathbb{Z} .

2- $a \oplus b = a^b$, for each $a, b \in \mathbb{Z}$.

3- $a * b = a + b - 2$, $a, b \in \mathbb{N}$.

Definition(1.3): Mathematical system

A mathematical system is a non-empty set of elements with one or more binary operation defined on this set.

Examples(1.4):

1- $(\mathbb{R}, +)$, $(\mathbb{R}, -)$, $(\mathbb{R} - \{0\}, \div)$.

2- $(\mathbb{R}, +, \times)$, $(\mathbb{R}, \div, \times)$, $(\mathbb{N}, +)$ and $(\mathbb{Z}_e, \times, +)$ are mathematical systems.

3- $(\mathbb{N}, -)$, (\mathbb{R}, \div) , $(\mathbb{Z}_{\text{Odd}}, +, -)$ are not mathematical systems.

Definition(1.5): Semigroup

A semigroup is a non-empty set with an associative binary operation $*$ defined on A .

Examples(1.6):

1- (\mathbb{Z}, \times) , $(\mathbb{Z}, +)$, $(\mathbb{N}, +)$, (\mathbb{N}, \times) , $(\mathbb{Z}_e, +)$ and (\mathbb{Z}_e, \times) are semigroups.

2- $(\mathbb{Z}_{\text{Odd}}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}_e, -)$ and $(\mathbb{R} - \{0\}, \div)$ are not semigroups.

Definition(1.7): Group

A group is a non-empty set with binary operation $*$ define on its such that it is satisfy the following :

- 1- The closure : for each $a,b \in G$ we have $a*b \in G$.
- 2- The associative : for each $a,b,c \in G$, we have $(a*b)*c = a*(b*c)$
- 3- The identity element : there exists identity element $e \in G$ such that for each $a \in G$, we have $a * e = e*a = a$.
- 4- The inverse : for each $a \in G$, there exists $a^{-1} \in G$ such that $a* a^{-1} = a^{-1}*a = e$.

Note: Every group is semigroup , but the converse is not true in general for example $(\mathbb{N},+)$ is semgroup but not group because there is no inverse element belong to \mathbb{N} .

Definition(1.8): commutative group (Abelian group)

A group is called commutative iff $a *b = b*a$ for each $a, b \in G$.

Examples(1.9):

- 1- Each of $(\mathbb{Z},+)$, $(\mathbb{Z}_e, +)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$ and $(\mathbb{C} , +)$ are commutative group .
- 2- $(\{1,0,-1,2\},+)$ is not group
- 3- $(\{-1,1\}, \bullet)$ is a commutative group .

Homework :

1- Let $G = \{a,b,c,d\}$. Define $*$ a binary operation on G as the following table shows :

| | | | | |
|---|---|---|---|---|
| * | a | b | c | d |
| a | a | b | c | d |
| b | b | c | d | a |
| c | c | d | a | b |

| | | | | |
|---|---|---|---|---|
| d | d | a | b | c |
|---|---|---|---|---|

Is $(G, *)$ commutative group or not .

2- Let $G = \{ 1, -1, i, -i \}$ be a mathematical system with multiplication (i.e. (G, \bullet)) . Show that G is commutative group .

3- Is $(Z, *)$ group , such that $a * b = a+b+2$ for each $a, b \in Z$.

Definition(1.9): Symmetric group

Let A be a non-empty set , then every (1-1) and onto map from A into itself is called permutation or symmetric on A , and it is denoted by $\text{symm}(A)$.

Example(1.10):

1- $(\text{Symm}(A), \circ)$ is group . (H.W.) .

2- Let $A = \{1, 2, 3\}$ be a set and $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$. (S_3, \circ) is symmetric group ,

where $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Definition(1.11): Let $a, b \in Z$, $n \in N$, then we said that a congruent to b modulo n iff $a-b = nk$, where $k \in Z$, and denoted by $a \equiv b$ or $a \equiv b \pmod{n}$.

Examples(1.12):

1- Is $30 \equiv 2 \pmod{4}$.

Sol. : $30 - 2 = 28 = 4 * 7$, so $k = 7 \in Z$ and $30 \equiv 2 \pmod{4}$

2- Is $-5 \equiv 2 \pmod{7}$. (H.W.)

3- Is $3 \equiv 1 \pmod{3}$. (H.W.)

