جامعة دمشق

كلية العلوم

قسم الرياضيات

السنة الدراسية الثانية

البنى الجبرية (1)

المحاضرة العاشرة

تاريخ المحاضرة: 10/11/2015

مدرس المقرر: د. حمزة الحاكي

مُبرهنة: لتكن G زمرة دوارة منتهية مولدة بالعنصر $a \in G$ ، ولنفرض أن مرتبة الزمرة G هي n. عندئذٍ الشروط التالية متكافئة:

-1 $G = < a^k >$ بحيث $0 \neq k \in \mathbb{Z}$.

-2 $gcd(n,k) = 1$.

البرهان: بما أن G زمرة دوارة مولدة بالعنصر a فإن $G = < a >$ ، ولدينا فرضاً مرتبة الزمرة المنتهية G هي n أي $(G:1) = n$.

$$\left.\begin{array}{c} G = < a > \\ and \\ (G:1) = n \end{array}\right\} \underset{\text{انظر للجزء الثاني من التمهيدية الأخيرة في المحاضرة السابقة}}{\Rightarrow} O(a) = n$$ أصبح لدينا

1 ⇐ 2 : لنفرض أن $G = < a^k >$ بحيث $0 \neq k \in \mathbb{Z}$ ، ولنثبت أن $gcd(n,k) = 1$.

لنفرض جدلاً أن

$$gcd(n,k) = d \quad ; \quad d > 1$$

بما أن d قاسم مشترك أعظم للعددين n,k فهذا يعني أن d قاسم لكُل من n و k.

$$\underbrace{0 < s < n}_{\text{لأن } d>1} \quad , \quad \exists\, s \in \mathbb{Z} : \; n = s.d \underset{\text{استناداً لتعريف القاسم}}{\Rightarrow} d \text{ قاسم لـِ } n$$

$$\underbrace{0 < t < k}_{\text{لأن } d>1} \quad , \quad \exists\, t \in \mathbb{Z} : \; k = t.d \underset{\text{استناداً لتعريف القاسم}}{\Rightarrow} d \text{ قاسم لـِ } k$$

لنفرض أن مرتبة العنصر a^k هي m أي

$$O(a^k) = m \Leftrightarrow (a^k)^m = e$$ يُحقق m أصغر عدد صحيح موجب

$$(a^k)^s = a^{k.s} \underset{\text{بالاستفادة مما سبق}}{\Rightarrow} (a^k)^s = a^{t.d.s} \underset{\text{بالاستفادة مما سبق}}{\Rightarrow} (a^k)^s = a^{t.n} \Rightarrow (a^k)^s = (a^n)^t$$ لدينا

$$\underset{\substack{a^n = e \\ \text{لأن } O(a)=n}}{\Rightarrow} (a^k)^s = e^t \Rightarrow (a^k)^s = e$$

$$\left.\begin{array}{c} (a^k)^m = e \text{ يُحقق } m \text{ أصغر عدد صحيح موجب} \\ and \\ (a^k)^s = e \end{array}\right\} \Rightarrow m \leq s$$ أصبح لدينا

وبما أن $s < n$ فإن $m \leq s < n$.

أصبح لدينا $\left.\begin{array}{c} \text{فرضاً } G=<a^k> \\ O(a^k)=m \\ m<n \end{array}\right\} \underset{\text{انظر للجزء الثاني من التمهيدية الأخيرة في المحاضرة السابقة}}{\Rightarrow} (G:1)=O(a^k)=m<n$

وهذا مُخالف كون $(G:1)=n$ مما يعني أننا وصلنا إلى تناقض.

التناقض الذي وصلنا إليه هو من الفرض الجدلي "$gcd(n,k)=d>1$" الخاطئ مما يعني أن

وهو المطلوب $gcd(n,k)=1$

2 ⇐ 1 : لنفرض أن $gcd(n,k)=1$ ولنثبت أن $G=<a^k>$ بحيث $0\neq k\in\mathbb{Z}$.

بما أن $gcd(n,k)=1$ فيوجد " بحسب المبرهنة صـ5 من المحاضرة الخامسة " عددين $\alpha,\beta\in\mathbb{Z}$ بحيث

$$\alpha.n+\beta.k=1 \quad ...*$$

لنثبت أن $<a>=<a^k>$.

