كلية : التربية للعلوم الصرفة

القسم او الفرع : الرياضيات

المرحلة: الثانية

أستاذ المادة : د. فراس شاكر فندي

اسم المادة باللغة العربية: النظرية الزمر

اسم المادة باللغة الإنكليزية: Groups Theorem

اسم المحاضرة الثامنة باللغة العربية: الزمرة الدورية

اسم المحاضرة الثامنة باللغة الإنكليزية: Cyclic of group

Cyclic Groups

الزمر الدورية

Definition: Let $(G,*)$ a group and $a \in G$, the cyclic subgroup of G generated by the a is denoted $\langle a \rangle$.

$$\langle a \rangle = \{ a^n : n \in Z \} = \{ a^0, a^1, a^{-1}, \dots \}$$

Then $G = \langle a \rangle$ is called cyclic group.

$\exists a \in G$ s.t $G = \langle a \rangle$ المجموعة * تسمى الزمرة زمرة دورية اذا وجد عنصر ينتمي الى الزمرة يولد

Example: In $(Z_6, +_6)$ find the cyclic sub group generated by $\bar{2}, \bar{3}$

$$\langle \bar{2} \rangle = \{ (\bar{2})^n : n \in Z \} = \{ \bar{2}^0, (\bar{2})^1, (\bar{2})^2 \} = \{ \bar{0}, \bar{2}, \bar{4} \}$$

مضافات $\bar{2}$

$$\langle \bar{3} \rangle = \{ (\bar{3})^n : n \in Z \} = \{ (\bar{3})^0, (\bar{3})^1 \} = \{ \bar{0}, \bar{3} \}$$

مضافات $\bar{3}$

ممكن ان نأخذ المضاعفات مباشرة.

---

* If $|G| = n$ & $a \in G$ s.t $G = \langle a \rangle = \{ a^k : k \in z \}$

Then g.c.d$(n,k) = 1$

Example: Find all generators element of $(Z_8, +_8)$

Solution:- Let g.c.d$(8,k) = 1 \Rightarrow k = 1, 3, 5, 7$

① $k = 1 \Rightarrow$ g.c.d$(8,1) = 1 \Rightarrow Z_8 = \langle \bar{1} \rangle$

② $k = 3 \Rightarrow$ g.c.d$(8,3) = 1 \Rightarrow Z_8 = \langle \bar{3} \rangle$

③ $k = 5 \Rightarrow$ g.c.d$(8,5) = 1 \Rightarrow Z_8 = \langle \bar{5} \rangle$

④ $k = 7 \Rightarrow$ g.c.d$(8,7) = 1 \Rightarrow Z_8 = \langle \bar{7} \rangle$

* اذا كان العامل المشترك الأعظم بين العدد وقيمة n يساوي 1 فإن $G = \langle a \rangle$

Theorem: Every cyclic group is commutative.

proof:. Let $(G,*)$ be a cyclic group.

$\therefore \exists\, a \in G$ s.t $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

Let $x, y \in G \Rightarrow x = a^n$, $y = a^m$, $n, m \in \mathbb{Z}$

$$x * y = a^n * a^m$$
$$= a^{n+m}$$
$$= a^{m+n}$$
$$= a^m * a^n = y * x$$

$\therefore$ G is Commutative group.

G is Commutative $\not\Rightarrow$ G is cyclic

The converse is not true , for example

Let $G = \{e, a, b, c\}$ s.t $a^2 = b^2 = c^2 = e$

Then $(G,*)$ is a Commutative group.

But not cyclic group Since.

① $\langle e \rangle = \{e\} \neq G$

② $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{e, a\} \neq G$

③ $\langle b \rangle = \{b^k : k \in \mathbb{Z}\} = \{e, b\} \neq G$

④ $\langle c \rangle = \{c^k : k \in \mathbb{Z}\} = \{e, c\} \neq G$

$(G,*)$ is not cyclic.

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

* $(G,*)$ is called (klein 4-group)

Theorem: Show that $\langle a\rangle = \langle a^{-1}\rangle$, $\forall a \in G$

proof:

$$\langle a\rangle = \{a^k : k\in Z\} = \{(a^{-1})^{-k} : -k \in Z\}$$

نفرض ان $n=-k$

$$= \{(a^{-1})^n : n\in Z\}$$

$$= \langle a^{-1}\rangle$$

توضيح

$$a^k = [(a^{-1})^{-1}]^k$$

$$= (a^{-1})^{-k}$$

---

* Let $G=\langle a\rangle$ & $|G|=n \Rightarrow |a|=n$

اذا كانت G زمرة منتهية وكان $(a\in G)$ فان رتبة (a) = رتبة G .

كل زمرة جزئية من زمرة دورية تكون دورية.

Theorem: A subgroup of a cyclic group is cyclic.

proof: Let $G=\langle a\rangle$ & $H \leq G$.

