مقدمة في

الجبْر المجرَّد

(العمليات الثنائية، الزمرة، الحلقة)

تأليـف

د. أمير عبد المجيد الخواجة
أستاذ مساعد في الرياضيات
كلية العلوم/ جامعة سرت

أ. محمـد محمد إدريس
محاضر في الرياضيات
كلية العلوم/ جامعة سرت

منشورات
جامعة سرت
سرت - الجماهيرية العظمى

مقدمة في

الجبر المجرد

(العمليات الثنائية، الزمرة، الحلقة)

تأليف

د. أمير عبد المجيد الخواجة

أستاذ مساعد في الرياضيات

كلية العلوم/ جامعة سرت

أ. محمد محمد إدريس

محاضر في الرياضيات

كلية العلوم/ جامعة سرت

منشورات

جامعة سرت

سرت – الجماهيرية العظمى

اسم الكتاب: مقدمة في الجبر المجرد (العمليات الثنائية، الزمرة، الحلقة)

تأليف: د. أمير عبد المجيد الخواجة – أ. محمد محمد إدريس

الطبعة الأولى: 2009

الترقيم الدولي: ردمك I.S.B.N.: 978-9959-891-06-8

رقم الإيداع: 994

[الوكالة الليبية للترقيم الدولي الموحد للكتاب]

دار الكتب الوطنية

بنغازي ـ ليبيا

هاتف: 9090509 - 9096379 - 9097074 61 (218+)

بريد مصور: 9097073 61 (218+)

البريد الإلكتروني: nat_lib_libya@hotmail.com

جامعة سرت

سرت/ الجماهيرية العظمى

ص. ب 674، سرت – ليبيا

هاتف: 5260363 -54 (218+)

فاكس: 5262152 -54 (218+)

البريد الإلكتروني: info@su.edu.ly

الموقع الإلكتروني: www.su.edu.ly

المحتـويات

المقدمة

الجبر المجرد كان ولا يزال مادة من أهم مواد الرياضيات الأساسية التي لا يخلو أي منهج لطلبة الرياضيات منها، وتزادا د الحاجة إليه يومًا بعد أخر ليس فقط لطلبة الرياضيات، وإنما لطلبة كليات العلوم، والتربية، و الهندسة ومعاهد المعلمين كذلك، والكثير من التخصصات الأخرى، ونتيجة للتطبيقات و الاستخدامات الواسعة التي يشكل الجبر المجرد أساسًا لها بالإضافة إلى كونه مادة رياضية تساهم في تطوير القدرة على التفكير و الإبداع .

هدفنا في تأليف هذا الكتاب هو تزويد الطالب بالمادة العلمية الأساسية التي يحتاجها في الجبر المجرد (I) في كليات العلوم و التربية ومعاهد المعلمين "السنة الثالثة" و بصفته مصدر عام في الرياضيات في موضوع الجبر المجرد لاستخدامه من قبل المتخصصين وطلبة الدراسات العليا، وقد تم عرض المادة العلمية فيه بطريقة تختلف عن بقية الكتب المتواجدة، حيث تم التطرق إلى النظام الجبري و العمليات الثنائية على هذا النظام بشكل مفصل ومبسط مما شكّل مدخلاً جيدًا إلى نظرية الزمرة والحلقة والمواضيع الأخرى في الجبر المجرد.

ولدراسة هذا الكتاب، يجب أن يكون الطالب على معرفة بأسس الرياضيات والجبر الخطي التي يجب أن يدرسها في السنتين الأولى والثانية خلال دراسته الجامعية.

يحتوى الكتاب على ثلاثة فصول هي :

الفصل الأول: تناول مفهوم النظام الجبري بصورة عامة ثم دراسة العملية الثنائية على هذا النظام الجبري، ودراسة خواص العملية الثنائية على النظام الجبري في التجميع والأبدال ثم وجود المحايد للنظام الجبري والنظير لكل عنصر في هذا النظام، ثم تطرقنا إلى الأنظمة الجبرية ذات العمليتين، حيث تمت دراسة مثل هذه الأنظمة في الفصل الثالث في نظرية الحلقة.

كما تناول الفصل الأول كذلك العلاقة بين النظام الجبري ذو العملية الثنائية ونظام أخر ذي عملية ثنائية ومتى تصبح هذه العلاقة تمثل تشاكل، وذكرنا أنواع التشاكل نسبة إلى نوع العلاقة (الدالة) بالإضافة إلى الأنظمة الجبرية المتشاكلة.

الفصل الثاني: وتضمن نظرية الزمرة، حيث تطرقنا في بداية الفصل تعريف عام للزمرة وبعض النظريات الخاصة بها ثم تطرقنا إلى زمرة التباديل والزمرة الجزئية والزمرة الدائرية و المجموعات المصاحبة للزمرة وكذلك تطرقنا إلى الزمرة الجزئية المتعامدة وزمرة العوامل معززة بالأمثلة والتمارين والنظريات، وفي البند الأخير تطرقنا على العلاقة بين زمرة وزمرة أخرى والتي تمثل هومورفيزم وتم تعريف نواة التشاكل ومدى التشاكل.

الفصل الثالث: وتضمن نظرية الحلقة، حيث في بداية الفصل تم استعراض بعض التمارين و النظريات للحلقة ثم تناولنا الحلقة الجزئية ومن ثم تطرقنا إلى المثاليات و حلقات متعدد حدود و في البند الأخير أشرنا إلى التشاكل أي العلاقة بين حلقتين و تم الإشارة إلى أنواع التشاكل وفي نهاية كل فصل وضعت تمارين عامة وشاملة حول بنود فصل.

ختامًا... نتمنى أن يكون قد وفقنا في تقديم ما يخدم المسيرة العلمية لامتنا العربية.

والله الموفق،

المؤلفان

د. أمير عبد المجيد الخواجة

أ . محمد محمد إدريس

الفصل الأول

العمليات الثنائية Binary Operations

[1-1] العمليات الثنائية على مجموعة
Binary Operations on a Set

تعريف (1.1-1)

العملية الثنائية * على مجموعة G غير خالية هي دالة (راسم – تطبيق) نطاقها GXG ومداها G ، أي أن

$$* : G \times G \longrightarrow G$$
$$(a,b) \longrightarrow a*b$$

وللدلالة على العمليات الثنائية المختلفة نستخدم الرموز+ , × , o, ⊕ , ⊗،... إلخ.

ملاحظة (2.1-1)

من أشهر العمليات الثنائية هي عملية الجمع والطرح والـضرب والقـسمة على مجموعة الأعداد الحقيقة.

تعريف (3.1-1)

إذا كانت * عملية ثنائية على G فإننا نقول إن(G ,*) نظام جبري مغلق ذو عملية ، وأحيانًا نقول إن G مغلقة بالنسبة للعملية *.

مثال (1-1. 4)

(I) $(N , +)$ مجموعة الأعداد الطبيعية مع عملية الجمع تمثل نظامًا ذا عملية.

(II) $(N, -)$ ليس نظامًا ذا عملية ثنائية.

(III) $(N, \times)$ نظام ذا عملية ثنائية.

(IV) $(N , \div)$ ليس نظامًا ذا عملية ثنائية.

(V) $(Z , +)$ نظام ذا عملية ثنائية.

(VI) $(\Phi^{\bullet}, \div)$ مجموعة الأعداد النسبية ماعدا الصفر مع القسمة تمثل نظامًا ذا عملية ثنائية.

مثال (1-1. 5)

إذا كانت $G = \{0,1,2,3,4\}$ فإن عملية الجمع و الضرب ليستا عمليتـــين ثنائيتين على G , كمثال

$2+3 =5 \notin G$ $\qquad$ $2 \times 3 = 6 \notin G$

مثال (1-1. 6)

نعتبر المجموعات

$G = \{ 2,4,6,8,... \}$
$S = \{1,3,5,7 ... \}$

نلاحظ أن $(G ,+)$ نظام ذا عملية ولكن $(S ,+)$ ليس نظامًا ذا عملية لان عمليــة الجمع على مجموعة الأعداد الطبيعية الفردية ليست مغلقة.

مثال (1-1. 7)

إذا كانت $G = \{-1, 1, 0\}$, فهل أن الزوج $(G, +)$ يكون نظامًا ذا عملية أم لا .

الحل:

نستخدم الجدول المصاحب ونلاحظ أن بعض العناصر الموجودة بداخله لا تنتمي إلى G فمثلاً:

$$1+1=2 \notin G$$

وبذلك نستنتج أن $(G, +)$ ليس نظامًا ذا عملية .

+	−1	0	1
−1	−2	−1	0
0	−1	0	1
1	0	1	2

مثال (1-1. 8)

اعتبر $G = R / \{1\}$ حيث R مجموعة الأعداد الحقيقية ولكن * عملية معرفة على G بحيث

$$a*b = a + b - ab \quad \forall \quad a,b \in G$$

ادرس النظام $(G,*)$.

الحل:

نلاحظ أن عدد عناصر G لا نهائي ومن تم فلا يمكن تكوين جدول، فينتج ما يلي:

ليكن $a , b \in G$ إذن

$$a * b = a + b - ab$$

إذا كان

$$a + b - ab = 1$$

فإن

$$a (1-b) = 1-b$$

وحيث إن $b \neq 1$, فإنه يمكن القسمة على $1-b$ والنتيجة $a = 1$ وهذا عكس الفرض، إذن

$$a*b \neq 1 \Rightarrow a*b \in G$$

وبذلك يكون $(G,*)$ نظامًا ذا عملية لان G مغلقة بالنسبة للعملية *.

مثال (9.1-1)

يمكن اعتبار $\vee , \wedge$ بمثابة عمليات ثنائية على مجموعة الصواب و الخطأ $G = \{ F,T\}$

كالآتي:

$\vee$	T	F
T	T	T
F	T	F

$\wedge$	T	F
T	T	F
F	F	F

وواضح أن كل من $(G, \wedge)$ ، $(G, \vee)$ هو نظام ذو عملية .

مثال (10.1-1)

نفرض أن $X=\{0,1,2,3,4,5,6,7\}$ و أن ρ هو علاقة معرفة علـــى X كالأتي:

$$a\,\rho\, b \iff (a-b)/3 \in Z \quad ,a,b \in X$$

أي أن a-b تقبل القسمة على 3.

إذن بيان ρ كالأتي:

$$\rho = \{(0,0),(0,3),(0,6),(1,1),(1,4),(1,7),(2,2),(2,5),(3,0),(3,3),(3,6)\ (4,1),(4,4),(4,7),(5,2),(5,5),(6,0),(6,3),(6,6),(7,1)(7,4),(7,7)\}\ .$$

واضح أن ρ علاقة تكافؤ على X حيث إنها

i- انعكاسية ii- متماثلة iii- متعدية

وصفوف التكافؤ هي:

$[0]=\{0,3,6\}=[3]=[6]$
$[1]=\{1,4,7\}=[4]=[7]$
$[2]=\{2,5\}=[5]$

نلاحظ أنه يتكون لدينا ثلاثة صفوف تكافؤ فقط هي: [0], [1], [2] وأنـــه يتكـــون لدينا تجزئة للمجموعة X بالشكل:

$$X / \rho=\{[0],[1],[2]\}$$

والتي يرمز لها بالرمز X_3 .

سنعرف الآن عملية الجمع والضرب على X_3 كالأتي:

$$[a] \oplus [b] = \{x : x = a`+b`, a` \in [a] , b` \in [b], \} = [a+b].$$

$$[a] \otimes [b] = \{x : x = a` \times b`, a` \in [a] , b` \in [b]\} = [a \times b] .$$

نكون الآن جدولي هاتين العمليتين:

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\otimes$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

واضح أن كلاً من $(X_3, \oplus)$ ، $(X_3 , \otimes)$ نظام ذو عملية .

ملاحظة (1-1. 11)

مجموعة أصناف الباقي قياس n :

ليكن n عددًا طبيعيًا ولتكن Z مجموعة الأعداد الصحيحة

$$Z=\{0, \pm 1 , \pm 2, \pm 3 , \pm ...\}$$

ولنعرف علاقة ρ على Z كما يلي:

$$x \rho y \quad \Leftrightarrow \quad (x-y)/n \quad \in Z$$

أي أن الشرط اللازم والكافئ لتكون $x \rho y$ هو

$$\exists \quad q \in Z : x - y = q n$$

وقد نعبر عن ذلك بالرموز كالأتي:

$$x \rho y \quad \Leftrightarrow \quad x \equiv y (\mathrm{mod}\ n)$$

ونقول عندئذ إن x تطابق y قياس n

مثال (1-1. 12)

أثبت أن العلاقة ρ في الملاحظة (1-1. 11) هي علاقة تكافؤ على Z

البرهان:

-1 $\forall x \in Z \Rightarrow x-x = 0 \times n, 0 \in Z \Rightarrow x \rho x$

إذن ρ علاقة عكسية .

-2

$$\begin{aligned} x \rho y &\Rightarrow x - y = qn, q \in Z \\ &\Rightarrow y - x = -qn, -q \in Z \\ &\Rightarrow y \rho x . \end{aligned}$$

إذن ρ علاقة متماثلة .

-3

$$\begin{aligned} x \rho y \wedge y \rho z &\Rightarrow x-y=q_1 n \wedge y-z=q_2 n, \\ q_1, q_2 \in Z &\Rightarrow (x-y) + (y-z) = (q_1+q_2)n, \\ &\Rightarrow x-z=qn, q \in Z \\ &\Rightarrow x \rho z \end{aligned}$$

إذن ρ علاقة متعدية .

من 1، 2، 3 نستنتج أن ρ علاقة تكافؤ على Z .

مثال (1-1. 13)

أكتب أصناف التكافؤ في المثال السابق :

الحل:

أصناف التكافؤ هي :

$$[0]=\{x\in Z : x\ \rho\ 0\}=\{x \in Z : x-0=qn\}$$
$$=\{\ldots,-3n,-2n,-n,0,n,2n,3n,\ldots\}$$
$$[1]=\{x\in Z : x\ \rho\ 1\}=\{x\in Z : x=1+qn\}$$
$$=\{\ldots,1-2n,1-n,1,1+n,1+2n,\ldots\}$$

$$[2]=\{\ldots,2-2n,2-n,2,2+n,2+2n,\ldots\}$$

.

.

$$[m]=\{\ldots m-2n,m-n,m,m+n,m+2n,\ldots\}$$

.

.

$$[n-1]=\{\ldots,n-1-2n,n-1-n,n-1,n-1+n,n-1+2n,\ldots\}$$

ولا توجد أصناف تكافؤ أخرى حيث إنها ستكرر مرة ثانية , فمثلاً:

$$n\in[0]\ ,\ n+1\in[1]\ ,\ldots,2n-1=[n-1]$$
$$[n]=[0],[n+1]=[1],\ldots,[2n-1]=[n-1]$$

نسمي مجموعة حاصل القسمة $Z\ /\ \rho$ مجموعة أصناف الباقي قياس n ويرمز لها بالرمز Zn .

إذن

$$Zn=\{[0],[1],[2],\ldots,[n-1]\}$$

مثال (14.1-1)

إذا عرفنا على Zn عملية الجمع الآتية:

$$[x]\oplus[y]=[x+y] \quad \forall \quad [x],[y] \in Z_n$$

فأثبت أن $\oplus$ عملية ثنائية على Zn .

البرهان:

حيث إن (Z ,+) نظام ذو عملية ,

إذن

$$x, y \in Z \Rightarrow x+y \in Z$$
$$\Rightarrow [x+y] \in Zn$$

إذن $\oplus$ عملية مغلقة على Zn , ولكن يبقى أن نبرهن على أن [x+y] وحيدة , أي مستقلة عن اختيار ممثلي الصنفين [x] , [y] , ولذلك

نفرض أن $x_1 \in [x]$, $y_1 \in [y]$,

إذن:

(a $[x_1]=[x], [y_1]=[y]$

(b $[x_1]\oplus[y_1]=[x]\oplus[y]$

لإثبات (a) نفرض أن

$$z \in [x_1] \Rightarrow x_1 \ \rho \ z$$

$$\because x_1 \in [x] \Rightarrow x \rho x_1$$
$$\therefore \quad x \rho x_1 \wedge x_1 \rho z \Rightarrow x \rho z \Rightarrow z \in [x]$$

$\therefore\ [x_1]\subset [x]$ .... (1)

الآن نفرض أن

$\omega \in [x] \quad \Rightarrow \quad x\,\rho\,\omega$

$\because\ x_1\in [x] \ \Rightarrow\ x\,\rho\, x_1 \ \Rightarrow\ x_1\,\rho\, x$

$\therefore\ x_1\,\rho\, x \ \wedge\ x\,\rho\,\omega \quad \Rightarrow x_1\,\rho\,\omega \Rightarrow\ \omega \in [x_1]$

$\therefore\ [x]\subset [x_1]$......... (2)

من (1),(2) ينتج أن $[x]=[x1]$. بالمثل يمكن إثبات أن $[y]=[y_1]$.

لإثبات (b) نستخدم (a) , في (1) و (2) نجد أن :

بما أن $[x_1]=[x]\Rightarrow x_1\,\rho\, x \Rightarrow x_1-x=qn, q \in Z$

$[y_1]=[y]\Rightarrow y_1\,\rho\, y \quad \Rightarrow\quad y_1-y=q`n,\ q` \in Z$

$\Rightarrow\ (x_1-x)+(y_1-y)=(q+ q`)n$

$\Rightarrow (x_1 +y_1)-(x+y)=q``n, q`` \in Z$

$\Rightarrow (x_1+y_1)\,\rho\, (x+y)\ \Rightarrow\ [x_1+y_1]=[x+y]$

$\Rightarrow [x_1] \oplus [y_1]=[x] \oplus [y]$.

مثال (1-1.15)

إذا عرفنا على Zn عملية الضرب الآتية:

$$[x]\otimes [y]=[xy] \quad \forall \quad [x],[y] \in Z_n$$

أثبت أن $\otimes$ عملية ثنائية على Z_n.

الحل:

حيث إن (Z,x) نظام ذو عملية ,

إذن $x,y\in Z \ \Rightarrow xy \in Z \Rightarrow\ [xy] \in Z_n$

والآن نثبت أن $[xy]$ مستقل عن اختيار ممثلــي الــصفتين $[x]$، $[y]$ لــذلك نفرض أن

$$x_1 \in [x] \quad y_1 \in [y]$$

إذن

a) $[x_1]=[x]\ ,\ [y_1]=[y]$

b) $[x_1] \otimes [y_1] = [x] \otimes [y]$

لإثبات (a) نستخدم نفس الأسلوب في المثال السابق

ونحصل على

$$[x_1] \subset [x] \quad ...(1)$$
$$[x] \subset [x_1] \quad ...(2)$$

من (1) و(2) ينتج $[x_1]=[x]$, وبالمثل إثبات $[y_1]=[y]$.

لإثبات (b) نستخدم (a)

من (1) ، (2) ينتج أن

$$[x_1]=[x] \Rightarrow x_1 \,\rho\, x \;\Rightarrow x_1-x = qn\ ,\ q \in Z$$
$$[y_1]=[y] \Rightarrow y_1 \,\rho\, y \Rightarrow y_1-y=q`n\ ,\ q` \in Z$$
$$\Rightarrow (x_1-x)(y_1-y)=qq`n^2$$
$$\Rightarrow x_1y_1-x_1y-xy_1+xy=qq`n^2$$
$$\Rightarrow x_1y_1-xy = x_1y+xy_1-2xy+qq`n^2$$
$$= (x_1y-xy)+(xy_1-xy)+qq`n^2$$
$$= (x_1-x)y+(y_1-y)x+qq`n^2$$
$$= qny+q`nx+qq`n^2$$
$$= (qy+q`x+qq`n)n$$
$$= q``n\ ,\ q \in Z$$

$$\Rightarrow x_1y_1 - xy = q``n, q`` \in Z \Rightarrow x_1y_1 \;\rho\; xy$$
$$\Rightarrow [x_1y_1] = [xy]$$
$$\Rightarrow [x_1 \otimes y_1] = [x] \otimes [y]$$

مثال (16.1-1)

اعتبر $(Z_8, \oplus)$, $(Z_8, \otimes)$ $(Z_8^*, \otimes)$

حيث $Z_n^* = Zn - \{[0]\}$

i- كون جدولاً لكل نظام .

ii- إذا كان النظام غير مغلق بين سبب ذلك

iii- أوجد مجموعة الحل لكل من المعادلات الآتية في النظام $(Z_8^*, \otimes)$

1- $[x] \otimes [2] = [3]$ 3- $[3] \otimes [x] = [5]$

2 - $[4] \otimes [x] = [0]$ 4- $[x] \otimes [1] = [4]$

iv- في النظام $(Z_8, \otimes)$ أحسب $[3]^3$, $[2]^3$

الحل:

i - واضح أن

$(Z_8, \oplus)$ نظام مغلق ذو عملية ثنائية .

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

جدول $(Z_8, \oplus)$

واضح أن

$(Z_8, \otimes)$ نظام مغلق ذو عملية ثنائية .

$\otimes$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

جدول $(Z_8, \otimes)$

ii- واضح أن

$(Z_8^*, \otimes)$ ليس نظامًا مغلقًا ذا عملية ثنائية لأن $[2] \otimes [4]=[0] \notin Z_8^*$

⊗	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[7]	[6]	[5]	[4]	3]	[2]	[1]

جدول $(Z_8^*, \otimes)$

iii-

1- من الجدول $(Z_8^*, \otimes)$ نلاحظ بأنه لا توجد $[x] \in Z_8^*$ تحقق المعادلة .
$[x] \otimes [2]=[3]$

لذلك فإن مجموعة الحل هي ϕ .

2- $[4]\otimes [x]=[0] \quad \Rightarrow \quad ([x]=[2]) \vee ([x]=[4]) \vee ([x]=[6])$

لذلك فإن مجموعة الحل هي $\{[2],[4],[6]\}$

3- $[3]\otimes[x]=[5] \quad \Rightarrow \quad [x]=[7]$

لذلك فإن مجموعة الحل هي $\{[7]\}$

4- $[x] \otimes[1]=[4] \quad \Rightarrow \quad [x]=[4]$

لذلك فإن مجموعة الحل هي $\{[4]\}$

iv-

$$[3]^3 = [3]\otimes [3] \otimes [3]$$
$$= [1]\otimes [3]=[3]$$
$$[2]^3 = [2] \otimes[2] \otimes [2]$$
$$= [4]\otimes [2]=[0]$$

[2-1] العمليات الثنائية الإبدالية
Commutative Binary Operations

تعريف (1-2. 17)

إذا كان ($G,*$) نظامًا ذا عملية وكان

$$a*b=b*a \quad \forall\ a,b \in G$$

فإنه يقال إن العملية الثنائية * إبدالية أو أن $(G,*)$ نظام إبدالي .

مثال (1-2. 18)

النظامان $(Z,+)$, ($Z,\times$) نظامان إبداليان , أما النظامان $(Z,-)$, $(Z^*\ ,\div)$ فإنهما ليس إبداليتين (بين السبب).

مثال (1-2. 19)

لتكن العملية o معرفة على مجموعة الأعداد الطبيعية N كالآتي :

$$a\,o\, b=a^b \quad \forall\ a ,b \in N$$

i) هل إن (N , o) نظام ذو عملية .

ii) هل العملية o عملية إبدالية على N.

الحل:

i) من الواضح أن o عملية ثنائية على N , أي أن (N,o) نظام ذو عمليـــة ثنائية.

ii) العملية o ليست إبدالية وذلك لأن

$$2 o 3 = 2^3 = 8$$

وأن

$$3 o 2 = 3^2 = 9$$

ونستنتج من هذا أن

$$2 o 3 \neq 3 o 2$$

مثال (1-2-20)

لتكن o عملية معرفة على المجموعة Z كالتالي :

$$a o b = \max \{a,b\} \;,\; \forall\, a,b \in Z$$

واضح أن o عملية ثنائية على Z لان

$$a\, o\, b = \begin{cases} a & \text{if } a \geq b \\ b & \text{if } b > a \end{cases}$$

وفي كل الحالات $a\, o\, b \in Z$ لان $a,b \in Z$

والآن البيان أن o هي عملية إبدالية , نفرض أن

$a,b \in Z$ حيث $a \geq b$ فإن

$$a\, o\, b = a \qquad b\, o\, a = a$$

إذن

$$a o b = b\, o\, a \quad \forall\, a,b \in Z \;;\; a \geq b$$

أما إذا كان $b > a$ فإن

$$a\, o\, b = b \;,\qquad b\, o\, a = b$$

إذن $a\, o\, b = b = b\, o\, a = b \;,\; \forall\; a,b \in Z \;; b > a$

إذن العملية " o " هي عملية إبدالية على Z.

مثال (21 . 2-1)

لتكن $M_{2\times2}$ هي مجموعة المصفوفات ذات العناصر الحقيقية على النظم 2×2 أي أن

$$M_{2\times2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in R \right\}$$

واضح أن عملية الجمع على $M_{2\times2}$ هي عملية ثنائية و إبدالية لان

$$A+B=B+A , \quad \forall \quad A,B \in M_{2\times2}$$

$$A= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad B= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$AB= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$\therefore \quad AB \neq BA$$

مثال (1-2. 22)

اعتبر النظام $(Z_3, \oplus)$ نظامًا ذا عملية ثنائية حيث $\oplus$ هي عملية الجمع بمقياس 3.

إذا تأملنا الجدول الذي يمثل هذا النظام الجبري نجد أنه متماثل حول القطر الرئيس وهذا معناه

$$a \oplus b = b \oplus a \quad \forall a,b \in Z$$

أي أن النظام $(Z_3, \oplus)$ إبدالي

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

ملاحظة (1-2. 23)

ستكون وسيلتنا في بيان أن نظامًا ذا عملية عدد عناصره محدود بأنه نظام إبدالي. هي النظر في الجدول الذي يمثله النظام . فإذا كان الجدول متماثلاً حول القطر الرئيسي قلنا أن النظام إبدالي.

ملاحظة (1-2. 24)

من الآن فصاعدًا سوف نتقاضى عن كتابة القوس المربع وسنكتفي بكتابة الأعداد مجردة بدون أقواس فمثلاً 3 بدلاً [3].

[3-1] العمليات الثنائية التجميعية
Associative Binary Operations

تعريف (25.3-1)

يقال إن النظام $(G , *)$ نظام تجميعي (دامج) إذا كان

$$(a*b)*c=a*(b*c) \quad \forall \; a,b,c \in G$$

وفي هذه الحالة نقول إن " * " تجميعية على G وعندئذ يمكن إهمال الأقواس وكتابة ذلك بالشكل a*b*c

مثال (26.3-1)

في النظام (N ,o) حيث " o " معرفة كالتالي:

$$a \, o \, b=a^{b} \quad \forall \quad a,b \in N$$

العملية " o " غير تجميعية فمثلاً

$$(2 \, o \, 3) \, o \, 4=2^3 \, o \, 4=(2^3)^4=2^{12}$$

ولكن

$$2 \, o \, (3 \, o \, 4) = 2 \, o \, 3^4=(2^3)^4=2^{81}$$

أي أن

$$(2 \, o \, 3) \, o \, 4 \neq 2 \, o \, (3 \, o \, 4)$$

مثال (1-3. 27)

النظام $(G,*)$ الموفي في المثال (1-1.8) هو نظام تجميعي

وذلك

$$(a*b)*c=(a+b-ab)*c$$
$$= a+b-ab+c-ac-bc+abc$$
$$=a+b+c-ab-ac-bc+abc....(1)$$

وبالمثل

$$a*(b*c)=a*(b+c-bc)$$
$$=a+b+c-bc-ab-ac+abc...(2)$$

من (1) و(2) ينتج أن العملية "*" تجميعية .