لدينا $a=a^1 \underset{\text{بالاستفادة مما سبق}}{\Rightarrow} a=a^{\alpha.n+\beta.k}\Rightarrow a=a^{\alpha.n}\cdot a^{\beta.k}\Rightarrow a=(a^n)^{\alpha}\cdot(a^k)^{\beta} \underset{\substack{\text{لدينا } a^n=e \\ \text{لأن } O(a)=n}}{\Rightarrow}$

$a=e^{\alpha}\cdot(a^k)^{\beta}\Rightarrow a=e\cdot(a^k)^{\beta}\Rightarrow a=(a^k)^{\beta} \underset{\text{بحسب تعريف عناصر }<a^k>}{\Rightarrow} a\in<a^k>$

أصبح لدينا $\left.\begin{array}{c} \text{برهاناً } a\in<a^k> \\ and \\ \text{وضوحاً } a\in<a> \end{array}\right\} \underset{\text{إن }<a^k> \text{ أصغر زمرة جزئية تحوي } a}{\Rightarrow} <a>\subseteq<a^k> \quad ...(1)$

وضوحاً $a\in<a> \underset{\text{". } <a> \text{ مغلقة بالنسبة للعملية "}}{\Rightarrow} \underbrace{a\cdot a\cdot ...\cdot a}_{k \text{ مرة}}\in<a>\Rightarrow a^k\in<a>$

أصبح لدينا $\left.\begin{array}{c} \text{برهاناً } a^k\in<a> \\ and \\ \text{وضوحاً } a^k\in<a^k> \end{array}\right\} \underset{\text{إن }<a^k> \text{ أصغر زمرة جزئية تحوي } a^k}{\Rightarrow} <a^k>\subseteq<a> \quad ...(2)$

من (1) و (2) نجد أن $<a>=<a^k>$.

وبما أن $G=<a>$ فإن $G=<a^k>$. **وهو المطلوب.**

<u>نستنتج من هذه المبرهنة ومن النتيجة الموجودة في صـ9 من المحاضرة السابقة ما يلي:</u>

ليكن $n>1$ عدد صحيح،عندئذٍ العنصر $0\neq k\in\mathbb{Z}_n$ يُحقق $\mathbb{Z}_n=<k>$ (أي العنصر k مولد للزمرة $\mathbb{Z}_n$) **إذا وفقط إذا** كان n,k أوليان فيما بينهما. وبتعبير آخر

$$\mathbb{Z}_n=<k>\Leftrightarrow gcd(n,k)=1$$

مثال(1): لنأخذ $(\mathbb{Z}_8, +)$ زمرة الأعداد الصحيحة بالنسبة لعملية الجمع بالمقاس 8.

نعلم أن

$$\mathbb{Z}_8 = \{0,1,2,\dots,8-1\} = \{0,1,2,3,4,5,6,7\}$$

لدينا $1,3,5,7 \in \mathbb{Z}_8$ ومن الملاحظ أن

$$gcd(1,8) = 1 \quad , \quad gcd(3,8) = 1 \quad , \quad gcd(5,8) = 1 \quad , \quad gcd(7,8) = 1$$

وهذا يُكافئ "بحسب النتيجة السابقة" أن الزمرة $\mathbb{Z}_8$ دوارة مولدة بالعناصر $1,3,5,7$. أي

$$\mathbb{Z}_8 = <1> = <3> = <5> = <7>$$

ونقول أن مولدات الزمرة $\mathbb{Z}_8$ هي $1,3,5,7$ أو نقول أن مجموعة مولدات الزمرة $\mathbb{Z}_8$ هي $\{1,3,5,7\}$.

مثال(2): لنأخذ $(\mathbb{Z}_{10}, +)$ زمرة الأعداد الصحيحة بالنسبة لعملية الجمع بالمقاس 10.

نعلم أن

$$\mathbb{Z}_{10} = \{0,1,2,\dots,10-1\} = \{0,1,2,3,4,5,6,7,8,9\}$$

لدينا $1,3,7,9 \in \mathbb{Z}_{10}$ ومن الملاحظ أن

$$gcd(1,10) = 1 \quad , \quad gcd(3,10) = 1 \quad , \quad gcd(7,10) = 1 \quad , \quad gcd(9,10) = 1$$

وهذا يُكافئ "بحسب النتيجة السابقة" أن الزمرة $\mathbb{Z}_{10}$ دوارة مولدة بالعناصر $1,3,7,9$. أي

$$\mathbb{Z}_{10} = <1> = <3> = <7> = <9>$$

ونقول أن مجموعة مولدات الزمرة $\mathbb{Z}_{10}$ هي $\{1,3,7,9\}$.

