كلية العلوم

القسم : **الرياضيات**

السنة : **الثانية**

المادة : بنى جبرية2

المحاضرة : الثانية/نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

تابع أولر: التابع

$$\phi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$$\phi(n) = \begin{cases} 1 & ; \quad n = 1 \\ S & ; \quad n \neq 1 \end{cases}$$

حيث S هو عدد الاعداد الصحيحة الموجبة الأصغر تماماً من n و أولية مع العدد n أي:

$$S = \left| \{ x ; \ 1 \leq x < n \ \& \ \gcd(x,n) = 1 \} \right|$$

مثال: احسب $\phi(4)$

$$\phi(4) = \left| \{ x ; \ 1 \leq x < 4 , \gcd(x,4) = 1 \} \right|$$
$$= \left| \{ 1, 3 \} \right| = 2$$

خواص دالة أولر:

1) $\forall n, m \in \mathbb{Z}^+ , \gcd(n,m) = 1$

n , m أوليات فيما بينهما ; $\phi(n.m) = \phi(n) . \phi(m)$

2) إذا كان P عدد أولي:

$$\phi(P) = P - 1$$

3) إذا كان P عدد اولي و $t \in \mathbb{Z}^+$ عندئذٍ

$$\phi(p^t) = p^{t-1} (P-1)$$

4) إذا كان $n = P_1^{t_1} \, P_2^{t_2} \cdots P_r^{t_r}$ حيث $P_1, P_2, \ldots, P_r$ اعداد اوليه

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{P_i} \right)$$

مثال: أوجد $\phi(15)$ و $\phi(120)$

ط1: $\phi(15) = \phi(3)\cdot\phi(5) = 2\times 4 = 8.$

ط2: $\phi(15) = 15\times(1-\frac{1}{3})(1-\frac{1}{5}) = 15\times(\frac{2}{3})\times(\frac{4}{5}) = 8$

ط1: $\phi(120) = \phi(2^3)\times\phi(3)\times\phi(5)$

$= 2^{3-1}\times(2-1)\times 2\times 4 = 4\times 2\times 4 = 32.$

ط2: $\phi(120) = 120\times(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 32.$

زمرة أولر (زمرة الواحدات):

ليكن n عدداً صحيحاً يحقق $n>1$ نعرّف على المجموعة

$U(n) = \{x ; 1\leq x<n \ \& \ gcd(x,n) = 1\}$

عملية ثنائية $\otimes_n$ عملية الضرب بالمقاس n

$\forall a,b\in U(n) : a\otimes_n b = \overline{ab} = r.$

حيث r هو باقي قسمة xy على العدد n.

تمّ الاثبات بأنّه $(U_n, \otimes_n)$ زمرة تبديلية منتهية

والحيادي هنا هو العدد 1 (بالنسبة الجبرية 1).

$|U(n)| = \phi(n).$

مثال: أوجد جدول كايلي للزمرة $(U(10), \otimes_{10})$ مبيناً ما هو معكوس (مقلوب) أي عنصر في الزمرة السابقة

$U(10) = \{x ; 1\leq x<10 ; gcd(x,10) = 1\}$

$= \{1,3,7,9\} = \phi(10) = 4.$

$|U(10)| = \phi(10) = \phi(2)\cdot\phi(5) = 4.$

الجدول:

$\otimes_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

العنصر	1	3	7	9
المقلوب	1	7	3	9

مثال: ما هي عناصر زمر أولر التالية

$(U(5), \otimes_5)$, $(U(11), \otimes_{11})$.

الحل:

$U(5) = \{1, 2, 3, 4\}$

$U(11) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

ملاحظة: إذا كان P عدد اولي عندئذٍ زمرة أولر

$U(P) = \{1, 2, 3, \dots, P-1\}$

مزودة بعملية الضرب بالمقاس P.

تعريف: لتكن $(G, *)$ زمرة ما وليكن $a \in G$ عندئذٍ نعرّف مرتبة العنصر a في G على أنها أصغر عدد صحيح موجب تماماً n من اجله $\boxed{a^n = e}$ حيث e هو الحيادي في الزمرة $(G, *)$.

- نقول عن العنصر a من G بأنه ذو مرتبة غير منتهية إذا كان $a^t \neq e \quad \forall t \in \mathbb{N}^* = \{1, 2, 3, \dots\}$ ونعبر عنه ذلك بـ $o(a) = \infty$.

ملاحظة: لإيجاد مرتبة عنصر ما a في الزمرة $(G, *)$ حيث e هو الحيادي في G نقوم بحساب متتالية الجداءات $a^1, a^2, a^3, \dots$ حتى نحصل على الحيادي e في G للاول مرة وفي هذه الحالة يكون الأس مساوياً لمرتبة العنصر a وإذا لم نحصل على الحيادي في G يكون العنصر a ذو مرتبة لانهائية.

مثال: لتكن لدينا الزمرة $(\mathbb{Z}_7, \oplus_7)$ زمرة الاعداد الصحيحة بالقياس 7.

المطلوب: اوجد رتبة $O(3)$

$\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

هنا الزمرة جمعية والحيادي فيها هو الصفر:

$n.a = 1.3 = 3 \neq 0 \; ; \; 2.3 = 3 \oplus_7 3 = 6 \neq 0$

$3.3 = 3 \oplus_7 3 \oplus_7 3 = 9 = 2 \neq 0$

$3.4 = 3 \oplus_7 3 \oplus_7 3 \oplus_7 3 = 12 = 5 \neq 0$

$5.3 = 1 \neq 0$

$6.3 = 4 \neq 0$

$7.3 = 0 \Rightarrow O(3) = 7$

مثال: لتكن لدينا الزمرة $(U(12), \otimes_{12})$ اوجد $O(7)$

$U(12) = \{x : 1 \leq x < 12 \; \& \; \gcd(x,12) = 1\}$
$= \{1, 5, 7, 11\}$

$7^1 = 7$

$7^2 = 7 \otimes_{12} 7 = 49 = 1 \Rightarrow O(7) = 2$

ومنه رتبة 7 تساوي 2.