مثال (1-3. 28)

عملية الجمع والضرب في مجموعة المصفوفات $M_{2\times2}$ التي سبق ذكرها في المثال (1-2. 21) هما عمليتان تجميعيتان

لأن

$$A+(B+C)=(A+B)+C \quad \forall \quad A,B,C \in M_{2\times 2}$$
$$(AB)C=A(BC) \quad \forall \quad A,B,C \in M_{2\times 2}$$

ملاحظة (1-3-29)

النظام الجبري التجميعي $(G ,*)$ يسمى بشبه زمرة (Semigroup)

[4-1] النظام ذو العنصر المحايد
Algebraic System With Identity Element

تعريف (1-4-30)

إذا كان $(G,*)$ نظامًا ذا عملية , فإننا نقــول إن العنــصر $e \in G$ عنصرًا محايدًا أيمن بالنسبة للعملية "*" إذا كان

$$a*e=a \quad \forall \quad a \in G$$

كما نقول إن $e \in G$ عنصر محايد أيسر إذا كان

$$e*a=a \quad \forall \quad a \in G$$

ونقول إن $e \in G$ عنصر محايد إذا كان

$$a*e=e*a=a \quad \forall \quad a \in G$$

مثال (1-4. 31)

إذا كانت $G=\{1,2,3,4\}$, العملية * معرفة كالتالي :

$$a*b=a \quad \forall \quad a,b \in G$$

أدرس هذا النظام و ابحث عن وجود عنصره المحايد .

الحل:

حيث إن عدد عناصر G محدود , فإنه واضح أن "*" عملية ثنائية مغلقة على G , أي أن $(G,*)$ نظام جبري.

إن الجدول غير متماثل حول قطره , فإن هذا النظام غير إبدالي وكمثال

$$3*2=3 \quad , \quad 2*3=2$$

إذن

$$3*2 \neq 2*3$$

*	1	2	3	4
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4

نلاحظ كذلك أن هذا النظام تجميعي لأن

$$(a*b)*c = a*(b*c)=a \quad \forall \quad a,b,c \in G$$

كذلك كل من العناصر 1,2,3,4 هي محايد أيمن حيث إن

$$a*1=a \quad , \quad a*2=a$$
$$a*3=a \quad , \quad a*4=a \quad \forall \quad a \in G$$

ولا يحتوي النظام $(G,*)$ على محايد أيسر ولهذا فإن النظام لا يملك محايد .

مثال (1-4. 32)

أدرس وجود محايد في النظام $(G,*)$ حيث $G=R\backslash\{1\}$ إن العملية *معرفة كالتالي:

$$a*b=a+b-ab \qquad \forall \quad a,b \in G$$

الحل:

$$\begin{aligned} e*a=a \quad &\Rightarrow e+a-ea=a \\ &\Rightarrow e-ea=0 \\ &\Rightarrow e(1-a)=0 \\ &\Rightarrow e=0 \quad \vee a=1 \end{aligned}$$

وإن $a=1$ لا يتحقق لان $a\in R \; / \; \{1\}$

إذن

$$e=0$$

حيث إن $(e=0)$ هو محايد أيسر للنظام $(G,*)$ وبما أن النظـــام $(G,*)$ نظـــام إبدالي (تم إثباته سابقًا) , لذا فالعنصر $(e=0)$ هو محايد أيمن أيضًا.

وعلى ذلك فإن الصفر هو العنصر المحايد لهذا النظام .

مثال (1-4. 33)

نفرض أن $G=\{2,4,6,8\} \subset Z_{10}$, و أن $\otimes$ هي عملية الــضرب مقيــاس 10, ادرس النظام $(G,\otimes)$.

الحل:

الجدول التالي يمثل النظام $(G, \otimes)$

$\otimes$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

نلاحظ في الجدول أن $(G, \otimes)$ نظام ذو عملية ثنائية وأن $(G, \otimes)$ نظام إبدالي لأن الجدول متماثل حول القطر الرئيسي.

وبتكوين جميع الثلاثيات

$(a \otimes b) \otimes c$ $\qquad\qquad$ $a \otimes (b \otimes c)$

نجد أن

$\forall \ a,b,c \in G$ $\qquad\qquad$ $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

فمثلاً

$$(2 \otimes 4) \otimes 6 = 8 \otimes 6 = 8$$
$$2 \otimes (4 \otimes 6) = 2 \otimes 4 = 8$$
$$2 \otimes (6 \otimes 8) = 2 \otimes 8 = 6$$
$$(2 \otimes 6) \otimes 8 = 2 \otimes 8 = 6$$

وهكذا، أي أن النظام تجميعي.

أما بالنسبة للعنصر المحايد، نلاحظ أن العمود الثالث يتطابق مع العمود الــذي على يسار الجدول وأن الصف الثالث يتطابق مع الصف أعلى الجدول، وأن العمود الثالث، والصف الثالث يتقاطعان عند العنصر "6" وهــذا يــدل علــى أن "6" هــو العنصر المحايد للنظام، أي أن

$$6 \otimes a = a \otimes 6 \qquad \forall \quad a \in G$$

[5-1] العنصر النظير (المعكوس)
Inverse Element

تعريف (1-5-34)

إذا كانت * عملية ثنائية على G وكان $e \in G$ عنصرًا محايدًا أيمن نقول عن العنصر $a^{-1} \in G$ إنه نظير (معكوس) أيمن للعنصر $a \in G$ إذا كان

$$a*a^{-1}=e$$

أما إذا كان $e \in G$ عنصرًا محايدًا أيسر فإننا نقول عن a^{-1} إنه نظير أيسر للعنصر $a \in G$ عندما يكون

$$a^{-1}*a=e$$

أما إذا كان $e \in G$ عنصرًا محايدًا فإننا نقول عن $a^{-1} \in G$ أنه نظير العنصر $a \in G$ عندما يكون

$$a* a^{-1}= a^{-1}*a=e$$

مثال (1-5.35)

نلاحظ من المثال (1-4-33)

ومن الجدول المرافق نحصل على

$2 \otimes 8 = 8 \otimes 2 = 6$

$4 \otimes 4 = 6$

$6 \otimes 6 = 6.$

وبما أن العنصر "6" هو المحايد للنظام الجبري، فنحصل على أن:

معكوس العنصر "2" هو العنصر "8" .

معكوس العنصر "4" هو نفسه .

معكوس العنصر "6" هو نفسه .

معكوس العنصر "8" هو العنصر 2.

مثال (1-5. 36)

إذا كانت $G = R \;/\; \{1\}$ وكانت * معرفة كالتالي

$$a*b=a+b-ab , \qquad \forall\ a,b \in G$$

أوجد معكوس أي عنصر $a \in G$

الحل:

أثبتنا في المثال (1-4. 32) أن العنصر المحايد للنظام $(G,*)$ هو الصفر .

$$\therefore\ a * a^{-1} = 0 \Rightarrow a + a^{-1} - a\,a^{-1} = 0$$
$$\Rightarrow a^{-1}(a-1) = a$$
$$\Rightarrow a^{-1} = a/(a-1) \quad \forall\ a \in G = R \;/\; \{1\}$$

إذن العنصر $a/(a-1)$ هو المعكوس الأيمن للعنصر a

وبالمثل يمكن إثبات أن $a/(a-1)$ هو المعكوس الأيسر للعنصر a

إذن $a/(a-1)$ هو معكوس العنصر a

مثال (1-5-37)

لتكن o عملية معرفة على Z بحيث إن

$$a \, o \, b = a+b-3 \quad \forall \quad a,b \in Z$$

ادرس النظام $(Z \, , o)$

الحل:

i- واضح أن

$$\forall \ a,b \in Z \quad \Rightarrow a+b-3 \quad \in Z \Rightarrow a \, o b \quad \in Z$$

أي أن $(Z \, , o)$ نظام ذو عملية ثنائية.

ii-

$$(a o b) o \, c = (a+b-3) \ \ o C$$

$$=a+b-3+c-3=a+b+c-6$$

$$a o \ (b \ o \ c) = \ a \ \ o(b+c-3)$$

$$= a+b+c-3-3=a+b+c- 6$$

إذن

$$(a o \ b) o c = a \ \ o \ \ (b \ o c) \quad \forall \quad A,b,c \quad \in Z$$

أي أن (Z, o) نظام تجميعي.

iii-

$$a o \ b= b \ o \ a=a+b-3$$

إذن النظام (Z, o) إبدالي.

iv-

$$a \, o \, e = a \quad \Rightarrow \quad a+e-3=a \quad \Rightarrow e=3$$
$$e \, o \, a=a \quad \Rightarrow \quad e+a-3= a \quad \Rightarrow e=3$$

إذن

$$a \, o \, e= e \, o \, a=a$$

العنصر المحايد للنظام $(Z \, , o)$ هو $e=3$.

v-

$$a \, o \, a^{-1} =3 \quad \Rightarrow \quad a + a^{-1} -3=3 \quad \Rightarrow a^{-1} =6-a$$
$$a^{-1} \, o \, a=3 \quad \Rightarrow \quad a^{-1}+a-3=3 \quad \Rightarrow a^{-1} =6-a$$

إذن معكوس العنصر a هو العنصر 6-a

[6-1] بعض النظريات والأمثلة
Some Theorems and Examples

نظرية (1-6. 38)

إذا كانت * عملية ثنائية على G وكان $e \in G$ عنصرًا محايدًا بالنسبة للعملية * فإن e عنصر وحيد .

البرهان: إذا لم يكن e عنصرًا محايدًا فإنه يوجد محايدًا أخر على الأقل ولذا نفرض أن `e عنصرا محايد أخر .

إذن نحصل على

$$e*e` = e$$

لأن `e عنصر محايد

وأن

$$e*e` = e`$$

لأن e عنصر محايد

إذن من المعادلتين نحصل على أنه

$$e = e`$$

وهذا يعني أن e هو العنصر المحايد الوحيد للعملية * على G.

نظرية (1-6. 39)

إذا كانت * عملية ثنائية تجميعية على G وكان $G \ni a^{-1}$ هو معكـــوس a فإن a^{-1} عنصر وحيد في المجموعة G

البرهان: لنفرض أن $G \ni b^{-1}$ هو معكوس آخر للعنصر $a \in G$

$$(a^{-1}*a)*b^{-1} = a^{-1}*(a*b^{-1})$$

$$\Rightarrow e * b^{-1} = a^{-1} * e$$

$$\Rightarrow b^{-1} = a^{-1}$$

إذن a^{-1} العنصر الوحيد المعكوس إلى العنصر a.

ملاحظة (1-6. 40)

1) في حالة وجود عنصر محايد أيمن فقط (أو أيسر فقط) بالنسبة للعملية الثنائية على مجموعة فإنه لا يشترط أن يكون هذا العنصر المحايد وحيدًا.

2) إذا وجد عنصر أيمن فقط (أو أيسر فقط) بالنسبة لعملية ثنائية على مجموعة وكان لكل عنصر في هذه المجموعة نظير أيمن (أو نظير أيسر) فلا يشترط أن يكون وحيدًا.

3) سيكون اهتمامنا منصبًا أكثر على دراسة بعض الأنظمة ذات العمليـــة التـــي يكون فيها عنصر محايد، أي أن العنصر المحايد (إن وجد) فهو أيمن وأيسر في آن واحد، وكذلك الحال بالنسبة لنظير كل عنصر (إن وجـــد) فيجـــب أن يكون أيمن و أيسر في آن واحد.

4) إذا كان $(G, *)$ نظامًا ذا عملية، وكانت * تجميعية وكان

$$a_1, a_2, \ldots, a_n \in G \Rightarrow a_1 * a_2 * a_3 = (a_1 * a_2) * a_3$$

لأن * تجميعية، وباستخدام مبدأ الاستنتاج الرياضي فإنه يمكن تعميم ما سبق على النحو التالي:

$$a_1 * a_2 * \ldots * a_n = (a_1 * a_2 * \ldots * a_{n-1}) * a_n$$

وكحالة خاصة إذا كان

$$a_1 = a_2 = \ldots = a_n = a$$

فإن

$$a * a * a * \ldots a * a = a^{n-1} * a = a^n$$

نظرية (41 .6-1)

إذا كان $(G, *)$ نظام ذو عملية ثنائية وتجميعية وكان $e \in G$ عنصرا محايدًا فيه وكان لكل $a \in G$ نظير $a^{-1} \in G$ فإن العنصر المحايد هو نظير لنفسه.

البرهان:

نفرض أن $e^{-1} \in G$ هو النظير إلى العنصر $e \in G$

والآن

$$e^{-1} * e = e$$

لأن e^{-1} هو النظير إلى e

وكذلك

$$e^{-1} * e = e^{-1}$$

لأن e هو المحايد للنظام $(G , *)$

إذن

$$e = e^{-1}$$

أي العنصر المحايد هو نظير نفسه.

مثال (1-6. 42)

لتكن * عملية معرفة على Z بحيث إن

$$a*b=2a+b \qquad \forall \quad a,b \in Z$$

ادرس النظام $(Z ,*)$ من حيث:

i. هل أن $(Z,*)$ نظام ذو عملية ثنائية أم لا ؟

ii. هل أن $(Z,*)$ نظام إبدالي؟

iii. هل أن $(Z,*)$ نظام تجميعي ؟

iv. ادرس وجود عنصر محايد أيمن، أيسر، محايد.

v. ادرس وجود نظير أيمن، أيسر، نظير لكل $a\in Z$.

الحل

i- واضح أن

$$a,b \in Z \Rightarrow 2a ,b \in Z \Rightarrow 2a+b \in Z$$
$$\Rightarrow a*b \in Z$$

إذن * عملية ثنائية على Z أي أن $(Z ,*)$ نظام ذو عملية.

ii-

$a*b=2a+b \neq 2b+a=b*a \quad \forall \quad a,b\in Z$

$\Rightarrow a*b \neq b*a$

إذن * ليست إبدالية بصورة عامة وتكون إبدالية فقط في حالة كون $a=b$

iii-

$(a*b)*c=(2a+b)*c$

$=2(2a+b)+c=4a+2b+c \ldots (1)$

$a*(b*c)=a*(2b+c)$

$=2a+2b+c \ldots\ldots \ldots \ldots\ldots (2)$

من (1)(2) ينتج أن * ليست تجميعية لأن

$(a*b)*c \neq a*(b*c) \quad \forall a,b,c \in Z$

رغم تساوي الطرفين عندما $a=0$

iv-

نفرض أن $e\in Z$ عنصر محايد أيمن , إذن

$a*e=a \quad \forall \ a \in \dot{Z}$

$\Rightarrow 2a+e=a \quad \Rightarrow \quad e=-a$

وهذا يعني أن e متغير ولا يحقق خاصية العنصر المحايد الأيمن إلى من أجل العناصر التي على الشكل $(a,-a) \in Z \times Z$ حيث يكون عندها

$a*(-a)= 2a+(-a)=a$

أما العناصر التي على شكل $(b,-a) \in Z^2$ حيث $b \neq a$ فلا تحقق خاصية العنصر المحايد الأيمن نجد أن

$$b*(-a)=2b+(-a) \neq b$$

وبالتالي فإنه لا يوجد عنصر محايد أيمن بالنسبة للعملية * لعدم تحقق خاصية المحايد الأيمن.

والآن نفرض أن $e \in Z$ عنصر محايد أيسر , إذن

$$e*a=a \quad \forall \quad a \in Z$$
$$\Rightarrow 2a+a=a \quad \Rightarrow e=0$$

وهذا يعني وجود عنصر محايد أيسر بالنسبة للعملية * ألا وهو الصفر .

لما كان في المتعذر وجود عنصر محايد أيمن بالنسبة للعملية * فإنه لا يوجد محايد في هذا النظام .

v- لما كان من المتعذر وجود عنصر محايد أيمن فإنه لا يوجد نظير أيمن لكل عنصر $a \in Z$ ، وكذلك لا يوجد نظير بصورة عامة للنظام لأنه فقد النظير الأيمن.

بقى أن ندرس وجود النظير الأيسر للعناصر .

نفرض أن $a^{-1} \in Z$ هو نظير أيسر للعنصر $a \in Z$

إذن

$$a^{-1}*a=e=0$$
$$\Rightarrow 2a^{-1}+a=0 \quad \Rightarrow \quad a^{-1} = -a / 2$$

ولكن $-a/2$ لا ينتمي دائمًا إلى Z (كمثال إذا كانت $a=1$ فإن $(a^{-1}= -1/2 \notin Z$
وبالتالي فإنه لا يوجد نظير أيسر لكل عنصر في Z بالرغم من وجود عنصر محايد أيسر.

مثال (1-6. 43)

اعتبر مجموعة أصناف الباقي قياس n

$Zn=\{[0],[1],...[n-1]\}$

مع عمليتي الجمع و الضرب $\oplus$, $\otimes$ بمقياس n المعرفتان كالتالي:

$[x] \oplus [y] = [x+y] \quad \forall \quad [x],[y] \in Zn$

$[x] \otimes [y] = [xy] \quad \forall \quad [x],[y] \in Zn$

اثبت أن

i- العمليتين $\oplus$, $\otimes$ ثنائيتان على Z n.

ii- العمليتين $\oplus$, $\otimes$ إبداليتان.

iii- العمليتين $\oplus$, $\otimes$ تجميعتان .

iv- يوجد عنصر محايد $[e] \in Zn$ بالنسبة للعملية $\oplus$.

v- يوجد عنصر محايد $[e`] \in Zn$ بالنسبة للعملية $\otimes$.

vi- لكل عنصر $[e] \in Zn$ يوجد نظير $[a]^{-1} \in Z$ بالنسبة للعملية $\oplus$.

vii- لكل عنصر $[a] \in Z$ $[a] \neq [0]$ يوجد نظير $[a]^{-1} \in Z$ بالنسبة للعملية $\otimes$ عندما يكون n,a أوليين فينا بينهما .

الحل:

i- تم إثباته في المثال (1-1. 14) والمثال (1-1.15)

ii- 1) العملية $\oplus$ إبدالية لأن $\forall \ [a],[b] \in Zn$

$[a] \oplus [b] = [a+b]$ تعريف $\oplus$

$= [b+a]$ لأن + إبدالية على Z

$= [b] \oplus [a]$ تعريف $\oplus$

2) العملية $\otimes$ إبدالية لأن $\forall\ [a],[b]\in Zn$

تعريف $\otimes$ $[a]\otimes [b]=[ab]$

لأن $\times$ إبدالية على Z $=[ba]$

تعريف $\otimes$ $=[b]\otimes[a]$

-iii

1) العملية $\oplus$ تجميعية لأن $\forall\ [a],[b],[c]\in Z_n$

تعريف $\oplus$ $([a]\oplus[b])\oplus[c]=[a+b]\oplus[c]=[(a+b)+c]$

تعريف $\oplus$ $=[(b+a)]+c]$

لأن + تجميعية على Z $=[a+(b+c)]$

تعريف $\oplus$ $=[a]\oplus([b+c]$

تعريف $\oplus$ $=[a]\oplus([b]\oplus[c])$

2) العملية $\otimes$ تجميعية لأن $\forall\ [a],[b],[c]\in Zn$

تعريف $\otimes$ $([a]\otimes[b])\otimes[c]=[ab]\otimes[c]$

لأن $\times$ تجميعية على Z $=[a(bc)]$

تعريف $\otimes$ $=[a]\otimes[bc]$

تعريف $\otimes$ $=[a]\otimes([b]\otimes[c])$

-iv نفرض أن $[e]\in Zn$ عنصر محايد بالنسبة للعملية $\oplus$,
إذن

$$\forall\ [a]\in Zn,\qquad [a]\oplus[e]=[a]$$
$$\Rightarrow [a+e]=[a]$$
$$\Rightarrow [e]=[0]$$

إذن $[0]$ هو العنصر المحايد بالنسبة للعملية $\oplus$ في Zn v- نفرض أن $[e`] \in Z_n$ عنصر محايد بالنسبة للعملية $\otimes$

إذن

$$\forall \quad [a] \in Zn , \qquad [a] \otimes [e`]=[a]$$
$$\Rightarrow [ae`]=[a]$$
$$\Rightarrow [e`]=[1]$$

إذن $[1]$ هو العنصر المحايد بالنسبة للعملية $\otimes$ في Z_n

vi- أن $[-a]$ هو نظير العنصر $[a]$ بالنسبة للعملية $\oplus$ ، لأن

$$[a] \oplus [-a]=[a-a]=[0]$$

vii- ليس لكل عنصر $[a] \in Zn$ معكوس بالنسبة للعملية $\otimes$ علـــى Zn ولكــن يمكن إيجاد معكوس إذا كان n , a أوليان فيما بينهما فـــإن $[a]$ لـــه نظيـــر $[a]^{-1} \in Zn$ ، من نظرية الأعداد إذا كان n,a أوليان فيما بينهما فأنه يوجد عددان صحيحان x,y بحيث إن:

$$xa+yn=1$$
$$\Rightarrow [xa+yn]=[1] \qquad \Rightarrow [xa]=[1],$$
$$([yn]=[0])$$ لأن

$$\Rightarrow [x] \otimes [a]=[1]$$
$$\Rightarrow [a]^{-1}=[x] \in Zn$$

وكنتيجة لهذا الجزء فأنه إذا كانت n عددًا أوليًا فأن كل عنـــصر $[0] \neq [a] \in Zn$ له معكوس $Z \ni [a]^{-1}$ وذلك لان a,n أولين فيما بينهما .

[7-1] الأنظمة ذات العمليتين
The System With Two Binary Operations

تعريف (1-7 .44)

نعرف على مجموعة ما مثل $G \neq \phi$ عمليتين $o,*$ فإذا كان النظامان $(G,*)$, (G,o) مغلقتين بالنسبة لهاتين العمليتين فإننا نكتب ذلك بالشكل $(G,*,o)$ ونسميه نظامًا ذا عمليتين ثنائيتين .

ملاحظة (1-7 .45)

إذا كان $(G,*,o)$ نظامًا ذا عمليتين ثنائيتين فإننا نقول إن العملية o تتوزع على العملية * من اليسار إذا كان

.i $\forall \quad a,b,c \in G \qquad a\,o\,(b*c)=(a\,o\,b)*(a\,o\,c)$

كما نقول إن العملية o تتوزع على العملية * من اليمين إذا كان

.ii $\forall \quad a,b,c \in G \qquad (b*c)\,o\,a=(b\,o\,a)*(c\,o\,a)$

ونقول إن العملية o تتوزع على العملية * إذا تحقق الشرطان (i)(ii) في آن واحد .

مثال (1-7 .46)

.i أن $(Z\,,+\,,\,\cdot)$ نظام ذو عمليتين ثنائيين تتوزع فيه عملية الضرب " . " على عملية الجمع " + " لأن

$$\forall \quad a,b,c \in Z \;,\; a.(b+c)=a.b+a.c=b.a+c.a=(b+c).a$$

ii. بالمثل فإن كل من $(Q , +, .)$, $(R, +, .)$ $(C ,+ , .)$ نظام ذو عمليتين ثنائيتين فيه عملية الضرب "." تتوزع على عملية الجمع " + " .

iii. إذا كانت $A = \phi$ فإن كل من $(P (A) , \cup , \cap)$,$(P (A) ,\cap,\cup)$ نظام ذو عمليتين ثنائيتين فيه العملية الثانية تتوزع على العملية الأولى .

iv. النظام $(Z ,+, -)$ نظام ذو عمليتين ثنائيتين ولكن عملية الطرح" − " لا تتوزع على عملية الجمع لا من اليسار ولا من اليمين لأن

$$\exists \quad a,b,c \in Z \quad ;a- (b+c) \neq (a-b)+(a-c) = 2a-(b + c)$$

وكذلك يوجد $a,b,c\in Z$ حيث إن

$$(b+c)-a \neq (b-a)+(c-a)=(b+c) -2a$$

مثال (1-7 . 47)

ادرس النظامين $(p(A), \cup,-)$ $(p(A), \cap,-)$ حيث A أية مجموعة

الحل:

واضح إن كلا من هذين النظامين نظام ذو عمليتين ثنائيتين.

أولاً: النظام $(p(A), \cup,-)$

1- عملية الطرح " − " لاتتوزع من اليسار على عملية الاتحاد " $\cup$ " لان

$$A_1-(A_2\cup A_3)=A_1\cap(A_2 \cup A_3)`$$
$$= A_1 \cap(A_2` \cap A_3`)$$
$$=(A_1\cap A_2`) \cap (A_1 \cap A_3`)$$
$$= (A_1-A_2) \cap(A_1-A_3)$$

$$\neq (A_1-A_2) \cup (A_1-A_3)$$

$$\forall\ A_1,A_2,A_3 \in P(A)$$

2- عملية الطرح " − " تتوزع من اليمين على عملية الاتحاد " $\cup$ " لان

$$(A_2 \cup A_3) - A_1 = (A_2 \cup A_3) \cap A_1`$$

$$= (A_2 \cap A_1`) \cup (A_3 \cap A_1`)$$

$$= (A_2 - A_1) \cup (A_3 - A_1)$$

$$, \forall\ A_1,A_2,A_3 \in P(A)$$

ثانيًا $(P(A)\ ,\ \cap\ ,-)$

1- عملية الطرح " − " لا تتوزع من اليسار على عملية التقاطع " $\cap$ " لأن

$$A_1-(A_2 \cap A_3) = A_1 \cap (A_2 \cap A_1)`$$

$$= A_1 \cap (A_2` \cup A_3`)$$

$$= (A_1 \cap A_2`) \cup (A_1 \cap A_3`)$$

$$= (A_1-A_2) \cup (A_1-A_3)$$

$$\neq (A_1-A_2) \cap (A_1-A_3)$$

$$\forall\ A_1,A_2,A_3 \in P(A)$$

[8-1] التشاكل (الهومومورفيزم)
Homomorphism

تعريف (48.8-1)

كان كل من $(G\ ,\ *)$, $(G^`,o)$ نظامًا ذا عملية وكان $f: G \to G^`$ تطبيقيًا (دالة) فإن f تسمى تشاكل (تطابق) من G إلى `G إذا كان

$$f(a*b)= f(a)\ o\ f(b)\ \forall \quad a,b \in G$$

ملاحظة (49.8-1)

يسمى التشاكل:

1- تشاكل متباين (مونومورفيزم) إذا كان f متباينًا .
2- تشاكل شامل (ابيمومورفيزم) إذا كان f شاملاً (غامرًا).
3- تشاكل تقابلي (ايزومورفيزم) إذا كان f تقابلاً .
4- تشاكل ذاتي (اندومورفيزم) إذا كان $G=G^`$.
5- تشاكل ذاتي تقابلي (اوتومورفيزم) إذا كان f ايزومورفيزم , $G=G^`$.

تعريف (50.8-1)

يمكن تعميم مفهوم التشاكل بيشمل نظامين لهما عمليتان ثنائيتان إذا كـــان $(G,*,\ o)$ $(G^`\ ,\oplus\ ,\ \otimes)$ نظامين مغلقين وكان $f:G \to G^`$ تطبيقيًا فإننا نقول إن f تشاكل (تطابق) (هومومورفيزم) إذا تحقق الشرطان الآتيان:

$$\text{i-}\ \ f(a*b)=f(a)\ \oplus F(b) \quad , \quad \forall\, a,b \ \in\ G$$
$$\text{ii-}\ \ f(a\,o\,b)=f(a)\otimes (b) \quad \forall\, a,b \ \in G$$

وهذا التعريف بالطريقة نفسها يسري على الحالات الخاصة الأخرى السابق ذكرها في التعريف والملاحظة السابقتين وخاصية التشاكل التقابلي.

