المحاضرة العاشرة :

• **برهنة** : لتكن G زمرة دوارة منتهية مولدة بالعنصر a مرتبتها n عندئذٍ الشروط التالية متكافئة :

1) $G = \langle a^k \rangle$ حيث : $k \in \mathbb{Z}$

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

الإثبات :

«1 ← 2» : لنفرض أنّ : $G = \langle a^k \rangle$ حيث : $k \in \mathbb{Z}$ ولنفرض جدلاً أنّ $gcd(n,k) = d > 1$ «نرى أنّ d هو القاسم المشترك الأعظم لـ : n, k».

• ومنه يوجد $s, t \in \mathbb{Z}$ بحيث : $n = d \cdot s \; , \; k = d \cdot t$

• لنفرض أنّ : $o(a^k) = m$ عندئذٍ :

$$(a^k)^s = (a^{d \cdot t})^s = a^{d \cdot s \cdot t} = (a^{d \cdot s})^t = (a^n)^t = (e)^t = e$$

«إنّ : $a^n = e$ لأنّ : G زمرة دوارة منتهية مولدة بالعنصر a ومرتبتها n».

$$m \leq s < n$$

• هذا يبين أنّ عدد عناصر الزمرة G يساوي s.

• لكن : $s < n$ «لأنّ s قاسم $\neq n$».

• ومنه نجد أنّ : a^k ليس مولد للزمرة G «مرتبتها n»

• وهذا يناقض الفرض ، وبالتالي الفرض الجدلي خاطئ ومنه :

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

«1 ⇐ 2» :

• لنفرض أنّ : $gcd(n,k) = 1$ عندئذٍ يوجد : $m, t \in \mathbb{Z}$ بحيث :

$$1 = n \cdot m + k \cdot t$$

$$a = a^{nm + k \cdot t} = a^{n \cdot m} \cdot a^{k \cdot t} = (a^n)^m \cdot (a^k)^t$$

$$= (e)^m \cdot (a^k)^t = (a^k)^t$$

$$\Rightarrow a = a^{k \cdot t} \Rightarrow a \in \langle a^k \rangle$$

$$\Rightarrow \forall x \in G : x = a = (a^k)^t \in \langle a^k \rangle$$

$$\Rightarrow G \subseteq \langle a^k \rangle \subseteq G \Rightarrow G = \langle a^k \rangle$$

مثال توضيحي من فارغ المحاضرة عن البرهنة: لتكن الزمرة: $U(10)=\{1,3,7,9\}$

نعلم أنّ $U(10)$ زمرة دوارة وبأنّ العنصر $3 \in U(10)$ مولّد للزمرة أي أنّ:

$$U(10) = \langle 3 \rangle$$

نستطيع مباشرة أن نستنتج من البرهنة السابقة أنّ: $U(10) = \langle 3^3 \rangle$ أي أنّ:

$7 \in U(10)$ مولّد للزمرة وذلك لأنّ: $gcd(9, 3) = 1$ أي أنّ: 9, 3 أوليان فيما بينهما

ونجد مباشرة أن: $U(10) = \langle 3^3 \rangle = \langle 7 \rangle$

أي أننا برهنا أن $7 \in U(10)$ مولّد لهذه الزمرة.

نتيجة: ليكن: $n \geq 1$ عدد صحيح عندئذٍ العنصر $K \in \mathbb{Z}_n$ تحقق: $\mathbb{Z}_n = \langle K \rangle$ إذا وفقط إذا كان: n, K أوليان فيما بينهما، مثلاً: $\mathbb{Z}_{10} = \{0,1,\dots,9\}$ سوف يكون:

$$\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$$

برهنة: كل زمرة جزئية من زمرة دوارة تكون أيضاً دوارة.

الإثبات:

لتكن: $G = \langle a \rangle$ زمرة دوارة حيث: $a \in G$

ولتكن: H زمرة جزئية في G عندئذٍ نميز حالتين:

- إذا كانت: $H = \{e\}$ عندئذٍ يكون: $H = \langle e \rangle$ - يتم المطلوب -
- إذا كانت: $H \neq \{e\}$ عندئذٍ يوجد $x \in H$ حيث: $x \neq e$

إنّ: $x \in G$, $G = \langle a \rangle$ ومنه يوجد $K \in \mathbb{Z}$ حيث:

$$x = a^K$$

لنأخذ المجموعة:

$$T = \{K : K \in \mathbb{N}^* \; ; \; a^K \in H\}$$

إنّ: $T \neq \emptyset$ لأنّ: $x = a^K \in H$, وبالتالي: $K \in T$

ومنه يوجد في T عنصر أصغر وليكن m ومنه:

$$a^m \in H \Longrightarrow \boxed{\langle a^m \rangle \subseteq H}$$

ولنثبت الآن الحد متراي المعاكس.

