المحاضرة الخامسة :

تعريف: لتكن $(G,.)$ زمرة ما يُقال أنه $g \in G$ له دور منتهي ويساوي n إذا كان $g^n = e_G$

ويُقال $|g| = o(g) = n$

نتيجة: لتكن $(G,.)$ زمرة و $g \in G$ بحيث $|g| = o(g) = n$ فإن $|\langle g \rangle| = n$

مثال: في $((\mathbb{Z}/4\mathbb{Z})^*,.)$ أوجد دور العنصر $[2]$.

$[2^1] = [2]$, $[2^2] = [0]$, $[2^3] = [0]$

~~إذن $[2]$ ليس لها دور منتهي~~

$[2] \notin (\mathbb{Z}/4\mathbb{Z})^*$

أوجد دور العنصر $[3]$.

$[3]^2 = [9] = [1] \Rightarrow |[3]| = 2$

أوجد $\langle [3] \rangle$: $\langle [3] \rangle = \{ g^k ; k \in \mathbb{Z} \}$

$\langle [3] \rangle = \{[1],[3]\}$

$|\langle [3] \rangle| = |[3]| = 2$

مثال: $((\mathbb{Z}/5\mathbb{Z})^*,.)$ أوجد دور $[4]$, أوجد الزمرة $\langle [4] \rangle$.

$[4]^1 = 4$, $[4]^2 = [16] = [1]$

$|[4]| = 2$

$\langle [4] \rangle = \{[1],[4]\}$

مثال: $(\mathbb{Z}/5\mathbb{Z}_{+})$ أوجد دور $[4]$ ثم أوجد $\langle [4] \rangle$.

$k.[4] = \overset{\text{محايد}}{0}_{(\mathbb{Z}/5\mathbb{Z}_{+})} \Rightarrow 5[4] = [20] = [0] \Rightarrow |[4]| = 5$

$\Rightarrow |\langle 4 \rangle| = 5$

$\langle 4 \rangle = \{0,1,2,3,4\}$

مبرهنة: لتكن $G = \langle g \rangle$ زمرة دوارة و لتكن H زمرة جزئية منها عندها يوجد $k \in N$ بحيث $H = \langle g^k \rangle$ إذا كانت $|G| = n$ فإن : $|H| = n/L$

حيث : $L = \gcd(n,k)$

مثال: بفرض $G=\langle g\rangle$ حيث $|G|=24$.

- لتكن $H=\langle g^{15}\rangle$ ما هو عدد عناصر H

$$|H|=\frac{24}{\gcd(24,15)}=\frac{24}{3}=8$$

- أوجد H.

$$H=\langle g^{15}\rangle=?$$

$$H=\{(g^{15})^0,(g^{15})^1,\dots(g^{15})^7\}$$

مبرهنة: لتكن $G=\langle g\rangle$ زمرة دورية فإن:

1) g له دور غير منتهي عندها $G\cong(\mathbb{Z},+)$

2) في حال g منتهية الدور حيث $o(g)=|g|=n$ عندها: $G\cong(\mathbb{Z}/n\mathbb{Z},+)$

$$f:(G,*)\longrightarrow(H,\#)$$

f تشاكل زمرات إذا كان: $f(x*y)=f(x)\#f(y)$

المحاضرة السابعة:

تعريف: ليكن $G_n=\langle x\rangle=\{e,x,\dots,x^{n-1}\}$ معرف عليها العملية $x^i\,x^j=x^k$ حيث $i+j\equiv k\pmod n$. إن $(C_n,\cdot)$ تشكل زمرة.

مثال: أثبت أنه $(C_3,\cdot)$ زمرة باستخدام جدول كيلي.

	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

1) مغلقة بالنسبة للقانون.

2) يوجد حيادي وهو $x^0=e$

3) نظير العناصر:

$$x^{-1}=x^2$$

$$(x^2)^{-1}=x$$

تعريف: دور العنصر (رتبة العنصر):

$g \in G$ هو أصغر عدد صحيح موجب n بحيث $g^n = e_G$ حيادي

نرمز له: $o(g) = |g| = n$

نتائج: 1) $|g| = 1 \Leftrightarrow \langle g \rangle = \{e_G\}$ إذا كان

2) ليكن π تبديل: هو جداء r حلقة π_i حيث طول كل منها k_i عناصرها:

$$|\pi| = o(\pi) = Lcm\{k_i : 1 \le i \le r\}$$

مثال: 1

$$|(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)(11\ 12 \dots 18)|$$

$$|\pi| = Lcm(10, 8) = 40$$

$$\langle \pi \rangle = \{\pi^0, \pi^1, \pi^2, \dots, \pi^{39}\}$$

$$|\langle \pi \rangle| = |\pi| = 40$$

2

$$\sigma = (1\ 3\ 4)(2\ 5)$$

$$|\sigma| = Lcm(3, 2) = 6$$

$$\sigma^6 = id$$

3

$$\delta = (1\ 3\ 4)(2\ 4\ 5)$$

δ تركيب تبديلين (لوجود عناصر مشتركة بين الحلقات).

$$\delta = (1\ 3\ 4\ 5\ 2)$$

$$|\delta| = 5$$

أوجد $\langle \delta \rangle$.