① If $H=\{e\} \Rightarrow H=\langle e\rangle$

② If $H=G \Rightarrow H=\langle a\rangle$

③ If $H\neq\{e\}$ & $H\neq G$

Let n be a Least positive integer, such that $a^n \in H$

T.P $H=\langle a^n\rangle$

نفرض ان n هو اصغر عدد صحيح موجب بحيث ان $a^n \in H$

* اذا كان عدد ينتمي الى المجموعة فانه اي قوة ترفع لهذا العدد تكون ايضا ينتمي للمجموعة

Let $x\in H \Rightarrow x\in G \Rightarrow x=a^k$, $k\in Z$

$\therefore k,n\in Z \Rightarrow \exists\ r,q\in Z$ s.t

$k = nq+r$ $\quad 0\leq r<n$

$r = k-nq$

$\therefore a^n, a^k \in H$

$$a^r = a^{k-nq} = a^k * (a^n)^{-q} \in H$$

($a^k \in H$, $(a^n)^{-q} \in H$)

$a^r \in H \Rightarrow r=0$

نقسم k على n و يجب ان نثبت ان k هو احد مضاعفات n لكي يكون a^k ينتمي الى $\langle a^n\rangle$ اي نثبت $r=0$

$$\begin{array}{r|l} n & k \\ -nq & q \\ \hline r & \end{array}$$

r الباقي

* لماذا $r=0$ لأن n هو اصغر عدد صحيح موجب بحيث $a^n \in H$ وبما ان $a^r \in H$ وان $r<n$ لذلك يجب ان تكون $r=0$

$\Rightarrow k-nq=0 \Rightarrow k=nq$ (n هو العدد مضافات k)

$\therefore a^k = a^{nq} = (a^n)^q \in \langle a^n \rangle$

$\therefore x \in \langle a^n \rangle$

$H \subseteq \langle a^n \rangle$ —①

$\Leftarrow$ Let $y \in \langle a^n \rangle \Rightarrow y = (a^n)^m$, for some $m \in Z$

$\therefore a^n \in H \Rightarrow (a^n)^m \in H \Rightarrow y \in H$

$\langle a^n \rangle \subseteq H$ —②

$\therefore H = \langle a^n \rangle$

= =

* كل زمرة دورية منتهية ورتبتها عدد اولي تكون هذه الزمرة لا تمتلك زمرة جزئية فعلية ((proper))

H is proper $\Rightarrow H \neq \{e\}$ & $H \neq G$.

= =

* اذا كانت $H=G$ & $H=\{e\}$ تسمى الزمر الجزئية التافهة trivil Subgroup

* اذا كانت $H \neq G$ & $H \neq \{e\}$ وكانت $H \leq G$ فتسمى H زمرة جزئية فعلية proper Subgroup

= =

Theorem: Every group of prime order is cyclic and hence is abelian.

Proof: Let $|G|=p$ (prime number) & $a \in G$, $a \neq e$

اي عنصر ينتمي للمجموعة فإن مولد العنصر زمرة جزئية من المجموعة.

$\therefore \langle a \rangle \leq G$

$\therefore |\langle a \rangle| \mid |G|$ (by Lagrange theorem)

اي عدد اولي يقبل القسمة على نفسه وعلى واحد في اذا كان عدد موجب

But p is prime number

$\therefore |\langle a \rangle| = 1$ or p

① If $|\langle a \rangle|=1 \Rightarrow \langle a \rangle=\{e\} \Rightarrow a=e$ c! (تناقض لأن $a \neq e$ بالفرض)

② If $|\langle a \rangle|=p \Rightarrow |\langle a \rangle|=|G| \Rightarrow G=\langle a \rangle$

$\therefore G$ is cyclic $\Rightarrow G$ is abelian.

Theorem: Let $G=\langle a \rangle$ be a finite group with $O(G)=n$,

$G=\{e, a, a^2, \ldots, a^{n-1}\}$

اذا كانت $G=\langle a \rangle$ زمرة منتهية بحيث عدد عناصرها يساوي n فيكون شكل كل عنصر كما هو موضع في المجموعة

Corollary:

① Let $G=\langle a \rangle$ s.t. $|G|=n$, then n the smallest positive integer such that $a^n=e$

اذا كانت $G=\langle a \rangle$ بحيث ان $|G|=n$ ، فإن n هو اصغر عدد صحيح يحقق العلاقة $a^n=e$

Theorem: Every group of order less than 6 (< 6) is abelian.

Proof: Let $|G| < 6$ T.P G is ablian.

If $|G|=1 \Rightarrow G=\{e\} \Rightarrow$ G is abelian.

If $|G|=2,3,5 \Rightarrow$ G is abelian. ($|G|=p$ is prime)

If $|G|=4$

(a) If G is cyclic $\Rightarrow$ G is abelian.

(b) If G is not cyclic $\Rightarrow$

$\forall\, a \neq e \in G$ then $a^2=e$

$\Rightarrow$ G is abelian.

Exercises (2):

(1) Find all subgroups of $(Z_5, +_5)$.

(2) Let $(Z_8, +_8)$ be a group and $H = \langle \bar{2} \rangle$. Is H a subgroup of Z_8?

(3) If $H = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}\}$, show that $(H, +_{24})$ is a cyclic subgroup of $(Z_{24}, +_{24})$. Also list the elements of each coset of H in Z_{24}.