مُبرهنة: لتكن G زمرة دوارة مولدة بالعنصر $a \in G$. عندئذٍ

1– كُل زمرة جزئية من G هي زمرة دوارة.

2– إذا كانت G زمرة منتهية مرتبتها n عندئذٍ مرتبة أي زمرة جزئية في G تقسم n.

3– إذا كانت G زمرة منتهية مرتبتها n ، وكان العدد $k \in \mathbb{Z}^+$ يقسم n عندئذٍ توجد زمرة جزئية واحدة فقط في G مرتبتها k هي $< a^{\frac{n}{k}} >$ "هذا الجزء هو عكس مبرهنة لاغرانج"

البرهان: بما أن G زمرة دوارة مولدة بالعنصر a فإن $G = < a >$.

1– لنفرض أن H زمرة جزئية كيفية في G ، ولنميز حالتين

الحالة الأولى: إذا كانت $H = \{e\}$. عندئذٍ يكون $H = < e >$ مما يعني أن H زمرة جزئية دوارة مولدة بالعنصر e والذي هو المحايد ويتم المطلوب.

الحالة الثانية: إذا كانت $H \neq \{e\}$. هذا يعني أنهُ يوجد في H عنصر $x \in H$ بحيث $x \neq e$ "لأن e محايد فهو موجود دائماً في H كونها زمرة".

مكتبـــة بريمـــا فيـــرا – مقابـل كليـة الفنـــون الجميلـــة
Mob : 0993586758 – Tel : 011 2124436

بما أن $x \in H \subseteq G$ فإن $x \in G$ ، وبما أن $G = < a >$ فإن $x \in < a >$ ومن هُنا نجد "استناداً لتعريف عناصر $< a >$" أنهُ يوجد $k \in \mathbb{Z}$ بحيث $x = a^k$.

لنفرض من دون المس بعمومية المسألة أن $k > 0$ ، ولنعرف المجموعة:

$$\ell = \{ t : \ t \in \mathbb{N}^* \ , \ a^t \in H \}$$

واضح من تعريف المجموعة ℓ أن $\ell \subseteq \mathbb{N}^*$. ولدينا $x = a^k \in H$ وأن $k > 0$ صحيح بالتالي نجد " استناداً لتعريف عناصر ℓ " أن $k \in \ell$ أي $\ell \neq \phi$.

بما أن ℓ مجموعة جزئية وغير خالية من $\mathbb{N}^*$ فيوجد في ℓ عنصر أصغر وليكن m.

$$m \in \ell \quad \underset{\text{استناداً لتعريف عناصر المجموعة } \ell}{\Rightarrow} \quad a^m \in H$$

أصبح لدينا

$$\left.\begin{array}{l} a^m \in H \text{ و } H \text{ زمرة جزئية في } G \\ and \\ a^m \in < a^m > \text{ وضوحاً} \end{array}\right\} \underset{\text{أصغر زمرة جزئية تحوي } a^m}{\Rightarrow} < a^m > \subseteq H \ \ldots (1)$$

لنأخذ $y \in H$ عنصر كيفي وبما أن $H \subseteq G$ فإن $y \in G$ ومنهُ $y \in < a >$ كون " $G = < a >$ فرضاً" ومن ثم نجد استناداً لتعريف عناصر $< a >$ أنهُ يوجد $s \in \mathbb{Z}$ بحيث $y = a^s$.

من أجل العددين الصحيحين s و $m \neq 0$ يوجد "بحسب خوارزمية القسمة" عددين صحيحين وحيدين q, r بحيث

$$s = m.q + r \ ; \quad 0 \leq r < m$$

لنفرض جدلاً أن $r \neq 0$ عندئذٍ

$$s = m.q + r \ ; \quad 0 < r < m$$

$$a^s \underset{\text{بالاستفادة مما سبق}}{=} a^{m.q+r} \Rightarrow a^s = (a^m)^q \cdot a^r \Rightarrow (a^m)^{-q} \cdot a^s = (a^m)^{-q} \cdot ((a^m)^q \cdot a^r)$$

$$\Rightarrow (a^m)^{-q} \cdot a^s = ((a^m)^{-q} \cdot (a^m)^q) \cdot a^r \Rightarrow (a^m)^{-q} \cdot a^s = e \cdot a^r$$

$$\Rightarrow a^r = (a^m)^{-q} \cdot a^s \Rightarrow a^r = a^{s-m.q}$$

لكن بما أن $a \in H$ و H زمرة فإن $a^{s-m.q} \in H$ أي أن $a^r \in H$ ، وبما أن $0 < r$ فنجد "استناداً لتعريف عناصر ℓ " أن $r \in \ell$.