Definition(1.13): Congruence class

Let $a \in \mathbb{Z}$, then the set of all integer congruent to a modulo n is denoted by $[a]$, where

$[a] = \bar{a} = \{ x \in \mathbb{Z} : x \equiv a \pmod{n} \}$. Then $[a]$ (or \bar{a}) is called congruence class of a .

Examples(1.14):

1- If $n = 3$, then find $[1]$, $[7]$. **(H.W.)**

2- If $n = 4$, then find $[-2]$.

Sol. : $[-2] = \{ x \in \mathbb{Z} : x \equiv -2 \pmod{4} \} = \{ x \in \mathbb{Z} : x = -2 + 4k , k = 0 , \pm 1 , \pm 2 , \dots \} = \{ \dots , -10 , -6 , -2 , 2 , 6 , 10 , \dots \}$.

Definition(1.15) : Division algorithm

Let $a, b \in \mathbb{Z}$ such $b \neq 0$, then there exists $r, t \in \mathbb{Z}$ such that $a = bt + r$, $0 \leq r < |b|$.

Note :

1- The set of all congruence classes is denoted by \mathbb{Z}_n , where $\mathbb{Z}_n = \{ [0] , [1] , \dots , [n-1] \}$.

2- $(\mathbb{Z}_n , +_n)$ is group . **H.W.**

3- $(\mathbb{Z}_n - \{0\} , \times_n)$ is group if n is prime number .

Example(1.16) :

1- Show that $(\mathbb{Z}_4 , +_4)$ is a commutative group .

Some properties of group :

Theorem(1.17): If $(G , *)$ is a group , then :

1- The identity element of a group $(G , *)$ is unique .

2- The inverse element of each element of G is unique .

3- $e^{-1} = e$.

4- $(a^{-1})^{-1} = a$, for each $a \in G$.

5- $(a*b)^{-1} = b^{-1} * a^{-1}$ for each $a, b \in G$.

Proof : H.W.

Theorem(1.18):Cancellation laws

Let $(G, *)$ be a group , then for each $a, b \in G$:

1- If $a*b = a*c$, then $b = c$.

2- If $b*a = c*a$, then $b = c$.

Proof :

1- Let $a, b, c \in G$, then $a^{-1} \in G$

$a^{-1} * (a*b) = a^{-1} *(a*c)$. As $*$ is associative , so we have $(a^{-1} *a)*b = (a^{-1} *a)*c$. Thus,
 $e *b = e *c$ which implies that $b = c$.

Theorem(1.19): In a group $(G,*)$, the equations $a*x = b$ and $y *a = b$ have unique solutions .

Proof : H.W.

Theorem(1.20): Let $(G,*)$ be a group . Then :

1- $(a*b)^{-1} = a^{-1}* b^{-1}$ iff G is abelian group .

2- If $a = a^{-1}$, then G is commutative group . The converse of this part is not true in general (find example H.W.).

Proof: H.W.

Definition(1.21) : Let $(G,*)$ is a group . The power of $a \in G$, is defined by :

1- $a^k = a * a * \dots * a$ (k-times) .

2- $a^0 = e$.

3- $a^{-k} = (a^{-1})^k$, $k \in \mathbb{Z}_+$.

4- $a^{k+1} = a^k * a$, $k \in \mathbb{Z}_+$.

Examples(1.22) :

1- In $(\mathbb{R}, +)$, we have :

$$3^0=0, 3^2 = 3+3 =6, 3^{-4} = (3^{-1})^4 = (-3)^4 = -3+(-3)+(-3)+(-3) = -12 .$$

2- In (\mathbb{R}, \cdot) , we have :

$$2^0 = 1, 2^3 = 2 * 2 * 2 = 8, 2^{-4} = (2^{-1})^4 = (1/2)^4 = 1/16 .$$

Definitions(1.23) :

1- **Order of group** : The order of a finite group $(G,*)$ is the number of all its elements and we denoted by $|G|$ (or $O(G)$) .

2- **Order of element** : The order of an element $a \in G$ is the least positive integer n such that $a^n = e$, where e is the identity element of G . We denoted order of a by $|a|$ (or $O(a)$) .

Example(1.24):

If (G, \cdot) is a group , such that $G = \{ 1, -1, i, -i \}$, then $|G| = 4$. $|a| = 2$ if $a = -1$.

Homework:

1- Find order of the rest of the group's elements G above .

2- Find the order of each element of the following groups (if exists) :

$(\mathbb{Z}_6, +_6)$, $(\mathbb{Z}_8, +_8)$ and (S_3, \circ) .

