نظري

◄ دكتور المادة: حمزة الحاكمي

◄ المحاضرة: الثانية عشر ◄ عنوان المحاضرة: الزمرة الدوارة

المحتوى العلمي : أهلاً بكم أصدقائي سندرس في هذه المحاضرة :

- ❖ مبرهنات
- ❖ تعاريف
- ❖ أمثلة

تذكرة: إذا كان $a \in G \quad ; \quad < a > = \{a^n \quad : n \in \mathbb{Z}\}$

تعريف الزمر الدوارة: نقول عن الزمرة G إنها دوارة اذا وجد $a \in G$ بحيث $G =< a >$

$$G =< a >= \{a^n \; : \; n \in Z \quad ; \quad a \in G\}$$

ـ زمرة دوارة أي مولدة لعنصر وحيد من خلال معرفتي لهذا العنصر يمكن معرفة كل عناصر الزمرة .

مثال : زمرة الأعداد الصحيحة هي زمرة دوارة مولدة بالعنصر 1 أي أن :

$$n \in \mathbb{Z} \quad ; \quad n = n.1 \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n \text{ مرة}} & : n > 0 \\ 0 = 0.1 & : n = 0 \\ (-1) + (-1) + \cdots + (-1) & : n < 0 \end{cases}$$

يمكن كتابة العلاقة الأخيرة بالشكل $(-n)(1)n$ مرة ..

مثلاً : $U(10) = \{ 1 , 3 , 7 , 9\}$

$$3^0 = 1 \quad , \quad 3^1 = 3 \quad , \quad 3^2 = 9 \quad , 3^3 = 7$$

$$U(10) = \{3^0 , 3^1 , 3^2 , 3^3\} =< 3 >$$

وأيضا $U(10) = \{7^0 , 7^1 , 7^2 , 7^3\} =< 7 >$

وهذا يبين لنا أن كلا من $3 , 7$ هي مولدات للزمرة $U(10)$ وبالتالي فإن الزمرة $U(10)$ هي زمرة دوارة ..

في الزمرة $U(8) = \{1,3,5,7\}$ نجد ان :

$$< 7 >= \{1,7\} \quad , < 5 > = \{1,5\} \quad , < 3 > = \{1,3\} \quad , < 1 > = \{1\}$$

وهكذا فإن $U(10) \neq a$ وذلك أيا كان $a \in U(8)$ وبالتالي $U(8)$ ليست دوارة ..

وهكذا نرى أن $U(n)$ ليست دوارة في الحالة العامة .

" إذا كانت الزمرة تحوي أكثر من مولد لا يمكن أن يكون المحايد مولد "

كيف نحصل على زمرة دوارة ؟؟ يمكن ان نحصل عليها في الحالة العامة من خلال التمهيدية التالية :

تمهيدية: لتكن G زمرة و S مجموعة جزئية وغير خالية في G فإن القضايا التالية صحيحة :

١) تقاطع جميع الزمر الجزئية في G التي كل منها يحوي S هو زمرة جزئية في G تحوي S نرمز لها $< S >$ وتسمى الزمرة الجزئية المولدة.
٢) الزمرة الجزئية $< S >$ هي أصغر زمرة جزئية في G تحوي S .
٣) إن $< S >$ هي عنصر أصغري في مجموعة كل الزمر الجزئية في G التي كل منها يحوي S .

الاثبات :((وظيفة))

لنفرض أن l هو مجموعة كل الزمر الجزئية في G والتي كل منها تحوي S

$$l : \{H : G \text{ زمرة جزئية في } H \quad S \subseteq H \}$$

إن $G \epsilon l$ ومنه $l \neq \emptyset$

١) وجدنا سابقا أن $\cap_{H\epsilon l} H$ هو زمرة جزئية في G وبما أن :

$$S \subseteq H \; ; \forall H \epsilon l$$

$$S \subseteq \cap_{H\epsilon l} H =< S >$$

٢) لتكن k زمرة جزئية في G تحوي S عندئذ $k \epsilon l$ ولنبرهن أن $< S > =< S > \subseteq k$ $\cap_{H\epsilon l} H \subseteq kk$ (هي إحدى مكونات التقاطع ومن ثم فهي تحوي التقاطع) .
٣) ينتج من (٢) وكون $< S > \epsilon l$ أي هي أصغر عناصر l .