مثال (1-8. 51)

لنأخذ النظامين $(Z_4, \oplus)$, $(Z_5^*, \otimes)$

وليكن

$$f: Z_4 \to Z_5^*$$

تطبيقيًا معرفًا كما يلي:

$$F=\{([0],[1])\ ([1],[2]),([2],[4])\ ([3],[3])\}$$

اثبت أن:

i- f تشاكل   ii- تشاكل تقابلي

الحل:

i- حيث إن العمليتين $\oplus$, $\otimes$ إبدالتين فيكفي حساب الآتي :

$f([0] \oplus [0])=f([0])=[1]$.
$f([0]) \otimes f([0])=[1]\otimes[1]=[1]$
$f([0]\oplus [1])=f([1])=[2]$
$f([0]) \otimes f([1])=[1]\otimes[2]=[2]$
$f([0] \oplus [2])=f([2])=[4]$.
$f([0]) \otimes f([2])=[1]\otimes [4]=[4]$.
$f([0] \oplus [3])=f([3])=[3]$.
$f([0]) \otimes f([3])=[1]\otimes [3]=[3]$
$f([1] \oplus [1])=f([2])=[4]$.
$f([1]) \otimes f([1])=[2]\otimes [2]=[4]$.
$f([1] \oplus [2])=f([3])=[3]$.
$f([1]) \otimes f([2])=[2]\otimes[4]=[3]$

$f([1] \oplus [3])=f([0])=[1].$

$f([1]) \otimes f([3])=[2]\otimes [3]=[1]$

$f([2] \oplus [2])=f([0])=[1].$

$f([2]) \otimes f([2])=[4]\otimes [4]=[1] .$

$f([2] \oplus [3])=f([1])=[2].$

$f([2]) \otimes f([3])=[4]\otimes [3]=[2]$

$f([3] \oplus [3])=f([2])=[4].$

$f([3]) \otimes f([3])=[3]\otimes [3]=[4] .$

من كل ما سبق نجد أن

$$f([a] \oplus [b])=f([a] \otimes F([b]), \qquad \forall [a],[b] \in Z_4$$

أي أن f هو تشاكل في Z_4 إلى Z_5^*

ii- f تطبيق متباين لأنه واضح من التفريق مباشرة

$f([a])=f([b]) \Rightarrow [a]=[b]$

كما أن f تطبيق غامر (شامل) لأن

$F(Z_4)= Z_5^*$

إذن f تقابلي وبالتالي يكون تشاكل تقابلي.

مثال (1-8. 52)

نعتبر النظامين $(Z,+)$, $(Z_4 , \oplus)$, وليكن

$f: Z\rightarrow Z_4$

تطبيقيًا معرفًا كالآتي:

$$f(a)=\begin{cases} [0], & \text{عدد زوجي } a \\ [2], & \text{عدد فردي } a \end{cases}$$

(i) أثبت أن f تشاكل ثم أوجد الصورة الهومومــورفيزم (التشاكلية) إلى z أي f(z) .

(ii) هل f تشاكلاً متباينًا ولماذا ؟

(iii) هل f تشاكلاً شاملا ولماذا ؟

(iv) هل f تشاكلاً تقابليًا؟

الحل:

(i) نفرض أن $a,b \in Z$, أذن حسب تعريف f لدينا

$$f(a+b) = \begin{cases} [0] & \text{إذا كان } a+b \text{ عددًا زوجيًا} \\ [2] & \text{إذا كان } a+b \text{ عددًا فرديا} \end{cases}$$

إذن هناك حالتان

1- a+b زوجي وهذا صحيح إذا كان العددان a,b زوجيــين معًــا أو فرديين معًا .

2- a+b فردي وهذا صحيح إذا كان أحد العــددين زوجيًــا والاخــر فرديًا.

والآن لدينا في الحالة (1) :

$f(a+b)=[0]$ .. ..(I)

وبفرض أن a,b عددان زوجيان فإن

$$f(a) \oplus f(b) = [0] \oplus [0] = [0] \quad \ldots\ldots\ldots\ldots(II)$$

وبفرض أن a,b عددان فرديان فإن

$$f(a) \oplus f(b) = [2] \oplus [2] = [4] = [0] \quad \ldots\ldots\ldots(III)$$

ومن (I), (II), (III) نجد أن

$$f(a+b) = f(a) \oplus f(b) = [0]$$

أما في الحالة (2) فلدينا

$$f(a+b) = [2] \quad \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \quad (I)$$

وبفرض أن a عدد زوجي و b عدد فردي فإن:

$$f(a) \oplus f(b) = [0] \oplus [2] = [2] \ldots\ldots \quad (II)$$

وبفرض a عدد فردي و b عدد زوجي فإن:

$$f(a) \oplus f(b) = [2] \oplus [0] = [2] \quad \ldots\ldots\ldots\ldots\ldots (III)$$

ومن(I), (II), (III) نجد أن

$$f(a+b) = f(a) \oplus f(b) = [2]$$

إذن f هو تشاكل

والصورة التشاكلية هي

$$f(2) = \{[0],[2]\}$$

ii- كلا ,f ليس تشاكلاً متابينًا , لأن f ليس تطبيقيًا متباينًا فمثلاً

$$\left.\begin{array}{l} f[0]=[0] \\ \\ f[2]=[0] \end{array}\right\} \Rightarrow f(0)=f(2) \qquad 0 \neq 2,$$

iii- كلا ليس f تشاكلاً شاملاً , لان f ليس تطبيقيًا غامرًا (شاملاً) حيث إن $f(Z) \neq Z_4$.

iv- لا، ليس f تشاكلاً تقابليًا، لأن f ليس تقابلاً.

نظرية (1-8. 53)

إذا كان كلاً من $(G,*)$, $(G`, o)$ نظامًا ذا عملية وأن $f:G \to G`$ تشاكل, فإن:

i- $(f(G) , o)$ نظام ذو عملية , حيث " o " هي العملية نفسها المعرفة على `G.

ii- إذا كانت " * " دامجة (تجميعية) فإن " o " تكون تجميعية على f(G) أيضًا.

ii- إذا كانت " * " إبدالية فإن " o " تكون إبدالية على f(G) أيضًا .

iv- إذا كان $e \in G$ عنصرًا محايدًا في f(G) بالنسبة للعملية " * " فإن $e`=f(e)$ عنصر محايد في f(G) بالنسبة للعملية "o"

v- إذا كان $a^{-1} \in G$ نظيرًا للعنصر $a \in G$ فإن $f^{-1}(a) \in f(G)$ يكون نظيرًا للعنصر $f(a) \in f(G)$, أي أن

$$f(a^{-1}) = [f(a)]^{-1}$$

البرهان:

المجموع $f(G)$ هي مدى التطبيق , لذلك فإن

$$f(G) \subset G`$$

نفرض أن$f(G)$ $\ni$ $a`,b`,c`$ أي ثلاثة عناصر اختيارية من $f(G)$ إذن

$$\exists \quad a,b,c \in G, \quad f(a) = a` \ , \ f(b)=b` \quad , f(c)=c`$$

i- لأن f هو تشاكل , إذن

$$f(a*b)= f(a) \ o \ f(b) = `a \ o \ b`$$

وحيث إن $a*b \in Z$, إذن

$$f(a*b) \in f(G)$$

أي أن

$$a` \ o \ b` \in f(G)$$

وهذا يعني أن $(f(G) \ , \ o)$ نظام ذو عملية ثنائية

ii- حيث إن " * " عملية تجميعية , إذن

$$(a*b)*c=a*(b*c)$$

ومنه

$$f((a*b)*c)=f(a*(b*c))$$

ولكن f تشاكل لذا فإن

$$f((a*b)*c)=f(a*b) o \ f(c) = (f(a) o \ f(b)) \ o f(c)= (a` o b`) \ o c`$$

$$f(a*(b*c)=f(a) o f(b*c)=f(a) \ o (f(b) \ o f(c))=a` o (b` o c`)$$

أي أن o عملية تجميعية على $f(G)$.

iii- حيث إن " * " إبدالية , إذن

$$a*b=b*a$$

$$f(a*b)=f(b*a)$$

لأن f تشاكل

$f(a) \circ f(b) = f(b) \circ f(a)$
$a' \circ b' = b' \circ a'$

أي أن العملية o إبدالية على f(G)

iv- حيث إن $e \in G$ هو عنصر محايد بالنسبة للعملية " * "

$\therefore \quad a*e=e*a=a \qquad \forall\ a \in G$
$\Rightarrow f(a*e) = f(e*a)=f(a)$

f تشاكل

$\Rightarrow f(a) \circ f(e) = f(e) \circ f(a) = f(a)$
$\Rightarrow f(e) = e'$

أي أن $e'=f(e)$ عنصر محايد في f(G).

v- إذا كان $a^{-1} \in G$ هو نظير العنصر $a \in G$, فإن

$a*a^{-1} = a^{-1}*a=e$
$\Rightarrow f(a*a^{-1}) = f(a^{-1}*a) = f(e)=e'$
$\Rightarrow f(a) \circ f(a^{-1}) = f(a^{-1}) \circ f(a) = e'$
$\Rightarrow f(a^{-1}) = [f(a)]^{-1}$

تعريف (54 . 8-1)

إذا كان $f:G \to G'$ هومومورفيزم من $(G , *)$ إلى (G', o) وكان $e \in G$, $e' \in G'$ عنصرين محايدين في هذين النظامين على الترتيب، فإن $f^{-1}(e')$ تسمى نواة التشاكل f ، أو اختصارًا النواة، التي يرمز لها بالرمز ker f ، أي أن

$$Ker\ f = f^{-1}(e') = \{ a \in G : f(a)=e' \}$$

نظرية (55.8-1)

إذا كان كل النظام ذي عملية $(G, *)$, $(G`, o)$ به عنصر محايد $(e`\in G` , e\in G)$ ولكل عنصر فيها نظير وكانت * تجميعية وكان f تشاكل من G إلى G`

فإن :

i- $\ker f \neq \phi$

ii- f تشاكل متباين $\Leftrightarrow$ $\ker f = \{e\}$

البرهان:

i- من النظرية (53 . 8-1) فإن

$$f(e)=e`$$
$$\Rightarrow e \in f^{-1}(e`)=\ker f$$
$$\Rightarrow \ker f \neq \phi$$

ii- أولاً : نفرض أنه f تشاكل متباين, إذن f متباين إذا كان

$$a\in \operatorname{Ker} f \Rightarrow f(a)=e`$$

لكن

$$f(e)=e`$$

فإن

$$f(a)=f(e) \Rightarrow a=e$$

$$\Rightarrow \ker f = \{e\}$$

ثانيًا:

نفرض أن $\ker f=\{e\}$ و أن $a,b \in G$ بحيث إن

$$f(a)=f(b) \Rightarrow f(a)\ o\ [f(b)]^{-1}=e`$$

$$\Rightarrow e`=f(a)\, o\, f(b^{-1})=f(a*b^{-1})$$

$$\Rightarrow a*b^{-1} \in \ker f$$

$$\Rightarrow a*b^{-1}=e \qquad \Rightarrow (a*b^{-1})*b=e*b$$

$$a*(b^{-1}*b)=e*b \quad \Rightarrow a=b$$

إذن f تطبيق متباين وبذلك يكون f تشاكل متباين

[1-9] تمارين عامة
Binary Operations on a Set

1- وضح بمثال واحد فقط كلاً مما يأتي:

i- (N ,−) ليس بنظام ذي عملية ثنائية .

ii- (N ,÷) ليس بنظام ذي عملية ثنائية

iii- (S ,+) ليس بنظام ذي عملية ثنائية حيث S معرفة كالتالي
$S=\{1,3,5,7...\}$

2- إذا كانت $G=\{1,0,-1\}$ ، فهل أن $(G , \times)$ يمثل نظامًا ذا عملية ثنائية أم لا ؟

3- اعتبر المجموعة $G=\{T,F\}$ هي مجموعة الصواب والخطأ، بين أي من الأزواج الآتية يمثل نظامًا ذا عملية ثنائية
$(G, \Rightarrow)$, $(G , \Leftrightarrow)$.
(أعمل جدول لكل زوج لتوضيح الأجابة).

4- أثبت أن الضرب عملية ثنائية على $G=\{1,-1, i ,-i\}$ حيث $i=\sqrt{-1}$

5- اعتبر $(Z_5 , \oplus)$, $(Z_5 , \otimes)$, $(Z_5^* , \otimes)$
حيث $Z^*n=Zn-\{[0]\}$ ، و العملية $\oplus$, $\otimes$ معرفة بالمثال
(1-1. 14) ، (1-1. 15)

i– كون جدول العملية لكل نظام .

ii– إذا كان النظام غير مغلق بين سبب ذلك .

iii- حل المعادلات الآتية في النظام $(Z_5^*\ ,\ \otimes)$.

1-$[x]\otimes[2]=[3]$

2- $[3]\otimes[x]=[1]$

3-$[2]\otimes[x]=[4]$

4-$[x]\otimes[1]=[4]$

iv– في النظام $(Z_5\ ,\ \otimes)$ احسب $[2]^3$, $[3]^3$

v – إذا كان النظام غير إبدالي بين سبب ذلك .

6– إذا كانت العملية o معرفة على مجموعة الأعداد الحقيقية كالتالي:

$$x\ o\ y=xy+1\ \forall\ x,y\ \in R$$

بين أن النظام $(R\ ,\ o)$ هو نظام إبدالي , وليس نظام تجميعيًا

7– اعتبر $(Z\ ,*)$ حيث إن العملية * معرفة كالتالي:

$$a*b=2a+b\ \forall\quad a,b\in Z$$

وضح بمثال أن * ليست إبدالية وليست تجميعية على Z.

8– لتكن o عملية معرفة على R بحيث إن

$$x\,o\,y=x+y+xy\ \forall\quad x,y\ \in R$$

ادرس النظام $(R\ ,\ o)$ من حيث

i- هل النظام $(R\ ,\ o)$ نظام ذو عملية ثنائية ؟

ii- هل النظام $(R\ ,\ o)$ ابدالي ؟

iii- هل النظام $(R\ ,\ o)$ تجميعي ؟

iv- هل يوجد محايد للنظام ؟

v- هل يوجد نظير لكل عنصر في R ؟

9- إذا كانت العملية * معرفة على مجموعة الأعداد الصحيحة Z كما يأتي:

$$a*b=a+b+1 \qquad \forall \ \ a,b \in \ Z$$

ادرس النظام $(Z\ ,\ *)$ من حيث

i- النظام $(Z\ ,*)$ نظام ذو عملية ثنائية ؟

ii – النظام $(Z\ ,*)$ ابدالي .

iii- النظام $(Z\ ,*)$ تجميعي .

iv- وجود العنصر المحايد للنظام $(Z\ ,*)$.

v- وجود النظير لكل عنصر من عناصر Z.

10- اعتبر $(Z_5\ ,\ \oplus)$, $(Z_5\ ,\ \otimes)$, $(Z_5^*\ ,\ \otimes)$ في تمرين (5),

i- عين الأنظمة التي لكل عنصر فيها نظير , و إذا كان لا يوجد نظير في النظام لكل عنصر فأعط مثالاً وعين العناصر التي لها نظير .

ii- في النظام $(Z_5\ ,\ \oplus)$ أحسب $[1]^{-5}$

11- إذا كانت $A=\{1,2,3\}$ و أن $P(A)$ هي مجموعة كل المجموعـــة الجزئيـــة للمجموعة A , فأدرس الأنظمة $(P(A) , \cup)$, $(P(A), \cap)$ من حيث :

i- النظام ذو عملية ثنائية .

ii- النظام إبدالي .

iii- النظام تجميعي .

iv- وجود عنصر محايد .

12- اعتبر النظامين $(Z ,+)$, $(Z_5 , \oplus)$

ولتكن الدالة f معرفة كالآتي:

$$f: Z \to Z_5$$
$$f(a) = [a] \qquad , \forall\ a \in Z$$

أثبت أن f هو تشاكل ولكنه ليس تشاكل تقابلي

13- اعتبر النظامين $(Z ,+)$, $(Z_8 , \oplus)$

وأن الدالة $f: Z \to Z_8$

معرفة كالآتي

$$f(a) = \begin{cases} [0] & \text{إذا كان } a \text{ عددًا زوجيًا} \\ [4] & \text{إذا كان } a \text{ عددًا فرديًا} \end{cases}$$

i- أثبت أن f تشاكل ثم أوجد الصورة التشاكلية إلى Z أي $f(Z)$

ii- هل أن f تشاكل متباين , ولماذا ؟

iii- هل أن f تشاكل شامل , ولماذا ؟

iv- هل أن f تشاكل تقابلي , ولماذا ؟

14- اعتبر النظامين $(Z,+)$, $(Z_6, \oplus)$

وأن الدالة $f:Z \to Z_6$

معرفة كالآتي

$$f(a) = \begin{cases} [0] & \text{إذا كان } a \text{ عددًا زوجيًا} \\ [3] & \text{إذا كان } a \text{ عددًا فرديًا} \end{cases}$$

هل أن f تمثل تشاكل أم لا مع بيان السبب ؟

الفصل الثاني

الزمر Groups

[1-2] تعاريف ونظريات للزمرة
Definitions and theorems of group

تعريف (56.1-2):

إذا كان $(G,*)$ نظامًا ذا عملية ثنائية وتجميعًا فإنه يسمى شبه زمرة، وإذا كان بالإضافة إلى ذلك به عنصر محايد ولكل عنصر في عناصره نظير (معكوس) قيل أن النظام $(G,*)$ زمرة، أو اختصارًا يقال أن G زمرة .

تعريف (57.1-2):

إذا كان $(G,*)$ زمرة، وإن * عملية إبدالية على G، فإن G تسمى زمرة إبدالية أو زمرة أبلية.

مثال (58.1-2):

النظام $(R,+)$ زمرة إبدالية لأنه يحقق كل الشروط الواردة في التعاريف السابقة، حيث

(i) $(R,+)$ نظام مغلق لأن

$$\forall\ a,b \in R \Rightarrow a+b \in R$$

(ii) نظام إبدالي لأن

$$a+b = b+a \quad \forall\ A,b \in R$$

(iii) نظام تجميعي لأن

$$a+(a+b) = (a+b) +c \quad \forall\ A,b,c \in R$$

(iv) يوجد عنصر محايد هو الصفر لأن

$$a+0 = a \qquad \forall\ a \in R$$

(v) لكل عنصر $a \in R$ معكوس $a^{-1} = -a \in R$ لأن

$$a+a^{-1} = a+(-a) = 0 \ \forall\ a \in R$$

مثال (2-1. 59):

كل من الأنظمة التالية يمثل زمرة إبدالية (لماذا)

(i) $(R^*, .)$ ، (ii) $(Q, +)$ ، (iii) $(Q^*, .)$

(iv) $(Z, +)$ ، (v) $(Zn, +)$ ، (vi) $(C, +)$

مثال (2-1. 60):

النظام $(G, .)$ هو زمرة إبدالية حيث

$$G = \{a : a = 3^n, n \in z\}$$

الحل:

(i) نفرض أن $a,b \in G$ ، إذن توجد $m,n \in z$ بحيث إن

$a=3^m, b=3^n$

$\Rightarrow a.b = =3^m . 3^n = 3^{m+n} \quad , \quad m+n \in z$

$\Rightarrow a.b \in G$

إذن $(G, .)$ نظام مغلق

(ii) نفرض أن $a,b,c \in G$ إذن توجد $m,n,k \in z$

بحيث إن

$a=3^m$ ، $b=3^n$ ،$c=3^k$

$3^m (3^n.3^k) = 3^m (3^{n+k}) = 3^{m+n+k}$

$3^{m+n} . 3^k = (3^m.3^n) . 3^k = (a.b) .c$

إذن $(G, .)$ نظام مغلق وتجميعي أي شبه زمرة.

(iii) العنصر المحايد للنظام $(G, .)$ هو $(e = 3^{\circ} = 1)$
حيث

$$a.1 = a \quad \forall\, a \in G$$

(iv) لكل عنصر $a \in G$ يوجد معكوس وهو a^{-1} حيث

$$a.a^{-1} = 3^{n} . 3^{-n} \qquad = 3^{n-n} = 3^{\circ} = 1$$

إذن $(G, .)$ زمرة

(v) النظام $(G, .)$ إبدالي حيث لكل $a.b \in G$ فإن

$$a.b = 3^{n}.3^{m} \quad = 3^{m+n} \; = 3^{m}.3^{n} \; = b.a$$

وهذا يعني أن $(G, .)$ زمرة إبدالية.

مثال (2-1. 61):

تحقق من أن $(R, .)$ نظام جبري يمثل شبه زمرة ولا يمثل زمرة

الحل:

(i) $(R, .)$ النظام يمثل شبه زمرة لأنه نظام مغلق وتجميعي ومن السهل التحقق من هذا.

(ii) لا يمثل زمرة وذلك لن العنصر $0 \in R$ ليس له معكوس حيث لا يوجد عدد حقيقي يحقق المعادلة

$$00^{-1} = 1 = e$$

فلذا أن $(R, .)$ يمثل شبه زمرة ولا يمثل زمرة .

نظرية (2-1. 62):

(i) العنصر المحايد في الزمرة وحيد.

(ii) معكوس كل عنصر في الزمرة وحيد.

البرهان:

(i) سبق برهان هذه النظرية في (2-1. 38)

(ii) سبق برهان هذه النظرية في (2-1. 39)

نظرية (2-1. 63):

النظام (G , *) يمثل زمرة إذا كان وفقط إذا كان:

(i) عملية ثنائية .

(ii) * عملية تجميعية .

(iii) يوجد $e \in G$ بحيث إن

$$e * a = a \ \forall \ a \in G$$

(iv) لكل $a \in G$ يوجد $a' \in G$ بحيث أن

$$a' * a = e$$

البرهان:

إذا كان (G , *) زمرة فإن كل الخواص السابقة في (i) إلى (iv) تكون صحيحة والآن لنفرض أن الخواص الأربعة السابقة صحيحة والمطلوب إثبات أن (G , *) زمرة .

نفرض أن $a \in G$

من (iv) $\Rightarrow \exists a' \in G : \ a' * a = e$

من (iv) $\Rightarrow \exists a'' \in G : \ a'' * a' = e$

من (i) و (iii) $\Rightarrow a * a' = e * (a * a')$

من الخطوة الثانية $\Rightarrow a * a' = (a'' * a') * (a * a')$

من (iv) $= a'' * (a' * a) * a'$

من (iii) $= a'' * e * a'$

من الخطوة الثانية $= a'' * a' = e$

والنتيجة التي توصلنا إليها تعني أنه لكل $a \in G$

$$\exists a' \in G : a' * a = a * a' = e$$

وهو شرط وجود المعكوس

لأن

من (iv) $a * e = a * (a' * a)$

من (ii) $= (a * a') * a$

تم برهانه $= e * a$

من (iii) $= a$

وهذا يعني انه يوجد $e \in G$ ، بحيث

$$e * a = a * e = a \quad \forall \quad a \in G$$

وهو شرط العنصر المحايد

إذن (G , *) زمرة .

نظرية (2-1.64):

إذا كانت (G , *) شبه زمرة فإنها تكون زمرة إذا كانت وفقط إذا كانت المعادلتان

$$x * a = b ,$$
$$a * y = b$$

لها حلول في (G , *) لكل $a,b \in G$

البرهان:

إذا كانت $(G, *)$ زمرة ، وكان $a,b \in G$ فإن

$$x = b*a^{-1} \qquad , \qquad y = a^{-1}*b$$

عنصران في G ويحققان المعادلتين المذكورتين

يبقى إثبات انه إذا تحقق الشرط المذكور فإن $(G, *)$ تمثل زمرة وإثبات ذلك. سنثبت (iii) نفرض أن $a \in G$ إذن المعادلة

$$x * a = a$$

لها حل في $(G, *)$.

نفرض أن $a_\circ$ هو هذا الحل ، أي أن

$$a_\circ * a = a$$

وحتى تكون (iii) صحيحة يجب أن نثبت أن $a_\circ$ لا يعتمد على a ، أي يجب إثبات أن

$$a_\circ * b = b \ \forall \ b \in G$$

ولكن في المعطيات

$$\begin{aligned} a_\circ * b &= a_\circ * (a * y) \\ &= (a_\circ * a) * y && \text{، لأن * تجميعية} \\ &= a * y && \text{، لأن } (a_\circ * a = a) \\ &= b && \text{من المعطيات} \end{aligned}$$

إذن (iii) صحيحة .

(iv) حيث إن

$$x * b = a_\circ$$

لها حل في $(G, *)$ ، حيث $a_\circ$ هو العنصر الذي أثبتنا وجوده ، b أي عنصر في G ، إذن (iv) تحققه.

إذن $(G, *)$ زمرة.

تعريف (2-1.65):

مثال لعنصر a في أي نظام ذي عملية ثنائية $(G , *)$ أنــه مختــزل لنفسه إذا كان

$$a * a = a \quad \forall \quad a \in G$$

نظرية (2-1.66):

إذا كانت $(G , *)$ زمرة فإن

(i) العنصر المحايد e هو العنصر الوحيد المختزل لنفسه .

(ii) معكوس المعكوس هو العنصر الأصل أي أن

$$(a^{-1})^{-1} = a$$

(iii) لكل $a,b \in G$ فإن

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

(iv) إذا كانت * إبدالية فإن

$$(a * b)^2 = a^2 * b^2 \quad \forall \quad a,b \in G$$

البرهان:

$$\begin{aligned} a * a = a \quad &\Rightarrow a^{-1} * (a * a) = a^{-1} * a \\ &\Rightarrow (a^{-1} * a) * a = e \\ &\Rightarrow e * a = e \\ &\Rightarrow a = e \end{aligned}$$

أي أن المحايد e هو العنصر الوحيد المختزل لنفسه .

(ii) نفرض أن

$$(a^{-1})^{-1} = b \Rightarrow a^{-1} * (a^{-1})^{-1} = a^{-1} * b$$
$$\Rightarrow e = a^{-1} * b$$
$$\Rightarrow a * e = a * (a^{-1} * b)$$
$$\Rightarrow a = (a * a^{-1}) * b$$
$$\Rightarrow a = e * b$$
$$\Rightarrow a = b$$

إذن $(a^{-1})^{-1} = a$

(iii)
$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$
$$= a * e * a^{-1}$$
$$= a * a^{-1} = e$$

إذن $b^{-1} * a^{-1}$ هو معكوس $a * b$ أي

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

(iv)

$$(a * b)^2 = (a * b) * (a * b)$$
$$= (a * b) * (b * a)$$
$$= a * (b * b) * a$$
$$= a * b^2 * a$$
$$= a * a * b^2 = a^2 * b^2$$

نظرية (2-1. 67):

إذا كانت $(G, *)$ زمرة فإن

(i) لكل المعادلتين $x * a = b$ و $a * x = b$

حل وحيد في G .

(ii) خاصية الحذف في اليمين واليسار:

$$a * x = a * y \Rightarrow x = y \quad \forall\ a, x, y \in G$$
$$x * a = y * a \Rightarrow x = y \quad \forall\ a, x, y \in G$$

البرهان:

(i) حيث عن G زمرة فإن كل عنصر فيها له نظير .

إذن

لأن * عملية ثنائية $a * x = b \Rightarrow (x * a) * a^{-1} = b * a^{-1}$

لأن * عملية تجميعية $\Rightarrow x * (a * a^{-1}) = b * a^{-1}$

تعريف النظير $\Rightarrow x * e = b * a^{-1}$

تعريف المحايد (I)........... $\Rightarrow x = b * a^{-1}$

إذن $x = b * a^{-1}$ هو حل للمعادلة $x * a = b$

ولإثبات أن هذا الحل الوحيد نفرض أن $t \in G$ هو حل آخر للمعادلة نفسها،

إذن

$$\begin{aligned} t * a = b &\Rightarrow (t * a) * a^{-1} = b * a^{-1} \\ &\Rightarrow t * (a * a^{-1}) = b * a^{-1} \\ &\Rightarrow t * e = b * a^{-1} \\ &\Rightarrow t = b * a^{-1} \quad \ldots\ldots\ldots\ldots\text{(II)} \end{aligned}$$

وفي (I) ، (II) ينتج أن $x = t$ ، أي أن المعادلة $x * a = b$ لها حل وحيد وهو $b * a^{-1}$

وبالمثل يمكن إثبات أن للمعادلة $a * x = b$ حل وحيد هو $x = a^{-1} * b$.

(ii) نفرض أن

$$\begin{aligned} a * x = a * y &\Rightarrow a^{-1} * (a * x) = a^{-1} * (a * y) \\ &\Rightarrow (a * a^{-1}) * x = (a^{-1} * a) * y \\ &\Rightarrow e * x = e * y \Rightarrow x = y \end{aligned}$$

وبالمثل يمكن إثبات خاصية الحذف في اليمين

ملاحظة (2-1. 68):

إذا كانت (* , G) زمرة وكانت G مجموعـــة منتهـــية فإننـــا نقـــول أن (* , G) زمرة منتهية ، ونسمى عدد العناصر |G| رتبة الزمرة G ، كما نقول أن G زمرة غير منتهية إذا كانت G مجموعة غير منتهية.

