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

الإثبات :

لنفرض أنّ G زمرة منتهية وأنّ $(G:1) = p$ 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 فإنّ :

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

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

تمهيدية :

لتكن G زمرة منتهية مرتبتها n , عندئذٍ القضايا التالية صحيحة :

1 - أياً كان $a \in G$ فإنّ $a^n = e$.

2 - أياً كان $a \in G$, $0(a) = k$ عندئذٍ فإنّ k يقسم n .

الإثبات :

ليكن G زمرة منتهية مرتبتها n :

1- إذا كان $a = e \Leftarrow e^n = e$

لنفرض أنّ $a \neq e$, لنأخذ الزمرة الجزئية $H = \langle a \rangle$ ولنفرض أنّ $(H:1) = m$ عندئذٍ حسب لاغرانج فإنّ m يقسم n

ومنه يوجد $k \in \mathbb{Z}$ بحيث : $n = m \cdot k$

$$m = (H:1) = 0(a)$$

$$a^n = a^{m \cdot k} = (a^m)^k = e^k = e$$

2 - لنفرض أنّ $0(a) = k$ ولنأخذ الزمرة $H = \langle a \rangle$, عندئذٍ: $(H:1) = 0(a) = k$

وحسب لاغرانج يكون k يقسم n .

تمرين : لتكون G زمرة , $a, b \in G$ ولنفرض أنّ $0(a) = n \;\; , \;\; 0(b) = m$
إذا كان $a \cdot b = b \cdot a$ وكان $e = \langle a \rangle \cap \langle b \rangle$ عندئذٍ :

$$0(a \cdot b) = Icm(n, m)$$

الحل : بالفرض n, m كلاهما موجب فالمضاعف موجود , لنفرض أنّ $k = Icm(n, m)$ ومنه حسب تعريف المضاعف يوجد $s, t \in \mathbb{Z}$ بحيث :

$$k = s \cdot n \quad , \quad k = t \cdot m$$

$$(a \cdot b)^k = (a \cdot b) \underbrace{(a \cdot b) \ldots (a \cdot b}_{\text{مرة } k} \underbrace{)= a^k \cdot b^k}_{a \cdot b = b \cdot a}$$

$$= a^{s \cdot n} \cdot b^{t \cdot m} = (a^n)^s \cdot (b^m)^t = e$$

لنفرض أنّ $\lambda = 0(a \cdot b)$ ومنه يكون $(a \cdot b)^\lambda = e$

ومنه يكون $\lambda \leq k \;\; \ldots (1)$

$$(a \cdot b)^\lambda = a^\lambda \cdot b^\lambda = e$$

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

ومنه : $\underbrace{b^\lambda = e}_{\lambda \text{ يقسم } m} \quad , \quad \underbrace{a^\lambda = e}_{\lambda \text{ يقسم } n}$ ومنه فإنّ $\lambda \geq k \;\; \ldots (2)$ ومن $(1), (2)$ يكون $\lambda = k$

تمرين : لتكن G زمرة , $a, b \in G$ وَ $0(a) = n \;\; , \;\; 0(b) = m$
إذا كان $a \cdot b = b \cdot a$ وأنّ $gcd(n, m) = 1$ عندئذٍ :

$$\langle a \rangle \cap \langle b \rangle = e \quad \wedge \quad 0(a \cdot b) = n \cdot m$$

الحل : ليكن $y \in \langle a \rangle \cap \langle b \rangle$ عندئذٍ :

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

لنفرض :

$0(y) = s$ ومنه $y^s = e$ ((حسب مبرهنة فإنّ s يقسم كل من n, m)) ومنه $y^m = y^n = e$

حسب الفرض $s = 1$ وبالتالي $y = e$ ومنه $\langle a \rangle \cap \langle b \rangle = e$

وحسب التمرين السابق :

$$0(a \cdot b) = Icm(n, m) = m \cdot n$$

تمرين : لتكن G زمرة تبديلية تحوي عنصرين مرتبة كل منهما 2
أثبت أنّ G تحوي زمرة جزئية مرتبتها 4 .

الحل : ليكن $a, b \in G$ وَ $0(a) = 2 \quad , \quad 0(b) = 2$

$$a^2 = b^2 = e$$

ولنأخذ المجموعة $H = \{e, a, b, a \cdot b\}$ فنجد :

	e	a	b	$a \cdot b$
e	e	a	b	$a \cdot b$
a	a	$a^2 = e$	$a \cdot b$	b
b	b	$a \cdot b$	$b^2 = e$	a
$a \cdot b$	$a \cdot b$	b	a	e

H زمرة جزئية في G وذلك لأنّ
$\forall\, a, b \in H \;\; ; \;\; a \cdot b \in H$
وذلك كونً H منتهية

