وزارة التعليم العالي والبحث العلمي
جامعة البصرة
كلية التربية للعلوم الصرفة
قسم الرياضيات

جبر الزمر وجبر الحلقات

مقدم إلى قسم الرياضيات كلية التربية للعلوم الصرفة جامعة البصرة

وهو جزء من متطلبات نيل شهادة بكالوريوس علوم الرياضيات

من قبل الطالبة

حنين

إشراف

م. جاسم محمد جواد

2025 - 2024

المحتويات

الفصل الأول

نظرية الزمر

1 - 1 مفاهيم أولية

تعريف 1 - 1 (العملية الثنائية)

لتكن G مجموعة غير خالية ، نطلق على التطبيق $* : G \to G \times G$ بأنه عملية ثنائية على G.

ملاحظة

اذا كانت $*$ عملية ثنائية على مجموعة G سنكتب العلاقة بين عناصرها بالشكل $a * b$ بدل من $*(a, b)$ لغرض السهولة.

مثال 1 - 1

عملية الجمع الاعتيادية على مجموعة الاعداد الصحيحة والطبيعية والنسبية والحقيقية تمثل عملية ثنائية وكذلك عملية الضرب الاعتيادي.

مثال 1 - 2

لتكن $X = \{1, 2, 3\}$ ، العملية $*$ معرفة على المجموعة X بالشكل

$*$	1	2	3
1	1	2	3
2	2	2	1
3	3	1	3

نلاحظ ان $*$ تمثل عملية ثنائية.

تعريف 1 - 2 (الانغلاق)

لتكن $*$ عملية ثنائية على المجموعة X ، المجموعة الجزئية A من G تسمى مغلقة تحت العملية $*$ اذا كان $a * b \in A$ لكل عنصرين $a, b \in A$.

مثال 1 - 3

نحن نعلم ان $+$ عملية الجمع الاعتيادي على مجموعة الاعداد الحقيقية ، نلاحظ ان $+$ عملية ثنائية مغلقة على مجموعة الاعداد الصحيحة لأن

$$a + b \in \mathbb{Z}, \quad \forall a, b \in \mathbb{Z}$$

تعريف 1 - 3 (النظام الرياضي)

هو مجموعة غير خالية G مع عملية ثنائية واحدة او اكثر معرفة عليه. ويرمز له بالرمز المرتب $(G,*,\#)$ او $(G,*)$.

تعريف 1 - 4 (العملية التجميعية)

ليكن $(G,*)$ نظاماً رياضياً مع $*$ عملية ثنائية معرفة عليه ، يقال ان العملية $*$ تجميعية اذا حققت الشرط

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

مثال 1 - 4

لتكن $X=\{1,2,3\}$ ، العملية $*$ معرفة على المجموعة X بالشكل

$*$	1	2	3
1	1	2	3
2	2	1	2
3	3	3	3

نلاحظ ان $*$ تمثل عملية تجميعية.

مثال 1 - 5

لتكن $*$ عملية معرفة على $\mathbb{Z}$ كما يأتي : $a*b=a+b-1$ لكل عنصرين $a,b\in\mathbb{Z}$ ، فإن $*$ عملية تجميعية.

تعريف 1 - 5 (العنصر المحايد)

ليكن $(G,*)$ نظاماً رياضياً ، يقال ان النظام الرياضي $(G,*)$ يمتلك عنصراً محايداً بالنسبة للعملية الثنائية $*$ اذا وجد عنصر $e\in G$ بحيث ان

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

مبرهنة 1 - 1

لتكن $(G,*)$ نظاماً رياضياً بعنصر محايد فإن المحايد وحيد.

البرهان

لتكن e, e' عنصران محايدان بالنسبة للعملية $*$ اذن

$e * e' = e'$ لان e عنصر محايد.

$e * e' = e'$ لان e' عنصر محايد.

اذن $e = e'$. □

تعريف 1 - 6 (monoid)

لتكن $(G, *)$ شبه زمرة ، اذا كانت تمتلك عنصر محايد فإنها تسمى (monoid).

تعريف 1 - 7 (المعكوس)

لتكن $(G, *)$ شبه زمرة بمحايد اذا كان $a \in G$ يحقق الخاصية : $a' * a = a * a' = e$ حيث ان $a' \in G$ ، فإن العنصر a' يسمى معكوس العنصر a بالنسبة للعملية $*$ ويرمز له بالرمز a^{-1}.

ملاحظة

لتكن $(G, *)$ شبه زمرة بعنصر محايد e فأن $e^{-1} = e$

مبرهنة 1 - 2

لتكن $(G, *)$ شبه زمرة بعنصر محايد وليكن $a \in G$ وله معكوس في G فأن المعكوس وحيد.

تعريف 1 - 8 (العملية الابدالية)

ليكن $(G, *)$ نظاماً رياضياً مع $*$ عملية ثنائية معرفة عليه ، يقال ان العملية $*$ ابدالية اذا حققت الشرط

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

مثال 1 - 6

عمليتي الجمع والضرب الاعتياديتين على مجموعة الاعداد الحقيقية والصحيحة والنسبية $\mathbb{Q}, \mathbb{Z}, \mathbb{R}$ تمثل عمليات ثنائية ابدالية.