- لتكن H و G زمرتان فإن:

1) $|G \times H| = |G| \cdot |H|$

$(g, h) \in G \times H$

رتبة العنصر (g,h): $|(g,h)| = Lcm\{|g|, |h|\}$

$((\mathbb{Z}/3\mathbb{Z})^*, \cdot)$

G

$|[2]| = 2$

$(S_5, \cdot) = (S_5, \circ)$ ← رمز تركيب التوابع

$\sigma = (1\ 3\ 4)(2\ 5)$

$|\sigma| = 6$

$([2], \sigma) \in G \times H$

$|([2], \sigma)| = \text{lcm}\{2, 6\} = 6$ ← المعادلة

(e_G, e_H) هو $G \times H$ حيادي

$(e_G, e_H) = ([1], id = (1)(2)(3)(4)(5))$

2016 / 4 / 12

7.4

بعض الخواص: نظرية: لتكن a و b عددين غير صفرين عندها

1) $gcd(a,b) = gcd(a, b+ka) \quad \forall k \in \mathbb{Z}$

2) $gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = 1$

إن $gcd(a,b)$ هو أصغر عدد يكتب كتركيب خطي بدلالة a و b

مجموعة كل التركيبات الخطية للعددين a, b هي مجموعة مضاعفات $gcd(a,b)$

$ax + by = $ عدد $\{ gcd(a,b)$ مضاعفات

تمارين: أوجد العدد الصحيح $k \geq 1$ الذي يجعل

$gcd(2k+3, 5k+4) = 1$

$= gcd(a, b-2a)$ (حسب خاصية)*

$= gcd\left(\underbrace{2k+3}_{a}, \underbrace{5k+4-4k-6}_{b}\right)$ لكل $k-2$

$= gcd(a-2b, b)$

$= gcd(2k+3-2k+4, k-2)$

$= gcd(7, k-2) = 1$

أي 7 و $k-2$ أوليان فيما بينهما (أو في مجموعتهما كل العوامل الأولية صغيرة)

$\Rightarrow k-2 \not\equiv 0 \pmod 7$

$k \not\equiv 2 \pmod 7$

$\Rightarrow k \in \mathbb{Z} / [2] \in (\mathbb{Z}/7\mathbb{Z})$

جميع الأعداد من $\mathbb{Z}$ حيث باقي قسمتها على 7 لا يساوي 2

تمرين: ليكن $a \in \mathbb{Z}$ ، $m, n \in \mathbb{N}$ بين أن:

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$$

خوارزمية أقليدس لإيجاد القاسم المشترك الأكبر:

ليكن $a, b \in \mathbb{Z}$ حيث $a \geq b > 0$

$$r_0 = a \ , \ r_1 = b$$

$$r_0 = q_1 r_1 + r_2 \quad ;$$

باقي قسمة r_0 على r_1

$$r_1 = q_2 r_2 + r_3$$

$$\vdots$$

$$r_{n-1} = q_n r_n$$

$\gcd(a,b)$ ← آخر باقي غير معدوم.

مثال:

$$r_0 = a - q$$

$$r_0 = 9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$$\Rightarrow 3 = \gcd(9, 6)$$

الملهم من خوارزمية السابقة:

لكتابة $\gcd(a,b)$ كتركيب خطي بدلالة a و b نستخدم عكس خوارزمية أقليدس

$$3 = \gcd(a,b) = 9 - 1 \cdot 6 = \underset{1}{x} \cdot a + \underset{-1}{y} b$$

عکس اقلیدس:

$$\gcd(a,b) = r_n = r_{n-2} - q_{n-1} r_{n-1}$$
$$= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2})$$
$$= \vdots$$
$$\Rightarrow \gcd(a,b) = x r_0 + y r_1$$

مثال آخر:

$$a = 102, \quad b = 26$$
$$102 = 3 \cdot 26 + 24$$
$$26 = 1 \cdot 24 + 2$$
$$24 = 12 \cdot 2 + 0$$
$$2 = \gcd(102, 26) = 26 - 24$$
$$= 26 - (102 - 3 \cdot 26)$$
$$= -102 + 4 \cdot 26$$
$$\Rightarrow \gcd(a,b) = xa + yb$$
$$= -1a + 4b$$