ملاحظة:

لتكن لدينا الزمرة $(G, *)$ الحيادي فيها هو e عندئذٍ

1) $\forall a \in G : O(a) = O(a^{-1})$

2) إذا كانت $a \in G$ و $a^m = e$ عندئذٍ $O(a) / m$

3) $O(a^t) = \dfrac{O(a)}{\gcd(t, O(a))} \; ; \; t \in \mathbb{Z}^+$

ملاحظة: إذا كانت G زمرة منتهية و $|G|=n$ عندئذٍ
$a \in G$ ، $O(a) \mid n$

مثال: لتكن لدينا الزمرة الغير تبديلية

$$G=\left\{A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a,b,c,d \in \mathbb{R} \ \& \ \det(A)=1\right\}$$

بالنسبة لعملية جداء المصفوفات والمطلوب:

(1) أوجد $O(B)$ حيث $B=\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ وأوجد $O(B^{-1})$ ، $O(B^6)$

الحل:

الزمرة ضربية والحيادي فيها هو $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$B^1 = B \neq I$

$$B^2 = B \times B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \neq I$$

$$B^3 = B^2 \times B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$O(B)=3$ ، $O(B)=O(B^{-1})=3$

$$O(B^6) = \frac{O(B)}{\gcd(O(B),6)} = \frac{3}{\gcd(3,6)} = 1$$

تعريف: لتكن $(G,*)$ زمرة $H \subseteq G$ ، $H \neq \phi$ يُقال بأنّه H زمرة جزئية في الزمرة G إذا تحقق الشرط التالي

$\forall x,y\in H: x*y^{-1}\in H$

ملاحظة: إذا كانت $(G,*)$ زمرة منتهية $\phi \neq H\subseteq G$
فلإثبات أنه H زمرة جزئية في G يكفي أن نتحقق من الشرط

$\forall x,y\in H: x*y\in H$

مثال: لتكن $\mathbb{C}$ مجموعة الأعداد العقدية اثبت أن

$$H=\{a+bi \,;\, a,b\in\mathbb{R} \ \& \ a^2+b^2=1\}$$

زمرة جزئية في زمرة الأعداد العقدية بالنسبة لعملية ضرب الأعداد العقدية.

الحل:

$\forall x,y\in H \overset{?}{\Rightarrow} x.y^{-1}\in H$

$x=a+bi \;;\; a^2+b^2=1$

$y=c+di \;;\; c^2+d^2=1$

$$x.y^{-1}=\frac{a+bi}{c+di}=\cancel{(a+bi)(c-di)}$$

$$=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

$$=\underbrace{(ac+bd)}_{T_1}+\underbrace{(bc-ad)}_{T_2}i$$

$T_1^2+T_2^2=1.$

$$(ac+bd)^2+(bc-ad)^2=a^2c^2+\cancel{2acbd}+b^2d^2+b^2c^2-\cancel{2adbc}+a^2d^2$$

$$=a^2(c^2+d^2)+b^2(d^2+c^2)=a^2\times1+b^2\times1=a^2+b^2=1.$$

$$\Rightarrow T_1+T_2 i\in H \Rightarrow \phi\neq H\subseteq \mathbb{C}$$

ومنه H زمرة جزئية في زمرة الأعداد الحقيقية بالنسبة لعملية الضرب

مثال:

لتكن لدينا الزمرة $(U(n), \otimes_n)$ أثبت أنه

$U_k(n) = \{x \in U(n) ; \; k \mid (x-1)\}$

حيث k عدد صحيح موجب.

زمرة جزئية في $U(n)$

الحل:

$\forall a, b \in U_k(n) \overset{?}{\Longrightarrow} a.b^{-1} \in U_k(n)$

$a \in U(n)$ & $k \mid a-1$

$b \in U(n)$ & $k \mid b-1$.

$a-1 = q_1 k \Longrightarrow a = q_1 k + 1$

$b-1 = q_2 k \Longrightarrow b = q_2 k + 1$.

هنا زمرة منتهية

$a.b = (q_1 q_2 k + q_1 + q_2) k + 1$

$\Longrightarrow ab - 1 = q k \; ; \; q = q_1 q_2 k + q_1 + q_2 \Longrightarrow k \mid (ab-1)$

$\Leftarrow ab \in U_k(n)$

$ab \in U(n)$ بشرط k يقسم $ab - 1$

نستنتج مما سبق أنه $U_k(n)$ زمرة جزئية في الزمرة $U(n)$.

تمرين: أوجد الزمر التالية:

$U_4(20)$ ، $U_5(20)$

$U(20) = \{x : 1 \le x < 2 \ \& \ gcd(x,20) = 1\} = \{1,3,7,9,11,13,17,19\}$

$\phi(20) = \phi(4) \times \phi(5) = \phi(2^2) \times \phi(5) = 2 \times 4 = 8.$

$U_4(20) = \{x : 1 \le x < 20 \ \& \ gcd(x,20) = 1\} = \{1,9,13,17\}$

$U_5(20) = \{1,11\}.$

انتهت المحاضرة