نظري

◄ دكتور المادة : حمزة الحاكمي

◄ المحاضرة : العاشرة ◄ عنوان المحاضرة : الزمر الدوارة

المستوى العلمي : أهلاً بكم أصدقائي سندرس في هذه المحاضرة :

١ـ سنتابع في الزمرة الدوارة ومبرهنات عنها.

٢ـ نتعرّف على بعض الزمر الجزئية في الزمرة الدوارة.

٣ـ شروط لأجلها تكون الزمرة المولدة بعنصرين دوارة.

مبرهنة: ((هذه المبرهنة تعطينا الشرط الازم والكافي كي تكون عناصر الزمرة الدوارة المنتهية مولدات لها))

النص : لتكن $G =< a >$ زمرة دوارة منتهية مرتبتها n حيث $a \in G$ ان الشروط الاتية متكافئة :

١) $k \epsilon Z; G =< a^k >$

٢) $\gcd(k,n) = 1$

الاثبات :

(1 ← 2) لنفرض أن $G =< a^k >$ حيث $k \in Z$ ولنفرض جدلا أن $\gcd(k,n) = d > 1$ عندئذ يوجد $s,t \epsilon Z$ حيث : $k = t.d$ و $n = s.d$ ومنه:

$$(a^s)^k = (a^s)^{td} = (a^{sd})^t = (a^n)^t = e$$

ومنه : $0 \leq S < n$: $(a^k)^s = e$

((قيم S لاتصل الى n . إذاً لن نحصل على جميع العناصر ،نصل الى جزء فقط)).

وهذا يناقض كون $G =< a^k >$ وبالتالي $\gcd(k,n) = 1$

(1 ← 2) لنفرض أن $\gcd(k,n) = 1$ عندئذ يوجد $\alpha, \beta \epsilon Z$ بحيث:

$1 = \alpha.n + \beta.k$ (α يعني الفا)

$$a^1 = a^{\beta.k+\alpha.n} = a^{\beta.k}.a^{\alpha.n} = (a^n)^{\alpha}.(a^k)^{\beta}$$
$$= e(a^k)^{\beta} = (a^k)^{\beta} \epsilon < a^k >$$

اصغر زمرة جزئية تحوي a $a \in < a^k >$ و $a \in < a >$

$$\Rightarrow G =< a > \subseteq < a^k > \subseteq G \Rightarrow \quad G =< a^k >$$

نتيجة: لنفرض ان $n \geq 1$ عدد صحيح وليكن $k \in Z_n$ عندئذٍ(الزمرة Z_n مولدة بالعنصر k)

$$\gcd(k,n) = 1 \Leftrightarrow Z_n =< k >$$

مثال:

$$Z_8 = \{0,1,2,3,4,5,6,7\}$$

$$Z_8 < 1 > =< -1 > =< 7 >$$

$$Z =< 5 > =< 3 >$$

مبرهنة : كل زمرة جزئية من زمرة دوارة تكون أيضا دوارة .

البرهان:

لتكن $G =< a >$ زمرة دوارة حيث $a \in G$ لتكن H زمرة جزئية في G:

١. $H = \{e\} \Leftarrow H =< e >$ ومنه H دوارة.(طالما المحايد بحد ذاته يؤلف زمرة جزئية عندها تكون $H =< e >$

٢. $H \neq \{e\}$ عندئذٍ يوجد $x \in H$ ومنه $x = a^s \in H$ حيث $s \in Z$ و $s \neq 0$

لنأخذ المجموعة ℓ: $\ell = \{k \ , k \epsilon N^* : \ a^k \epsilon H \}$

إن $\ell \neq 0$ لان $s \in \ell \Leftarrow \ell$ تحوي عنصر اصغر وليكن m ان $a^m \in H$ وبالتالي:

$$< a^m > \subseteq H \ldots (1)$$

((لنثبت الاحتواء المعاكس))

ليكن $y \epsilon H$ عندئذٍ $y = a^k$ حيث $k \epsilon Z$ وحسب خوارزمية القسمة فإنه

$$k = qm + r \text{ حيث } 0 \leq r < m$$

لنفرض جدلا أن $r \neq 0$ عندئذ $0 < r < m$

$$a^k = a^{qm+r} = a^{qm}.a^r \quad \underset{\text{ولنضرب من اليسار ب } a^{-q}}{\Rightarrow} \quad a^r = a^{-qm}.a^k \in H$$