أصبح لدينا

$$\left.\begin{array}{l} r \in \ell \\ and \\ r < m \end{array}\right\} \Rightarrow m \text{ ليس عنصر أصغر في } \ell$$

مما يعني أننا توصلنا إلى تناقض لأن m عنصر أصغر في المجموعة ℓ.

إن التناقض الذي توصلنا إليه هو من الفرض الجدلي "$r \neq 0$" الخاطئ مما يعني أن $r = 0$.

$$r = 0 \Rightarrow s = m.q$$

$$y = a^s \underbrace{\Rightarrow}_{\text{بالاستفادة مما سبق}} y = a^{m.q} \Rightarrow y = (a^m)^q$$

وبما أن $a^m \in < a^m >$ ، وأن $< a^m >$ زمرة بالتالي فإن $(a^m)^q \in < a^m >$ أي $y \in < a^m >$.

أخذنا عنصر كيفي $y \in H$ و وجدنا أن $y \in < a^m >$ مما يعني أن $\underbrace{H \subseteq < a^m >}_{(2)}$.

من (1) و (2) نحصل على:

$$H = < a^m >$$

وهذا يعني أن الزمرة الجزئية الكيفية H هي زمرة دوارة في G. **وهو المطلوب.**

2– بما أن الزمرة G منتهية فرضاً فنجد "استناداً لمبرهنة لاغرانج" أن مرتبة أي زمرة جزئية في G تقسم مرتبة الزمرة G أي تقسم n.

3– **برهان الوجود:** لنفرض أن الزمرة G منتهية ومرتبتها n أي $(G:1) = n$ ، ولنفرض أن k قاسم موجب لـِ n.

لدينا $\left.\begin{matrix} G = < a > \text{ فرضاً} \\ and \\ (G:1) = n \end{matrix}\right\} \underbrace{\Rightarrow}_{\text{انظر للجزء الثاني من التمهيدية الأخيرة في المحاضرة السابقة}} O(a) = n$

بما أن k قاسم موجب لـِ n ، وأن $O(a) = n$ فنجد "استناداً للجزء الأول من التمهيدية الأخيرة في المحاضرة السابقة " أن $O\left(a^{\frac{n}{k}}\right) = k$. لنأخذ الزمرة الجزئية الدوارة في G والمولدة بالعنصر $a^{\frac{n}{k}} \in G$.

أي لنأخذ

$$H = < a^{\frac{n}{k}} >$$

بما أن $O\left(a^{\frac{n}{k}}\right) = k$ فنجد "استناداً للجزء الثاني من التمهيدية الأخيرة في المحاضرة السابقة " أن

$$(H:1) = \left(< a^{\frac{n}{k}} >:1\right) = k$$

وهذا يعني أنهُ توجد الزمرة الجزئية $H =< a^{\frac{n}{k}} >$ في G وأن مرتبتها k.

برهان الوحدانية: لنفرض أن K زمرة جزئية أُخرى في G مرتبتها k أي $(K:1)=k$. بما أن G زمرة دوارة مولدة بالعنصر a أي $G=<a>$ فنجد **"استناداً لبرهان 1−"** أن K زمرة جزئية دوارة في G ، وأن $K=<a^m>$ بحيث أن m هو أصغر عدد صحيح موجب يُحقق $a^m \in K$.

من أجل العددين الصحيحين n و $m \neq 0$ يوجد "بحسب خوارزمية القسمة" عددين صحيحين وحيدين q,r بحيث

$$n = m.q + r \quad ; \quad 0 \leq r < m$$

لنفرض جدلاً أن $r \neq 0$ عندئذٍ

$$n = m.q + r \quad ; \quad 0 < r < m$$

$$a^n \underbrace{=}_{O(a)=n \text{ لأن}} e \underbrace{\Rightarrow}_{\text{بالاستفادة مما سبق}} a^{m.q+r} = e \Rightarrow a^{m.q} \cdot a^r = e \Rightarrow a^r = a^{-m.q} \Rightarrow a^r = (a^m)^{-q}$$

بما أن $a^m \in K$ و K زمرة جزئية في G "أي زمرة بحد ذاتها" فإن $(a^m)^{-q} \in K$ ، وبما أن $a^r = (a^m)^{-q}$ فإن $a^r \in K$.