II- Subgroups

Definition(2.1) : Let $(G,*)$ be a group and $A \subseteq G$, A is a non-empty subset of G . Then $(A,*)$ is a subgroup of $(G,*)$ if $(A,*)$ is itself group .

Or:

Let $(G,*)$ be a group and $A \subseteq G$, A is a non-empty subset of G . Then $(A,*)$ is a subgroup of $(G,*)$ if :

1- For each $a,b \in A$, we have $a*b \in A$.

2- $e \in A$, e is the identity element of G .

3- For each $a \in A$, there exists $a^{-1} \in A$.

Remark :Each group $(G,*)$ has at least two subgroups $(\{e\},*)$ and $(G,*)$, which are called trivial subgroups and any subgroup different from these subgroups known proper subgroup .

Examples(2.2):

1- $(Z_e, +)$ is subgroup of the group $(Z, +)$.

2- $(Q, +)$ is not subgroup of (R, \cdot) .

3- $A = \{ [0] , [2] , [4] \} \subseteq Z_6$, then $(A, +_6)$ is subgroup of Z_6 .

Theorem (2.3) :

Let $(G,*)$ be a group and $A \neq \phi$, $A \subseteq G$. Then , $(A,*)$ is a subgroup of $(G,*)$ iff $a*b^{-1} \in A$ for each $a,b \in A$.

Proof : Let $(A,*)$ is a subgroup and $a,b \in A$, then $a,b^{-1} \in A$ and so $a*b^{-1} \in A$ (by closure property) . Conversely , let $a*b^{-1} \in A$. As $A \neq \phi$, so there exists $b \in A$ which implies that $b * b^{-1} \in A$. Hence , $e \in A$. Now , since $b \in A$ and $e \in A$, so $e*b^{-1} \in A$

and then $b^{-1} \in A$. Finally, let $a \in A$ and $b^{-1} \in A$, so $a * (b^{-1})^{-1} \in A$ which implies that $a * b \in A$. Therefore, $(A, *)$ is subgroup of $(G, *)$.

Example(2.4):

Let $(Z, +)$ be a group and $A = \{5A, a \in Z\}$. Then A is subgroup of Z .

Theorem(2.5): If $(A_i, *)$ is the collection of subgroups of $(G, *)$, then $(\cap A_i, *)$ is also subgroup of G .

Proof :

1- $\cap A_i \neq \phi$, since there exists $e \in A_i$, for each i , so $e \in \cap A_i$.

2- Let $x, y \in \cap A_i$, then $x, y \in A_i$ for each i . Thus $x * y^{-1} \in A_i$ for each i (since each A_i is subgroup). Then $x * y^{-1} \in \cap A_i$ and $(\cap A_i, *)$ is subgroup of G .

Theorem (2.6): Let $(A_1, *)$ and $(A_2, *)$ are two subgroups of $(G, *)$, then $(A_1 \cup A_2, *)$ is subgroup of $(G, *)$ iff $A_1 \subseteq A_2$ or $A_2 \subseteq A_1$.

Proof: Let $A_1 \cup A_2$ is subgroup and $A_1 \not\subseteq A_2$ and $A_2 \not\subseteq A_1$. Then, there exists $a \in A_1$ and $a \notin A_2$ and $b \in A_2$, $b \notin A_1$. This implies that $a, b \in A_1 \cup A_2$ and then $a * b^{-1} \in A_1 \cup A_2$. Thus, $a * b^{-1} \in A_1$ or $a * b^{-1} \in A_2$. Now, $a, b \in A_1$ or $a, b \in A_2$ and this means that $A_1 \subseteq A_2$ or $A_2 \subseteq A_1$. Conversely, let $A_1 \subseteq A_2$ or $A_2 \subseteq A_1$. If $A_1 \subseteq A_2$, then $A_1 \cup A_2 = A_2$. If $A_2 \subseteq A_1$, then $A_1 \cup A_2 = A_1$. Therefore $(A_1 \cup A_2, *)$ is subgroup of G .

Note: $(A_1 \cup A_2, *)$ is not subgroup in general unless the condition of theorem (2.5) is satisfy. For example: Let $R^2 = R \times R$, $A = \{(a, 0) \mid a \in R\}$ and $B = \{(0, b) \mid a \in R\}$. Then, $(A, +)$ and $(B, +)$ are subgroups of $R \times R$, but $A \cup B$ is not subgroup, since $(1, 0) \in A$ and $(0, 1) \in B$, but $(1, 1) \notin A \cup B$.