ومنه وجدنا عنصر لأجله $a^r \in H$ وأن $r \in \ell$ و $r < m$ وهذا يناقض كون m هو العنصر الأصغرفي ℓ

ومنه نجد ان $r = 0$ وبالتالي: $y = a^k = a^{qm} = (a^m)^q \in < a^m >$

$$\Rightarrow H \subseteq < a^m > \cdots (2)$$

ومن الإحتوائين 1 و 2 نجد ان $H =< a^m >$ زمرة مولدة بالعنصر a^m حيث m اصغر عدد صحيح موجب يحقق

$$a^m \in H$$

بعض الزمر الجزئية في الزمرة الدوارة

مبرهنة: لتكن $G =< a >$ زمرة دوارة منتهية مرتبتها n حيث $a \in G$ وليكن $k \in Z$ قاسم للعدد n

عندئذ يوجد في G زمرة جزئية واحدة فقط مرتبتها k وهي المولدة بالعنصر $< a^{\frac{n}{k}} >$.

((ان $k > 0$ لان المرتبة لايمكن ان تكون سالبة))

البرهان:

بما ان الزمرة الدوارة مرتبتها n فإن العنصر المولّد لها مرتبته n أي ان $0 < a >= n$

و $0\left(a^{\frac{n}{k}}\right) = k$ ومنه فإن $< a^{\frac{n}{k}} >$ زمرة دوارة مرتبتها k

((لنثبت انها وحيدة))

لتكن H زمرة جزئية في G مرتبتها k وحسب المبرهنة السابقة فإن $H =< a^m >$

حيث $m \in Z$ اصغر عدد صحيح موجب لأجله $a^m \in H$

$$k = (H:1) = (< a^m >:1) = 0(a^m) = \frac{n}{m} \Rightarrow m = \frac{n}{k}$$

ومنه فإن : $< a^{\frac{n}{k}} >=< a^m >= H$ فهي وحيدة.

- ان عملية الجمع بالمقاس n . (Z_n) جميعها دوارة.
- اما عملية الضرب بالمقاسn . $(U(n))$ جزء منها فقط.
- **مبرهنة : كل زمرة منتهية مرتبتها عدد أولي تكون دوارة .**

الإثبات :

- لنفرض أن G زمرة منتهية مرتبتها P حيث P عدد أولي ((ان هذه الزمرة تحوي على الأقل عنصرين))

$$\exists a \in G : a \neq e$$

- إن $G =< a >$ (a يولد زمرة جزئية فيG) وحسب لاغرانج فإن مرتبة الزمرة $< a >$ تقسم مرتبة الزمرة $(G:1) = p$

(حيث $1, p$ قواسم ال p) $(< a >:1) \in \{1, p\}$

١) $(< a >:1) = 1 \Rightarrow 0(a) = 1 \Rightarrow a = e$ مرفوض

٢) $(< a >:1) = p \Longrightarrow G =< a >$

مجموعتين منتهيتين لهما نفس كمية العناصر وكل مجموعة محتواه بالآخر يكونان متساويان

ومنه G تكون $G =< a >$

تمهيدية: لتكن G زمرة منتهية مرتبتها n **عندئذٍ**

١) $\forall a \in G \ ; \ a^n = e$

٢) $\forall a \in G \ ;$ **n** يقسم $\mathbf{0}(a)$

البرهان:

١- ليكن $a \in G$ **عندئذٍ** $< a >$ زمرة جزئية في G منتهية ولنفرض ان مرتبة الزمرة $< a >$ هي k

$$(< a >: 1) = k$$

عندئذٍ: k يقسم n ومنه: $n = k.t : t \in Z$

$$a^n = a^{kt} = (a^k)^t = e \quad : \quad 0(a) = k \text{ إن}$$

٢- ليكن $a \in G$ عندئذٍ $< a >$ زمرة جزئية في G ومرتبتها من مرتبة العنصر المولد a

$(< a >: 1) = 0(a)$ وحسب لاغرانج فإن $< a >$ تقسم مرتبة G ومنه تم المطلوب

مبرهنة: لتكن G زمرة و $a, b \in G$ وأن $0(a) = n \ , \ 0(b) = m$

لنفرض ان $a.b = b.a$ وان $< a > \cap < b > = < e >$

عندئذ $0(a.b) = Icm(n,m)$))) $Icm(n,m)$ هو المضاعف المشترك الأصغر للعددين (n,m)

البرهان:

لنفرض ان

$$k = Icm(n,m)$$

$$\Rightarrow \ k = s.n \quad , \quad k = t.m \quad \text{بحيث } s,t \in Z$$

$$(a.b)^k = a^k.b^k$$

تنبيه: $(a.b)^2 = a.b.ab = a.a.b.b = a^2.b^2)$

لان $a.b = b.a$

$$a^k.b^k = a^{sn}.b^{tm} = (a^n)^s.(b^m)^t = e$$

ومنه $k \geq 0(a.b)$ لنفرض ان $\lambda = 0(a.b)$

$$\Longrightarrow k \geq \lambda$$

$$\Longrightarrow (a.b)^{\lambda} = e \Longrightarrow a^{\lambda}.b^{\lambda} = e$$

نضرب من اليمين بمقلوب a^{λ}

$$a^{\lambda}.b^{\lambda}a^{-\lambda} = e.a^{-\lambda} \Longrightarrow b^{\lambda} = a^{-\lambda} \Longrightarrow a^{\lambda} = b^{-\lambda}$$

$$b^{-\lambda} \in < a > \cap < b > = < e >$$

وبالتالي $\begin{cases} \lambda \text{ يقسم } n \\ \lambda \text{ يقسم } m \end{cases} \Leftarrow \lambda \geq k$ ومنه: $k = \lambda \Leftarrow 0(a.b) = Icm(n,m)$

تمرين: لتكن G زمرة و $a,b \in G$ وأن $0(a) = n \ , \ 0(b) = m$

و $a.b = b.a$ و $\gcd(n,m) = 1$ عندئذ :

$$< a > \cap < b > = < e >$$

$$0(a.b) = 0(a).0(b)$$

الحل :

ليكن $x \in < a > \cap < b >$ ولنفرض أن $0(x) = \lambda$

عندئذٍ:

$$x \in < a > ; x^{n} = e$$

$$x \in < b > ; x^{m} = e$$

ومنه فإن λ يقسم كلاً من n,m وحسب الفرض $\lambda = 1$ ((القاسم)) ومنه:

$$x^{\lambda} = e \Rightarrow x = e$$

ومنه فإن: $\Longrightarrow < a > \cap < b > = < e >$

$$0(a.b) = Icm(n,m) = n.m$$

وحسب المبرهنة السابقة نجد: $0(a.b) = 0(a).0(b)$

تمرين: لتكن G زمرة و $a,b \in G$ بحيث $0(b)=m \quad , \quad 0(a)=n$ وان $\gcd(n,m)=1$

وبفرض $a.b=b.a$ عندئذ: $< a.b >=< a,b >$.

الحل :

لدينا $a,b \in < a,b >$ ومنه $a.b \in < a,b >$ ومنه فإن $< a.b > \subseteq < a,b >$

((لنثبت الاحتواء المعاكس))

لما كان $\gcd(n,m)=1$ فإن $1 = sn+tm : s,t \in Z$

$$a = a^{sn+tm} = a^{n.s}.a^{t.m} = \underbrace{(a^n)}_{=e}^{s}.(a^m)^t = e.a^{mt} = a^{mt} = a^{tm}\underbrace{(b^m)^t}_{=e}$$

$$a^{tm}.b^{tm} = (a.b)^{tm} \in < a.b >$$

بنفس الطريقة نثبت ان $b \in < a.b >$ ومنه نجد ان

$$< a,b > \subseteq < a.b >$$

$$\Rightarrow < a.b > = < a,b >$$

وعناصرها هي : $0 \le k < n,m \ : \ (a.b)^k = a^k.b^k$

وظيفة: لتكن $n=2, m=3$ اوجد هذه العناصر

$$< a.b > = \left\{ a^i b^j \quad \begin{matrix} 0 \le i < n \\ \\ 0 \le j < m \end{matrix} \right.$$

لنثبت ان $j=0$ ولنأخذ $i=0,1$

$$a^0 b^0 = e$$
$$a^1 b^0 = a$$

لنثبت ان $j=1$ ولنأخذ $i=0,1$

$$a^0 b^1 = b$$
$$a^1 b^1 = a.b$$

لنثبت ان $j=2$ ولنأخذ $i=0,1$

$$a^0 b^2 = b.b = b^2$$
$$a^1 b^2 = a.b^2$$

وبالتالي $< a.b > \{e, a, b, a.b, b^2, ab^2\}$

انتهت المحاضرة

إعداد: ناريمان جلو – ولاء الأخضر – هلا هيج