أصبح لدينا $\left.\begin{matrix} a^m \in K \\ and \\ a^r \in K \text{ بحيث } 0 < r < m \end{matrix}\right\} \Rightarrow a^m \in K$ ليس أصغر عدد صحيح موجب يُحقق

من الأخيرة نكون قد وصلنا إلى تناقض لأن m هو أصغر عدد صحيح موجب يُحقق $a^m \in K$.

التناقض الذي وصلنا إليه هو من الفرض الجدلي "$r \neq 0$" الخاطئ مما يعني أن $r = 0$.

$$r = 0 \Rightarrow n = m.q \Rightarrow \frac{n}{m} \text{ عدد صحيح موجب}$$

بما أن $O(a) = n$ ، وأن $\frac{n}{m} \in \mathbb{N}^*$ ويقسم n فإننا نجد "استناداً للجزء الأول من التمهيدية الأخيرة في المحاضرة السابقة " أن $O\left(a^{\frac{n}{m}}\right) = \frac{n}{m}$ أي $O(a^m) = \frac{n}{m}$.

ومنهُ نجد أن:

$$k \underbrace{=}_{\text{بحسب فرضيتنا}} (K:1) \underbrace{=}_{K=<a^m>} (<a^m>:1) \underbrace{=}_{\substack{\text{مرتبة الزمرة الدوارة} \\ \text{تساوي مرتبة العنصر} \\ \text{الذي يولدها}}} O(a^m) \underbrace{=}_{\text{بالاستفادة مما سبق}} \frac{n}{m}$$

$$\Rightarrow k = \frac{n}{m} \Rightarrow m = \frac{n}{k}$$

وهذا يعني أن:

مكتبـــة بريمـــا فيـــرا — مقابـل كليـة الفنـــون الجميلـــة
$Mob: 0993586758 - Tel: 011\ 2124436$

$$K = < a^m > = < a^{\frac{n}{k}} > = H$$

مما يعني أنهُ **<u>توجد</u>** زمرة جزئية **<u>واحدة فقط</u>** في G **<u>مرتبتها k</u>** وهي $H = < a^{\frac{n}{k}} >$.

وهو المطلوب.

<u>نستنتج من هذه المبرهنة ومن النتيجة الموجودة في صـ9 من المحاضرة السابقة ما يلي:</u>

لتكن $\mathbb{Z}_n$ زمرة الجمع بالمقاس n بحيث $n > 1$ عدد صحيح. عندئذٍ إذا كان $k \neq 0$ يقسم n فإن الزمرة الجزئية الوحيدة في $\mathbb{Z}_n$ التي مرتبتها k هي $< \frac{n}{k} >$. وبتعبير آخر

$$n \text{ يقسم } k \neq 0 \Rightarrow < \frac{n}{k} > \text{ الزمرة الجزئية الوحيدة في } \mathbb{Z}_n \text{ التي مرتبتها } k \text{ هي}$$

مُبرهنة: كُل زمرة منتهية مرتبتها عدد أولي تكون زمرة دوارة.

البرهان: لنفرض أن G زمرة منتهية مرتبتها العدد الأولي p أي $(G:1) = p$.

بما أن مرتبة الزمرة G عدد أولي p (أي عدد عناصرها أكبر تماماً من الواحد ومساوٍ للعدد الأولي p) فهي تحوي على عناصر مخالفة للعنصر المحايد ، وهذا يعني أنهُ يوجد $a \in G$ بحيث $a \neq e$.

إن $< a >$ زمرة جزئية في G ، وإن مرتبة الزمرة الجزئية $< a >$ أكبر تماماً من الواحد أي أن

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

وذلك لأن $a \neq e$ و e, a عناصر من $< a >$ على الأقل.

بما أن G زمرة منتهية مرتبتها p فإن **"استناداً لمبرهنة لاغرانج"** مرتبة أي زمرة جزئية فيها تقسم مرتبتها أي $(< a >: 1)$ تقسم p ، وبما أن p عدد أولي فإن قواسمهُ الموجبة إما 1 أو p وكون $(< a >: 1) > 1$ فإن

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

أصبح لدينا

$$\left.\begin{array}{c} (G:1) = p \\ < a > \subseteq G \\ (< a >: 1) = p \end{array}\right\} \Rightarrow G = < a >$$

مما يعني أن G زمرة دوارة مولدة بالعنصر a. **وهو المطلوب.**

تعريف تمهيدي إضافي: ليكن n, m عددين صحيحين غير معدومين عندئذٍ نسمي L مضاعف للعددين n, m إذا كان n يقسم L وكان m يقسم L.