تمهيدية : لتكن G زمرة و $a \epsilon G$ عندئذ $< a^{-1} > =< a >$

الاثبات :

الاحتواء الأول : لدينا $< a >$ زمرة وإن $a \epsilon < a >$ وأيضا $a^{-1} \in < a >$

ومنه $a = (a)^{-1} \in < a^{-1} >$ و $< a^{-1} > \subseteq < a >$

الاحتواء الثاني : لدينا $< a^{-1} >$ زمرة وأن $a^{-1} \in < a^{-1} >$ وأيضا $a \in < a >$

ومنه $a^{-1} \in < a >$ و $< a > \subseteq < a^{-1} >$ نجد أن $< a > = < a^{-1} >$

نتيجة: كل زمرة دوارة تكون تبديلية.

البرهان :

لتكن $G = < a >$ زمرة دوارة حيث $a \in G$ ليكن $x, y \in G$

$$x = a^n \quad , \quad y = a^m \qquad : n, m \in Z$$

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

$$= a^m . a^n = y . x$$

تمهيدية: لتكن $G = < a >$ زمرة دوارة مولدة بالعنصر حيث $a \epsilon G$ أي عندئذ :

العلاقة $\varphi : \mathbb{Z} \longrightarrow G$ المعرفة بالشكل التالي :

$\forall\, n \epsilon \mathbb{Z} \; ; \varphi(n) = a^n \epsilon G$ هي تطبيق غامر دوماً .

الاثبات : ((وظيفة))

$$\forall n, m \in Z \;\; : \;\; n = m$$

$\varphi(n) = a^n = a^m = \varphi(m)$ فهو تطبيق

أياً كان $y \epsilon G$ فإن: $y = a^t$ حيث $t \in Z$

$\varphi(t) = a^t = y$ إذاً هو تطبيق غامر.

مبرهنة: لتكن $G = < a >$ زمرة دوارة حيث $a \epsilon G$ عندئذ الشروط الاتية متكافئة :

١) التطبيق φ متباين .

٢) $\forall\, n, m \epsilon Z \;\; ; \;\; n \neq m \implies a^n \neq a^m$

٣) $\forall\, n, m \epsilon Z \;\; ; \; a^n = a^m \implies n = m$

٤) الزمرة G غير منتهية

الاثبات :

$1 \longrightarrow 2)$ليكن $n, m \in \mathbb{Z}$ بحيث $n \neq m$ ولنفرض جدلا ان $a^n = a^m$ عندئذ يكون= $\varphi(m)$ $\varphi(n)$ ولكون φ تطبيق متباين ينتج أن $n = m$ وهذا يناقض الفرض إذا $a^n \neq a^m$ ..

$2 \longrightarrow 3)$ليكن $n\,, m\ \in \mathbb{Z}$ بحيث $a^n = a^m$ نفرض أن $n \neq m$ ومنه حسب (2) فإن $n \neq m \Longrightarrow a^n \neq a^m$ وهذا يناقض الفرض إذا $n = m$..

$3 \longrightarrow 4)$إن الشرط (3) يبين لنا أن التطبيق φ متباين ولكونه غامر نجد ان φ تقابل وبالتالي تكون $card\ \mathbb{Z} = card\ G$ وهذا يبين لنا أن الزمرة G غير منتهية ..