نظرية (2-1. 69):

شبه الزمرة المنتهية (* , G) تكون زمرة ، إذا كان وفقــط إذا كـــان خاصيتا الحذف في اليمين واليسار متحققتين .

البرهان:

رأينا فيما سبق أن خاصيتي الحذف متحققتان في أي زمرة نظرية (2-1. 56) الآن نفرض أن (* , G) شبه زمرة منتهية تتحقق فيها خاصيتا الحذف ، وأن

$$G = \{ a_1 , a_2 , ... , a_n \}$$

حيث $|G| = n$ ، أي أن n عدد عناصر G .

ونفرض أن

$$a \in G \Rightarrow a_1 * a , a_2 * a , ... , a_n * a \in G$$

نلاحظ أن كل العناصر التي حصل عليها مختلفة لأنه إذا كان

$$a_i * a = a_j * a \qquad , \qquad a_i , a_j \in G$$

$\Rightarrow a_i = a_j$ في خاصية الحذف من اليمين

إذن

$$a_1 * a , a_2 * a_1 , ... , a_n * a$$

عناصر مختلفة في G عددها n

$$\therefore\ G = \{ a_1 * a , a_2 * a , \ldots\ldots , a_n * a \}$$

بالطريقة نفسها يمكن استنتاج أن (باستخدام خاصية الحذف اليسرى)

$$G = \{ a * a_1 , a * a_2 , \ldots\ldots , a * a_n$$

إذن

$$G = \{ a_1 , a_2 , \ldots , a_n \}$$

$$= \{ a_1 * a , a_2 * a , \ldots\ldots , a_n * a \}$$

$$= \{ a * a_1 , a * a_2 , \ldots\ldots , a * a_n \}$$

وهذا معناه انه إذا كانت

$$b \in G \Rightarrow \exists\ a_r , a_s \in G : a_r * a = b , a * a_s = b$$

وهذا يبين أن المعادلتين

$$x * a = b \qquad , \qquad a * y = b$$

لهما حلول في G لأي عنصرين $a,b \in G$ ومن نظرية (2–64.1) ينتج أن $(G , *)$ زمرة .

[2-2] زمرة التباديل
Permutation Group

تعريف (2-2 .70) :

نفرض أن $S = \{1,2,\ldots\ldots,n\}$ أي تقابل $f : s \to s$ يسمى تبدلية، معلوم أن عدد التقابلات على S يساوي $(n!)$ ، مجموعة التقابلات على المجموعة S تسمى مجموعة التبديلات من الدرجة n ويرمز لها بالرمز S_n.

والتطبيق (الدالة) f يسمى تبديلاً لأن تأثيره على عناصر S هو مجرد تبديل في ترتيبها وستكتب التبديلة دائمًا f على هيئة مصفوفة عدد صفوفها 2 وأعمدتها n .

مثال (2-2 .71) :

جد عناصر S_3

الحل:

$$S_3 = \left\{ I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

ملاحظة (2-2 .72) :

(i) بما أن التبديلة تطبيق فإننا سنعرف عملية تحصيل التبديلة " o " على أنها عملية تحصيل التطبيقات التي درسها الطالب فيما سبق.

(ii) بما أن تحصيل تطبيقات تقابلان هو تقابل ، إذن محصلة تبديلين هي تبديلة إذن (S_n ,o) هو نظام ذو عملية.

(iii) العملية " o " دامجة لأن عملية تحصيل التطبيقات تجميعية.

(iv) يوجد عنصر محايد في S_n وهو تطبيق الوحدة $I_s : S \to S$ ، المعروف بالصيغة

$$I_s = \begin{pmatrix} 1 & 2 & ..... & n \\ 1 & 2 & ..... & n \end{pmatrix}$$

(v) لكل $f \in S_n$ يوجد f^{-1} بحيث إن

$$f\, o\, f^{-1} = f^{-1}\, o\, f = I_s$$

لأن f تقابل.

مما تقدم نستنتج أن (S_n ,o) هي زمرة ، وتسمى زمرة التماثل في الدرجة n (أو زمرة التباديل من الدرجة n) (أو زمرة التناظر من الدرجة n).

ملاحظة (73. 2-2):

إذا كانت $f \in S_n$ فإننا نكتب f بالشكل

$$f = \begin{pmatrix} 1 & 2 & 3 & ...... & n \\ f(1) & f(2) & f(3) & ...... & f(n) \end{pmatrix}$$

لاحظ أن $f_{(j)}$ هو صورة العنصر $j \in S$ هذا ويمكن كتابة f بأشكال أخرى بشرط أن نحافظ على صورة عناصر S تحت تأثير f (أي نكتب $f_{(j)}$ تحت j لجميع قيم j) .

فمثلاً إذا كانت

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in S_5$$

فإن

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \dots$$

ملاحظة (2-2 .74):

سنعتبر أن f مكتوب في الصورة القياسية عندما تكون عناصر S مكتوبة في الصف الأول (العلوي) بشكل تصاعدي من اليسار لليمين لاحظ أن رتبة الزمرة (S_n , o) تساوي $n!$ ، أي أن $|S_n| = n!$.

مثال (2-2 .75):

إذا كان $f,g \in S_6$ ، حيث

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \quad , \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

أوجد كلاً من f^{-1} ، f^2 ، $g o f$ ، $(f o g)^{-1}$ ، $f^{-1} o g^{-1}$ ، $g^{-1} o f^{-1}$ هل S_n إبدالية ؟

هل $(f o g)^{-1} = f^{-1} o g^{-1}$ ؟ تحقق أن $(f o g)^{-1} = g^{-1} o f^{-1}$ ؟

الحل:

(i) لإيجاد f^{-1} نبادل بين موضعي الصفين في f فتحصل على

$$f^{-1} = \begin{pmatrix} 2 & 3 & 1 & 6 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$$

لاحظ أننا وضعنا f^{-1} في الصورة القياسية في الخطوة الثانية .

(ii)

$$f^2 = f_o f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix} \, o \, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}$$

(iii)

$$f_o g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix} \, o \, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 4 & 2 \end{pmatrix}$$

(iv)

$$g_o f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 6 & 5 \end{pmatrix}$$

(v)

$$(f_o g)^{-1} = \begin{pmatrix} 3 & 1 & 6 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$$

(vi)

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix}$$

(vii)

$$g^{-1} \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$$

واضح أن S_n ليست إبدالية لأن عملية تحصيل التطبيقات ليست إبدالية في الحالة العامة وكمثال على ذلك فإن

$$f \circ g \neq g \circ f$$

(viii) واضح كذلك أن

$$(f \circ g)^{-1} \neq f^{-1} \circ g^{-1}$$

وكذلك

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

تعريف (2-2. 76):

سوف نحاول كتابة التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ بالصورة (4 3 2 1) حيث كتب صورة كل عنصر على يمينيه، صورة العنصر 1 هي 2 وصورة العنصر 2 هي 3 وصورة العنصر 3 هي 4 أما صورة العنصر 4 هي 1 المكتوب في أقصى اليسار، وهذه الصورة في كتابة التبديلات تسمى التعبير الدائري للتبديلات.

مثال (2-2. 77):

نكتب التبديلة التالية بالتعبير الدائري للتبديلات

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 4\ 2\ 5) = (2\ 5\ 1\ 3\ 4)$$

ملاحظة (2-2. 78):

نلاحظ التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ والآن لو حاولنا كتابة التبديلة بالتعبير الدائري للتبديلات وبدأنا بالعنصر 1، فإنه يمكننا كتابة التبديلة بالصورة الدائرية والأفضل أن نكتب تلك التبديلة بالصورة (4)(3) (12) أو بالصورة الأسهل (12) ويفهم منها أن صورة العنصر 2 هي 1 وصورة 1 هي 2 وصورة 3 هي 3، أما صورة العنصر 4 فهو نفسه 4.

مثال (2-2. 79):

(i) يمكن التعبير عن التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ بالصورة الدائرية

كالتالي $(12)\ (35)$

(ii) نكتب عناصر S_3 بالتعبير الدائري

$$S_3 = \{ (1)(2)(3), (23), (13), (12), (123), (132) \}$$

تعريف (2-2. 80):

لنأخذ التبديلة $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ التي تكتب بالصورة (12) نلاحظ أن تأثير تلك التبديلة على المجموعة $S=\{1, 2, 3, 4\}$ هو مجرد تبادل موضعي العنصرين 2 ،1 وترك باقي العناصر في مواضعها وكل تبديلة تؤول إلى تبديلة طولها 2 تسمى تبادل موضع .

ملاحظة (2-2. 81):

لنأخذ الآن محصلة التبديلتين

$$(12), (13) \in S_3$$

$$(13) \circ (12) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

وبالمثل نجد

$$(12)\,o\,(13) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \,o\, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ \ 3\ \ 2)$$

أي أن كل في التبــديلتين $(3\ \ 2\ \ 1)$ ، $(2\ \ 3\ \ 1)$ يمكــن كتابتهــا كمحصلة تبادلين للموضع، وفي الواقع فإن، أي تبديلة يمكن كتابتها كمحصلة عــدة تبادلات للموضع.

مثال (2-2. 82):

(i) أوجد محصلة $(12)\ o\ (13)\ o\ (14)$ في S_4

(ii) أوجد محصلة $(12)\ o\ (13)\ o\ (14)\ o\ (15)$ في S_5

الحل:

(i) $(14)\ o\ (13)\ o\ (12) = (1\ 2\ 3\ 4)$

(ii) $(15)\ o\ (14)\ o\ (13)\ o\ (12) = (1\ 2\ 3\ 4\ 5)$

مثال (2-2. 83):

عبر عن كل من التبــديلتين $(4\ 3\ 2\ 1)$، $(2\ 4\ 1)$ محــصلة عــدة تبــادلات للموضع.

الحل:

$$(1\ 2\ 3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (14)\ (13)\ (12)$$

يترك الجزء الآخر للطالب.

تعريف (2-2. 84):

التبديلات الزوجية هي تلك التي يمكن كتابتها على هيأة محصلة عدد زوجي من تبادلات الموضع أما التبديلات الفردية فهي التي يمكن كتابتها على هيأة محصلة عدد فردي في تبديلات الموضع .

سنرمز لمجموعة التبديلات الزوجية بالرمز S_n^+ ولمجموعة التبديلات الفردية بالرمز S_n^-.

مثال (2-2.85):

في المثال (2-2. 72) ، أن التبديلة (4 3 2 1) فردية في حين إن التبديلة (2 4 1) زوجية.

مثال (2-2. 86):

$$S_3^+ = \{I,(123),(132)\},$$
$$S_3^- = \{(12),(13),(23)\},$$
$$S_4^+ = \{I,(234),(243),(134),(143),(124),(142),(123),(132),(12)(34),(13)(24),(14)(23)\}$$
$$S_4^- = \{(1234),(1342),(1432),(1243),(1324),(1432),(12),(13),(14),(23),(24),(34)\}$$

نظرية (2-2. 87):

(i) محصلة تبديلتين زوجيتين تبديلة زوجية.

(ii) محصلة تبديلتين فرديتين تبديلة زوجية.

(iii) تحصيل تبديلتين واحدة زوجية والأخرى فردية تبديلة فردية.

البرهان:

حيث إن التبديلة تكون زوجية أو فردية تبعًا لكونها محصلة عدد زوجي أو فردي في تبادلات الموضع فإن برهان النظرية واضح من كون:

(i) عدد زوجي + عدد زوجي = عددًا زوجيًّا.

(ii) عدد فردي + عدد فردي = عددًا زوجيًّا.

(iii) عدد زوجي + عدد فردي = عددًا فرديًّا.

ملاحظة: فيما يلي طريقة مبسطة كمعرفة كون تبديلة ما زوجية أو فردية وهو أن يوصل كل عنصر في الصف الأول بنفسه في الصف الثاني، إذا كان عدد التقاطعات التي تحدث في عملية التوصيل زوجيًّا فإن التبديلة تكون زوجية أما إذا كانت عدد التقاطعات فرديًا فإن التبديلة تكون فردية .

مثال (2-2. 88):

صنف التبديلات الآتية من حيث كونها زوجية أو فردية .

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

الحل:

(i)

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

تبديلة زوجية لأن عدد التقاطعات = 2

(ii)

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

تبديلة فردية لأن عدد التقاطعات = 1

(iii)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

تبديلة زوجية لأن عدد التقاطعات = 2

(iv)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

تبديلة فردية لأن عدد التقاطعات = 5

(v)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

تبديلة زوجية لأن عدد التقاطعات = 3

نظرية (2-2. 89):

لتكن g,f تبدليتين من الدرجة نفسها أي $f,g \in S_n$ إذن

$$(f\,o\,g)^{-1} = g^{-1}\,o\,f^{1}$$

البرهان:

المطلوب إثباته هو أن معكوس $f\,o\,g$ و هو $g^{-1}\,o\,f^{1}$ ، أي أن

$$(f\,o\,g)\;o\;(g^{-1}\,o\,f^{1}) = I$$

كن

$$(f \circ g) \circ (g^{-1} \circ f^{1}) = (f \circ (g \circ (g^{-1} \circ f^{1}))$$

$$f = f \circ ((g \circ g^{-1}) \circ f^{-1}))$$

$$= f \circ (I \circ f^{-1})$$

$$= f \circ f^{-1} = I$$

مثال (2-2. 90):

أثبت أن $(S_3 , \circ)$ زمرة غير إبدالية.

الحل:

$S_3 = \{I , (1\,2\,3) , (1\,3\,2) , (12) , (13) , (23)\}$

نكون الجدول الذي يمثل هذا النظام ، وأوضح أن $(S_3 , \circ)$ نظام ذو عملية ، أي أن "$\circ$" عملية ثنائية على S_3 وحيث إن عملية تحصيل الرواسم عملية تجميعية، إذن عملية تحصيل التبديلات ∘ تجميعية على S_3 من الجدول نستنتج أن I هو العنصر المحايد وأن معكوسات العناصر هي حسب الجدول كالتالي:

$\circ$	I	(1 2 3)	(1 3 2)	(12)	(13)	(23)
I	I	(1 2 3)	(1 3 2)	(12)	(13)	(23)
(1 2 3)	(1 2 3)	(1 3 2)	I	(13)	(23)	(12)
(1 3 2)	(1 3 2)	I	(1 2 3)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	I	(13 2)	(1 2 3)
(13)	(13)	(12)	(23)	(1 2 3)	I	(1 3 2)
(23)	(23)	(13)	(12)	(1 3 2)	(1 2 3)	I

العنصر : (23) (13) (12) (1 3 2) (1 2 3) I

معكوسه : (23) (13) (12) (1 2 3) (1 3 2) I

لذا فإن النظام (S_3 , o) زمرة ، ولكنها ليست إبدالية لأن الجدول غير متماثــل حول قطره الرئيسي ، فمثلاً :

$$(12) \; o \; (13) = (1\,3)$$
$$(13) \; o \; (12) = (1\,2\,3)$$
$$\Rightarrow (12) \; o \; (13) \neq (13) \; o \; (12)$$

ملاحظة (2-2. 91):

نلاحظ من الجدول أن:

(i) جميع العناصر تظهر في كل صف وكل عمود .

(ii) لايتكرر ظهور أي عنصر في أي صف أو أي عمود .

(iii) وإذا لم يتحقق هذان الشرطان فإن الجدول لا يمثل زمرة .

[3-2] الزمرة الجزئية
Subgroup

تعريف (2-3. 92):

نفرض أن $(G\ ,\ *)$ زمرة، وأن $\phi \neq H \subseteq G$ ، إذا كانت $(H\ ,\ *)$ زمرة أيضًا فإننا نقول إن $(H\ ,\ *)$ هي زمرة جزئية في $(G\ ,\ *)$.

ملاحظة (2-3. 93):

في أي زمرة $(G\ ,\ *)$ توجد دائمًا زمرتان جزئيتان وأن كانتا غير هامتين هما $(\{e\}\ ,\ *)$ و $(G\ ,\ *)$ نفسها حيث e عنصر الوحدة في الزمرة.

مثال (2-3. 94):

(i) $(Z\ ,\ +)$ زمرة جزئية من الزمرة $(Q\ ,\ +)$ ، لماذا ؟

(ii) $(\{1,-1\}\ ,\ o)$ زمرة جزئية من الزمرة $(\{1,-1,i,-i\}\ ,\ o)$، لماذا؟

(iii) $(\{[1], [2],[4]\}\ ,\ \otimes)$ زمرة جزئية في الزمرة $(Z_7^*, \otimes)$، لماذا؟

(iv) $(\{[1], [2]\}\ ,\ \otimes)$ ليست زمرة جزئية في الزمرة $(Z_7^* \otimes)$، لماذا؟

(v) $(Z^+\ ,\ +)$ ليست زمرة جزئية في الزمرة $(Z\ ,\ +)$، لماذا؟

حيث Z^+ مجموعة الأعداد الصحيحة الموجبة فقط.

نظرية (2-3. 95):

(i) أي زمرة جزئية في زمرة إبدالية تكون أيضًا إبدالية ، ولكن إذا كانت الزمرة الجزئية إبدالية فليس في الضروري أن تكون الزمرة الأصلية إبدالية.

(ii) العنصر المحايد في أي زمرة جزئية هو العنصر المحايد في الزمرة الأصلية .

(iii) معكوس أي عنصر في زمرة جزئية هو معكوسه في الزمرة الأصلية .

البرهان:

(i) نفرض أن $(G , *)$ زمرة إبدالية وأن $(H , *)$ زمرة جزئية منها.

$$a,b \in H \subseteq G \Rightarrow a,b \in G \Rightarrow a*b = b*a$$

لأن G زمرة إبدالية.

إذن $(H , *)$ زمرة إبدالية أيضًا.

ولإثبات باقي هذا الجزء نعتبر المثال التالي:

باعتبار (S_3 , o) , (S_3^+ , o) ، نعلم بأن (S_3 , o) زمرة ليست إبدالية من المثال (2-2. 80).

الآن نكون جدول (S_3^+ , o) ، ويتضح أن (S_3^+ , o) هي زمرة جزئية إبدالية من (S_3 , o) على الرغم من أن (S , o) ليست إبدالية.

o	I	(1 2 3)	(1 3 2)
I	I	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	I
(1 3 2)	(1 3 2)	I	(1 2 3)

(ii) الآن نفرض أن العنصر المحايد في الزمرة الأصلية $(G , *)$ هــو e وأن العنصر المحايد في الزمرة الجزئية $(H , *)$ هو e' .

إذن

$$a * e = a \quad , \quad a * e' = a \qquad \forall a \in H \subseteq G$$

$$\Rightarrow a * e = a * e'$$

وباستخدام خاصية الحذف اليسرى من الزمر نحصل على

$$e = e'$$

(iii) نفرض أن معكوس العنصر $a \in H$ هو $b \in H$.

إذا كانت $d \in G$ هي معكوس a في G فإن ، وحسب (ii)

$$a * b = e \quad , \quad a * d = e$$

$$\Rightarrow a * b = a * d$$

وباستخدام خاصية الحذف ينتج

$$b=d$$

وبهذا يتم برهان النظرية

نظرية (2-3. 96):

إذا كانت H مجموعة جزئية غير خالية في G حيث $(G , *)$ زمرة ، فإن $(H , *)$ تكون زمرة جزئية في $(G , *)$ إذا كان وفقط إذا كان:

(i) H مغلقة بالنسبة للعملية * أي أن

$$a, b \in H \Rightarrow a * b \in H$$

(ii) معكوس أي عنصر في H ينتمي إلى H ، أي أن

$$a \in H \Rightarrow a^{-1} \in H$$

البرهان:

أولاً: إذا كانت (* , H) زمرة جزئية في (* , G) ، فإن الشرطين (i) ، (ii) يتحققان.

ثانيًا: نفرض أن الشرطين (i) ، (ii) يتحققان وسوف نثبت أن (* , H) هي زمرة

1) في الشرط (i) نجد أن (* , H) نظام ذو عملية .
2) وحيث $H \subseteq G$ ، وأن العملية * تجميعية على جميع عناصر G ، إذن فهي تجميعية على عناصر H .
3) من (ii)

$$\forall a \in H \exists a^{-1} \in H$$

ومن (i) نستنتج أن

$$a * a^{-1} \in H \Rightarrow e \in H$$

4) معكوس أي عنصر في H ينتمي إلى H في الشرط (ii) وعلى هذا فإن جميع شروط الزمرة تتحقق بالنسبة للنظام (* , H) فإن ، (* , H) زمرة جزئية في (* , G).

نظرية (2-3-97):

إذا كانت H مجموعة جزئية غير خالية في G حيث (* , G) زمرة، فإن (* , H) تكون زمرة جزئية من (* , G) إذا كانت وفقط إذا كانت

$$a * b^{-1} \in H \quad \forall \quad a , b \in H$$

البرهان:

أولاً : إذا كانت H جزئية في الزمرة (* , G) ، فإن

$$a,b \in H \Rightarrow a * b^{-1} \in H$$

ثانيًا: نفرض أن

$a * b^{-1} \in H \forall a, b \in H$

(من الشرط أن $H \neq \phi$)

$\Rightarrow \exists a \in H \Rightarrow a * a^{-1} \in H$

$\Rightarrow e \in H$

إذن H تحتوي على العنصر المحايد e

الآن من الشرط المعطى

$\forall a \in H, e * a^{-1} = a^{-1} \in H$

أي أن لكل عنصر $a \in H$ يوجد معكوس $a^{-1} \in H$ ومن الشرط المعطي وفي كون كل عنصر في H له معكوس في H نستنتج أن (H , *) نظام ذو عملية لأن

$a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

وحيث إن $H \subseteq G$ ، فإن (H , *) تجميعية .

إذًا (H , *) زمرة جزئية من (G , *) .

نظرية (2-3. 98):

إذا كانت (H , *) زمرة جزئية في (G , *) ، فإن

$aH = Ha \Leftrightarrow a^{-1} Ha = H \ , a \in H$

البرهان:

(i) نفرض أن

$aH = Ha \ , a \in G$

ونريد أن نثبت أن

$H = a^{-1}Ha$

لذلك نفرض أن

$$\begin{aligned} b\in H &\Rightarrow ab\in aH \Rightarrow ab\in Ha \\ &\Rightarrow ab = ha \quad , \quad h\in H \\ &\Rightarrow b = a^{-1}ha \\ &\Rightarrow b \in a^{-1}Ha \\ \Rightarrow H &\subseteq a^{-1}Ha \quad ....(I) \end{aligned}$$

الآن نفرض أن

$$d \in a^{-1}Ha \Rightarrow d= a^{-1}h_1a \quad , \quad h_1 \in H$$

ولكن

$$\begin{aligned} &h_1a \in Ha = aH \\ &\therefore h_1a = ah_2 , \quad h_2 \in H \\ &\therefore d=a^{-1}ah_2 , \quad h_2\in H \\ &\Rightarrow d= h_2 \in H \\ &\Rightarrow a^{-1}Ha \subseteq H \quad ....(II) \end{aligned}$$

ومن (I) , (II) ينتج أن $H = a^{-1}Ha$

(ii) نفرض أن

$$H = a^{-1}Ha \quad , \quad a \in G$$

ونريد إثبات أن $aH = Ha$

لذلك نفترض أن

$$\begin{aligned} b\in aH &\Rightarrow b=ah_1 , h_1 \in H \\ &\Rightarrow b=ah_1 , h_1 \in a^{-1}Ha \\ &\Rightarrow b=ah_1 , h_1= a^{-1}h_2a , h_2 \in H \\ &\Rightarrow b=aa^{-1} h_2a = eh_2a \\ &\Rightarrow b=h_2a , h_2\in H \\ &\Rightarrow b\in Ha \\ &\Rightarrow aH\subseteq Ha \quad ....(I) \end{aligned}$$

الآن نفرض أن

$$d \in Ha \Rightarrow d = h_1 a \;,\; h_1 \in H$$
$$\Rightarrow d = e_1 h_1 a = a a^{-1} h_1 a \;,\; h_1 \in H$$

ولكن

$$h_1 \in H \Rightarrow a^{-1} h_1 a \in a^{-1} Ha = H$$
$$\Rightarrow a^{-1} h_1 a = h_2 \in H$$
$$\therefore d = a h_2 \;,\; h_2 \in H \Rightarrow d \in aH$$
$$\Rightarrow aH \subseteq Ha \text{ ....(II)}$$

ومن (I) , (II) ينتج أن $aH = Ha$

نظرية (2-3. 99):

إذا كانت $(H_i , *)$ حيث $i = 1,2,...,n$ ، زمرة جزئية من الزمرة $(G , *)$ فإن $(H , *)$ هي زمرة جزئية من الزمرة $(G , *)$ ، حيث

$$\bigcap_{i=1}^{n} Hi = H$$

البرهان:

حيث إن $(H_i , *)$ زمرة جزئية من الزمرة $(G,*)$ لكل $i = 1,2,...,n$ فإن

$$e \in Hi \;\forall\; i = 1,2,........,n$$

$$\Rightarrow e \in \bigcap_{i=1}^{n} Hi = H \Rightarrow e \in H \Rightarrow H \neq \phi$$

الآن نفرض أن $a,b \in H$

$$a,b \in \bigcap_{i=1}^{n} Hi \Rightarrow a,b \in Hi \forall i = 1,2,..........,n$$

من نظرية (2-3. 87)

$$\Rightarrow\ a * b^{-1} \in\ H_i\ \forall\ \ i = 1,2,.......,n$$

$$\Rightarrow a,b^{-1} \in \bigcap_{i=1}^{n} Hi = H$$

$$\Rightarrow\ a * b^{-1} \in H$$

ومن نظرية (2-3. 87) نستنتج أن $(H , *)$ زمرة جزئية من $(G , *)$

مثال (2-3. 100):

على الرغم من أن تقاطع أي عدد منتهٍ من الزمر، ما هو إلا زمـــرة جزئيـــة منها، فإن اتحاد زمرتين جزئيتين من زمرة ما ليس بالضرورة زمرة جزئية منها. وكمثال على ذلك نعتبر (S_3 , o).

واضح أنه ، إذا كان

$H_1= \{I , (12)\}$, $H_2= \{I , (13)\}$

فإن (H_1 , o) , (H_2 , o) هي زمرة جزئية من (S_3 , o)، حيــث $(H_1 \cup H_2 , o)$ ليست زمرة جزئية في (S_3 , o).

تعريف (2-3. 101):

إذا كانت $(H_i , *)$ زمرة ، $a \in G$ فإن رتبة العنصر a هي أقل عــدد صحيح n (أن وجد) بحيث إن $a^n = e$ ، حيث إن e هو العنصر المحايد في الزمرة $(G ,*)$، وفي هذه الحالة تكتب $|a|=n$.

وإذا كان $a^n \neq e$ لأي $n > 0$، قيل أن رتبة العنصر a لانهائية.

واضح أن $|e|= 1$ أي أن رتبة العنصر المحايد في أي زمرة هي الواحد الصحيح.

مثال (2-3. 102):

في الزمرة $(Z , +)$ أي عنصر ماعدا الصفر لانهائي الرتبة أما $|0|=1$

مثال (2-3. 103):

في الزمرة $(S3 , o)$ رتبة العناصر هي الآتي :

العنصر	I	(12)	(13)	(23)	(1 2 3)	(1 3 2)
الرتبة	1	2	2	2	3	3

فمثلاً :

$$(12)\, o\, (12) = I \Rightarrow |(12)| = 2$$
$$(1\ 2\ 3)\, o\, (1\ 2\ 3)\, o\, (1\ 2\ 3) = (1\ 2\ 3)\, o\, (1\ 3\ 2) = I$$
$$\Rightarrow |(1\ 2\ 3)| = 3$$

ملاحظة (2-3. 104):

في الأمثلة السابقة يتضح أنه توجد بعض الزمر كل عناصرها لها رتبة، كما توجد بعض الزمر ليس لكل عناصرها رتبة.

نظرية (2-3. 105):
إذا كانت $(G , *)$ زمرة منتهية فإن جميع عناصرها لها رتبة.