كما ونسمي L مضاعف مشترك أصغر للعددين n, m إذا تحققت الشروط الآتية:

-1 $L > 0$

-2 n يقسم L و m يقسم L.

مكتبـــة بريمـــا فيـــرا — مقابـل كليـة الفنـــون الجميلـــة
Mob : 0993586758 − Tel : 011 2124436

3- إذا كان $L_1 > 0$ مُضاعف مشترك للعددين n, m فإن $L \leq L_1$.

- نرمز للمضاعف المشترك الأصغر للعددين n, m بـ $Lcm(n, m)$.

مُبرهنة إضافية: إذا كان n, m عددين صحيحين موجبين وكان $n.m \neq 0$ و $gcd(n, m)$ هو القاسم المشترك الأعظم للعددين n, m فإن:

$$Lcm(n, m) = \frac{n.m}{gcd(n, m)}$$

تمارين

تمرين(1): لتكن G زمرة ، وليكن $a, b \in G$ عنصرين كيفيين ، ولنفرض أن $O(a) = n\ ,\ O(b) = m$.

فإذا كان $a \cdot b = b \cdot a$ ، وكان $< e > = < a > \cap < b >$ ، فإن

$$O(a \cdot b) = Lcm(n, m)$$

البرهان: لدينا

$$\underbrace{O(a) = n \quad , \quad O(b) = m}_{\text{فرضية (1)}} \quad , \quad \underbrace{a \cdot b = b \cdot a}_{\text{فرضية (2)}} \quad , \quad \underbrace{< e > = < a > \cap < b >}_{\text{فرضية (3)}}$$

لنفرض أن $Lcm(n, m) = k$ ، وأن $O(a \cdot b) = \lambda$ ، ولنثبت أن $\lambda = k$.

بما أن k مضاعف مُشترك أصغر للعددين n, m فيوجد عددين $\alpha, \beta \in \mathbb{Z}$ بحيث

$$\underbrace{k = \alpha.n \quad and \quad k = \beta.m}_{(4)}$$

يُمكن باستخدام مبدأ الاستقراء الرياضي إثبات أن $(a \cdot b)^k = a^k \cdot b^k$ لكُل $k \geq 2$.

خطوة البداية: لنثبت صحة المطلوب من أجل $k = 2$.

$$(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) \underbrace{\Rightarrow}_{\text{العملية "." تجميعية}} (a \cdot b)^2 = a \cdot (b \cdot a) \cdot b \underbrace{\Rightarrow}_{\text{بالاستفادة من الفرضية (2)}}$$

$$(a \cdot b)^2 = a \cdot (a \cdot b) \cdot b \underbrace{\Rightarrow}_{\text{العملية "." تجميعية}} (a \cdot b)^2 = (a \cdot a) \cdot (b \cdot b)$$

$$\Rightarrow (a \cdot b)^2 = a^2 \cdot b^2 \quad \text{" والمطلوب صحيح من أجل } k = 2 \text{"}$$

خطوة الاستقراء: لنفرض أن المطلوب صحيح من أجل $k > 2$. أي

$$\underbrace{(a \cdot b)^k = a^k \cdot b^k}_{\text{خطوة الاستقراء}} \quad ; \quad k > 2$$

ولنبرهن على صحة المطلوب من أجل $k + 1$.

$$(a\cdot b)^{k+1}=(a\cdot b)^k\cdot(a\cdot b)\underset{\text{بالاستفادة من فرضية الاستقراء}}{\Rightarrow}(a\cdot b)^{k+1}=(a^k\cdot b^k)\cdot(a\cdot b)$$

$$\underset{\text{العملية "." تجميعية}}{\Rightarrow}(a\cdot b)^{k+1}=a^k\cdot(b^k\cdot a)\cdot b\underset{\substack{\text{بالاستفادة من الفرضية (2)}\\ \text{عدد من المرات مساوٍ لـ } k \text{ مرة}}}{\Rightarrow}(a\cdot b)^{k+1}=a^k\cdot(a\cdot b^k)\cdot b$$

$$\underset{\text{العملية "." تجميعية}}{\Rightarrow}(a\cdot b)^{k+1}=(a^k\cdot a)\cdot(b^k\cdot b)\Rightarrow(a\cdot b)^{k+1}=a^{k+1}\cdot b^{k+1}$$