ليكن: $y \in H$ عندئذٍ: $y = a^s$ حيث $s \in \mathbb{Z}$.

وبحسب خوارزمية القسمة لعددين: s, m فإنّه:

يوجد $q, r \in \mathbb{Z}$ حيث: $s = m.q + r$

وأنّ: $0 \leq r < m$

إذا كان: $r = 0$ يتم المطلوب لذلك نفرض جدلاً أنّ: $r \neq 0$

ومنه:

$$a^s = a^{mq+r} = a^{m.q} . a^r = (a^m)^q . a^r$$

$$\Rightarrow a^r = \underbrace{[(a^m)^q]^{-1}}_{\in H} . \underbrace{a^s}_{\in H} \Rightarrow a^r \in H$$

$a^r \in H$. ولكن: $a^m \in H$ ، m هو العنصر الأصغري T

ومنه: $a^r \notin H$ والفرض الجدلي خاطئ، ومنه: $r = 0$

ومنه: $s = q . m$

$$y = a^s = a^{q.m} = (a^m)^q \in \langle a^m \rangle \Rightarrow y \in \langle a^m \rangle$$

ومنه: $\boxed{H \subseteq \langle a^m \rangle}$

ومن الاحتواءين: $H = \langle a^m \rangle$

برهنة: لتكن: $G = \langle a \rangle$ زمرة دوارة منتهية حيث: $a \in G$ ورتبتها n عندئذٍ:

1) إذا كانت H زمرة جزئية في G رتبتها k فإنّ k يقسم n.

2) إذا كان العدد $k \in \mathbb{Z}^+$ يقسم n عندئذٍ توجد زمرة جزئية واحدة فقط في G مرتبتها k هي: $\langle a^{\frac{n}{k}} \rangle$

الإثبات:

1) بما أنّ الزمرة G منتهية فحسب نتيجة كل زمرة جزئية في G تقسم مرتبة الزمرة الأصلية G.

2) لتكن: $G=\langle a\rangle$ ، $(G:1)=n$.

لدينا: $(a^{\frac{n}{k}})^k = a^n = e$. وحسب الفرض فإنّ: k يقسم n ، ومنه: $\frac{n}{k}\in\mathbb{Z}$.

ومنه: أيّاً كان: $t<k$ فإنّ: $(a^{\frac{n}{k}})^t \neq e$.

لتكن الزمرة الجزئية H في G رتبتها k. ولبرهن أنّ:

$$H=\langle a^{\frac{n}{k}}\rangle$$

وبحسب البرهنة السابقة فإنّ:

الزمرة H دوارة وإنّ: $H=\langle a^m\rangle^z$

وحسب خوارزمية القسمة لعددين n , m يوجد $q,r\in\mathbb{Z}$ بحيث:

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

لنفرض جدلاً أنّ $r\neq 0$ عندئذٍ $0<r<m$.

$$a^n = a^{qm+r} = a^{q.m}.a^r \Rightarrow e = a^{q.m}.a^r$$

$$\Rightarrow a^r = [a^{q.m}]^{-1} \in H$$

وهذا يناقض كون: $H=\langle a^m\rangle$. ومنه الفرض الجدلي خاطئ.

ويكون: $r=0$

ومنه: $n=q.m$

ومنه: $\frac{n}{m}\in\mathbb{Z}$ «وهذا يعني أنّ m يقسم n»

$$K=(H:1)=(\langle a^{\frac{n}{k}}\rangle:1)=(\langle a^m\rangle:1)$$
$$=o(a^m)$$
$$=\frac{n}{m}$$

$(a^m)^{\frac{n}{m}}=a^n=e$ لأنّ:

$\Rightarrow o(a^m)=\frac{n}{m}$

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

$$\Rightarrow H=\langle a^m\rangle=\langle a^{\frac{n}{k}}\rangle$$

مبرهنة: كل زمرة منتهية مرتبتها عدد أولي تكون زمرة دوارة.