البرهان:

نفرض أن $a \in G$ ،

$$X = \{a^0 = e, a, a^2, a^3, ...\} \subseteq G$$

وحيث إن عدد عناصر G منته فإن عناصر X لا يمكن أن تكون كلها مختلفة وإلا كان عدد عناصر G لانهائيًا نفرض أن

$$a^m = a^n \quad , \quad m<n \quad ....(I)$$

وحيث إن $a^m \in G$ فإن له معكوس وهو a^{-m} وبضرب طرفي (I) في a^{-m} نحصل على

$$a^m * a^{-m} = a^n * a^{-m}$$
$$\Rightarrow e = a^{n-m} = a^k \ , \ k = n-m \in Z^+$$

إذن يوجد عدد صحيح موجب k بحيث إن $a^k = e$

ولكن في المحتمل أن هذا العدد ليس وحيدًا ،

نفرض أن

$$y = \{k_{1,}, k_2, k_3, ..., k_i \in Z^i, a^{ki} = e, i = 1,2,.......\}$$

وحيث إن المجموعة y هي مجموعة أعداد صحيحة موجبة، إذن فهي محـــددة من أسفل.

نفرض أن (من فرضية أكبر من سفلي)

$$L = \min y \in Z^+$$

إذن L هو أصغر عدد صحيح موجب بحيث إن $a^L = e$ ، أي أن $|a| = L$.

إذن رتبة العنصر a هي L ، وحيث إن a عنصر اختياري في الزمـــرة $(G , *)$، إذن كل عناصرها لها رتب.

[2-4] الزمرة الدائرية والمجموعات المصاحبة
Cyclic group and Cosets

تعريف (2-4. 106):

يقال إن $(G , *)$ زمرة دائرية إذا وجد بها عنصر a بحيث إن :

$\forall\ x \in G\ \exists\ n \in Z : x = a^n$

أو ($x=na$ في حالة الجمع).

في هذه الحالة $(G , *)$ تسمى زمرة دائرية مولدة بالعنصر a وتكتب

$G = \langle a \rangle = \{a^n : n \in Z\}$

مثال (2-4. 107):

النظام (G , o) حيث $G = \{1 , -1 , i , -i\}$ ، $\sqrt{-1}$ ، هو زمرة دائرية مولدة بالعنصر i لأن

$i^1 = i \quad , \quad i^2 = -1 \quad , \quad i^3 = -i \quad , \quad i^4 = 1$

إذن كان عناصر الزمرة (G , o) حصلنا عليها كقوى للعنصر (i-) هو مولد آخر لها لأن

$(-i)^1 = -i \quad , \quad (-i)^2 = -1 , (-i)^3 = +i \quad , \quad (-i)^4 = 1$

لاحظ أن

$| i | = | -i | = 4$

إذن $G = \langle i \rangle = \langle -i \rangle$

مثال (2-4. 108):

الزمرة (G , o) حيث

$G = \{I , (1\ 2\ 3\ 4) , (1\ 3)(2\ 4) , (1\ 4\ 3\ 2)\} \subseteq S_4$

هي زمرة دائرية مولدها (1 2 3 4) لأن

$$(1\ 2\ 3\ 4)^1 = (1\ 2\ 3\ 4)$$
$$(1\ 2\ 3\ 4)^2 = (13)\ (24)$$
$$(1\ 2\ 3\ 4)^3 = (1\ 4\ 3\ 2)$$
$$(1\ 2\ 3\ 4)^4 = I$$

وعلى الطالب التأكد من أن (G, o) هي فعلاً زمرة .
وبهذا يمكن كتابة G بالشكل التالي:

$$G = \langle\ (1\ 2\ 3\ 4)\ \rangle$$
$$|G| = |(1\ 2\ 3\ 4)| = 4$$

مثال (2-4. 109):
النظام $(Z, +)$ زمرة دائرية مولدة بالعنصر $1 \in Z$
لأن

$$\langle\ 1\ \rangle = \{1^n : n \in Z\} = Z$$

لاحظ أن

$$1^n = \underbrace{1 + 1 + \ldots\ldots + 1}_{n\ \text{مرة}} = n$$

ماذا تلاحظ عن رتبة العنصر $1 \in Z$ ؟

مثال (2-4. 110):
النظام $(Z_6, \oplus)$ زمرة دائرية مولدة بالعنصر [1]

$$[1]^1 = [1]\ ,\quad [1]^2 = [1] \oplus [1] = [2]\ ,$$
$$[1]^3 = [1]^2 \oplus [1] = [2] \oplus [1] = [3], \ldots\ldots\ldots\ldots$$
$$[1]^6 = [1]^5 \oplus [1] = [5] \oplus [1] = [6] = [0] = e$$
$$\Rightarrow |[6]| = 6 = |Z_6|$$
$$\therefore \langle [1] \rangle = \{ [1], [1]^2, [1]^3, [1]^4, [1]^5, [1]^6 \}$$
$$= \{ [1], [2], [3], [4], [5], [0] \} = Z_6$$

مثال (2-4. 111):

أوجد $\langle [1] \rangle$ ، $\langle [2] \rangle$ ، $\langle [2]^{-1} \rangle$ ، في الزمرة $(Z^*_{13},\otimes)$

الحل:

(i) حيث إن $[1]$ هو العنصر المحايد في النظام $(Z^*_{13},\otimes)$

إذن

$$[1]^n = [1] \ \forall\, n \in Z \ \Rightarrow \ \langle [1] \rangle = \{ [1] \}$$

(ii)

$$[2]^1 = [2] \ , \quad [2]^2 = [2] \otimes [2] = [4]$$
$$[2]^3 = [2]^2 \otimes [2] = [4] \otimes [2] = [8] \ ,$$
$$[2]^4 = [2]^3 \otimes [2] = [8] \otimes [2] = [3] \ ,$$
$$[2]^5 = [2]^4 \otimes [2] = [3] \otimes [2] = [6] \ ,$$
$$[2]^6 = [2]^5 \otimes [2] = [6] \otimes [2] = [12] \ ,$$
$$[2]^7 = [2]^6 \otimes [2] = [12] \otimes [2] = [11] \ ,$$
$$[2]^8 = [2]^7 \otimes [2] = [11] \otimes [2] = [9] \ ,$$
$$[2]^9 = [2]^8 \otimes [2] = [9] \otimes [2] = [5] \ ,$$
$$[2]^{10} = [2]^9 \otimes [2] = [5] \otimes [2] = [10] ,$$
$$[2]^{11} = [2]^{10} \otimes [2] = [10] \otimes [2] = [7] \ ,$$
$$[2]^{12} = [2]^{11} \otimes [2] = [7] \otimes [2] = [1] \ ,$$

$$\therefore \langle 2 \rangle = \{[2],[4],[8],[3],[6],[12],[11],[9],[5],[10],[7],[1]\} = Z^*_{13}$$
$$|\,[2]\,| = 12 = |\,Z^*_{13}\,|$$

أي أن $[2]$ مولد للزمرة $(Z^*_{13},\otimes)$.

(ii) حيث إن $[2]^{-1} = [7]$ لأن

$$[2] \otimes [7] = [1]$$

إذن

$$\langle [2]^{-1} \rangle = \langle [7] \rangle = \{[7],[7]^2,\ldots,[7]^{12}\} = Z_{13}^{*} = \langle [2] \rangle$$

$$\left| [2]^{-1} \right| = 12 = \left| Z_{13}^{*} \right|$$

ملاحظة (2-4. 112):

في المثال السابق نلاحظ ما يلي:

(i) رتبة العنصر في أي زمرة هو رتبة الزمرة المولدة بهذا العنصر ، أي أن

$$|\langle a \rangle| = |a|$$

(ii) الزمرة المولدة بأي عنصر هي الزمرة المولدة نفسها بمعكــوس هــذا العنصر ، أي أن

$$\langle a \rangle = \langle a^{-1} \rangle$$

(iii) رتبة أي عنصر تساوي رتبة معكوس هذا العنصر، أي أن

$$|a| = |a^{-1}|$$

ملاحظة (2-4. 113):

إذا كانت $(G, *)$ زمرة دائرية ، فأنه يوجد $a \in G$ بحيث إن

$$G = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots\}$$

وهنا تظهر لنا حالتان:

(i) إذا كانت جميع العناصر مختلفة وفي هذه الحالة فإن الزمرة تكون لانهائية

(ii) إذا كانت العناصر الناتجة ليست كلها مختلفة وفي هذه الحالــة ســنرى أن الزمرة تكون منتهية.

نظرية (114.4-2):

نفرض أن $(G, *)$ زمرة دائرية وأن $G = \langle a \rangle$

إذا وجد $m_1, m_2 \in Z$ بحيث إن

$$a^{m1} = a^{m2} \ , \ m_1 \neq m_2$$

فأنه يوجد $n \in Z^+$ بحيث إن

$$G = \{a, a^1, \ldots, a^n = e\} \ ;$$

$$a^{k_1} \neq a^{k_2} \forall k_1 k_2 = 1,2,\ldots\ldots, n$$

البرهان:

نفرض أن

$$a^{m1} = a^{m2} \ , m_1 , m_2 \in Z \quad ; \ m_1 > m_2$$

وحيث إن $(G, *)$ زمرة ، إذن

$$a^{-m2} \in G$$

$$a^{m1} * a^{-m2} = a^{m2} * a^{-m2}$$

$$\Rightarrow a^{m1-m2} = e$$

$$\Rightarrow a^k = e \quad , \quad k \in Z^+ \quad , \ k = m_1 - m_2$$

إذن العنصر a له رتبة.

وبفرض أن رتبة العنصر a هي n ، تكون المجموعة

$$X = \{a , a^2 , a^3 , \ldots , a^n = e \} \subseteq G \ldots \ (I)$$

الآن إذا كانت

$$a^m \in G, m \in Z \ \exists k_1 \in Z^+, k_2 \in Z^+ : k_2 < n \ , m = k_1 n + k_2$$

$$\therefore G \subseteq X \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (II)$$

ومن (I) , (II) ينتج أن $G = X$

وبهذا يتم البرهان.

ملاحظة (2-4. 115):

إذا كانت $(G , *)$ زمرة دائرية لانهائية ، وكــان $G = \langle a \rangle$ أي أن a مولد للزمرة وكان هناك مولد آخر للزمرة a^m مثلاً ، فإنه يوجد $n \in Z$.

بحيث إن:

$$a = (a^m)^r = a^{mr}$$

وذلك لأن مولد الزمرة لانهائية ، a^m مولد لها .

$$\therefore mr = 1$$
$$\Rightarrow \quad m = 1 , r = 1 \qquad \vee \qquad m = -1 , r = -1$$

ومن ثم إذا كان a مولدًا للزمرة فإن المولد الآخر يكون a^{-1}

$$\therefore G = \langle a \rangle = \langle a^{-1} \rangle$$

نظرية (2-4. 116):

إذا كانت $(G , *)$ زمرة دائرية منتهية $G = \langle a \rangle$ ، $|G| = n$ فــإن n , m أوليان فيما بينهما إذا كان $G = \langle a^m \rangle$

البرهان:

أولاً نفرض أن $G = \langle a^m \rangle$

$$\Rightarrow a = (a^m)^r \ , \quad r \in Z$$
$$\Rightarrow a^1 = a^{mr} \quad \Rightarrow a^1 * a^{-mr} = a^{mr} * a^{-mr}$$
$$\Rightarrow a^{1-mr} = e = a^n = a^{2n} = \dots$$

أي أن $1\text{-}mr$ يقبل القسمة على n

$$\Rightarrow \exists \ q \in Z \ : \ 1 - mr = qn$$
$$\Rightarrow mr + nq = 1$$

إذن m,n أوليان فيما بينهما .

نتيجة (2-4 .117):

إذا كانت $(G , *)$ زمرة دائرية عدد عناصرها n حيث n عدد أولي فإنــه يوجد للزمرة مولد وحيد $a \neq e$.

نظرية (2-4 .118):

إذا كانت $(G , *)$ زمرة ، $a \in G$ ، فإن $(\langle a \rangle , *)$ زمرة جزئية من الزمرة $(G , *)$.

البرهان:

واضح أن

$$\langle a \rangle = \{a^n : n \in Z\} \subset G$$
$$\therefore a^1 = a \in \langle a \rangle \neq \phi$$

كذلك

$$\forall m,n \in Z \Rightarrow a^m , a^n \in \langle a \rangle$$
$$\Rightarrow a^m , a^{-n} \in \langle a \rangle$$ في تعريف $\langle a \rangle$,
$$\Rightarrow a^m * a^{-n} = a^{m+(-n)} \in \langle a \rangle$$

لأن $m + (-n) \in Z$

إذن $(\langle a \rangle , *)$ زمرة جزئية في $(G , *)$ وفق نظرية (2-3 .97) .

مثال (2-4. 119):

أكتب جميع الأحداث الجزئية للزمرة (S_3, o).

الحل:

في نظرية (2-4. 96) نستطيع الحصول على هذه الزمرات الجزئية كالتالي:

$$\langle I \rangle = \{I\}$$

$$\langle (12) \rangle = \{ I, (12) \} ,$$

$$\langle (13) \rangle = \{ I, (13) \} ,$$

$$\langle (23) \rangle = \{ I, (23) \} ,$$

$$\langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle = S_3^+$$

وعلى الطالب التأكد بنفسه في ذلك.

تعريف (2-4. 120):

إذا كانت $(G, *)$ زمرة وكانت $(H, *)$ زمرة جزئية فإن المجموعة

$$aH = \{a * h : h \in H\}$$

حيث $a \in G$ تسمى مجموعة مصاحبة يسرى للزمرة الجزئية $(H, *)$ كما يسمى a ممثل المجموعة aH.

وبالمثل المجموعة

$$Ha = \{h * a : h \in H\}$$

تسمى مجموعة مصاحبة يمنى للزمرة الجزئية $(H, *)$.

مثال (2-4. 121):

باعتبار الزمرة $(G, .)$، حيث $G = \{1,-1,i,-i\}$ ، وكانت $(H, .)$ زمرة جزئية في $(G, .)$، حيث $H=\{1,-1\}$.

$$\therefore\ iH = \{ih : h \in H\} = \{i, -i\},$$
$$Hi = \{hi : h \in H\} = \{i, -i\}$$

مثال (2-4. 122):

باعتبار الزمرة (S_3, o) حيث

$$S_3 = \{I, (12), (13), (23), (1\ 2\ 3), (1\ 3\ 2)\},$$
$$S_3^+ = \{I, (1\ 2\ 3), (1\ 3\ 2)\},$$
$$S_3^- = \{(12), (13), (23)\}$$
$$a = (12)$$
$$\therefore\ aS_3^+ = \{a \circ I, a \circ (1\ 2\ 3), a \circ (1\ 3\ 2)\}$$
$$= \{(12), (23), (13)\} = S_3^-$$
$$S_3^+a = \{I \circ a, (1\ 2\ 3) \circ a, (1\ 3\ 2) \circ a\} = S_3^-$$

الآن باعتبار $X_3 = \{I, (12)\}$ ، إذن $(X_3, \circ)$ زمرة جزئية في (S_3, o) كما بينا في المثال (2-3. 100).

باعتبار

$$b = (13) \in S_3$$
$$\therefore\ bx = \{b \circ I, b \circ (12)\} = \{(13), (1\ 2\ 3)\},$$
$$xb = \{I \circ b, (12)(13)\} = \{(13), (1\ 3\ 2)\},$$

لاحظ أن $bx \neq xb$ وكلا منهما لا يكون زمرة جزئية في $(S_3, \circ)$.

ملاحظة (2-4. 123):

(i) إذا كانت $(G , *)$ زمرة إبدالية وكانت $(H , *)$ زمرة جزئية فيها فإنه في الواضح أن $aH = Ha$ وذلك لأي $a \in G , h \in H$ أن

$$a * h = h * a$$

(ii) إذا كانت $(G , *)$ زمرة وكانت $(H , *)$ زمرة جزئية فيها فإن

$$aH = Ha \Leftrightarrow H = a^{-1}Ha$$

حيث $a \in G$ (لماذا ؟)

نظرية (2-4. 124):

إذا كانت $(G , *)$ زمرة ، $(H , *)$ زمرة جزئية فيها فإن:

أولاً: $aH = H \Leftrightarrow a \in H$

ثانيًا: $a^{-1} * b \in H \Leftrightarrow aH = bH$

ثالثاً: $aH \cap bH \neq \phi \Leftrightarrow aH = bH$

رابعاً: كل عنصر $(G , *)$ ينتمي إلى مجموعة مصاحبة يسرى واحدة فقط للزمرة الجزئية $(H , *)$.

خامسًا: يوجد تقابل بين أي زمرة $(H , *)$ في الزمرة $(G , *)$ ومجموعتها المصاحبة اليسرى (أي أن عدد العناصر في كل منهما مساو لعدد العناصر في الأخرى).

سادسًا: اتحاد جميع المجموعات المصاحبة اليسرى يساوي الزمرة الأصلية.

البرهان:

أولاً: (i) نفرض أن $aH = H$ ، ولكن $e \in H$ ، وذلك

لأن $(H , *)$ زمرة جزئية ، إذن

$$a * e \in aH = H \Rightarrow a \in H$$

(ii) نفرض أن $a \in H$ ونريد إثبات أن $aH = H$ ،

لذلك نفرض أن

$$b \in aH \Rightarrow b = a * h \quad , h \in H$$

$$\Rightarrow b \in H$$ لأن $(H , *)$ زمرة جزئية

$$\therefore \quad aH \subset H \quad \text{..(I)}$$

الآن نفرض أن

$$c \in H \Rightarrow c = e*c = (a * a^{-1}) * c$$
$$= a * (a^{-1} * c)$$

وحيث إن $a \in H$ ، إذن $a^{-1} \in H$ لأن $(H , *)$ زمرة جزئية .

$$\therefore \quad c = a * h \quad , \quad h = a^{-1} * c \in H$$

لأن $(H , *)$ زمرة جزئية ، إذن $c \in aH$

$$\therefore \quad H \subset aH \quad \text{..(II)}$$

ومن (I) ، (II) ينتج

$$aH = H$$

ثانيًا:

$$\begin{aligned} aH = bH &\Leftrightarrow a^{-1}(aH) = a^{-1}(bH) \\ &\Leftrightarrow (a^{-1} * a) H = (a^{-1} * b) H \\ &\Leftrightarrow H = (a^{-1} * b) H \\ &\Leftrightarrow a^{-1} * b \in H \end{aligned}$$

ثالثًا:

$$\begin{aligned} aH \cap bH \neq \phi &\Leftrightarrow \exists c \in aH \cap bH \\ &\Leftrightarrow c \in aH \wedge c \in bH \\ &\Leftrightarrow c = a * h_1 = b * h_2 , \quad h_1, h_2 \in H \\ &\Leftrightarrow h_1 * h_2^{-1} = a^{-1} * b \end{aligned}$$

ولكن $h_1 * h_2^{-1} \in H$ (لماذا ؟) ، إذن

$$a^{-1} * b \in H$$

ومن ثانيًا ، إذن

$$aH = Ha$$

رابعًا:

نفرض أن $a \in G$ ونعتبر aH .

وحيث إن $e \in H$ ، إذن

$$a * e \in aH \Rightarrow a \in aH$$

ومن ثالثًا لا توجد مجموعة مصاحبة يسرى أخرى تحوي العنصر a

خامسًا:

نفرض أن

$$f : H \rightarrow aH \quad , a \in G$$

حيث إن

$$f(h) = a * h \vee h \in H$$

نلاحظ أن f تطبيق لأن

$$\forall\ h_1, h_2 \in H , \qquad \begin{aligned} h_1 = h_2 &\Rightarrow a * h_1 = a * h_2 \\ &\Rightarrow f(h_1) = f(h_2) \end{aligned}$$

ولأن f تطبيق متباين ، لأن

$$f(h_1) = f(h_2) \Rightarrow a * h_1 = a * h_2$$

قانون الحذف $\Rightarrow h_1 = h$

وكذلك f تطبيق شامل (غامر) ، لأن

$$y \in aH \Rightarrow \exists\ h \in H : y = a*h = f(h)$$

إذن f تطبيق تقابل

إذن

$$|H| = |aH|$$

سادسًا:

نريد إثبات أن

$$G = \bigcup_{a \in G} aH \qquad \forall \quad a \in G$$

وهذا واضح من (رابعًا) حيث إن $a \in aH$

ملاحظة (2-4. 125):

الخصائص السابقة نفسها صحيحة أيضًا بالنسبة للمجموعات المصاحبة اليمنى.

نظرية (2-4. 126) (نظرية لاجرانج):

إذا كانت $(G , *)$ زمرة عدد عناصرها محدود (n مثلاً) وكانت $(H , *)$ زمرة جزئية منها عدد عناصرها m ، فإن n تقبل القسمة على m.

البرهان:

نفرض أن

$a_1H , a_2H , a_3H , ... , a_\ell H$

هي كل المجموعات المصاحبة اليسرى المختلفة للزمـــرة الجزئيـــة $(H , *)$ ، حيث أحد العناصر $a_1,a_2,....,a_\ell$ هو عنصر الوحدة e ، ليكن $a_1= e$ ، إذن فـــي النظرية (2–4. 114) ثالثًا وسادسًا نستنتج أن

$$\{H, a_2H, a_3H, ..., a\lambda H\}$$

تجزيء المجموعة G أي أن

$$G = H \cup a_2H \cup ... \cup a_\ell H$$
$$| G | = H + | a_2H | + | a_3H | + ... + |a_\ell H |$$

حيث |A| يرمز لعدد عناصر المجموعة A

ولكن في النظرية نفسها (2–4. 124) خامسًا نستنتج أن

$$|G| = \underbrace{H + |H| + |H| + ... + |H|}$$

ℓ في المرات

$$\therefore | G | = \ell \ | H |$$

$$\therefore n = \ell m \Rightarrow \frac{n}{m} = \ell \in Z^+$$

ملاحظة (2-4. 127)

1- يسمى العدد ℓ الوارد في النظرية (2-4. 126) دليل H في G ويرمز لـه بالرمز [G : H] ، إذن

$$|G| = [G : H]\,|H|$$

2- من النظرية (2-4. 126) نستنتج أنه لا يمكن أن تكون (H , *) زمرة جزئية في الزمرة (G , *) ما لم تكن رتبة G تقبل القسمة على عدد عناصر H وهذا شرط لازم فقط ولكنه ليس كافيًا ، أي أن عكس نظريـة (2-4. 126) غيـر صحيح على وجه العموم (كما موضح في الأمثلة التي تلي الملاحظة) .

3- مما سبق نستنتج أنه إذا كانت (G , *) زمرة ، $a \in G$ ، فإن

$$|G| = [G : \langle a \rangle]\,|\langle a \rangle|$$

4- إذا كانت (G , *) رتبتها عدد أولي فإنه لا يوجد لها زمرة جزئية فعلية غيـر تابعة ، وبذلك فلابد أن تكون G زمرة دائرية مولدة بعنصر a ، حيث $e \neq a \in G$ أي أن $G = \langle a \rangle$.

مثال (2-4. 128) :

نعتبر $(G , \otimes)$ حيـث $G = \{1,2,4,5,7,8\}$ ، $\otimes$ هـي عمليـة الـضرب بمقياس 9.

من السهل التحقق من أن $(G , \otimes)$ زمرة ، $|G| = 6$ باعتبار

$H_1 = \{1, 4, 7\}$, $H_2 = \{1 , 8\}$

إذن $(H_1, \otimes)$ ، $(H_2, \otimes)$ زمرة جزئية في الزمرة $(G, *)$ ،
$|H_1| = 3$ ، $|H_2| = 2$ والعدد 6 يقبل القسمة على كل من 2,3 وأن

$$[G : H_1] = \frac{|G|}{|H_1|} = 2$$
$$[G : H_2] = \frac{|G|}{|H_2|} = 3$$

مثال (2-4. 129):

إذا كان عدد عناصر زمرة ما $(G, *)$ يساوي n وكان العدد n يقسم على العدد m فليس من الضروري أن نجد زمرة جزئية $(H, *)$ في $(G, *)$ عدد عناصرها يساوي m ، أي أن عكس نظرية لاجرانج غير صحيح ولبرهان ذلك نعتبر زمرة التبديلات الزوجية من الدرجة الرابعة

$$S_4^+ = \{I, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), (12)(34), (13)(24), (14)(23)\}$$
$$\therefore |S_4^+| = 12$$

ولكن لا توجد زمرة جزئية منها عدد عناصرها (6)
(على الطالب التحقق من ذلك)

[2-5] الزمرة الجزئية القياسية وزمرة القسمة
Normal Subgroup and Quotient Group

تعريف (2-5. 130):

الزمرة الجزئية (H , *) من الزمرة (G , *) تسمى زمرة جزئية قياسية(سوية) إذا كان:

$$aH = Ha \quad \forall \quad a \in G$$

مثال (2-5. 131):

نعتبر $(S_3^+ \ , o)$ ، الآن

$$I S_3^+ = S_3^+ = S_3^+ I$$

$$(1\ 2\ 3)\ S_3^+ = S_3^+ (1\ 2\ 3) = S_3^+ ,$$

$$(1\ 3\ 2)\ S_3^+ = S_3^+\ (1\ 3\ 2) = S_3^+$$

$$(12)\ S_3^+ = S_3^+\ (12) = S_3^-$$

$$(13)\ S_3^+ = S_3^+\ (13) = S_3^-$$

$$(23)\ S_3^+ = S_3^+ (23) = S_3^-$$

إذن $(S_3^+ \ , o)$ زمرة جزئية قياسية من $(S_3 \ , o)$

نظرية (2-5. 132):

الزمرة الجزئية (H , *) من الزمرة (G , *) تكون قياسية إذا وفقط إذا كان:

$$aha^{-1} \in H \quad \forall \quad a \in G \ , \ h \in H$$

البرهان:

(i) نفرض أن الزمرة الجزئية $(H , *)$ قياسية

$$\therefore\ aHa^{-1} = H \qquad \forall\ a \in G$$

الآن نفرض أن $a \in G \quad , \quad h \in H$

$$\therefore\ aha^{-1} \in aHa^{-1} = H \Rightarrow aha^{-1} \in H$$

(ii) نفرض أن

$$aha^{-1} \in H \qquad \forall \qquad a \in G \quad , \quad h \in H$$

ونريد إثبات أن $(H , *)$ قياسية لذلك

نفرض أن

$$b \in H \Rightarrow b = ebe$$
$$= aa^{-1}\, b\, aa^{-1}$$

ولكن من الفرض $h = a^{-1}ba \in H$

$$\therefore\ b = aha^{-1} , h \in H \Rightarrow b \in aHa^{-1}$$
$$\therefore\ H \subset aHa^{-1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (I)$$

نفرض أن

$$C \in aHa^{-1} \Rightarrow C = aha^{-1} \quad , \quad h \in H$$
$$\Rightarrow C \in H$$
$$\therefore\ aHa^{-1} \subset H \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (II)$$

من (I) , (II) ينتج أن

$$H = aHa^{-1}$$

أي أن $(H , *)$ قياسية .

ملاحظة (2-5. 133)

(i) الزمرة الجزئية $(H , *)$ من الزمرة $(G , *)$ تكون زمرة جزئية قياسية إذا كان وفقط إذا كان

$$aHa^{-1} = H \quad , \forall \quad a \in G$$
$$\Leftrightarrow \quad aha^{-1} \in H \quad , \quad \forall \quad a \in G \ , \quad h \in H$$

(ii) إذا كانت $(G , *)$ زمرة إبدالية فإن كل زمرة جزئية منها قياسية .