Definition(2.7): Let $(G, *)$ be a group and $(A, *)$, $(B, *)$ are two subgroups of G , then the product of A and B is the set $A * B = \{ a * b : a \in A, b \in B \}$.

Theorem(2.8): Let $(G, *)$ be group and $(A, *)$, $(B, *)$ be two subgroups of G , then :

1- $A*B \neq \phi$ and $A*B \subseteq G$.

2- If $(G,*)$ is commutative group , then $(A*B,*)$ is a subgroup of G .

Proof : H.W.

Note : $A*B \neq B*A$.

Example(2.9) :

1- In $(\mathbb{Z}_8, +_8)$, let $A = \{[0], [6]\}$ and $B = \{[0],[4],[8]\}$. Then $A+B = \{[0],[4],[8],[6],[2]\}$.

2- Is $H = \{ [0], [1], [2] \}$ subgroup of $(\mathbb{Z}_4, +_4)$.

3- Is $A = \{f_1, f_2, f_3\}$ subgroup of (S_3, \circ) .

Definition (2.10): Center of the group

The center of the a group $(G,*)$ which is denoted by $C(G)$ is equal to the following set: $\{ c \in G : c*x = x*c, \forall x \in G \}$.

Note :

The set of the center of a group is always non-empty set since there exists $e \in G$ such that $a*e = e*a$ for each $a \in G$.

Example(2.11) :

1- In the group $(\mathbb{R}-\{0\}, \cdot)$, $C(\mathbb{R}) = \mathbb{R}$ (since \mathbb{R} is commutative group with multiplication) .

2- In the group (S_3, \circ) , $C(S_3) = f_1$ where f_1 is the identity element .

Theorem(2.12): Let $(G,*)$ be a group . Then $(C(G),*)$ is a subgroup of $(G,*)$.

Proof: $C(G) \neq \phi$ since $e \in C(G)$. Let $a, b \in C(G)$.

If $a \in C(G)$, so $a*x = x*a, \forall x \in G$.

If $b \in C(G)$, so $b * x = x * b, \forall x \in G$.

$$\begin{aligned} (a * b^{-1}) * x &= a * (b^{-1} * x) = a * (x^{-1} * b)^{-1} = a * (b * x^{-1})^{-1} \text{ (since } b \in C(G) \text{)} \\ &= a * (x * b^{-1}) = (a * x) * b^{-1} = (x * a) * b^{-1} \text{ (since } a \in C(G) \text{)} \\ &= x * (a * b^{-1}). \end{aligned}$$

Thus, $a * b^{-1} \in C(G)$ and $C(G)$ is subgroup of G .

Theorem(2.13): Let $(G, *)$ be a group. Then $C(G) = G$ iff G is commutative group.

Proof : H.W.

Definition(2.14) : Cyclic group

Let $(G, *)$ be a group and $a \in G$, the cyclic subgroup of G generated by a is denoted by $\langle a \rangle$ (or $\langle a \rangle$) and defined as follows : $\{ a^k : k \in \mathbb{Z} \}$ where a is called generator of $\langle a \rangle$.

Examples(2.15): In $(\mathbb{Z}_9, +_9)$. Find the cyclic subgroup generated by $[2], [3], [1]$.

$$\text{Sol. : } \langle [3] \rangle = \{ [3]^k : k \in \mathbb{Z} \} = \{ \dots, [3]^{-2}, [3]^{-1}, [3]^0, [3], [3]^2, \dots \} = \{ [0], [3], [6] \}$$

$$\langle [2] \rangle = \{ [2]^k : k \in \mathbb{Z} \} = \{ \dots, [2]^{-2}, [2]^{-1}, [2]^0, [2], [2]^2, \dots \} = \{ [0], [1], [2], [3], [4], [5], [6], [7], [8] \} = \mathbb{Z}_9.$$

$$\langle [1] \rangle = \{ [1]^k : k \in \mathbb{Z} \} = \{ \dots, [1]^{-2}, [1]^{-1}, [1]^0, [1], [1]^2, \dots \} = \{ [0], [1], [2], [3], [4], [5], [6], [7], [8] \} = \mathbb{Z}_9.$$

Homework :

1- In $(\mathbb{Z}, +)$, find cyclic group generated by $1, -1, 2$.

2- In $(\mathbb{Z}_6, +_6)$, find cyclic subgroup generated by $[5], [2]$.

Theorem(2.16) : Every cyclic group is commutative .

