نظري

◄ دكتور المادة : حمزة الحاكمي

◄ المحاضرة : التاسعة ◄ عنوان المحاضرة : الزمر الدوارة

المحتوى العلمي : أهلاً بكم أصدقائي سندرس في هذه المحاضرة :

١ـتعريف الزمر الدوارة.

٢ـ مبرهنات على الزمر الدوارة.

٣ـ تعريف مرتبة عنصر.

٤ـ مبرهنة تتضمن دراسة بعض خواص مرتبة العنصر.

الزمر الدوارة

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 $G \in l$ ومنه $l \neq \emptyset$

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

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

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

٢) لتكن k زمرة جزئية في G تحوي S عندئذ $k \in l$ ولنبرهن أن $< S > = < S > \subseteq k$

$\cap_{H\in l} H \subseteq k$ (k هي إحدى مكونات التقاطع ومن ثم فهي تحوي التقاطع) .

٣) ينتج من (٢) وكون $< S > \in l$ أي هي أصغر عناصر l .

تعريف: لتكن G زمرة و S مجموعة جزئية وغير خالية في G.

١. اذا كانت S منتهية نقول $< S >$ منتهية التوليد.
٢. اذا كانت S غير منتهية نقول ان $< S >$ غير منتهية التوليد.
٣. اذا كانت $s = \{a\}$ فإن $< s > = < a > = \{a^n : n \in Z\}$

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

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

توضيح: اذا وجد عنصر في الزمرة يولد هذه الزمرة فحسب التعريف هي اصغر زمرة جزئية في G تحوي S .

- يعود سبب التسمية لإمكانية الحصول على عناصر الزمرة G من العنصر a

أي: تكون الزمرة دوارة اذا وجد فيها عنصر من خلاله نستطيع تحديد جميع العناصر الأخرى.

مثال : هل الزمرة U_{10} زمرة دوارة ؟

$$U_{10} = \{1,3,7,9\}$$
$$3 \in U(10)$$
$$e^0 = 1 \quad , \quad e^1 = 1 \quad , \quad e^2 = 1$$

لذلك نستثني المحايد .

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

U_{10} زمرة دوارة مولدة بالعنصر (3)

$$U_{10} = < 3 > = \{3^0, 3^1, 3^2, 3^3\} \quad ; \; < 3 > = < 3^{-1} > = \underbrace{< 7 >}_{\text{نظير مقلوب عند ظهور المحايد}}$$

ملاحظة: أي زمرة دوارة تملك عنصرين على الأقل وهما: العنصر ومقلوبه.

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

الاثبات :

لدينا $< a >$ زمرة وإن $a \in < a >$ و $a^{-1} \in < a >$

كما أن $< a^{-1} >$ زمرة تحوي نفس العنصر ومنه $< a^{-1} > \subseteq < a >$

لدينا $< a^{-1} >$ زمرة وأن $a^{-1} \epsilon \ < a^{-1} >$

فهي تحوي مقلوبه $a = (a^{-1})^{-1} \epsilon \ < a^{-1} >$

$< a >$ أصغر زمرة جزئية تحوي العنصر a

ومنه $< a > \subseteq < a^{-1} >$

ومن الاحتوائين نجد أن $< a > = < a^{-1} >$

لو عدنا للمثال السابق: $U(10) =< 3 > =< 7 >$

حيث $< 7 >$ هي مقلوب$< 3 >$

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

$U_{10} =< 7 > = \{7^0, 7^1, 7^2, 7^3\}$

U_{10} زمرة دوارة مولدة بالعنصر (7) و(3).

ليكن لدينا:$Z_n = \{0,1,2 \dots , (n-1)\}$

$$\forall m \in Z_n; m = 1 + \underbrace{1 + \cdots + 1}_{n\text{مرة}} = m.1$$

$Z_n =< 1 >=< -1 > =< n-1 >$ مولدة ب 1

حسب التمهيدية السابقة:

لو اخذنا : $Z_5 = \{0,1,2,3,4\}$

$$Z_5 =< 1 > =< 4 >$$

زمرة الاعداد الصحيحة Z دوارة مولدة بالعنصر 1

$$Z_5 =< 1 >$$

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

مثال: هل الزمرة U_8 زمرة دوارة ؟

$$U_8 = \{1,3,5,7\}$$

$$3^0 = 1 \quad , \quad 3^1 = 3 \quad , \quad 3^2 = 9 \quad , \quad 3^3 = 3 \quad , \quad 3^4 = 1$$

اذا الزمرة المولدة من العنصر 3 هي $\{1,3\}$ $< a > =$

$$U_8 \neq < 3 >$$

U_8 ليست مولدة بالعنصر (3)

$$< 5 > = \{1,5\}$$

$$5^0 = 1 \quad , \quad 5^1 = 5 \quad , \quad 5^2 = 1 \quad , \quad 5^3 = 5 \quad , \quad 5^4 = 1$$

$$U_8 \neq < 5 >$$

U_8 ليست مولدة بالعنصر (5)

$<$

مقلوب 7 هو 7 لانه نتج المحايد من جداءه مع نفسه

$$7^0 = 1 \quad , \quad 7^1 = 7 \quad , \quad 7^2 = 1 \quad , \quad 7^3 = 7 \quad , \quad 7^4 = 1$$

$$U_8 \neq < 7 >$$

U_8 ليست مولدة بالعنصر (7)

وبالتالي U_8 ليست دوارة لأنها ليست مولدة بأي عنصر .