(iii) أي زمرة $(G , *)$ ، حيث $|G| \geq 2$ ، لها على الأقل زمرتين جزئيتين قياسيتين هما $(\{e\}, *)$ ، $(G , *)$

نظرية (2-5. 134):

إذا كانت الزمرة الجزئية $(H , *)$ زمرة قياسية من الزمرة $(G , *)$ وعرفنا العملية "." على المجموعة

على النحو الآتي $T = \{aH : a \in G\}$

$$(aH) .(bH) = (a * b) H \ , \quad \forall \ aH , bH \in T$$

فإن النظام $(T, .)$ زمرة رتبتها $[G : H]$

البرهان:

(i) العملية "." عملية ثنائية على T : يتم برهان ذلك ، إذن أثبتنا أن تعريف العملية "." مستقل من إختيار ممثلي aH , bH وهما b, a على الترتيب، أي إذا أثبتنا أن

$$aH = a'H \ \wedge \ bH = b'H \Rightarrow (a * b)H = aH \ . \ bH$$
$$= a'H \ . \ b'H = (a' * b')H$$

وهذا تحقق فعلاً لأن

$$aH = a'H \ \Rightarrow a * e \ = a' * h_1 \Rightarrow a = a' * h_1 \ , \ h_1 \in H$$
$$bH = b'H \ \Rightarrow b * e \ = b' * h_2 \Rightarrow b = b' * h_2 \ , \ h_2 \in H$$

إذن

$$(a * b)H = (a' * h_1 * b' * h_2)H$$

$= (a' * h_1 * b') * h_2 H$ لأن G زمرة

$= (a' * h_1 * b')H$ لأن $h_2 H = H$

$= a' * (h_1 * b')H$ لأن G زمرة

$= a' * (b' * h_1)H$

لأن H زمرة جزئية قياسية .

أي أن : $Hb' = b'H$

$$\Rightarrow \exists\, h_1 \in H : h_1 * b' = b' * h_1$$

لأن G زمرة

$= (a' * b') * h_1 H$

$= (a' * b')H$ لأن $h_1 H = H$

(ii) العملية "." تجميعية (دامجة) لأن

$$\forall\ aH, bH, cH \in T$$

$(aH . bh) . cH = (a * b)H . cH$ تعريف "."

$= ((a * b) * c)H$ تعريف "."

$= (a * (b * c))H$ لأنه G زمرة

$= aH . (b * c)H$ تعريف "."

(iii)

$H = eH \in T$ هو العنصر المحايد: لأن

$\forall\ aH \in T$

$eH \,.\, aH = (e * a)H = aH$

$aH \,.\, eH = (a * e)H = aH$

(iv) كل عنصر $aH \in T$ له نظير $(aH)^{-1} = a^{-1}H \in T$ لأن

$a^{-1}H \,.\, aH = (a^{-1} * a)\, H = eH = H ,$

$aH \,.\, a^{-1}H = (a * a^{-1})\, H = eH = H$

في (i) – (iv) نستنتج أن (. , T) زمرة ومن نظرية لاجرانج ينتج أن

$| T | = [G : H]$

تعريف (2-5. 135):

إذا كانت $(H , *)$ زمرة جزئية قياسية من الزمرة $(G,*)$ فإن الزمرة $(T , .)$ حيث

$T = \{aH : a \in G \}$

$aH \,.\, bH = (a * b)\, H , \quad \forall\ aH , bH \in T$

يرمز لها بالرمز G / H ، وتقرأ G قياس H ، وتسمى زمرة القسمة (أو زمرة حاصل قسمة G بالنسبة للزمرة الجزئية القياسية H) أو زمرة العوامل.

ملاحظة (2-5. 136):

(i) إذا كانت $(H , *)$ زمرة جزئية من الزمرة $(G , *)$ فإننا نرمز للمجموعة المصاحبة اليسرى إلى H بالرمز $a + H$ حيث $a \in G$ وهي:

$a + H = \{ a + h : h \in H \}$

ونرمز للمجموعة المصاحبة اليمنى إلى H بالرمز H+a حيث $a \in G$ وهي

$$H + a = \{ h + a \ : \ h \in H \}$$

(ii) إذا كانت H زمرة جزئية قياسية من G فإن

$$a + H = H + a \quad \forall \quad a \in G$$

كما يكون

$$| G | = | a_1 + H | + |a_2 + H | + \ . \ . \ .$$

مثال (2-5. 137):

نعتبر زمرة التباديل من الدرجة الثالثة (S_3 , o) ،

$$H = \{I , (1\ 2\ 3) , (1\ 3\ 2) \}$$

من السهل إثبات أن (H , o) زمرة جزئية قياسية من (S_3 , o) لإيجـــاد زمرة القسمة S_3 / H نلاحظ أن

$$S_3 * H = \{aH : a \in S_3 \}$$

$$IH = H ,$$

$$(1\ 2\ 3)\ H = \{(1\ 23)\ o\ I ,\ (1\ 2\ 3)\ o\ (1\ 2\ 3) , (1\ 2\ 3)\ o(1\ 3\ 2) \}$$

$$= \{(1\ 2\ 3) , (1\ 3\ 2)\ , I \}= H ,$$

$$(12)\ H = \{ (12)\ o\ (1\ 2\ 3) , (12)\ o\ I\ , (12)\ o\ (1\ 3\ 2) \}$$

$$= \{ (23) , (12) , (13) \}= S_3^-$$

$$(13)\ H = \{ (13)\ oI , (13)\ o\ (1\ 2\ 3),(13)\ o(1\ 3\ 2)\ \}$$

$$= \{ (13) , (12) , (23) \}= S_3^-$$

$$(23)\ H = \{ (23)\ oI,(23)\ o(1\ 2\ 3) , (23)\ o\ (1\ 3\ 2) \}$$

$$= \{ (23) , (13) , (12) \}= S_3^-$$

$$\therefore\ S_3^- / H = \{H , S_3^- \}$$

لاحظ أن $H = S_3^+$ هو العنصر المحايد للزمرة S_3 / H وأن العنصر (12)H مولدها رتبة 2 لأن

$$((12)H)^2 = (12)H \, o \, (12)H = (12) \, o \, H = IH = H \;.$$

مثال (2-5. 138):

باعتبار الزمرة $(Z , +)$ ، $m Z$ تعرف كما يلي:

$$m Z = \{\ldots , -2m , -m , 0 , m , 2m , \ldots\}$$

حيث $m \in Z^+$:

(i) أثبت أن $(mZ , +)$ زمرة جزئية قياسية من $(Z , +)$.

(ii) أوجد زمرة القسمة Z / mZ .

(iii) أثبت أن زمرة القسمة هي زمرة دائرية رتبتها m .

الحل:

(i)

أولاً: بما أن

$$m Z = \{\ldots , -2m , -m , 0 , m , 2m , \ldots\}$$

إذن كل عناصر $m Z$ هي مضاعفات العدد الصحيح الموجب m، إذن مجموع أي عنصرين من $m Z$ هو عنصر وحيد ينتمي إلى mZ، أي أن $(mZ , +)$ نظام ذو عملية.

ثانيًا: خاصيتا التجميع والإبدال متحققتان لأن $mZ \subset Z$

ثالثًا: النظام $(mZ , +)$ به عنصر محايد هو الصفر لأن

$$ma + 0 = ma \quad \forall \quad ma \in mZ \quad , \quad a \in Z$$

رابعًا:

لكل $ma \in mZ$ يوجد نظير $(-ma) \in mZ$ لأن

$$ma + (-ma) = 0$$

إذن من أولاً – رابعًا ينتج أن $(mZ , +)$ زمرة جزئيـــــة مــن $(Z , +)$،
حيث إن $(Z , +)$ إبدالية، إذن $(mZ , +)$ زمرة جزئية قياسية منها:

(ii)

$$Z/mZ = \{0 + mZ , 1+mZ , 2+mZ , \ldots , (m-1)+mZ \}$$
$$=\{mZ , 1+mZ , 2+mZ , \ldots , (m-1)+mZ\}$$

(iii)

Z/mZ زمرة دائرية ، لأنه تمكن توليدها بالعنصر $1+ mZ$ أي أن

$$Z/mZ = \langle 1+mZ \rangle$$
$$\therefore |Z/mZ| = m$$

[6-2] التشاكل (الهمومورفيزم)
Homomorphism

تعريف (2-6. 139):

يقال للدالة $f: (G, *) \to (G', 0)$

إنها تشاكل من الزمرة $(G, *)$ إلى الزمرة $(G', 0)$

إذا كان وفقط إذا كان

$$f(a * b) = f(a) \ o \ f(b) \quad \forall \quad a,b \in G$$

مثال (2-6. 140):

نعلم من البنود السابقة أن $(Z, +)$, $(G, .)$ ، حيث $G = \{1, -1, i, -i\}$

كل منهما تمثل زمرة ، نعرف $f: Z \to G$ بالطريقة الآتية:

$$f(n) = \begin{cases} 1 \text{ ، إذا كانت } n \text{ زوجية} \\ -1 \text{ ، إذا كانت } n \text{ فردية} \end{cases}$$

هل أن f تشاكل (تطابق)

الحل:

نفرض أن $m,n \in Z$

أولاً:

إذا كانت كل من n,m زوجية

$$\therefore f(m) = 1 \quad , \quad f(n) = 1$$

كذلك $m+n$ زوجية

$$\therefore f(m+n) = 1 \quad , \quad f(m) \,.\, f(n) = 1$$

ثانيًا:

إذا كانت كل من n,m فردية

$$\therefore f(m) = -1 \quad , \quad f(n) = -1$$

وتكون $m+n$ زوجية

$$\therefore f(m+n) = 1=(-1)\,(-1) = f(m) \,.\, f(n)$$

ثالثًا:

إذا كانت m زوجية ، n فردية

$$\therefore f(m) = 1 \quad , \quad f(n) = -1$$

وتكون $m+n$ فردية

$$\therefore f(m+n) = -1= 1 \,.\, (-1) = f(m) \,.\, f(n)$$

مثال (2-6. 141):

نعلم أن $(S3 \;,\; o)$ زمرة غير إبدالية ، وأن $(G \;,\; \oplus)$ حيث $G=\{0,1,2,3 \;,4,5\}$ هي عملية الجمع بمقياس 6 ، تكون زمرة إبدالية ، تعرف $f : S_3 \to G$ كما يلي:

$$f\,(I) = 0 \;\; , f\,(12) = f\,(13) = f\,(23) = 3 \,,$$
$$f\,(1\;2\;3) = f\,(1\;3\;2) = 0$$

هل أن f تشاكل ؟

الحل:

نعم أن f تشاكل وعلى الطالب التأكد من ذلك، وكمثال:

$$f\,(12) = 3 \quad , \quad f\,(12\,3) = 0$$
$$f\,((12)\;\; o(1\;3\;2)) = f\,(13) = 3$$
$$f\,(12) \;\; \oplus f\,(1\;3\;2) = 3 \oplus 0 = 3$$
$$\therefore\; f\,((12)\;\; o\;(1\;3\;2)) = f\,(12) \;\; \oplus f\,(1\;3\;2\,)$$

ملاحظة (2-6. 142):

(i) نلاحظ أن المثال السابق يثبت أن التشاكل لا يحافظ على الزمر الإبداليــة، ولكنه يحافظ على العمليات ، وعنصر الوحدة ، والمعكوس .

(ii) نواة التشاكل هي

$$\text{Ker } f = f^{-1}(e') = \{ a \in G = f(a) = e' \} \subset G$$

وفي المثال السابق نلاحظ أن النواة هي

$$\text{Ker } f = \{ I , (1\ 2\ 3), (1\ 3\ 2) \} = S_3^{+}$$

(iii) نواة التشاكل هي زمرة جزئية من الزمرة الأصلية .

تعريف (2-6. 143):

يعرف مدى التشاكل

$$f : (G , *) \to (G' , o)$$

كالتالي

$$R_f = \{a' \in G' : a \in G ; f(a) = a' \}$$
$$= f(G) \subset G'$$

مثال (2-6. 144):

(i) في المثال (2-6. 141) نجد أن

$$R_f = \{0 , 3 \}$$

(ii) في المثال (2-6. 140) نجد أن

$$\text{Ker } f = \{ n \in Z : f(n) = I \}$$
$$= \{n \in Z : \text{زوجيه } Z \}$$
$$= \{ 0 , \pm 2, \pm 4 , \ldots \}$$
$$R_f = \{1 , -1 \}$$

نظرية (2-6. 145):

إذا كانت $(G , *)$ ، (G' , o) ، $(G'' , \otimes)$

ثلاث زمر وكان

$$f : G \to G' \quad , \quad g : G' \to G''$$

تشاكل، فإن $g \, o \, f : G \to G''$

البرهان:

$(g \, o f)(a * b) = g(f(a * b))$ تعريف تركيب الدالة

$= g(f(a) \; o \; f(b))$ لأن f تشاكل

$= g(f(a)) \otimes g(f(b))$ لأن g تشاكل

$= (g \; o f)(a) \otimes (g \; o \; f)(b)$ تعريف التركيب

إذن $g \; o \; f$ تشاكل

نتيجة (2-6. 146):

إذا كانت $(G , *)$ ، (G' , o) ، $(G'' , \otimes)$ ثلاث زمر وكان

$$f : G \to G' \quad , \quad g : G' \to G''$$

ايزومورفيزم فإن $g \circ f : G \to G''$ تشاكل تقابلي .

البرهان:

من النظرية (2-6. 145) ، ينتج أن $g \; o \; f$ تشاكل ولما كان كل من f ، g تقابلاً فإن $g \circ f$ يكون تقابلاً أيضًا وهذا يؤدي إلى أن $g \; o f$ تشاكل تقابلي.

[7-2] تمارين عامة

1- بين أن الأنظمة التالية : $(R, +)$ ، $(R, .)$ ، $(p(A), \cap)$ ، $(p(A), \cup)$

تمثل شبه زمرة وأن النظام $(R, -)$ لا يمثل شبه زمرة .

2- إذا كانت العملية "o" معرفة على مجموعة الأعداد الحقيقية كالآتي

$$x \; o \; y = x + y + xy \quad , \quad \forall \quad x, y \in R$$

فأثبت أن (R, o) يمثل شبه زمرة وعنصرها المحايد هو " 0 " .

3- إذا كانت المجموعة $G = R / \{-1\}$

معرف عليها العملية " 0 " كما في السؤال السابق أي

$$x \; o \; y = x + y + xy \quad , \quad \forall \quad x, y \in G$$

فأثبت أن النظام (G, o) يمثل زمرة .

4- اعتبر $(p(A), \oplus)$ ، حيث $p(A)$ هي مجموعة كل المجموعات الجزئية إلى المجموعة A وأن $\oplus$ معرفة كالآتي

$$A \oplus B = A \cup B - (A \cap B)$$

بين أن $(p(A), \oplus)$ يمثل زمرة إبدالية .

5- اعتبر $(G, .)$ حيث المجموعة $G = \{1, -1, i, -i\}$ ، حيث $i = \sqrt{-1}$ ، ولتكن العملية " . " هي عملية الضرب الاعتيادية على الأعداد ، فهل أن النظام $(G, .)$ يمثل زمرة ؟ وهل أنها إبدالية أم لا ؟

6- اعتبر النظام $(Z_5, \oplus)$ حيث مجموعة صفوف التكافيء
$Z_5 = \{[0], [1], [2], [3], [4]\}$ والعملية $\oplus$ معرفة كالآتي

$$[a] \oplus [b] = [a+b] \quad , \quad \forall \quad [a], [b] \in Z_n$$

أثبت أن $(Z_5, \oplus)$ يمثل زمرة ، ثم جد عنصرها المحايد والمعكوس (النظير لكل عنصر فيها) .

7-إذا كانت المجموعة $G = \{I, A, B, C, D, E\}$
حيث إن

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad , \quad C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$D = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \quad , \quad E = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$$

ولتكن " . " عملية الضرب الاعتيادية على المصفوفات
أثبت أن $(G, .)$ تمثل زمرة هل هي إبدالية أم لا ؟ ولماذا ؟

8-إذا كانت S_5 هي مجموعة التبديلات ومعرف عليها g , f كالآتي :

$$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 5 & 1 & 2\end{pmatrix} \quad , \quad g=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 1 & 2 & 3 & 4\end{pmatrix}$$

فأوجد كلاً مما يأتي : f^{-1} ، g^2 ، $f\,o\,g$ ، $g\,o\,f$ ، $(f\,o\,g)^{-1}$ ، $f^{-1}\,o\,g^{-1}$ ، $g^{-1}\circ f^{-1}$ ، هل أن S_5 إبدالية ؟

هل أن $(f\,o\,g)^{-1} = f^{-1}\,o\,g^{-1}$ ؟

تحقق من أن $(f\,o\,g)^{-1} = g^{-1}\,o\,f^{-1}$.

9- إذا كانت S_4 هي مجموعة التبديلات:

أولاً: أكتب عناصرها بالشكل الاعتيادي.

ثانيًا: أعد كتابة عناصرها بالتعبير الدائري.

ثالثًا: أكتب عناصر مجموعة التبديلات الزوجية S_4^+ وكذلك عناصر مجموعة التبديلات الفردية S_4^-.

رابعًا: ما هي رتبة العنصر (4) (3 2 1) ورتبة العنصر (34) (12).

خامسًا: جد محصلة $(14)\,o\,(23)\,o\,(21)$.

سادسًا: عبر عن كل من التبديلتين (3 2 4 1) ، (2 3 4 1) . لمحصلة عدة تبادلات للموضع .

10 – صنف التبديلات التالية كونها زوجية أم فردية .

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \quad , \quad \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix} \quad ,$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix} \quad , \quad \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 2 & 5 & 4\end{pmatrix}$$

11– أثبت أن النظام (S_4 , o) يمثل زمرة غير إبدالية ، أستخدم جـــدول يمثل النظام (S_4 , o) ، وموضحًا منه معكوس كل عنصر، ما هي رتبة الزمرة .

12– من السؤال السابق أن (S_4 , o) تمثل زمرة غير إبدالية ، الآن هـــل أن (S_4^+ , o) تمثل زمرة جزئية إبدالية ؟ وكذلك (S_4^- , o) هل تمثل زمرة جزئية إبدالية ؟.

13– بين أن النظام $(Z_4 , \oplus)$ يمثل زمرة دائرية مولدة بالعنصر [1] .

14– من الزمرة الدائرية $Z_{15}^* , \oplus$ جد ما يلي:

$\langle [1] \rangle$ ، $\langle [2] \rangle$ ، $\langle [2]^{-1} \rangle$.

15– إذا كانت المجموعة G عناصرها التبديلات التالية

$G = \{I, (1\ 3\ 2), (1\ 2\ 3)\} \subseteq S_3$

فاثبت أن (G , o) هي زمرة دائرية مولدها التبديلة (2 3 1)

وكيف يمكن التعبير عن G ، وما هي |G| ؟ .

16- باعتبار أن $(S_4\,,\,o)$ تمثل زمرة التباديل وأن $(S_4^+\,,\,o)$ هي زمرة جزئية من S_4 ، إذا كان $a=(14)$ فأوجد

أولاً : المجموعة المصاحبة اليمنى S_4^+a

ثانيًا : المجموعة المصاحبة اليسرى aS_4^+

ثالثًا : هل أن $S_4^+a = aS_4^+$ ولماذا ؟

رابعًا : هل أن المجموعة المصاحبة اليمنى S_4^+a تمثل زمرة جزئية زمرة التباديل S_4^+ ؟

17- إذا كانت $(S_4\,,\,o)$ تمثل زمرة التباديل وأن $H_1=\{I\,,(13)\}$ ، $H_2=\{I\,,(14)\}$ فهل أن :

أولاً : $(H_1\,,\,o)$ تمثل زمرة جزئية من $(S_4\,,\,o)$ ؟

ثانيًا : $(H_2\,,\,o)$ تمثل زمرة جزئية من $(S_4\,,\,o)$ ؟

ثالثًا : $(H_2 \cup H_1, o)$ تمثل زمرة جزئية من $(S_4\,,\,o)$ ؟

18- إذا كانت $(S_4\,,\,o)$ تمثل زمرة التباديل فأثبت أن $(S_4^+\,,\,o)$ زمرة جزئية قياسية من $(S_4\,,\,o)$.

19- لتكن $G=\{i\,,a\,,b\,,c\,,d\,,e\}$ حيث إن

$$i=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \quad , \quad a=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$$

$$b = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad , \quad c = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$d = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad , \quad e = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

إذا كانت عملية الجمع لعناصر المصفوفات معرفة كالآتي :

$$1+1 = 0+0 = 0$$
$$1+0 = 0+1 = 1$$

فإن

أولاً : $(G , \times)$ تكون زمرة ، حيث "×" تمثل عملية الضرب للمصفوفات

ثانيًا : إذا كانت $H = \{i , d , e\}$ فإن $(H , \times)$ زمرة جزئية قياسية في $(G , \times)$.

20- برهن أن $(Z_7 , \otimes)$ تمثل زمرة دائرية ، ثم جد رتبة كل عنصر فيها .

21- في السؤال السابق (20) ، برهن على أن Z_7 تحتوي على عدد فردي من العناصر ذات الرتبة (2) ، إذا كانت $| G |= 2n$ حيث $n\in N$.

22- إذا كانت (S_4 , o) تمثل زمرة التباديل مـــن الدرجـــة الرابعـــة ، وأن $H = S_4^{+}$

أولاً: أثبت أن (H , o) زمرة جزئية قياسية من (S_4 , o) .

ثانيًا: جد زمرة القسمة S_4 / H .

ثالثًا: إذا كانت $H = S_4^{-}$ ، فهل أن (H , o) تمثل زمرة جزئية قياســـية من (S_4 , o) .

23- إذا كانت $(Z_{15} , \otimes)$ مجموعة صفوف التكافؤ بمقياس (15) تمثل زمرة وأن $H = \{[1] , [2] , [4] , [8]\}$ ، فهل أن النظام $(H , \otimes)$ يمثـــل زمرة جزئية قياسية من $(Z_{15} , \otimes)$ أم لا ؟

24- لتكن $(Z , +)$ و $(Z_7 , \oplus)$ زمرتين ولتكن الدالة f معرفة كالآتي

$$f : Z \to Z_7$$
$$f(a) = [a] \qquad , \qquad \forall\ a \in Z$$

(i) أثبت أن f تشاكل من Z إلى Z_7

(ii) هل أن f تشاكل تقابلي ؟ ولماذا .

(iii) جد نواة التشاكل (Ker f) .

25- لتكن $(Z , +)$ و $(Z_7 , \oplus)$ زمرتين ولتكن الدالة f معرفة كالآتي

$$f : Z \to Z_4$$

$$f(a) = \begin{cases} [0] & \text{إذا كان } a \text{ عدداً زوجيًا} \\ [2] & \text{إذا كان } a \text{ عدداً فرديًا} \end{cases}$$

(i) أثبت أن f تشاكل من Z إلى Z_4 .

(ii) هل أن f تشاكل متباين ؟ ولماذا .

(iii) هل أن f تشاكل تقابلي ؟ ولماذا .

(iv) جد مدى تشاكل R_f ؟

26- إذا كانت $(S_3 , \circ)$ زمرة غير إبدالية وأن $(Z_6 , \oplus)$ هي زمرة إبدالية وأن الدالة

$$f : S_3 \to Z_6$$

معرفة كالآتي:

$$f(I) = 0 \quad , \quad f(1\ 2\ 3) = f(1\ 3\ 2) = 0$$
$$f(12) = f(13) = f(23) = 5$$

هل أن f تمثل هومورفيزم (تشاكل) ؟ وإذا كان يمثل تشاكل فما هي نواة هذا التشاكل (Ker f) ، وما هو مدى التشاكل (R_f).

27- في السؤال السابق إذا كانت الدالة

$$f : S_3 \to Z_6$$

معرفة كالآتي :

$f(I) = 0 \quad , \quad f(1\ 2\ 3) = f(1\ 3\ 2) = 5$

$f(12) = f(13) = f(23) = 0$

فهل أن f تمثل تشاكل ؟ ولماذا ؟

28- إذا كانت $(Z , +)$, $(Z_6 , \oplus)$, (S_3 , o) تمثل ثلاث زمر وكانت

$g : Z_6 \to S_3 \quad , \quad f : Z \to Z_6$

ومعرفة كالآتي :

$f(a) = [a] \quad , \quad \forall\ a \in Z$

$g[0] = I \quad , g[1] = (12) \quad , g[2] = (13) ,$

$g[3] = (23) \quad , g[4] = (12\ 3) \quad , g[5] = (1\ 3\ 2) ,$

(i) هل أن f تمثل تشاكل ؟

(ii) هل أن g تمثل تشاكل ؟

(iii) إذا كانت g , f تمثل تشاكل فهل أن $g\ o f : Z \to S_3$ تمثل تشاكل؟

الفصل الثالث

الحلقات Rings

[1-3] تعريف ونظريات للحلقة

Definitions and Theorems of Ring

تعريف (3-1 .147):

إذا كانت R مجموعة غير خالية معرف عليها عمليتان ثنائيتان " + " ، "." فإن النظام $(R,+,.)$ يسمى حلقة (Ring) إذا تحقق ما يلي:

i- $(R,+)$ زمرة تبديلية .

ii- $a.(b.c) = (a.b).c$ لكل $a,b,c \in R$, أي إن العملية " . " تجميعية.

iii- لكل $a,b,c \in R$ فإن

$$a.(b+c)=a.b+a.c$$

$$(b+c).a=b.a+c.a$$

أي أن العملية " . " توزيعية على " + " من اليمين ومن اليسار .

ملاحظة (3-1 . 148):

(i) يسمى العنصر " 0 " بصفر الحلقة وتسمى الزمرة $(R, +)$ بالزمرة التجميعية للحلقة.

(ii) إذا تحقق $ab= ba$ لكل $a,b \in R$ فإن الحلقة تسمى حلقة تبديلية.

(iii) يقال للحلقة إنها ذات عنصر محايد إذا كان $1 \in R$ حيث $a.1=1.a=a$ لكل $a \in R$.

مثال (3-1. 149) :

مجموعة الأعداد الصحيحة مع عمليتي الجمع والضرب العاديتين $(Z,+,.)$ تحقق كل الشروط المطلوبة في تعريف الحلقة، وبالإضافة إلى ذلك فإنها تحقق شرط الإبدال والعنصر المحايد، أي أنها حلقة تبديلية ذات عنصر محايد.

مثال (3-1. 150) :

i- مجموعة الأعداد الصحيحة الزوجية مع عمليتي الجمع والضرب $(Z_e,+,.)$، تكون حلقة تبديلية و لكنهما لا تحقق خاصية العنصر المحايد أي لا تحتوي على عنصر محايد حيث إن :

$$1 \notin Z_e$$

ii- مجموعة كل المصفوفات التي من نوع 2×2 المعرفة على الأعداد الحقيقية مع عمليتي جمع وضرب المصفوفات $(M_{2\times2},+,.)$ تمثل حلقة ولكنها ليست تبديلية .

نظرية (3-1. 151)

إذا كانت R حلقة لها محايد، فإنه يكون وحيدًا.

البرهان:

نفرض أنه يوجد أكثر من محايد واحد فمثلاً 1 , `1 كل منها عنصر محايد بالنسبة للعملية " . " على R .

وهذا يعني أن

$$\left.\begin{array}{l} \text{R } \text{ في } \text{ محايد } 1 \text{ وذلك لان } 1` = 1` .1 \\ \\ \text{R } \text{ في } \text{ محايد } 1` \text{ وذلك لان } 1 = 1` .1 \end{array}\right\} \Rightarrow \quad 1 = 1`$$

نظرية (3-1.152)

إذا كانت (., +, R) تمثل حلقة و أن $a,b \in R$ فإن:

i - $0.a=a.0=0$

ii - $(-a)(b)=(a)(-b)=-(ab)$

iii - $(-a)(-b)=ab$

البرهان:

i – من المعلوم أن $(R, +)$ تمثل زمرة وهذا من تعريف الحلقة أي أن $0 \in R$ ، ومن خواص هذا العنصر هو

$$0+0=0$$

$$\therefore a.0= a.(0+0) \quad , \forall \quad a \in R$$

من خواص الحلقة

$$\Rightarrow a.0=a.0+a.0$$

$$\Rightarrow a.0+0=a.0+a.0$$ من خواص 0

$$\Rightarrow 0=a.0$$ من خواص الحذف

ii – بما إن

$$a+(-a)=0$$

$\therefore\ \{a+(-a)\}.b=0.b$

$\Rightarrow a.b+(-a).b=0.b$

$\Rightarrow a.b+(-a).b=0$

وهذا يعني أن $(-a).b$ هو معكوس جمعي للعدد ab ولكن معكوس ab هـو $-(ab)$.