$4 \longrightarrow 1)$لنفرض أن G غير منتهية والمطلوب إثبات أن التطبيق φ متباين

لنفرض جدلا أن التطبيق φ غير متباين عندئذٍ يوجد $n, m \in Z$بحيث $\varphi(n) = \varphi(m)$

وان $a^n = a^m \Longleftarrow n \neq m$(*)

لنفرض أن $n > m$ عندئذ $n - m > 0$أي ان $n - m \in N^*$

نضرب (*) ب a^{-m}:

$$a^{n-m} = e$$

لنأخذ المجموعة

$$\ell = \{t \ \ : t \in N^* \ , \qquad a^t = e\}$$

$$\emptyset \neq \ell \subset N \quad \text{لان} \ n - m \in \ell$$

ومنه يوجد في ℓ عنصر اصغر وليكن $a^k = e$بحيث $K \in N^*$

لدينا :

$$\{e, a, a^2, \dots \dots \dots, a^{k-1}\} \subseteq G$$

ولنثبت الان الاحتواء المعاكس أي : $G = \{e\,, a\,, \dots, a^{k-1}\}$

ليكن $x \in G$ عندئذ $m \in Z$: $x = a^m$ وحسب خوارزمية القسمة لأجل K, m يوجد $q, r \in Z$ بحيث $0 \leq r < K$ و $m = qK + r$ومنه $x = a^m = a^{qK+r} = a^{qK}.a^r = (a^k)^q\,.a^r$

$x = a^m \in \{e,\ a\ \ \dots, a^{k-1}\}$ وهذا يبين أن $G \ \subseteq \{e, a, a^2, \dots \dots \dots, a^{k-1}\}$

ومنه

$$G = \{e, a, a^2, \dots \dots \dots, a^{k-1}\}$$

وبالتالي G منتهية وهذا يناقض الفرض ومنه التطبيق φ متباين ..

- **نتيجة :** كل الزمر الدوارة غير المنتهية تكون قابلة للعد .
- الشرط اللازم والكافي كي تكون الزمرة الدوارة منتهية هو أن تكون جميع القوى لعنصر المولد مختلفة مثنى مثنى ..
- المبرهنة الأخيرة بينت لنا متى تكون الزمرة الدوارة غير منهية والمبرهنة الآتية تبين لنا متى تكون الزمرة الدوارة منتهية ..

مبرهنة : لتكن G زمرة دوارة مولدة بالعنصر $a \in G$ أي أن $G =< a >$ فإن القضايا التالية متكافئة

١) التطبيق φ غير متباين

٢) يوجد في $Z \epsilon n, m$ بحيث $a^n = a^m$ وأن $n \neq m$.

٣) يوجد في $k \epsilon N^*$ بحيث :

$$G = \{e, a, a^2, \dots \dots \dots, a^{k-1}\}$$

وأن هذه العناصر مختلفة مثنى مثنى .

الاثبات :

$(1 \longrightarrow 2)$ لنفرض أن التطبيق φ غير متباين عندئذ يوجد $m\,, n \in \mathbb{Z}$ حيث $\varphi(n) = \varphi(m)$ وإن $n \neq m$ ومنه حسب تعريف φ يوجد $a^n = a^m$ أن $m \neq n$

$(2 \longrightarrow 3)$ ليكن $n, m \epsilon Z$ بحيث $n \neq m$ و $a^n = a^m$ عندئذٍ: $n > m$ ومنه $n - m > 0$

ولو ضربنا $a^n = a^m$ ب a^{-m}:

$$a^{n-m} = e$$

لنأخذ المجموعة $l = \{t : t \in \mathbb{Z} \ : \ a^t = e \}$

$\emptyset \neq l \subseteq N^*$ لان $n - m \in l$ ومنه l يحوي عنصر أصغري وليكن k إن

$$G = \{e\,, a\,, a^2, \dots, a^{k-1}\}$$

جميع العناصر مختلفة مثنى مثنى

ليكن $x\,, y \in G$ بحيث $x = y$ حيث $y = a^j$, $x = a^i$ وأن $i \neq j$ لنفرض أن $i > j$