نتيجة: كل زمرة دوارة تكون تبديلية.

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 .

الاثبات :

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

$\varphi(n) = a^n = a^m = \varphi(m)$ 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) $\forall\, n, m \,\epsilon\, Z\ \ ; a^n = a^m \ \Longrightarrow\ n = m$
٣) $\forall\, n, m \,\epsilon\, Z\ \ ;\ n \neq m \Longrightarrow a^n \neq a^m$
٤) الزمرة G غير منتهية

الاثبات :

$(1 \longrightarrow 2)$ لنفرض ان $n, m \,\epsilon\, Z$ فإن $a^n = a^m$ ومنه $\varphi(n) = \varphi(m)$ وبالتالي نجد: $n = m$

$(2 \longrightarrow 3)$ ليكن $n, m \,\epsilon\, Z$ بحيث $n \neq m$ لنفرض جدلا أن $a^n = a^m$ عندئذ حسب الفرض $n = m$ وهذا تناقض ومنه $a^n \neq a^m$

$(3 \longrightarrow 4)$واضح.

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

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

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

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

نضرب (*) ب a^{-m}:

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

لنأخذ المجموعة

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

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

ومنه يوجد في ℓ عنصر اصغر وليكن K بحيث $a^k = e$
لدينا :

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

ولنثبت الان الاحتواء المعاكس
ليكن $y \in G$ عندئذ $n \in Z$: $y = a^n$ وحسب خوارزمية القسمة لاجل K, n يوجد $q, r \in Z$ بحيث

$$n = qK + r$$

جعلنا القسمة على k لأنه مفروض
بالمجموعة ℓ لايساوي الصفر اما
n فقد يكون صفر او لا

$$0 \leq r < K$$

$$y = a^n = a^{qK+r} = a^{qK} . a^r = \underbrace{(a^k)^q}_{e \text{ حسب تعريف المجموعة } \ell} . a^r = a^r$$

ومنه $y = a^r \in \{e, a, a^2, \dots \dots \dots, a^{k-1}\}$ ومنه $G \subseteq \{e, a, a^2, \dots \dots \dots, a^{k-1}\}$

ومن الاحتوائين ينتج:

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

ومنه G منتهية . وهذا يناقض الفرض 4 ومنه φ متباين .

نستنتج: كل الزمر الدوارة غير المنتهية تكون قابلة للعد .

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

١) الزمرة G منتهية .
٢) يوجد في $n, m \in Z$ بحيث $a^n = a^m$ وأن $n \neq m$.
٣) يوجد في $k \in N^*$ بحيث :

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

وأن هذه العناصر مختلفة مثنى مثنى .

الاثبات :

(1 ⟵ 2) لنفرض جدلاً انه أياً كان

$a^n = a^m\ ; n, m \epsilon Z$ فإن $n = m$ عندئذٍ: حسب المبرهنة السابقة تكون الزمرة G غير منتهية وهذا يناقض الفرض.

ومنه يوجد $n, m \epsilon Z$ بحيث $a^n = a^m$ وان $n \neq m$

وان $n \neq m$ لأنه اذا كان لأجل كل $n, m \epsilon Z$ يحققان $a^n = a^m$ فإن$n = m$ ينتج ان f متباين وبالتالي G غير منتهية وهذا تناقض

(2 ⟵ 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 $l = \{t : t \epsilon N^* \ : \ a^t = e\ \}$

$\emptyset \neq l \subseteq N^*$ لان $n - m \in l$ ومنه يوجد في l عنصر أصغر وليكن k وأن $a^k = e$

(لأنها مجموعة جزئية في N و غير خالية)

لنأخذ المجموعة: $\{e, a, a^2, \dots \dots \dots, a^{k-1}\}$ وبنفس الطريقة السابقة نجد ان

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

اثبات أن عناصر المجموعة السابقة مختلفة مثنى مثنى لنفرض جدلا أنه يوجد $a^s, a^t \in G$ بحيث

$$a^s = a^t \quad , \qquad s \neq t$$

$$0 \leq s, t < k$$

بفرض $s > t$ نجد أن $s - t > 0$

لنضرب طرفي العلاقة $a^s = a^t\ a^j$ بa^{-t} $\quad 0 \leq \underbrace{s - t}_{\text{موجب}} < k \quad ; \quad a^{s-t} = e$

حيث))s, t عدد طبيعي وأصغر من k لأجله $a^{s-t} = e$ وهذا غير ممكن لان k هو العنصر الأصغر في مجموعة الاعداد الصحيحة الموجبة والتي لأجلها $a^k = e$ في المجموعة(لذلك هذا يناقض كون k عنصر اصغر في N وبالتالي العناصر : $\{e, a, a^2, \dots \dots \dots, a^{k-1}\}$ مختلفة مثنى مثنى .