ولهذا فإن $(-a)b=-(ab)$

iii - باستخدام الخاصة (ii) وبوضع $b=-b$, ينتج أن

$(-a)(-b)=a(-(-b))=a(b)=(ab)=ab$

[3-2] الحلقات الجزئية
Subrings

تعريف (3-2. 153):
لتكن المجموعة S مجموعة جزئية غير خالية من الحلقة R نقول أن S هي حلقة جزئية من R ، إذا كانت S حلقة تحت العمليتين نفسيهما المعرفتين على R.

مثال(3-2. 154)

لكل حلقة R توجد حلقتان جزئيتان هما $\{0\}$, R

مثال (3-2. 155)

مجموعة الأعداد الصحيحة الزوجية $(Z_e,+,.)$ هي حلقة جزئية من حلقة الأعداد الصحيحة مع عمليتي الجمع والضرب الاعتياديتين $(Z,+,.)$.

نظرية (3-3. 156)

تكون المجموعة الجزئية غير خالية Sمن الحلقة R حلقة جزئية من R إذا وفقط إذا كان

$$\text{i-}\quad a+b \in S \qquad \forall\ a,b \in S$$
$$\text{ii-}\quad ab \in S \qquad \forall\ a,b \in S$$

البرهان:

استخدام تعريف الزمرة الجزئية من الفصل الثاني نلاحظ بإن $(S,+)$ تمثل زمرة جزئية في R.

وأن عملية التجميع والتوزيع متحققة في S لأنها مجموعة جزئية من R ، إذن $(S,+,.)$ حلقة جزئية من $(R,+,.)$.

تعريف (3-2. 157):

إذا كانت R حلقة فإن العنصر $a \in R$ يكون قاسمًا للصفر من اليمين إذا وجد $0 \neq b \in R$

بحيث إن $ba=0$

وكذلك يكون قاسمًا للصفر من اليسار إذا وجد

$0 \neq b \in R$ بحيث إن $ab=0$

ويسمى العنصر a قاسمًا للصفر بصورة عامة إذا كان قاسمًا للصفر من اليمين ومن اليسار

ملاحظة (3-2. 158):

i- إذا كان R حلقة غير صفرية فإن , 0 قاسمًا للصفر لأنه

$$a.0=0.a=0 \quad \forall \ 0 \neq a \in R$$

ii- القاسم الحقيقي للصفر هو قاسم الصفر المختلف عن الصفر .

تعريف (3-2. 159):

إذا كانت R حلقة ذات عنصر محايد , فإن العنصر $b \in R$ يكون قابل للعكس إذا وجد $a \in R$

بحيث إن $ab=ba=1$

مثال (3-2. 160):

المجموعة $Z_6 = \{[0],[1],[2],[3],[4],[5]\}$ مع عمليتي الجمع والضرب بمقياس 6 تكون حلقة تبديلية ذات عنصر محايد $(Z_6 , \oplus , \otimes)$.

كما نلاحظ بأنه $[4]$, $[3]$, $[2]$ هي قواسم حقيقية للصفر , كما نلاحظ أن $[5]$, $[1]$ عناصر قابلة للعكس وذلك لأن $[1] = [5][5]$, $[1][1] = [1]$ وهذا يكون واضحًا عند تكوين جدول ألى Z_6 بالعمليتين $\oplus$, $\otimes$ (يترك هذا كتمرين للطالب)

نظرية (3-2. 161):

إذا كانت R حلقة تبديلية ذات عنصر محايد، فإن إي عنصر قابل للعكس في هذه الحلقة لا يمكن أن يكون قاسمًا للصفر.

البرهان:

نفرض أن العنصر $a \in R$ قابل للعكس، وكذلك يكون قاسمًا للصفر وهذا يعني أنه

$$\exists \ 0 \neq b \in R : b.a = a.b = 0$$

ومن كون العنصر a قابل للعكس نحصل على

$\exists \quad 0 \neq c \in R \quad : a.c=1$

ومنه نحصل على

$$b=b.1=b.(a.c)$$

$$= (b.a).c=0.c=0$$

وهذا يناقض الفرض حيث إن $b \neq 0$ وعلى هذا فإن a لا يمكن أن يكون قاسمًا للصفر.

تعريف (3-2. 162):

i- إذا كانت R تمثل حلقة فإن العنصر $a \in R$ يقال عنه أنه عنصر جامد إذا كان $a^2 = a$.

ii - وكذلك يقال عن $a \in R$ إنه عديم القوى من الدرجة n إذا كان $a^n = 0$ ولكن $a^{n-1} \neq 0$ حيث $n \geq 1$.

مثال (3-2. 163):

الحلقات التي تحتوي على العنصر المحايد , يكون العنصران 1 , 0 بها عناصر جامدة.

مثال (3-2. 164):

إذا كانت المجموعة A غير خيالية فإن مجموعة المجموعات الجزئية من A وهي $P(A)$ تكون حلقة تحت عمليتي الجمع و الضرب المعرفتين كالأتي:

$$A_1+A_2=A_1 \cup A_2-(A_1 \cap A_2) \qquad \forall \; A_1 , A_2 \in P(A)$$

$$A_1.A_2 = A_1 \cap A_2 \qquad \forall \; A_1 , A_2 \in P(A)$$

وبهذا يكون

1- المجموعة الخالية ϕ هي صفر الحلقة P(A).

2- المجموعة A هي العنصر المحايد لهذه الحلقة .

3- عناصر الحلقة P(A) عناصر جامدة وذلك لأن

$$A_1^2 = A_1 \cap A_1 = A_1 \qquad \forall \quad A_1 \in P(A)$$

ملاحظة (3-2. 165):

إذا كان العنصر a عديم القوى في الحلقة R فإن a يكون قاسمًا للصفر (لماذا؟).

مثال (3-2. 166):

هذا المثال يوضح أن العكس غير صحيح في الملاحظة (3-2. 165) أي ن ليس كل عنصر قاسم للصفر يكون عديم القوى فمثلاً في المثال (3-2. 164) نلاحظ أنه إذا كانت $A_1 \neq \phi$, $A_2 \neq \phi$ فإنه يمكن أن نجد أن

$$A_1 \cap A_2 = \phi$$

$$\Rightarrow \quad A_1 . A_2 = A_1 \cap A_2 = \phi$$

وبالتالي تكون A_1 قاسمًا للصفر .

ولكن نلاحظ كذلك بأن

$$A_1^n = A_1 . A_1 . A_1 \ldots A_1 = A_1 \cap A_1 \cap A_1 \cap A_1 \ldots = A_1$$

أي أن A_1 ليست عديمة القوى .

تعريف (3-2. 167):

إذا كانت R حلقة تبديلية ذات عنصر محايد و لا تحتوي على قواسم للصفر فإن R تسمى حلقة كاملة.

مثال (3-2. 168):

الحلقة $(Z ,+,.)$، حيث " + " ، " . " عمليتا الجمع والضرب العاديتان على مجموعة الأعداد الصحيحة، هي حلقة كاملة و ذلك لأنهما حلقة تبديلية ذات عنصر محايد و لا تحتوي على قواسم للصفر.

نظرية (3-2. 169):

إذا كانت R تمثل حلقة وأن $a,b \in R$ فإن

$$i-\ ac=ab \quad \Rightarrow \quad c=b \quad \forall \quad a \neq 0$$
$$ii-\ ca=ba \quad \Rightarrow \quad c=b \quad \forall \quad a \neq 0$$

خاصيتا الحذف أعلاه تحقق في R إذا وفقط إذا كانت R لا تحتوي على قواسم للصفر.

البرهان:

1- لنفرض أن R حلقة تحقق فيها خاصيتا الحذف ، وبفرض أن $a,b \in R$ فإن $ab=0$ حيث $a \neq 0$.

خاصية الحذف من اليسار $\therefore ab=0=a.0 \Rightarrow b=0$

وكذلك $ab=0$ حيث $b \neq 0$

خاصية الحذف من اليمين $\therefore ab=0=0\ .b \Rightarrow a=0$

وبهذا فإن R لا تحتوي على قواسم للصفر .

2- لبرهان العكس نفرض أن R حلقة لا تحتوي على قواسم للصفر .

إذا كان $ab = ac$ حيث $a \neq 0$ فإن ذلك يؤدي إلى

$$ab-ac=0$$
$$a(b-c)=0$$

وحيث إن R لا تحتوي على قواسم للصفر فإن

$$b-c=0 \qquad \Rightarrow b=c$$

وهذا يعني أن خاصية الحذف من اليسار متحققة في R وكذلك بالطريقة نفسها يمكن إثبات أن

$$ca=ba \qquad \Rightarrow \quad c=b \quad \forall \quad a \neq 0$$

أي خاصية الحذف من اليمين .

تعريف (3-2. 170):

لتكن $(R, *, o)$ حلقة , إذا وجد عدد صحيح موجب مثل n بحيث إن $na=0$ لكل $a \in R$ وكانت n أصغر عدد صحيح موجب يحقق ذلك , ففي هذه الحالة يقال إن n هو المميز للحلقة R.

ويكتب بالشكل char (R)

ملاحظة (3-2. 171):

من التعريف السابق في حالة عدم وجود n تحقق $na=0$ لكل $a \in R$ فــإن مميز الحلقة يكون الصفر .

مثال (3-2. 172)

i- الحلقة $(Z_6 , \oplus , \otimes)$, لها مميز 6.

ii- الحلقة $(Z , + , .)$ لها مميز 0 .

نظرية (3-2. 173):

إذا كانت R حلقة ذات عنصر محايد 1 ، فإن R يكون لها المميز n إذا وفقط إذا كان n أصغر عدد صحيح موجــب بحيــث إن $n.1=0$ ، أي أن n رتبة العنصر (1) في الزمرة $(R ,+)$.

البرهان:

i- بما أن R لها المميز n حيث $n > 0$,

إذن $na=0$ لكل $n \in R$, ومنه نحصل على $n . 1 =0$

ii- الآن نثبت العكس

لكل $a \in R$ فإن

$$\begin{aligned} na &= n\,(1a) =1a+1a+...+1a \\ &=(1+1+...+1)\, a \\ &=(n\,.\,1)\, a=0a =0 \end{aligned}$$

ومنه نحصل على أن R لها المميز n

نظرية (3-2. 174):

مميز الحلقة الكاملة يكون صفرًا أو عددًا أوليًا.

البرهان:

إذا كانت R حلقة كاملة لها المميز n حيث $n > 0$ ، فإذا فرضنا أن n عدد مركب أي أن $n = n_1 n_2$ حيث $n_1,n_2 < n$ و أن $1 < n_1,n_2$ ، فإن

$$0 = n1 = (n_1 n_2)1$$
$$=(n_1 . 1)(n_2 . 1)$$

أي أن $0 = (n_2 .1)(n_1 . 1)$ ولكن R حلقة كاملة ,

إذن $0 = 1 . n_1$ أو $0 = 1 . n_2$, حيث إن كل من n_1 , n_2 أقل من n وهذا يتناقض مع ان $\text{char}(R)=n$ لذلك فإن n يجب أن يكون عددًا أوليًا.

[3-3] المثاليات
Ideals

تعريف (3-3 . 175):

المجموعة الجزئية غير الخالية I من الحلقة R، تسمى مثالية، إذا تحقق الشرطان الآتيان:

i- $(I,+)$ زمرة جزئية من $(R\ ,\ +)$.

ii- لكل $x \in R\ ,\ a \in I$ فإن

1- $ax \in I$ (تسمى مثالية يسرى)

2- $xa \in I$ (تسمى مثالية يمنى)

ويقال أن I مثالية إذا كانت مثالية يسرى ومثالية يمنى في الوقت نفسه .

مثال (3-3. 176):

إذا كانت R حلقة إبدالية وكان العنصر $R \ni a \neq 0$ فإن المجموعة

$$aR = \{ ax : x \in R \}$$

مثالية في الحلقة R

الحل:

نبرهن أولاً أن $(aR\ ,\ +)$ زمرة .

ليكن v,u عناصر من aR , فيوجد $x_1\ ,\ x_2$ في R بحيث إن

$$u = ax_1 \quad , \quad v = ax_2$$

وبما أن

$$u+v = ax_1+ax_2 = a(x_1+x_2) \in aR$$

$$-u=-ax_1=a(-x_1) \ni a R$$

$$0=a\ .\ 0 \in a R$$

وبما أن قانون التجميع متحقق لكون R حلقة، فإن (+ , aR) زمرة.

الآن لتكن x أي عنصر في R ، فيكون لدينا

$$xu = x(ax_1) = (xa)x_1 = (ax)x_1 = a(xx_1) \in aR$$

إذن aR مثالية في الحلقة R .

ملاحظة (3-3. 177):

i- في المثال (3-3. 176) المجموعة المثالية aR تدعي بالمثالية الأساسية المتولدة بالعنصر a ويرمز لها بالرمز " (a) ".

ii- إذا كانت R حلقة بحيث إن كل مثالية فيها تكون أساسية , فإن R تدعي بحلقة مثاليات أساسية.

تعريف (3-3. 178):

ليكن I مثالية في الحلقة R , يرمز لمجموعة المجموعات المشاركة إلى I في R بالرمز R/I ، أي أن

$$R/I = \{a + I : a \in R\}$$

تعرف عملية الجمع و الضرب على R/I كما يلي:

i- $(a+I) + (b+I) = (a+b) + I$

ii- $(a+I) . (b+I) = (ab) + I$

نظرية (3-3. 179):

ليكن I مثالية في الحلقة R، فإن R/I مـــع العمليتـــين المعـــرفتين فـــي التعريف السابق تكون حلقة.

البرهان:

أولاً: نتحقق من كون عملية الجمع معرفة تعريفًا جيدًا و أن (+ , R/I) تؤلـــف زمرة إبدالية، ويترك هذا للطالب .

ثانيًا: لنتحقق من أن عملية الضرب معرفة تعريفًا جيدًا، نفرض أن

$$a+I=a`+I \quad , \quad b+I=b`+I$$

ونبرهن أن

$$(a+I) . (b+I) = (a`+I).(b`+I)$$

أي أن

$$(ab)+I=(a`b`)+I$$

وبما ان

$$a+I=a`+I \ , \ b+I=b`+I$$

فإن

$$a=a`+i_1 \quad , i_1 \in I$$

وكذلك

$$b=b`+i_2 \quad , i_2 \in I$$

وعليه فإن

$$ab = (a`+i_1)( b`+i_2) =a`b`+a`i_2+b`i_1+i_1i_2$$

وبما أن I في R مثالية فإن

$$a`i_2 \in I \quad , \quad b`i_1 \in I \quad , \quad i_1i_2 \in I$$

وهذا يعني أن

$$a`i_2+b`i_1+i_1i_2 \quad \in I$$

وبالتالي فإن

$$ab = a`b`+(a`i_2+b`i_1+i_1i_2)$$

لذا يكون

$$ab+I = a`b`+(a`i_2+b`i_1+i_1i_2)+I$$
$$ab+I = a`b`+I$$

وهذا يبين أن عملية الضرب معرفة تعريفاً جيدًا و بالتالي فإن $(R\backslash I\ ,\ .)$ شبه زمرة لأن $(R\ ,\ .)$ شبه زمرة , بقى أن نتحقق من خاصية التوزيع.

ليكن كل من

$$x = a+I\ ,\quad y= b+I\quad ,\quad z=c+I$$

عنصرًا في $R\backslash I$ حيث إن $a,b,c \in R$

فإن

$$\begin{aligned}(x+y)z &= ((a+I)+(b+I)).(c+I)= ((a+b)+I).(c+I)\\ &= ((a+b)c+I)=((ac+bc)+I)\\ &=(ac+I)+(bc+I)\\ &= (a+I).(c+I)+(b+I).(c+I)\\ &= xz+yz\end{aligned}$$

وبهذا حققنا جميع متطلبات الحلقة أي أن $R\backslash I$ حلقة .

مثال (3-3. 180):

المجموعة $I= \{[0],[2],[4]\}$ مثالية في Z_6 كما أن

$$Z_6 \backslash I = \{I,[1] + I\}$$

جد جدولي الجمع والضرب بالنسبة لعناصر $Z_6 \backslash I$

الحل:

$(I , +)$ زمرة عناصرها المحايد هو [0] ونظير العنصر [2] هو العنصر [4]

بما أن:

$$[0]+I = [2] + I = [4] + I = I$$
$$[1] + I = [5] + I = [3] + I$$

فإن

$$Z_6 \backslash I = \{I,[1] + I\}$$

وأن عملية الجمع والضرب معرفتان كما يأتي:

+	I	[1]+I
I	I	[1]+I
[1]+I	[1]+I	I

.	I	[1]+I
I	I	I
[1]+I	I	[1]+I

ملاحظة (3-3. 181):

i- من النظرية (3-3. 179) يتضح أنه إذا كانت R حلقة تبديليــة فإن $R\backslash I$ تكون حلقة إبدالية أيضًا و ذلك لأن:

$$(a+I) . (b+I) = (ab)+I = (ba) +I = (b+I). (a+I)$$

ii- العكس ليس صحيح.

iii- يمكن إثبات أن $I + [1]$ هو العنصر المحايد بالنسبة لعملية الضرب $R\backslash I$, إذا كان " 1" هو العنصر المحايد في R بالنسبة لعملية الضرب , يترك الإثبات للطالب .

تعريف (3-3. 182):

إذا كان M مثالية في الحلقة R وكان $M \neq R$ فإن M يدعى مثالية عظمى ، إذا لم يكن هناك مثالية أخرى مثل N بحيث إن

$$M < N < R$$

تعريف (3-3. 183):

لتكن R حلقة إبدالية لا تحتوي على قواسم الصفر , تسمى R حلقة إقليدية إذا كان لكل عنصر $0 \neq a \in R$ ، فإن هناك عددًا صحيحًا غير سالب $d(a)$ بحيث إن

i- $d(a) \leq d(ab)$ لكل عناصر b ي R التي تختلف عن الصفر.

iii- لكل $a,b \in R$ حيث $a,b \neq 0$, يوجد $r,t \in R$ بحيث إن

$$a=tb+r$$

حيث إن $d(b) > d(r)$ or $r=0$

مثال (3-3. 184):

مجموعة الأعداد الصحيحة، حيث $d(a)$ يساوي القيمة المطلقة للعدد a، هي حلقة إقليدية.

نظرية (3-3 . 185):

إذا كان I مثالية في حلقة إقليدية R فيوجد في I عنصر مثل a_0 بحيث إن

$$I=\{ a_0x : x \in R\}$$

البرهان:

أولاً: إذا كان $I=\{0\}$ فإن $a_0=0$ و المبرهنة تحقق .

ثانيًا: إذا كان $I \neq \{0\}$, فإنه يوجد عنصرا $a \in I$ $a \neq 0$ الآن نختار a_0 في A بحيث يكون $d(a_0)$ أصغر عدد صحيح غير سالب، وبما أن R حلقة إقليدية، إذا يوجد r , t في R بحيث إن

$$a=ta_0+r$$

حيث

$$d(r)<d(a_0) \quad \text{or} \quad r=0$$

بما أن a_0 عنصر في I و أن I مثالية في R , فإن ta_0 يكون عنصرًا في I وهذا يعني أن $a-ta_0$ يكون عنصرًا في I و بالتالي فإن

$$r=a-ta_0$$

يكون عنصرًا في I أيضًا.

.

إذا كان العنصر $r \neq 0$, فيجب أن يكون $d(r) < d(a_0)$ وهذا أيضًا تناقض $d(a_0)$ هو أصغر عدد صحيح غير سالب يمكن أن يقرن بعنصر في A إذن r يساوي صفرًا , وهذا يعني أن : $a=ta_0$.

[4-3] حلقات متعددات الحدود
Ring of Polynomials

تعريف (3-4. 186):

لتكن R حلقة إبدالية ذات عنصر محايد , تعرف متعـــددة حـــدود فـــي المجهول x على R بالصيغة التالية :

$$a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n$$

حيث $a_0, a_1, a_2 .. a_n \in R \quad ; \quad n \in N$

وللاختصار، نكتب في بعض الأحيان بالشكل P(x) أو q(x) أو… إلخ

ملاحظة (3-4. 187):

i- لتمثيل متعددات حدود , يسمى العنصر a_i بمعامل x^i حيث $0 \leq i \leq n$

ii- إذا كان معامل x^i صفرًا فأننا نهمل كتابة الحد $0x^i$ ، أما إذا كان معامـــل x^i يساوي 1 فإننا نكتب x^i بدلاً من $1x^i$.

iii- إن المجهول x هو رمز يحافظ على ترتيب المعاملات و لا نشترط أن يكون عنصرًا في الحلقة R.

iv- العلامة " + " لا تفيد الجمع، وإنما رمز عام .

ملاحظة (3-4. 188):

i- يمكن تعريف متعددة حدود معاملاتها في R على أنها متتابعـــة غيـــر منتهيـــة $(a_0, a_1, a_2 \ldots)$ حيث إن جميع حدود المتتابعة a_i تكون عناصر في R وأن جميع هذه الحدود (باستثناء عدد منهيه منه) تكون مساوية للصفر.

ii- يرمز للعنصر $(0, a, 0, 0, \ldots)$ بالرمز ax و العنصر $(0, 0, a, 0, \ldots)$ بالرمز ax^2 وهكذا .

تعريف (3-4, 189):

إذا كانت جميع معاملات متعددة حدود أصفارًا , فإنها تـسمى متعـددة حدود صفرية ويعبر عنها $f(x) = 0$.

تعريف (3-4. 190):

ليكن $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

إذا كان n هو أكبر عدد صحيح بحيث إن $a_n \neq 0$ فإن درجة $p(x)$ هي n ونكتب $\deg p(x) = n$, و المعامل a_n يسمى بالمعامل الدليل .

ملاحظة (3-4. 191):

i- إذا كانت معاملات $p(x)$ كلها أصفارًا ماعدا a_0 فإن درجة $p(x)$ هي صفر , وتسمى متعـددات حـدود ذات الدرجـة صـفر بمتغيرات حدود ثابتة.

ii- متعددات الحدود الصفرية ليس لها درجة , أي أن درجتها غيـر معرفة.

مثال (3-4. 192):

لتكن Z حلقة، مجموعة الأعداد الصحيحة مـع عمليتـي الجمـع والـضرب الاعتياديتين.

i- متعدد الحدود $5x^0$ درجة صفر .

ii- متعدد الحدود $5x^0 + 3x^1$ درجة "1".

iii- متعدد الحدود $5x^0 + 3x^1 + 7x^2$ درجة "2".

تعريف (3-4. 193)

لتكن R حلقة إبدالية ذات عنصر محايد، نرمز لمجموعة متعددات الحدود في x على R بالرمز $R[x]$ أي أن

$$R[x] = \{a_0x^0+a_1x^1+a_2x^2+\dots+a_nx^n : a_i \in R \quad , \quad n \in N\}$$

تعريف (3-4. 194)

إذا كان $p(x)$, $q(x)$ متعدد الحدود في $R[x]$ حيث

$$p(x) = a_0x^0+a_1x^1+\dots+a_mx^m$$

$$q(x) = b_0x^0+b_1x^1+\dots+b_nx^n$$ فإن:

i- نقول أن $p(x) = q(x)$ إذا وفقط إذا كان $a_i = b_i$ لكل الأعداد الصحيحة $i \geq 0$.

ii- تعرف مجموع $p(x)+q(x)$ كما يلي:

$$P(x)+q(x) = c_0 + c_1x + c_2x^2+\dots+c_tx^t$$

حيث إن $c_i = a_i + b_i$ لكل الأعداد الصحيحة $i \geq 0$ و أن t أكبر من العددين m , n

iii- حاصل ضرب $p(x)$ في $q(x)$ يعرف كمايلي :

$$P(x)q(x) = c_0x^0+c_1x^1+c_2x^2+\dots+c_tx_t$$

حيث إن

$$c_t = a_tb_0+a_{t-1}b_1+a_{t-2}b_2+\dots+a_0b_t$$

مثال (3-4. 195):

ليكن كل من

$$p(x) = 1x^0 + x^1 - x^2$$
$$q(x) = 2x^0 + x^2 + x^3$$

متعدد الحدود في $Z[x]$, جد

i- $p(x)+q(x)$

ii- $P(x)q(x)$

الحل:

من الواضح أن

$a_0=a_1=1$, $b_0=2$, $b_1=0$
$a_2=-1$,$b_2=b_3=1$
$a_3=a_4=...=0$, $b_4=b_5=...0$

(i) لإيجاد الجمع فإن

$$P(x)+q(x)=(1+2)x^0+(1+0)x^1+(-1+1)x^2+(0+1)x^3=3x^0+x^1+x^3$$

(ii) لإيجاد حاصل الضرب فإننا نحسب أولاً c_t وكما يلي :

$c_0=a_0b_0=1.2=2$
$c_1=a_1b_0+a_0b_1=1.2+1.0=2$
$c_2=a_2b_0+a_1b_1+a_0b_2=(-1)(2)+1.0+1.1=-1$
$c_3=a_3b_0+a_2b_1+a_1b_2+a_0b_3=0.2+(-1)(0)+1.1+1.1=2$
$c_4=a_4b_0+a_3b_1+a_2b_2+a_1b_3+a_0b_4=0.2+0.0+(-1)(1)+1.1+1.0=0$
$c_5=a_5b_0+a_4b_1+a_3b_2+a_2b_3+a_1b_4+a_0b_5=0.2+0.0+0.1+$
$+(-1)(1)+1.0+0.0=-1$
$c_6=a_6b_0+a_5b_1+a_4b_2+a_3b_3+a_2b_4+a_1b_5+a_0b_6=0.2+0.0+0.1+0.1+$
$+(-1)(0)+1.0+1.0=0$

وبالطريقة نفسها نجد أن

$c_7=c_8=...=0$
$$p(x)q(x)=c_0+c_1x+c_2x^2+c_3x^3+c_4x^4+c_5x^5+0+0=2+2x-x^2+2x^3-x^5$$

نظرية (3-4. 196):

لتكن R حلقة إبدالية ذات عنصر محايد . فإن (.,+, R[x]) حلقة إبدالية حيث إن "+" ، ". " يمثلان عمليتي الجمع والضرب المعرفتين في التعريف (3-4. 194).

البرهان:

i - لاحظ بأن R[x] مغلقة بالنسبة لعمليتي الجمع والضرب المعرفتي عليها .

ii- عملية الجمع والضرب تجميعية (يترك التمرين للطالب).

iii- إذا عرفنا

$$-f(x)=-(a_0x^0+a_1x^1+a_2x^2+\ldots a_mx^m)$$
$$=(-a_0)x^0+(-a_1)x^1+\ldots(-a_m)x^m$$

حيث إن a_i- هو النظير الجمعي للمعامل a_i في الحلقة R يكون f(x)- النظير الجمعي لمتعدد الحدود f(x).

iv- عملية الجمع و الضرب إبدالية على R[x] (يترك الأثبات للطالب).

v- إن عملية الضرب تتوزع على عملية الجمع (يترك الأثبات للطالب).

وبذلك يكون R[x] مع عمليتي الجمع والضرب المعرفتين عليها حلقة إبدالية .

ملاحظة (3-4. 197):

إذا كان العنصر "1" هو المحايد الضربي للحلقة R فإن "$1x^0$" يكون محايدًا ضربيًا للحلقة R[x].

نظرية (3-4. 198):

إذا كانت $R[x]$ هي حلقة متعدد الحدود للحلقة R, فــإن $R[x]$ تحتــوي على حلقة جزئية بحيث إن الدالة $f: R \to S$ تمثل هومومورفيزم تقابل .

البرهان:

نأخذ المجموعة

$$S=\{ ax^0 \in R[x] : a \in R\}$$

i- نثبت أن S مع عمليتي الجمع و الضرب هــي حلقــة جزئيــة مــن $R[x]$ (يترك هذا التمرين للطالب ليثبته).

ii- تعرف الدالة f من R إلى S كالتالي:

$$f(ax^0)=a$$

إن هذه الدالة متباينة و شاملة (لماذا ؟)

وكذلك فإن

$$f(ax^0+bx^0) = f((a+b)x^0)= a+b$$
$$f((ax^0)(bx^0))=f((ab)x^0)=ab$$

أي أن هذه الدالة تحافظ على عمليتي الجمع و الضرب وبذلك تحقق خــواص الهومومورفيزم التقابلي من S إلى R.