عندئذ $i - j > 0$

إذا $a^i = a^j$ وبالتالي $a^{i-j} = e$ وبالتالي فإن $i - j \in l$

وهذا يناقض كون k عنصر أصغر في المجموعة l .. وبالتالي فإن عناصر المجموعة

$\{e\ ,a\ ,\ldots.,a^{k-1}\}$ مخلفة مثنى مثنى

$(3 \longleftarrow 1)$واضح

تعريف: ليكن G زمرة و $a \in G$ نسمي أصغر عدد صحيح موجب n يحقق $a^n = e$ مرتبة العنصر a ونرمز له $0(a) = n$ وهذا في الحالة العامة ، واذا كان $\forall m \in N^*$ $a^m \neq e$

نقول ان للعنصر aمرتبة لانهائية ونرمز لذلك $0(a) = \infty$.

مثال: لنأخذ الزمرة $U(15) = \{1,2,4,7,8,11,13,14\}$

بالنسبة إلى عملية الضرب بالمقاس 15

$0(7) = 4$ $\quad$ $0(4) = 2$ $\quad$ $0(2) = 4$ $\quad$ $0(1) = 1$

$0(14) = 2$ $\quad$ $0(13) = 4$ $\quad$ $0(11) = 2$ $\quad$ $0(8) = 4$

نلاحظ أنه $U(15) \neq < a >$; $\forall a \in U(15)$

إذا $U(15)$ ليست دوارة ..

مثال: لنأخذ الزمرة $Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$

بالنسبة إلى عملية الجمع بالمقاس 10

لإيجاد مرتبة العنصر 2 نقوم بحساب متتالية العناصر $2\ ,2.2\ ,2.3\ , \ldots ..$ فنجد :

$2.5 = 0$ $\quad$ $2.4 = 8$ $\quad$ $2.3 = 6$ $\quad$ $2.2 = 4$ $\quad$ $2.1 = 2$

ومنه تكون $0(2) = 5$ بطريقة مشابهة نجد :

$0(6) = 5$ $\quad$ $0(5) = 2$ $\quad$ $0(7) = 10$ $\quad$ $0(0) = 1$

" لإيجاد مرتبة العنصر g من الزمرة G يكفي حساب متتالية الجداءات $g\ ,\ g^2 m$ حتى نصل إلى عنصر الوحدة للزمرة G لأول مرة ، ويكون في هذه الحالة الأس مساويا مرتبة العنصر g وإذا لم نحصل على عنصر الوحدة عندئذ يكون العنصر g ذا مرتبة غير منتهية "

سندرس خواص المرتبة من خلال المبرهنة الآتية :

تمهيدية : لتكن G زمرة و $a \in G$ مرتبته n $0(a) = n$عندئذ :

١) $0(a^{-1}) = n$: $0(a^{-1}) = 0(a)$

٢) $0(a^s) = 0(a^{n-s})$ فإن $\forall s \in Z : 1 \leq s \leq n$

٣) إذا كان $k \in Z$ يحقق $a^k = e$ فإن n يقسم k.

٤) لأجل أي عدد صحيح موجب t يقسم n فإن $0\left(a^{\frac{n}{t}}\right) = t$

٥) اذا كان $G =< a >$ فإن $(G:1) = 0 < a >= n$

الاثبات :

١) لدينا $e = a^n$ ومنه $e = a^{-n}$ ومنه

$e = (a^{-1})^n$ ليكن t عدد صحيح موجب بحيث $e = (a^{-1})^t$ عندئذ $e = a^{-t}$

ومنه $a^t = e$ ولما كانت $0(a) = n$ نجد أن $n \leq t$ وبالتالي فإن $0(a^{-1}) = n$