البرهان:

لنفرض أنّ G زمرة منتهية، وأنّ: $P = (G:1)$ حيث: P عدد أولي "هذه الزمرة تحوي على الأقل عنصرين"

ليكن: $x \in G$ بحيث: $x \neq e$ ومنه: $\langle x \rangle$ زمرة جزئية في G

فإنّ: $(\langle x \rangle : 1) > 1$ لأنّ: $x \neq e$

وحسب مبرهنة لاغرانج:

$$(G:1) = (G:\langle x \rangle).(\langle x \rangle : 1)$$

$$P = (G:\langle x \rangle).\underbrace{(\langle x \rangle : 1)}_{(\langle x \rangle : 1) > 1}$$

$$\Rightarrow (\langle x \rangle : 1) = P \Rightarrow G = \langle x \rangle$$

تمرين: لتكن: G زمرة، $a, b \in G$ ولنفرض أنّ: $o(a)=n, o(b)=m$

عندئذٍ:

- إذا كان: $a.b=b.a$ ، وكان: $\langle e \rangle = \langle a \rangle \wedge \langle b \rangle$

فإنّ: $Icm(n,m) = o(a.b)$

البرهان:

- من الفرض نجد أنّ: n , m كلاهما موجب فالمضاعف موجود

لنفرض أنّ: $K = Icm(n,m)$

- ومنه حسب تعريف المضاعف يوجد $s,t \in \mathbb{Z}$ بحيث:

$$K = s.n \ , \ K = t.m$$

$$(a.b)^K = \underbrace{(a.b).(a.b).\dots.(a.b)}_{K \text{ مرة}} = a^K.b^K$$

$$\overset{a.b=b.a}{=} a^{s.n}.b^{t.m}$$

$$\Rightarrow (a.b)^K = (a^n)^s.(b^m)^t = e$$

- لنفرض أنّ: $\lambda = o(a.b)$ ومنه يكون: $(a.b)^\lambda = e$

ويكون: $\boxed{\lambda \leq K}$ ... (1)

وبالتالي:

$$(a.b)^\lambda = a^\lambda . b^\lambda$$

$$\Rightarrow e = a^\lambda . b^\lambda$$

$$\Rightarrow a^\lambda = b^{-\lambda} \in \langle a \rangle \cap \langle b \rangle = \langle e \rangle$$

$$\Rightarrow \underbrace{a^\lambda = e}_{\text{لأن } \lambda \text{ يقسم } n} \quad , \quad \underbrace{b^\lambda = e}_{\text{لأن } \lambda \text{ يقسم } m}$$

لأن: n مرتبة العنصر a — لأن: m مرتبة العنصر b

• وهذا يبين لنا أن: λ مضاعف مشترك للعددين: n, m

• وبما أن: $K = Icm(n,m)$ أي K هو المضاعف المشترك الأصغر لـ: n, m

فإن: $\boxed{\lambda \leq K}$ ... (2).

من (1) و (2): $\boxed{\lambda = K}$ $\quad K = Icm(n,m)$, $\lambda = o(a.b)$

ومنه: $Icm(n,m) = o(a.b)$

تمهيدية: لتكن G زمرة، $a, b \in G$ ولنفرض أن: $o(a)=n, o(b)=m$:

وإذا كان: $a.b = b.a$ وكان: $gcd(n,m) = 1$

فإن: $o(a.b) = o(a).o(b)$ $\wedge$ $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$

البرهان:

• ليكن: $y \in \langle a \rangle \cap \langle b \rangle$: عندئذٍ $(y \in \langle a \rangle \wedge y \in \langle b \rangle)$ أي:

$$\exists \beta, \delta \in \mathbb{Z} \; ; \; y = a^\beta , \; y = b^\delta$$

• لنفرض أن: $o(y) = s$ ومنه: $y^s = e$

• لكن وحسب مبرهنة سابقة فإن: s يقسم كل من: m, n

ومنه: $y^m = y^n = e$

• وبما أن: $gcd(n,m) = 1$ فإن: $s = 1$

« أي بما أن: n, m أوليان فيما بينهما وبما أن s يقسم كل من n, m فإن: $s = 1$ »

لأن n يقسم n إذن: $y \in \langle a \rangle$ و $o(y) = s$ إذن: $o(a) = n$

ومنه: $y = e$

ومنه: $\{<a> \cap <b> = <e>\}$

وحسب المبرهنة السابقة فإنّ:

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

الدرس المحاضرة (15)

ملاحظة: توجد الكثير من الأمثلة المفيدة عن هذه المحاضرة في المحاضرات عملي (4 + 3).