ملاحظة (3-4. 199):

i- من النظرية السابقة يمكن إعتبار R حلقة جزئية من $R[x]$ و أن عناصر R غير الصفرية متعددات الحدود ذات درجة صفر في $R[x]$.

ii- سوف نكتب a_0 بدلاً من a_0x^0 وكذلك x بدلاً من x^1 .

نظرية (3-4. 200):

إذا كانت R حلقة إبدالية لا تحتوي قواسم الصفر وكان كل من $p(X),q(X)$ متعدد الحدود لا صفريًا في $R[x]$ فإن

$$\deg (p(x)q(x)) = \deg p(x) + \deg q(x)$$

البرهان: ليكن

$$P(x)= a_0+a_1x^1+a_2x^2+...+a_nx^n$$
$$q(x)= b_0+b_1x^1+b_2x^2+...+b_mx^m$$

حيث إن a_n , b_m يختلفان عن الصفر .

فإن $\deg p(x)=n$, $\deg q(x)=m$

بما أن

$$P(x)q(x)=c_0+c_1x+c_2x^2+...+c_tx^t$$

حيث إن

$$C_t = a_tb_0 +a_{t-1} b_1 +a_{t-2}b_2+...a_0b_1$$

فإن

$$C_{m+n} =a_nb_n$$

بما أن R لا تحتوي على قواسم للصفر و أن كلاً من a_n , b_m تختلف عن الصفر ,

إذن

$c_{m+n} \neq 0$ وهذا يعني أن درجة متعدد الحدود $p(x)q(x)$ هي عدد أكبر من أو تساوي $(m+n)$.

وبما أن

$$c_i= \sum \ a_j(b_{i-j})$$

فإن

$$i > (m+n) \Rightarrow j+(i-j) > (m+n)$$

$$\Rightarrow (\ j\ > m) \vee\ ((i-j) > n\ )$$
$$\Rightarrow (a_j = 0) \vee (b_{i-j} = 0\ ) \Rightarrow c_i = 0$$

نتيجة (3-4. 201) :

إذا كان كل من $p(x)$, $q(x)$ متعدد الحدود لا صفريًا في $R[x]$ حيث R حلقة إبدالية لا تحتوي قواسم للصفر فإن

$$\deg p(x) \le \deg (p\ (x) q\ (x))$$

البرهان:

من النظرية السابقة (3-4. 200)

نحصل على

$$\deg (p(x)q(x)) = \deg p(x) + \deg q(x)\ \ge \deg p(x)$$

وذلك كون

$$\deg q(x) \ge\ 0$$

نتيجة (3-4. 202) :

إذا كانت R حلقة إبدالية لا تحتوي قواسم للصفر فإن $R[x]$ حلقة إبدالية لا تحتوي قواسم للصفر .

البرهان:

لدينا $(R[x]\ ,\ +\ ,\ .)$ حلقة إبدالية

إذا كان كل من $p(x)$, $q(x)$ متعدد الحدود لا صفريًا في $R[x]$ فإن $(p(x)q(x))$ متعدد الحدود لا صفري وذلك من النتيجة السابقة (3-4. 201).

[5-3] التشاكل (الهمومورفيزم)
Homomorphism

تعريف (3-5. 203):

إذا كانت كل من R , S حلقة فإنه يقال للدالة $f:R\to S$ أنها هومورفيزم (تشاكل) إذا تحقق مايلي :

$$i\text{- } f(a+b)=f(a)+f(b) \quad \forall \quad a,b \in R$$
$$ii\text{- } f(ab)=f(a)f(b) \quad \forall \quad a,b \in R$$

مثال (3-5. 204):

إذا كانت كل من S,R حلقة وكانت الدالة f , $f: R\to S$ معرفة كما يلي:

$$f(a)=0s$$

فإن f تمثل تشاكل من R إلى S وذلك لأن

$$i\text{- } f(a+b)=0 \quad \forall\ a,b \in R$$
$$=0+0=f(a)+f(b)$$
$$ii\text{- } f(ab)=0\ \forall\ a,b \in R$$
$$=0+0=f(a).f(b)$$

ملاحظة (3-5. 205):

إذا كانت الدالة f تشاكل من الحلقة R إلى الحلقة S فإن

i- يسمى التشاكل ، تشاكل متباين إذا كانت الدالة f متباينة .

ii- ويسمى التشاكل ، تشاكلاً شاملاً (اميبومورفيزم) إذا كانت الدالة f شاملة .

iii- ويسمى التشاكل ، تشاكل تقابلي (ايزومورفيزم) إذا كانت الدالة متباينة وشاملة.

iv- في حالة التشاكل التقابلي , فإن الحلقتين S, R تكونا متماثلتين .

v- إذا كانت R=S فإن f تسمى تشاكل ذاتي (اندومورفيزم) وتسمى تشاكل تقابلي ذاتي (اوتومورفيزم) إذا كانت بالإضافة إلى هذا دالة تقابل.

نظرية (3-5. 206):

إذا كانت f تمثل تشاكل من الحلقة R إلى الحلقة S فإن :

i - $f(0_R)=0_S$

ii - $f(-a)=-f(a)$

iii- إذا كان (1_R) يمثلا المحايد للحلقة R و (1_S) المحايد للحلقة Sوأن f شاملة فإن:

$$f(1_R)=1_S$$

البرهان:

i- لكل $a \in R$ فإن

$$a=a+0$$
$$f(a)=f(a+0)$$
$$\therefore = f(a)+f(0)$$
$$\therefore f(0_R)=0_S$$

ii- بما أن

$$0_R=a+(-a)$$
$$\therefore f(0_R)=f(a+(-a))$$
$$f(0_R)=f(a)+f(-a)$$

$\therefore 0_S = f(a)+f(-a)$
$\Rightarrow f(-a)=-f(a)$

iii- بما أن f شاملة فإنه ،

$$\forall \quad s\in S\ \exists\ a\in R: s=f(a)$$
$$= f(1_R .a)$$
$$= f(1_R).f(a)$$
$$= f(1_R).S$$

وهذا يني أن $f(1_R)$ هو عنصر محايد في S , وبمـــا أن المحايـــد وحيد فإن ،

$$f(1_R)=1_S$$

تعريف (3-5. 207):

إذا كانت $f: R \rightarrow S$ تشاكل من الحلقة R إلى الحلقة S فإن نـــواة التشاكل (ker f) هي المجموعة :

$$\text{Ker } f=\{ a\in R : f(a)= 0_S\}$$

نظرية (3-5. 208):

إذا كانت $f:R\rightarrow S$ تشاكل من الحلقة R إلى الحلقة S فإن $\ker f= \{a\in R : f(a)= 0_S\}$ مثالية في R

البرهان:

من الملاحظة (2-6. 142) نعلم أن ker f هي زمرة جزئية من الزمـــرة (R ,+).

لإثبات أن ker f مثالية , نفرض أن

$a \in R$, $x \in \text{Ker } f$

$f(xa)=f(x)f(a)=0.f(a)=0$

$f(ax)= f(a)f(x)=f(a).0=0$

وهذا يعني أن $ax , xa \in \ker f$

إذن ker f مثالية في R

مثال (3-5. 209) :

في المثال (3-5. 205) حيث $f:R \to s$ تشاكل من الحلقة R إلى الحلقة S

فإن نواة التشاكل هي :

$\text{Ker } f=R$

مثال (3-5. 210) :

إذا كانت R تمثل ، حلقة وأن الدالة $f:R \to R$ معرفة كالأتي:

$f(a) =a \quad \forall \ a\in R$

i – أثبت أن f هو تشاكل من R إلى R .

ii -جد نواة التشاكل .

الحل:

i -

$$f(a+b)= a+b \quad \forall \ a,b \in R$$
$$= f(a)+f(b)$$

وكذلك

$$f(ab)=ab \quad \forall \ a,b\in R$$
$$= f(a)f(b)$$

إذن f هو تشاكل

ii – نواة هذا التشاكل هي :

$$\text{Ker } f = \{0\}$$

نظرية (3-5. 211):

إذا كانت الدالة $f: R \to S$ تشاكل من الحلقة R إلى الحلقة S فإنه:

i– إذا كانت H حلقة جزئية من R فإن $f(H)$ حلقة جزئية من S.

ii– إذا كانت M حلقة جزئية من S فإن $f^{-1}(M)$ حلقة جزئية من R.

البرهان:

i–

$f(H) = \{f(h) : h \in H\}$ حيث

فإن

$$f(x) , f(y) \in f(H) \text{ لكل } x.y \in H$$

حيث إن H: حلقة جزئية ، فإن

$$x-y , xy \in H$$

وبما أن f هو تشاكل ، فإن

$$f(x-y) = f(x) - f(y)$$
$$f(xy) = f(x).\ f(y)$$

ولكن

$$f(x-y) \in f(H) , f(x,y) \in f(H)$$

لهذا فإن

$$f(x)-f(y) , f(x)f(y) \in f(H)$$

وهذا يثبت أن $f(H)$ حلقة جزئية .

ii- نعلم أن

$$f^{-1}(M)=\{m \in R,\ f(m) \in M\}$$

لكل

$$x,y \in f^{-1}(M)$$

فإن

$$f(x), f(y) \in M$$

ولكن M حلقة جزئية , لهذا فإن

$$f(x).f(y),\ f(x)-f(y) \in M$$

ولكن

$$f(x)-f(y)=f(x-y)$$
$$f(x).f(y)=f(xy)$$

إذن

$$f(x-y),\ f(xy) \in M$$

وهذا يعني أن

$$x-y,\ xy \in f^{-1}(M)$$

وهذا يثبت أن $f^{-1}(M)$ حلقة جزئية من R.

نظرية (3-5. 212):
إذا كانت f تشاكل من الحلقة R إلى الحلقة S فإن $\ker f=\{0\}$ إذا وفقط إذا كان: f تشاكل متباين .

البرهان:

i -إذا كان f تشاكل متباين

نفرض أن $x \in \ker f$ لهذا فإن

$$f(x)=0_S=f(0_R)$$

وحيث إن f متباينة فإن $x=0$

إذن $\ker f = \{0\}$

ii – الآن نثبت العكس أي إذا كان $\ker f = \{0\}$

فإن f متباينة .

نفرض أن x,y حيث إن

$$f(x)= f(y) \Rightarrow f(x)-f(y) =0$$

لأن f تشاكل

$$\Rightarrow f(x-y)=0$$

وهذا يعني أن $x-y \in \ker f$

ولكن $\ker f= \{0\}$, وهذا يعني أن $x-y=0$ أي أن $x=y$

إذن f تشاكل متباين .

نظرية (3-5.213):

إذا كانت I مثالية في الحلقة R , فإن هناك تشاكل شامل $f:R \to R\backslash I$

بحيث إن $\mathrm{Ker}\, f =I$

البرهان:

نعرف $f:R \to R\backslash I$ كالآتي:

$$f(a) =a+I \quad \forall \ a \in R$$

لكل $x,y \in R$ إذا كان $x=y$ فإن

$$y+I =x+I$$
$$\Rightarrow f(y) =f(x)$$

لهذا فإن f معرفة تعريفًا جيدًا .

لكل $x,y \in R$ فإن

$$\begin{aligned} f(x+y) &= (x+y)+I \\ &= (x+I)+(y+I) \\ &= f(x)+f(y) \end{aligned}$$

وكذلك

$$\begin{aligned} f(xy) &= xy+I \\ &= (x+I)(y+I) \\ &= f(x)f(y) \end{aligned}$$

ولهذا فإن f هي تشاكل من الحلقة R إلى الحلقة $R\backslash I$.

لكل $a+I \in R\backslash I$ فإن $a \in R$ تحقق $f(a)=a+I$

وهذا يثبت أن f تشاكل شامل .

بقى أن نلاحظ أن

$$\begin{aligned} \ker f &= \{ a \in R : f(a)=0+I \} \\ &= \{ a \in R : a+I = I \} \end{aligned}$$

[6-3] تمارين عامة

1- أثبت أن المجموعة $Z_4=\{[0],[1],[2],[3]\}$ مع عمليتي الجمـــع والــضرب بمقياس "4" تكون حلقة إبدالية $(Z_4 ,\oplus , \otimes)$ ذات عنصر محايد .

لتكن المجموعة $G=\{0,a,b\}$ و العمليتان $\oplus$ $\otimes$, معرفتان على G كالأتي :

$\oplus$	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

$\otimes$	0	a	b
0	0	0	0
a	0	a	b
b	0	a	b

اثبت أن $(G , \oplus ,\otimes)$ يمثل حلقة غير إبدالية و لاتحتوي على محايد .

3- اعتبر $(H , + , .)$ حيث $H=\{ a+b\sqrt{2} \ : a,b \in Q\}$ و العمليتان " . " , " + " هما عمليتان الضرب و الجمع الأعتيادتين على الأعداد :

i - أثبت أن $(H , + , .)$ يمثل حلقة .

ii - أثبت أنها حلقة إبدالية .

iii - هل $(H , + , .)$ تمثل حلقة جزئية من $(R , + , .)$ ؟ ولماذا؟

Iv - هل أنها حلقة ذات عنصر محايد ؟

4- إذا كانت $p(x)$ تمثل مجموعة كل المجموعات الجزئية للمجموعــة x غيــر الخالية .

أولاً : أثبت أن $(p(x) , \Delta , \cap)$ يمثل حلقة إبدالية ذات عنصر محايد ,

حيث العملية Δ تمثل الفرق المتماثل ومعرفة كالأتي :

$$A \Delta B=(A\cup B) \setminus (A\cap B) =(AB)\cup (BA)$$

ثانيًا : هل توجد فيها عناصر جامدة ؟

ثالثًا : هل توجد فيها عناصر عديمة لاقوى ؟

رابعًا : هل توجد فيها قواسم للصفر ؟

خامسًا : هل إنها حلقة كاملة ؟

سادسًا : ماهي نواة الحلقة $\ker f$؟

سابعًا : هل يوجد مميز للحلقة ؟

5- اعتبر $(2Z , + , .)$ حيث " . " , " + " عمليتا الضرب والجمع الاعتياديان على مجموعة الأعداد لاصحيحة ,

i- هل أن $(2Z , + , .)$ يمثل حلقة ؟

ii- هل هي حلقة إبدالية وتحتوي على محايد ؟

iii- هل أنها تمثل حلقة جزئية من الحلقة $(Z , + , .)$؟

iv- هل يوجد مميز للحلقة ؟

6- بين أن النظام $(Z_6 , \oplus , \otimes)$ يمثل حلقة إبدالية ذات عنصر محايد , هل أنها حلقة كاملة ؟ ولماذا ؟ .

هل يوجد مميز للحلقة ؟ ما هو ؟

7- إذا كانت لمجموعــة $G=\{ e , d, c ,d \}$ و أن العمليــات $\oplus$, $\otimes$ معرفــة كالأتي :

$\oplus$	e	d	c	d
e	e	d	c	b
d	d	e	b	c
c	c	b	e	d
b	b	c	d	e

$\otimes$	e	d	c	b
e	e	e	e	e
d	e	d	e	d
c	e	e	c	c
b	e	d	c	b

i- أثبت أن $(G , \oplus , \otimes)$ يمثل حلقة .

ii- هل إنها حلقة إبدالية ؟ هل لها محايد ؟

iii- هل يمكن إيجاد حلقة جزئية منها ؟

8- إذا كانت S_1 , S_2 تمثل حلقتين جزئيتين من الحلقة R,

أثبت أن $S_1 \cap S_2$ حلقة جزئية من R.

بين بمثال ان $S_1 \cup S_2$ ليس حلقة جزئية من R

9- من السؤال الخامس $(2Z , +, .)$ حيث " . " , " + " العمليات الاعتيادية علــى الأعداد , أثبت أن $(2Z , + , .)$ مثالية في الحلقة $(Z , + , .)$.

10- إذا كانت المجموعة $I= \{[0],[2],[4],[6]\}$ مثالية في الحـــلقة $(Z_8 , \oplus , \otimes)$ و أن $Z_8\backslash I = \{I ; 1 \oplus I\}$

i- كون جدولي الجمع و الضرب بالنسبة لعناصر $Z_8\backslash I$.

ii- هل أن $Z_8\backslash I$ تكون حلقة إبدالية .

iii- ما هو العنصر المحايد بالنسبة لعملية الضرب في $Z_8\backslash I$

11- بين أي من الحلقات التالية حلقة اقليدية :

$$(Z_8 , \oplus , \otimes) , (2Z , + . .) , (R, + , .)$$

12- إذا كانت $(Z \quad + , .)$ تمثل حلقة إبدالية , وكان $0 \neq a \in Z$ فأثبت أن المجموعة

$aZ=\{ax : x \in Z\}$ مثالية في Z.

13- لتكن $(R , + , .)$ حلقة إبدالية و لتكن المجموعة $G=\{x \in R : x^n =0\}$ لبعض الأعداد الصحيحة n , برهن أن G مثالية في R .

14- بين أن $(Z , +, .)$ هي حلقة جزئية من الحلقة $(Q , + , .)$ ولكنهــا ليــست مثالية .

15- لتكن V مجموعة معرفة كما يلي:

$$V= \{ (v_1,v_2,v_3,v_4): v_1, v_2 ,v_3 ,v_4 \in R\}$$

ولنعرف عملية الجمع وعملية الضرب كما يلي:

$(v_1,v_2,v_3,v_4)+(u_1,u_2,u_3,u_4)=(v_1+u_1, v_2+u_2, v_3+u_3, v_4+u_4)$

$(v_1,v_2,v_3,v_4).(u_1,u_2,u_3,u_4) = v_1u_1+v_2u_3, v_1u_2+v_2u_4, v_3u_1+v_4u_3, v_3u_2+v_4u_4)$

$\forall \quad (v_1,v_2,v_3,v_4), (u_1,u_2,u_3,u_4) \quad \in R$

i- أثبت أن $(V,+,.)$ حلقة .

ii- هل $(V,+,.)$ حلقة إبدالية ؟

iii- ما هو العنصر المحايد بالنسبة لعملية الضرب ؟

iv- ما هو مميز هذه الحلقة (char V) ؟

v- هل أن V تكثل حلقة كاملة ؟

vi- هل توجد عناصر جامدة في الحلقة ؟

16- لتكن $(R,+,.)$ حلقة تبديلية ، ذات عنصر محايد وكان $a\in R$ برهن أن $(a)=\{r.a : r \in R\}$ مثالية في R وتحتوي على a.

17- ليكن كل من

$$f(x) = 2x^0 + x^1 + 3x^3$$
$$g(x) = 3x^0 + 2x^1$$

متعدد الحدود في $Q[x]$, جد $f(x)\,g(x)$, ماهي درجته ؟

18- أثبت أن النظام $(Z_5, \oplus, \otimes)$, يمثل حلقة غير منتهية ، ما هو مميز هذه الحلقة ؟ حيث العمليات $\oplus$, $\otimes$ هي عملية الجمع و الضرب الاعتيادية على المجموعة بمقياس " 5 ".

19- لتكن $(R\,,+\,,\,.\,)$ حلقة إبدالية ذات عنصر محايـد , وأن$(R[x]\,,+,\,.\,)$ حلقة متعدد الحدود للحلقة R , فأثبت أن النظام $(S\,,+\,,\,.\,)$ يمثل حلقـة جزئية من الحلقة $(R[x]\,,+\,,\,.)$ حيث إن :

$$S=\{\, ax^0 \in R[x] : a \in R\}$$

20- إذا كانت المجموعة $I=\{0,2,4\}$ مثالية في $(Z_6\,,\oplus\,,\otimes)$ و أن

$$Z\backslash I=\{\, I\,,\, 1\oplus I\}$$

إذا عرفت الدالة

$$f: Z_6 \rightarrow Z_6/I$$

كالأتي :

$$f(a)=[a]\oplus I\,,\ \forall\ [a]\in Z_6$$

فأثبت :

أولاً : أن f تمثل تشاكل .

ثانيًا : هل أن f تشاكل شامل (اميبومورفيزم) ؟

ثالثًا : هل تمثل f اندومورفيزم (تشاكل ذاتي) ؟

رابعًا : هل تمثل f ايزومورفيزم (تشاكل تقابلي) ؟

21- من المثال (3-5. 210)

الدالة $f: R \rightarrow R$ تمثل تشاكل ومعرفة كالأتي

$$f(a)=a\,,\ \forall\ a\in R$$

i- هل أن f تمثل تشاكل متباين ؟

ii- هل أن f تمثل تشاكل شامل ؟

iii- هل أن f تمثل تشاكل تقابلي ؟

iv- هل أن f تمثل تشاكل ذاتي ؟

v- هل أن f تمثل تشاكل تقابلي ذاتي ؟

22- إذا كانت $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} , a \in R \right\}$ = M وأنه

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} , a,b,c,d \in R \right\}$$

فأثبت ما يلي:

أولاً : أن كل من M , S حلقات تحت عمليتي الجمع والضرب للمصفوفات

ثانيًا : هل هي حلقات إبدالية ؟

ثالثًا : هل يوجد محايد لكل حلقة ؟

رابعًا : إذا كانت الدالة $f : M \rightarrow S$

معرفة كالآتي :

$$f \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

فأثبت أن f تمثل تشاكل

هل f تمثل تشاكل تقابلي؟

23- إذا كانت الدالة $f : R \rightarrow S$ تشاكل شامل من الحلقة R إلى الحلقة S وكانت المجموعة N مثالية من R فأثبت أن f(N) مثالية من S .

المراجع

المراجع العربية:

1- د. عادل غسان ، د. باسل عطا عبد الحميد ، د. محمد صالح بابان : مقدمة في نظرية الزمر ، وزارة التعليم العالي والبحث العلمي العراقي (1982).

2- أ. كوروش : الجبر العالي (مترجم عن الروسية) , دار مير للطباعة والنشر الطبعة الثالثة (1984).

المراجع الإنكليزية :

3- Gilbert , W.j.; Modern algebra with Applications , John Wiley and Sons (1976).

4- Green , J.A .; Sets and Groups , ELBS ed (1977).

5- Hall,F.M.;An introduction to Abstract Algebra,Combridge University Press 1969.

6- Herstin , I . N. ; Abstract Algebra , Macmillan publihing Company, (1975) .

7- Lederman , w . ; Indroduction To Groubs Theory , Longman (1973).

8- Rotmen , J.; The Theory of Groups , An Introduction , 2nd ed Allyn and Bacon , (1973).

9- Sharpe , D. ; Rings and Factorization , Combridge University Press 1987.

10- Wielandt , H . ; Finite Permutation Groups , Academic Press , New york (1964) .

قائمة المصطلحات

A

abelian	تبديلة (أبلية)
abelian group	زمرة تبديلية
abstract algebra	جبر مجرد
addition	جمع
additive identity	محايد جمعي
additive inverse	نظير جمعي
algebraic	جبري
algebraic system	نظام جبري
alternating group	زمرة متناوبة
annihilator	معدم
associative	تجميعي
automorphism	تشاكل تقابلي (ذاتي)

B

bijective	متباينة
binary operation	عملية ثنائية

C

center	مركز
commutative	ابدالي
composite function	دالة تركيبية
corollary	نتيجة
cosset	مجموعة مشاركة
cycle	دورة
cyclic group	زمرة دائرية (دورية)

D

definition	تعريف
degree	درجة
direct product	ضرب مباشر
direct sum	جمع مباشر
division Ring	حلقة قسمة
divisor	قاسم

E

element	عنصر
emptyset	مجموعة خالية
equal	يساوي
equation	معادلة
equivalence classes	صفوف التكافؤ
equivalence relation	علاقة التكافؤ
even	زوجي
even number	عدد زوجي

even permutation	تبديلية زوجية
example	مثال
exercises	تمارين
exist	موجود

F

factor	عامل
family of sets	عائلة المجموعات
finite	منته
finite set	مجموعة منتهية
function	دالة

G

general	عام
general solution	حل عام
generator	مولد
group	زمرة
group theory	نظرية الزمرة

H

homeomorphism	تشاكل (هومومورفيزم)

I

ideal	مثالية
idempotent	جامد
identity	محايد
identity element	عنصر محايد
image	صورة

inclusion	احتواء
independent variable	متغير مستقل
indeterminate	غير محدد
index	دليل
indirect	غير مباشر
infinite set	مجموعة غير منتهية
injective	متباين
integer number	عدد صحيح
integral domain	نطاق كامل
interval	فترة
inverse	نظير (معكوس)
inverse element	العنصر النظير
inverse function	الدالة العكسية
irrational number	عدد غير نسبي
isomorphism	تشاكل تقابلي (هومورفيزم تقابل) أو(ايزومورفزم)

K

kernel	نواة
kernel of homeomorphism	نواة الهومورفيزم

L

left coset	مصاحبة يسرى
left distributive low	قانون التوزيع من اليسار
left ideal	مثالية يسرى
linear	خطي
linear independent	مستقل خطيًا

M

mapping	تطبيق (راسم)
mathematics	علم الرياضيات
matrix	مصفوفة
maximal ideal	مثالية عظمى
maximum	الأعلى
minimum	الأدنى
minimal ideal	مثالية صغرى
manic polynomial	متعدد حدود أحادي
multiplication	عملية الضرب
multiplicative inverse	نظير ضربي

N

natural number	عدد طبيعي
negative number	عدد سالب
nilpotent	معدوم القوى
nilpotent element	عنصر معدوم القوى
normal	قياس (سوي)
normal subgroup	زمرة جزئية قياسية (سوية)
normal space	الفضاء القياسي
number	عدد

O

odd	فردي
odd number	عدد فردي
one-to-one	تقابل
onto	شامل

omebomorphism	تشاكل شامل
operation	عملية
order	رتبة
order of group	رتبة الزمرة

P

permutation	تبادل
permutation group	زمرة التبادل
polynomial	حدودية
positive	موجب
positive number	عدد موجب
product	ضرب (جداء)
proof	برهان
proper subset	مجموعة جزئية فعلية
prove	يبرهن

Q

quotient group	زمرة القسمة (كسرية)
quotient ring	حلقة القسمة

R

rational number	عدد نسبي (قياسي)
real number	عدد حقيقي
relation	علاقة
ring	حلقة

S

semigroup	نصف زمرة (شبه زمرة)
set of numbers	مجموعة الأعداد
simple group	زمرة بسيطة
subgroup	زمرة جزئية
subring	حلقة جزئية
subset	مجموعة جزئية
surjective	شامل
symmetric group	زمرة التماثل
system	نظام

T

term	حد
theorem	نظرية (مبرهنة)
trival subqroup	زمرة جزئية تافهة

U

unbounded set	مجموعة غير محدودة
union	اتحاد
unique	وحيد

Z

zero divisors	قواسم للصفر
zero element	عنصر صفري

تنفيذ وطباعة

ARAB NILE GROUP

Print, Pub., Dist.

P.O. Box: 4051. 7th District-Nasr City-11727 Cairo-Egypt

Tel: +202 26717134-5 Fax: +202 26717135

E-mail: sales@arabnilegroup.com

مجموعة النيل العربية

"نشر - طباعة - توزيع"

ص. ب: 4051 الحي السابع/ م. نصر 11727 القاهرة/ ج.م.ع.

هاتف: 5-26717134 202+ فاكس: 26717135 202+

E-mail: info@arabnilegroup.com

www.arabnilegroup.com

هدفنا من تألـيف هذا الكتاب هو تزويد الطـالب (القارئ) بصورة عـامة بالمادة العلمـية الأساسية في الجبر المجـرد ، نأمـل أن نكون قد أضفنا إلى المكتبة العربية ما يساعد على الفهم والاستيعاب للرياضيات بلغتنا العربية .

جامعة سرت

الرقم الدولي ردمك ISBN 978 - 9959 - 891 - 06 - 8
رقم الإيداع : 994 دار الكتب الوطنية - بنغازي