Proof : H.W.

Note : The converse of theorem(2.17) is not true in general , for example :

$G = (\{e, a, b, c\}, *)$ such that $a^2 = b^2 = c^2 = e$. Since $a^2 = a*a = e$, so $a = a^{-1}$. Similarly for other element of G . Thus $x = x^{-1}$, for each $x \in G$ and then G is commutative group . But G is not cyclic since :

$$\langle e \rangle = \{e\} \neq G .$$

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{e, a\} \neq G .$$

$$\langle b \rangle = \{b^k : k \in \mathbb{Z}\} = \{b, e\} \neq G .$$

$$\langle c \rangle = \{c^k : k \in \mathbb{Z}\} = \{c, e\} \neq G . \text{ Thus } G \text{ is not cyclic .}$$

Theorem(2.17) : In a group G , $\langle a \rangle = \langle a^{-1} \rangle$, $\forall a \in G$.

Proof : H.W.

Theorem (2.18) : Every subgroup of cyclic group is cyclic .

Proof : Let $(G, *)$ be cyclic group . Then there exists $a \in G$ such that $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Let $(H, *)$ be subgroup of G . Now , if $H = G$, then H is cyclic group .

If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic . If $H \neq G$ and $H \neq \{e\}$, then H is proper subgroup of G . Let $x \in H$, so $x = a^m$, $m \in \mathbb{Z}$ and $x^{-1} \in H$, then $x^{-1} = a^{-m}$, $-m \in \mathbb{Z}$.

Let m be the least positive integer such that $a^m \in H$. To prove $H = \langle a^m \rangle = \{(a^m)^g : g \in \mathbb{Z}\}$. Let $y \in H$, so $y = a^s$, $s \in \mathbb{Z}$. By division algorithm of s and m , we have $s = mg+r$, $r = s-mg$. Now, $a^r = a^s * (a^m)^{-g}$, $0 \leq r < m$. Then $a^r \in H$, but $0 \leq r < m$, so $r = 0$ and $s = mg$. Thus $a^s = (a^m)^g \in \langle a^m \rangle$ which implies that $y = a^s \in \langle a^m \rangle$ and $H \subseteq \langle a^m \rangle \dots(1)$.

Let $x \in \langle a^m \rangle$, then $x = (a^m)^g$ such that $g \in \mathbb{Z}$. $a^m \in H$, then $(a^m)^g \in H$. Thus, $x \in H$, then $\langle a^m \rangle \subseteq H \dots (2)$. From (1) and (2), we have $H = \langle a^m \rangle$ and $(H, *)$ is cyclic subgroup.

Examples (2.19):

1- Find all subgroups of $(\mathbb{Z}_{14}, +_{14})$.

$m = 1, 2, 7, 14$.

$m = 1 = \langle [1] \rangle = \mathbb{Z}_{14}$.

$m = 2 = \langle [1]^2 \rangle = \{ [0], [2], [4], [6], [8], [10], [12] \}$.

$M = 7 = \langle [1]^7 \rangle = \{ [0], [7] \}$.

$M = 14 = \langle [1]^{14} \rangle = \{ [0] \}$.

2- Find all subgroups of $(\mathbb{Z}_7, +_7)$. **H.W.**

Definition(2.20) : A positive integer c is said to be greatest common divisor of two non-zero numbers x, y iff :

1- c/x and c/y .

2- If a/x and a/y , then a/c .

Thus, $\text{g.c.d}(x, y) = c$.

Examples(2.21):

1- Find $\text{g.c.d}(12, 18) = 6$. Since $6/12$ and $6/18$.

Also $3/12$ and $3/18$ which implies that $3/6$. Finally $1/12$ and $1/18$ which implies that $1/6$.

2- Find $\text{g.c.d}(12, 24)$. **H.W.**

Note : If $(G,*)$ is finite cyclic group of order n generated by a , then the generator of G is a^k such that $\text{g.c.d}(k,n) = 1$.

Example(2.22): Find all generators of $(Z_6, +_6)$.

Sol. : $\text{g.c.d}(k,6)=1$, $k = 1,2,3,4,5$.

$\text{g.c.d}(1,6)=1$, $\text{g.c.d}(2,6)\neq 1$, $\text{g.c.d}(3,6)\neq 1$, $\text{g.c.d}(4,6)\neq 1$, $\text{g.c.d}(5,6)=1$. Thus , the generators of $Z_6 = \{[1], [5]\}$.

