البنى الجبرية 1

الدكتور : حمزة الحاكمي

المحاضرة : الحادية عشر

التاريخ : ٣١/١٠/٢٠١٦

إعداد : أحمد أبو التوت

Web: www.syriamath.net

group: Improve our mathematics

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) بفرض أن G زمرة منتهية اعتماداً على المبرهنة السابقة نجد أن التطبيق f ليس متباين ((لأنه لو كان متباين لكانت G غير منتهية))

إن f غير متباين عندئذ : $\exists\, n, m \in Z\,; a^n = a^m$

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

(2 ⟵ 3) لنفرض انه يوجد $n, m \in Z$ بحيث $n \neq m$ و $a^n = a^m$ لنفرض أن $n > m$ أيضا لدينا

$$t = n - m > 0 \;\; ; a^t = a^{n-m} = e \;\; ((a^n = a^m \text{ لأن}))$$

لنأخذ المجموعة $\quad l = \{s : s \in N^* \;:\; a^s = e\}$

وجدنا ان l ليست خالية بسبب أن $t \in l$ وو بالتالي هي تحوي عنصر أصغر وليكن k وأن $a^k = e$ (لأنها مجموعة جزئية في N و غير خالية)

لنأخذ المجموعة: $\{e, a, a^2, \dots \dots \dots, a^{k-1}\}$

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

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

ولنثبت الاحتواء المعاكس

ليكن $y \in G$ عندئذ :

$$y = a^{\alpha} \quad : \alpha \in Z$$

وحسب خوارزمية القسمة يوجد $\alpha, k \in Z$

$$\alpha = qk + r \quad : \ 0 \le r < k$$

$$y = a^{\alpha} = a^{qk+r} = a^{qk}.a^{r} = \underbrace{(a^{k})^{q}}_{=e} a^{r} = a^{r} \in \{e, a, a^{2}, \dots \dots \dots, a^{k-1}\}$$

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

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

أما لكي نثبت أن عناصر المجموعة السابقة مختلفة مثنى مثنى لنفرض جدلا أنه يوجد

$$0 \le i, j < k$$

وأن $i \neq j$ وأن $a^{i} = a^{j}$ و إذا أن $i > j$ فهذا يعطي $i - j > 0$.

لنضرب طرفي العلاقة $a^{i} = a^{j}$ بمقلوب a^{j} و هذا يعطي $0 < \underbrace{i - j}_{\text{موجب}} < k \quad ; \quad a^{i-j} = e$

((حيث i, j كل منهما أصغر من k كوننا أخذناهما من المجموعة G حيث الأسس فيها بين الصفر والـ $k - 1$ فإن $i - j < k$))).

نلاحظ إذاً أنه وجد $i - j$ عدد طبيعي وأصغر من k لأجله $a^{i-j} = e$ وهذا غير ممكن لأننا اخترنا k هو العنصر الأصغر في مجموعة الأعداد الصحيحة الموجبة والتي لأجلها $a^{k} = e$ لذلك هذا يناقض كون k عنصر أصغر في N

وبالتالي عناصر $\{e, a, a^{2}, \dots \dots \dots, a^{k-1}\}$ مختلفة مثنى مثنى

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

تعريف:

ليكن G زمرة و $a \in G$ نسمي أصغر عدد صحيح موجب k لأجله $a^{k} = e$ بمرتبة العنصر a ونرمز له $0(a) = k$ وهذا في الحالة العامة ، ولكن عندما $\forall t \in N^{*} \quad a^{t} \neq e$

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))

أمثلة : ""عملية الضرب بالمقاس n ""

لنأخذ زمرة الضرب بالمقاس (15) وهي :

$$U_{15} = \{1,2,4,7,8,11,13,14\}$$

$$0(1) = 1$$

ملاحظة (١): المرتبة تتعلق بقوة العنصر نوجد كل القوى الموجبة و عندما نحصل على أصغر عدد موجب لأجله $a^k = e$ فإن المرتبة تساوي الأس

$$2^1 = 2 \quad ,2^2 = 4 \quad ,2^3 = 8 \quad ,2^4 = 1 \Rightarrow 0(2) = 4$$

. فمثلا هنا حصلنا على المحايد 1 وكان الاس هو 4 وبالتالي بالمرتبة هي 4

$$4^1 = 4 \quad ,4^2 = 1 \Rightarrow 0(4) = 2$$

$$7^1 = 7 \quad ,7^2 = 4 \; ,7^3 = 14, \; 7^4 = 1 \quad \Rightarrow 0(7) = 4$$

(حاول من أجل باقي العناصر) ☺

ملاحظة (٢): في الزمر المنتهية جميع العناصر لها رتبة .