والمطلوب صحيح من أجل $k+1$. مما سبق نستنتج "استناداً لمبدأ الاستقراء الرياضي" أن

$(a\cdot b)^k=a^k\cdot b^k$ وذلك لكُل عدد صحيح $k\geq 2$

$$(a\cdot b)^k=a^k\cdot b^k\underset{\text{بالاستفادة من(4)}}{\Rightarrow}(a\cdot b)^k=a^{\alpha.n}\cdot b^{\beta.m}\Rightarrow(a\cdot b)^k=(a^n)^\alpha\cdot(b^m)^\beta$$

$$\underset{\substack{\text{من الفرضية (1)}\\ O(a)=n \text{ لأن } a^n=e\\ O(b)=m \text{ لأن } b^m=e}}{\Rightarrow}(a\cdot b)^k=e^\alpha\cdot e^\beta\Rightarrow(a\cdot b)^k=e\cdot e\Rightarrow(a\cdot b)^k=e\quad;\quad\forall\,k\geq 2$$

أصبح لدينا

$$\left.\begin{matrix}O(a\cdot b)=\lambda \text{ أي } \lambda \text{ أصغر عدد صحيح موجب يُحقق}\\ and\\ (a\cdot b)^k=e\end{matrix}\right\}\Rightarrow\underbrace{\lambda\leq k}_{*}$$

إن $(a\cdot b)^k=e$ كما وجدنا مُحقق من أجل جميع قيم $k\geq 2$ بما فيها λ. أي $(a\cdot b)^\lambda=e$.

$$(a\cdot b)^\lambda=e\underset{\substack{(a\cdot b)^k=a^k\cdot b^k \text{ مُحقق لكُل } k\geq 2\\ (a\cdot b)^\lambda=a^\lambda\cdot b^\lambda \text{ بما فيها } \lambda \text{ أي}}}{\Rightarrow}a^\lambda\cdot b^\lambda=e\Rightarrow(a^\lambda\cdot b^\lambda)\cdot b^{-\lambda}=e\cdot b^{-\lambda}$$

$$\Rightarrow a^\lambda\cdot\left(b^\lambda\cdot b^{-\lambda}\right)=b^{-\lambda}\Rightarrow a^\lambda\cdot e=b^{-\lambda}\Rightarrow a^\lambda=b^{-\lambda}$$

بما أن $a\in<a>$ فإن $a^\lambda\in<a>$ ، وبما أن $a^\lambda=b^{-\lambda}$ فإن $b^{-\lambda}\in<a>$.

بما أن $b\in<b>$ فإن $b^{-\lambda}\in<b>$ ، وبما أن $a^\lambda=b^{-\lambda}$ فإن $a^\lambda\in<b>$.

أصبح لدينا

$$\left.\begin{matrix}a^\lambda\in<a>\\ and\\ a^\lambda\in<b>\end{matrix}\right\}\Rightarrow a^\lambda\in<a>\cap<b>\underset{\text{بالاستفادة من الفرضية (3)}}{\Rightarrow}a^\lambda\in<e>$$

$$\underset{<e>=\{e\}}{\Rightarrow}a^\lambda\in\{e\}\Rightarrow a^\lambda=e$$

أصبح لدينا $\left.\begin{array}{c} a^{\lambda}=e \\ and \\ a^{n}=e \text{ أي } O(a)=n \end{array}\right\} \underset{\text{استناداً للجزء الثاني من التمهيدية صـ 18 في المحاضرة السابقة}}{\Rightarrow}$ λ يقسم n

بما أن $b^{-\lambda} \in <b>$ فإن $\left(b^{-\lambda}\right)^{-1} \in <b>$ أي $b^{\lambda} \in <b>$.

بما أن $b^{-\lambda} \in <a>$ فإن $\left(b^{-\lambda}\right)^{-1} \in <a>$ أي $b^{\lambda} \in <a>$.

أيضاً لدينا $\left.\begin{array}{c} b^{\lambda} \in <a> \\ and \\ b^{\lambda} \in <b> \end{array}\right\} \Rightarrow b^{\lambda} \in <a> \cap <b> \underset{\text{بالاستفادة من الفرضية (3)}}{\Rightarrow} b^{\lambda} \in <e>$

$\underset{<e>=\{e\}}{\Rightarrow} b^{\lambda} \in \{e\} \Rightarrow b^{\lambda}=e$

أصبح لدينا $\left.\begin{array}{c} b^{\lambda}=e \\ and \\ b^{m}=e \text{ أي } O(b)=m \end{array}\right\} \underset{\text{استناداً للجزء الثاني من التمهيدية صـ 18 في المحاضرة السابقة}}{\Rightarrow}$ λ يقسم m