(3 ⟵ 1) واضح لان G تحوي K عنصر ومنه فهي منتهية.

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

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

((معنى ∞ لا يوجد عدد صحيح موجب لأجله المساواة صحيحة ولا يدل هذا الرمز على اللانهاية التي نتعامل معها في التحليل و المواد الأخرى))

نعود لمثالنا: ١- $U(8) = \{1,3,5,7\}$

$0(1) = 1$ مرتبة المحايد 1 دائماً

$$3^1 = 3 \;, \quad 3^2 = \underbrace{1}_{\text{نتوقف عند اول اس نحصل من خلاله على المحايد}} \;, \quad 0(3) = 2$$

$$5^1 = 5 \quad , 5^2 = 1 \quad , 0(5) = 2 \quad , \quad 0(7) = 2$$

٢- $U(10) = \{1,3,7,9\}$

$$0(1) = 1 \;, \quad 0(3) = 4 \;, \quad 0(7) = 4 \;, \quad 0(9) = 2$$

بحالة الزمر الجمعية:

٣- لتكن $Z_4 = \{0,1,2,3\}$ حيث $0(0) = 1$

$1.1 = 1$	$1.2 = 2$	$3.1 = 3$
$1.2 = 2$	$2.2 = 0$	$3.2 = 2$
$1.3 = 3$		$3.3 = 1$
$1.4 = 0$		$4.3 = 0$
$0(1) = 4$	$0(2) = 2$	$0(3) = 4$

٤- في زمرة الاعداد الصحيحة لدينا:

$$0(0) = 1 \quad , \quad 0(2) = \infty$$

$$\forall a \in Z \,, \quad a \neq 0 \;;\; 0(a) = \infty$$

مبرهنة : ((دراسة بعض الخواص لمرتبة العنصر))

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

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

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

٣) إذا كان $k \epsilon Z$ 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 $n = 0 < a >= (G:1)$

الاثبات :

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

$e = (a^{-1})^{n}$ و بقي أن نثبت أن n أصغر عدد صحيح موجب يحقق المساواة السابقة وليكن K عدد صحيح موجب لأجله : بحيث $e = (a^{-1})^{k}$ ومنه $e = a^{-k}$ ولو ضربنا ب a^{k} يعطي $e = a^{k}$ وحسب تعريف المرتبة نجد ان : $n \leq k$

اذاً $0(a^{-1}) = n$

٢) ليكن $e = a^{n} = a^{n-s}.a^{s}$

نضرب بمقلوب a^{s} من اليمين نحصل على $a^{-s} = a^{n-s}$

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

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

$$k = qn + r \qquad q,r \epsilon Z$$
$$0 \leq r < n$$

لنبرهن ان $r = 0$ ، لنفرض جدلا أن $r \neq 0$ عندئذ $0 < r < n$ كما أنه يحقق :

$$a^{k} = a^{qn+r} = a^{qn}.a^{r} = (a^{n})^{q}.a^{r} = e.q^{r} = a^{r}$$

$$a^{k} = a^{qn+r} = a^{qn}.a^{r} = (a^{n})^{q}.a^{r} = e.a^{r} = a^{r}$$

وهذا يناقض لأنه لا يوجد عدد صحيح موجب أصغر من n يحقق هذه المساواة كون $0(a) = n$ ومنه $r = 0$ وبالتالي $k = qn$.

٤) ليكن $t > 0$ وأن t يقسم n وبالتالي $\frac{n}{t} \in Z$, $0 < t \leq n$ وبالتالي $a^{\frac{n}{t}} \in G$

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

ولنأخذ عدد آخر يحقق نفس الشرط وليكن K عدد صحيح موجب يحقق $\left(a^{\frac{n}{t}}\right)^{k} = e$ عندئذٍ : $\left(a^{\frac{n.k}{t}}\right) = e$

- مرتبة العنصر a هي n اذا n أصغر عنصر تحقق المساواة :

$$n \le \frac{nk}{t}$$

$$1 \le \frac{k}{t} \Rightarrow t \le k$$

إذاً t اصغر الاعداد الموجبة التي تحقق المساواة ومنه $0\left(a^{\frac{n}{t}}\right) = t$

٥) اذا كانت G دوارة منتهية مولدة بالعنصر a

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

وهذا يبين أن $(G:1) = n = 0(a)$

انتهت المحاضرة

تنويه: في المحاضرة السابقة وجد خطأ بسيط(الصفحة الخامسة)(السطر الثامن)

الخطأ :

$$\forall aH \in M_i \; ; \; \emptyset(a11) = Ha^{-1}$$

التصحيح:

$$\forall aH \in M_i \; ; \; \emptyset(aH) = Ha^{-1}$$

إعداد: ناريمان جلو – ولاء الأخضر – هلا همج