ملاحظة(٣) : بحالة الزمرة كانت ج معية فإن $ka = 0$.

أمثلة بحالة الزمر جمعية:

$$Z_6 = \{0,1,2,3,4,5\}$$

حيث $0(0) = 1$

$1.1 = 1$	$1.2 = 2$	$3.1 = 3$	$1.4 = 4$	$1.5 = 5$
$1.2 = 2$	$2.2 = 4$	$3.2 = 0$	$2.4 = 2$	$2.5 = 4$
$1.3 = 3$	$3.2 = 0$		$3.4 = 0$	$3.5 = 3$
$1.4 = 4$				$4.5 = 2$
$1.5 = 5$				$5.5 = 1$
$1.6 = 0$				$6.5 = 0$
$0(1) = 6$	$0(2) = 3$	$0(3) = 2$	$0(4) = 3$	$0(5) = 6$

مثال:

في زمرة الأعداد الصحيحة $(Z, +)$ نجد أن كل عنصر مغاير للصفر مرتبته غير منتهية

$\forall \; 0 \neq a \in Z$ فإن $a, 2a, 3a, \dots \dots$

إن كل عنصر من هذه العناصر مغاير للصفر .

لا يوجد k يحقق هذه المساواه من اجل ايا كان $ka=0$

أي أنه لا يوجد عدد صحيح مغاير للصفر يمكن ضربه بـ (a) نحصل من خلاله على المحايد ((الصفر)) .

وبالتالي

$$0(a)=\infty \quad \forall a\in Z\backslash\{0\}$$

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 $\forall\, s\,\epsilon\, Z : s\le n$

٣) إذا وجد $k\,\epsilon\, Z$ بحيث $a^k=e$ 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 يحق المساواة السابقة وليكن $s\in Z$ بحيث
$e=(a^{-1})^s$ ومنه $e=a^{-s}$ وبالتالي $e=a^s$ وبالتالي $n\le s$
ومنه $0(a^{-1})=n$

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

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

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

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

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 $\frac{n}{t} \in Z$, $0 < t \leq n$

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

وان $0\left(a^{\frac{n}{t}}\right) = t$ لآنه $\forall \beta \in N^* \;\; ; \beta < t$

لأن $\frac{n.\beta}{t} < n$ $((\frac{\beta}{t} < 1\,))$ وهذا غير ممكن لأنه لا يوجد عدد أصغر منه يحقق المساواة ومنه فإن

$$0\left(a^{\frac{n}{t}}\right) = t$$

٥) إن

$$G =< a >= \{a^s \quad : s \in Z\}$$
$$= \{e, a, a^2 \ldots \ldots a^{n-1}\} = G$$

وهذا يبين أن $(G:1) = n$

مبرهنة :

((هذه المبرهنة تعطينا الشرط الازم والكافي كي تكون عناصر الزمرة الدوارة المتهية مولدات لها))

النص : لتكن G زمرة دوارة مولدة بالعنصر a أي أن $G =< a >$ مرتبتها n

الشروط الاتية متكافئة :

١) $G =< a^k >$ حيث $k \in Z$

٢) $\gcd(k, n) = 1$

الاثبات :

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

حيث $1 < t < n$, $1 < s < k$

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

سنحصل الان على t عنصراً و t اصغر من n وبالتالي لن يكون مولد لـ G $G \neq< a^k >$ وهذا يناقض الفرض ومنه

$$\gcd(k, n) = 1$$

(2 ← 1) لنفرض أن $\gcd(k,n)=1$ عندئذ يوجد $s,t\in Z$ بحيث:

$1=s.k+t.n$ ولنبرهن أن $G=<a^k>$.

$$a=a^1=a^{s.k+t.n}=a^{s.k}.a^{t.n}$$
$$\Rightarrow \quad =(a^k)^s.\underbrace{(a^n)^t}_{e}=(a^k)^s\epsilon<a^k>$$
$$G=<a>\subseteq<a^k>\subseteq G$$
$$\Rightarrow \quad G=<a^k>$$

لانه $<a>\subseteq<a^n>$ كون $<a>$ أصغر زمرة تحوي a ووجدنا $<a^k>$ أصغر زمرة تحوي a ومنه الاحتواء محقق .

من جهة أخرى $a^k\epsilon<a>$

ولدينا $a^k\epsilon <a^k>$ حيث أصغر زمرة تحوي $a^k \Leftarrow <a>\subseteq<a^k>$

ومن الإحتوائين نجد $G=<a>=<a^k>$.

"انتهت المحاضرة"