تمرين : لتكن G زمرة , $a, b \in G$ بحيث $a \cdot b = b \cdot a$ ولنفرض أنّ
$0(a) = n \quad , \quad 0(b) = m$, إذا كان $gcd(n, m) = 1$ عندئذٍ :

$$\langle a \cdot b \rangle = \langle a, b \rangle = \{\, a^i \cdot b^j \quad 0 \le i < n \ , \ 0 \le j < m \,\}$$

الحل :

لنبرهن أولاً أنّ $\langle a \cdot b \rangle = \langle a, b \rangle$

لدينا $a, b \in \langle a, b \rangle$ ومنه $a \cdot b \in \langle a, b \rangle \Longleftarrow \langle a \cdot b \rangle \subseteq \langle a, b \rangle$

من جهة أخرى بما أنّ $gcd(n, m) = 1$ يوجد $s, t \in \mathbb{Z}$ بحيث :

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

$$a^1 = a^{s \cdot n + t \cdot m} = a^{s \cdot n} \cdot a^{t \cdot m} = a^{t \cdot m} = a^{t \cdot m} \cdot (b^m)^t = (a \cdot b)^{t \cdot m} \in \langle a \cdot b \rangle$$

$$b^1 = b^{s \cdot n + t \cdot m} = b^{s \cdot n} \cdot b^{t \cdot m} = b^{s \cdot n} = b^{s \cdot n} \cdot (a^n)^s = (a \cdot b)^{s \cdot n} \in \langle a \cdot b \rangle$$

أصبح لدينا $a, b \in \langle a \cdot b \rangle \Longleftarrow \langle a, b \rangle \subseteq \langle a \cdot b \rangle$ ومن الاحتوائين يكون $\langle a \cdot b \rangle = \langle a, b \rangle$

$$\langle a \cdot b \rangle = \{\, (a \cdot b)^k \quad k \in \mathbb{Z} \,\}$$

$$(a \cdot b)^k = a^k \cdot b^k \qquad 0 \le k < n \ , \ 0 \le k < m$$

الـزمرة الجزئيـة الناظميـة

تعريف :

لتكن G زمرة و H زمرة جزئية في G , نقول عن الزمرة الجزئية H إنها ناظمية في G إذا حققت الشرط :

$$\forall\, a \in G \quad ; \quad a \cdot H = H \cdot a$$

مبرهنة :

لتكن G زمرة و H زمرة جزئية في G , الشروط التالية متكافئة :

1 - الزمرة الجزئية H ناظمية في G .

2 - $\forall\, a \in G \quad ; \quad a \cdot H \cdot a^{-1} \subseteq H$

3 - $\forall\, a \in G \quad ; \quad a^{-1} \cdot H \cdot a \subseteq H$

الإثبات : $(1 \Longrightarrow 2)$: لنفرض أنّ الزمرة الجزئية H ناظمية في G عندئذٍ :

$$a \cdot H = H \cdot a \quad \forall\, a \in G$$

ليكن $x \in a \cdot H \cdot a^{-1}$ عندئذٍ يوجد $h \in H$ بحيث يحقق : $x = a \cdot h \cdot a^{-1}$

لدينا $a \cdot h \in a \cdot H = H \cdot a$ ومنه يوجد $h_1 \in H$ بحيث $a \cdot h = h_1 \cdot a$

$$x = a \cdot h \cdot a^{-1} = h_1 \cdot a \cdot a^{-1} = h_1 \cdot e = h_1 \in H \Longrightarrow a \cdot H \cdot a^{-1} \subseteq H$$

$(2 \Longrightarrow 3)$: ليكن $y \in a^{-1} \cdot H \cdot a$ عندئذٍ يوجد $h \in H$ بحيث يحقق : $y = a^{-1} \cdot h \cdot a$

$$= a^{-1} \cdot h \cdot (a^{-1})^{-1} = b \cdot h \cdot b^{-1} \in H \Longrightarrow a^{-1} \cdot H \cdot a \subseteq H$$

$(3 \Longrightarrow 1)$: ليكن $\mu \in a \cdot H$ عندئذٍ يوجد $h_1 \in H$ بحيث يحقق : $\mu = a \cdot h_1$

$$\mu = a \cdot h_1 \cdot e = (a \cdot h_1 \cdot a^{-1}) \cdot a = [(a^{-1})^{-1} \cdot h_1 \cdot a^{-1}] \cdot a$$

$$= [b^{-1} \cdot h_1 \cdot b] \cdot a \in H \cdot a \Longrightarrow a \cdot H \subseteq H \cdot a$$

ليكن $\lambda \in H \cdot a$ عندئذٍ يوجد $h_2 \in H$ بحيث يحقق : $\lambda = h_2 \cdot a$

$$\lambda = e \cdot h_2 \cdot a = a(a^{-1} \cdot h_2 \cdot a) \in a \cdot H \Longrightarrow H \cdot a \subseteq a \cdot H$$

ومن الاحتوائين $H \cdot a \subseteq a \cdot H \;,\; a \cdot H \subseteq H \cdot a$ يكون $a \cdot H = H \cdot a$.

... انتهت المحاضرة ...