أصبح لدينا $\left.\begin{array}{c} \lambda \text{ يقسم } n \\ and \\ \lambda \text{ يقسم } m \end{array}\right\} \Rightarrow n, m$ مضاعف مُشترك للعددين λ

وبما أن k مُضاعف مُشترك أصغر للعددين n, m فإن k أصغر من أي مضاعف مشترك للعددين n, m أي

$$k \leq \lambda \quad \ldots **$$

من * و ** نجد أن $\lambda = k$ أي أن $O(a \cdot b) = Lcm(n, m)$. **وهو المطلوب.**

تمرين(2): لتكن G زمرة ، وليكن $a, b \in G$ عنصرين كيفيين ، ولنفرض أن $O(a)=n\ ,\ O(b)=m$.

فإذا كان $a \cdot b = b \cdot a$ ، وكان $gcd(n, m) = 1$ ، فإن

$$O(a \cdot b) = O(a).O(b)$$

البرهان: لنثبت أولاً أن $<a> \cap <b> = <e>$.

$$\underbrace{e \in <a>}_{\text{لأن <a> زمرة جزئية في } G} \quad and \quad \underbrace{e \in <b>}_{\text{لأن <b> زمرة جزئية في } G} \Rightarrow e \in <a> \cap <b> \Rightarrow$$

$$\{e\} \subseteq <a> \cap <b> \underset{\text{كون } <e>=\{e\}}{\Rightarrow} <e> \subseteq <a> \cap <b> \quad \ldots (1)$$

لنأخذ عنصر كيفي $x \in <a> \cap <b>$ وهذا يعني أن $x \in <a>$ وأن $x \in <b>$.

$$x \in < a > \underset{\text{استناداً لتعريف عناصر } <a>}{\Rightarrow} \exists\, s \in \mathbb{Z} \;:\; x = a^s$$

$$x \in < b > \underset{\text{استناداً لتعريف عناصر } <b>}{\Rightarrow} \exists\, t \in \mathbb{Z} \;:\; x = b^t$$

$$x = a^s \;\Rightarrow\; x^n = (a^s)^n \Rightarrow x^n = (a^n)^s \underset{O(a)=n \text{ لأن } a^n=e}{\Rightarrow} x^n = e^s \Rightarrow x^n = e$$

$$x = b^t \;\Rightarrow\; x^m = (b^t)^m \Rightarrow x^m = (b^m)^t \underset{O(b)=m \text{ لأن } b^m=e}{\Rightarrow} x^m = e^t \Rightarrow x^m = e$$

لنفرض أن $O(x) = k$.

$$\left.\begin{array}{l} m \text{ يقسم } k \\ n \text{ يقسم } k \end{array}\right\} \underset{\text{استناداً للجزء الثاني من التمهيدية صـ 18 في المحاضرة السابقة}}{\Rightarrow} \text{أصبح لدينا} \left\{\begin{array}{c} x^n = e \,,\; x^m = e \\ and \\ x^k = e \text{ أي } O(x) = k \end{array}\right.$$

من الأخيرة نستنتج أن k قاسم مشترك لـ n, m. لكن من الفرض لدينا $gcd(n,m) = 1$ أي أن القاسم المشترك **الأعظم** للعددين n, m هو الواحد مما يعني أن $k = 1$.

$$k = 1 \Rightarrow O(x) = 1 \Rightarrow x^1 = e \Rightarrow x = e \Rightarrow x \in \{e\}$$

أخذنا عنصر كيفي $x \in < a > \cap < b >$ و وجدنا أن $x \in \{e\}$ مما يعني أن

$$< a > \cap < b > \subseteq < e > \quad \ldots (2)$$

من (1) و (2) نحصل على:

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

$$\left.\begin{array}{l} O(a) = n \,,\; O(b) = m \text{ فرضاً} \\ a \cdot b = b \cdot a \text{ فرضاً} \\ < e > = < a > \cap < b > \text{ برهاناً} \end{array}\right\} \underset{\text{بحسب التمرين السابق}}{\Rightarrow} \text{أصبح لدينا} \quad O(a \cdot b) = Lcm(n,m)$$

لكن:

$$Lcm(n,m) = \frac{n.m}{gcd(n,m)} \underset{gcd(n,m)=1 \text{ فرضاً}}{\Rightarrow} Lcm(n,m) = n.m$$

بالعودة نجد أن:

$$O(a \cdot b) = n.m = O(a).O(b)$$

وهو المطلوب.

انتهت المحاضرة العاشرة