٢) ليكن sعدد صحيح بحيث $1 \leq s < n$ عندئذ $n - s > 0$

$$e = a^n = a^{n-s}.a^s$$

$$a^{n-s} = a^{-s}$$

$$0(a^s) = 0(a^{-s}) = 0(a^{n-s})$$

٣) ليكن $k \in Z$ بحيث $a^k = e$وحسب خوارزمية القسمة لأجل n,k نجد أن

$$k = qn + r \qquad q,r \in Z$$

بحيث $0 \leq r < n$

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

$$a^k = (a^n)^q a^r$$

ومنه $a^r = e$ وهذا يناقض كون $0(a) = n$ ومنه $r = 0$ وبالتالي $k = qn$.

٤) ليكن $t > 0$ وأن t يقسم nعندئذ :

$$\frac{n}{t} \leq n : \quad (a^{\frac{n}{t}})^t = a^{\frac{n.t}{t}} = a^n = e$$

ولنفرض ان $k < t$ عدد صحيح موجب يحقق $\left(a^{\frac{n}{t}}\right)^k = e$ عندئذٍ : $\left(a^{\frac{n.k}{t}}\right) = e$

وحسب (3) فإن n يقسم $\frac{nk}{t}$ وبالتالي $\frac{nk}{t} = \alpha.n$

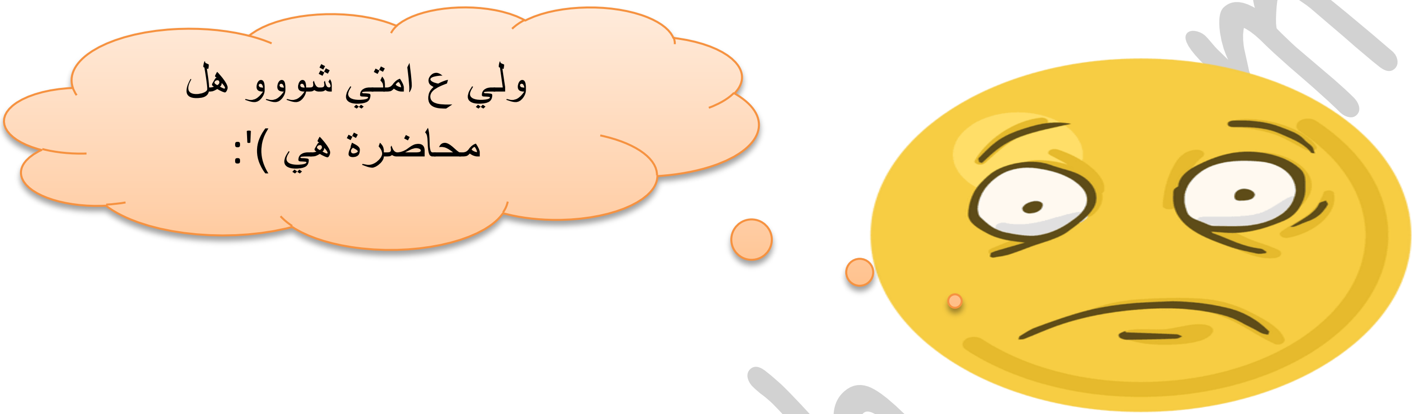
$$\Leftarrow \quad \frac{k}{t} = \alpha \quad \Leftarrow \quad k = t.\alpha \quad \Leftarrow \quad k \geq t \quad \Leftarrow \quad k = t$$

٥) لنفرض أن $G =< a >$ وأن $(G:1) = m$ حسب مبرهنة سابقة فإن :

$$G = \{e, a, a^2 \dots \dots a^{m-1}\}$$

وحيث إن m هو أصغر عدد صحيح موجب من أجله $a^m = e$ وهذا يبين أن :

$$G = \{e, a, a^2 \dots \dots a^{m-1}\}$$



انتهت المحاضرة

إعداد: رهف دادا – آية اليافي – آية بسيكي

تنسيق: ولاء الأخضر