1 - 2 تعريف الزمرة وبعض خصائصها

تعريف 1 - 9 (الزمرة)

لتكن $(G, *)$ شبه زمرة بعنصر محايد فأن G تسمى زمرة Group اذا كان كل عنصر فيها له معكوس بالنسبة للعملية الثنائية $*$. او نقول ان $(G, *)$ زمرة اذا تحققت الشروط التالية

$\boxed{1}$ مغلقة بالنسبة للعملية $*$ اي : $a * b \in G, \forall a, b \in G$.

$\boxed{2}$ العملية $*$ تجميعية : $a * (b * c) = (a * b) * c, \forall a, b, c \in G$.

$\boxed{3}$ G تمتلك عنصر محايد مثل e : $a * e = e * a = a, \forall a \in G$.

$\boxed{4}$ كل عنصر $a \in G$ يمتلك معكوس : $\forall a \in G, \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$.

مثال 1 - 7

كل الانظمة الرياضية التالية تمثل زمرة

$$(\mathbb{Q} - \{0\}, \cdot), \quad (\mathbb{R} - \{0\}, \cdot), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{Z}, +)$$

تعريف 1 - 10 (الزمرة الابدالية)

الزمرة $(G, *)$ تسمى زمرة ابدالية اذا كانت العملية $*$ عملية ثنائية ابدالية.

مثال 1 - 8

كل الانظمة الرياضية التالية تمثل زمرة ابدالية

$$(\mathbb{R} - \{0\}, \cdot), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{Z}, +)$$

تعريف 1 - 11 (الزمرة المنتهية وغير المنتهية)

الزمرة $(G, *)$ تسمى زمرة منتهية اذا كانت المجموعة G منتهية. عدا ذلك تسمى الزمرة $(G, *)$ زمرة غير منتهية.

تعريف 1 - 12 (رتبة الزمرة)

لتكن $(G, *)$ زمرة منتهية ، نطلق على عدد عناصر المجموعة G اسم رتبة الزمرة ويرمز له بالرمز $O(G)$ اما اذا كانت المجموعة غير منتهية فتكون رتبتها غير منتهية ايضاً.

تعريف 1 - 13 (قوى العنصر)

لتكن $(G,*)$ زمرة وليكن n عدد موجب فأن $a^n = \underbrace{a * a * \cdots * a}_{\text{من المرات } n}$

مبرهنة 1 - 3

لتكن $(G,*)$ زمرة وليكن $n, m \in \mathbb{Z}$ فإن

$\boxed{1}$ $e^n = e$

$\boxed{2}$ $a^0 = e, \forall a \in G$

$\boxed{3}$ $(a^m)^n = a^{mn}$

$\boxed{4}$ $a^m * a^n = a^{m+n}$

$\boxed{5}$ $a^{-m} = (a^{-1})^m$

تعريف 1 - 14 (الزمرة الدوارة)

$(G,*)$ تسمى زمرة دوارة اذا وجد عنصر فيها $a \in G$ بحيث ان اي عنصر اخر في الزمرة $b \in G$ يمكن كتابته بالصيغة $b = a^k, k \in \mathbb{Z}$ ، يطلق على العنصر a بالعنصر المولد للزمرة. او يقال ان الزمرة G مولدة بواسطة العنصر a ونكتب $G = \langle a \rangle$ او $G = (a)$

مثال 1 - 9

لتكن $G = \{1, -1, i, -i\}$ حيث ان $i = \sqrt{-1}$ ، فإن $(G, \cdot)$ تمثل زمرة دوارة.

مبرهنة 1 - 4

الزمرة $(G,*)$ تكون ابدالية اذا وفقط اذا كان $(a * b)^{-1} = a^{-1} * b^{-1}$.

1 - 3 زمرة التناظر (التباديل)

تعريف 1 - 15 (زمرة التناظر)

لتكن X مجموعة غير خالية ، الدالة $f : X \to X$ تسمى تباديل على X اذا كانت f تقابل على X ، مجموعة كل التباديل على X يرمز لها بالرمز $\operatorname{sym} X$ حيث ان

$$\operatorname{sym} X = \{f \mid f : X \to X \text{ bijective}\}$$

مثال 1 - 10

لتكن $X = \{1,2,3\}$ و $f \in S_3$ معرفة كالآتي

$$f(1) = 1, f(2) = 3, f(3) = 2$$

نستطيع كتابة عناصر الدالة f بالشكل التالي

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

ترتيب الاعمدة هنا ليس مهماً فنستطيع كتابة الدالة كما يأتي

$$\begin{pmatrix} 2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{او} \quad \begin{pmatrix} 2 & 1 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

ملاحظة

طريقة تعريف دالة التركيب على عناصر $f, g \in S_n$

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix},$$

فأن دالة التركيب تكتب بالشكل

$$f \circ g = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(g(1)) & f(g(2)) & \cdots & f(g(2)) \end{pmatrix},$$

وتكتب الدالة المحايدة بالشكل

$$(1) = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

وتكتب دالة المعكوس بالشكل

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix},$$

تعريف 1 - 16

لتكن $f \in S_n$ بحيث ان $x_1, x_2, \ldots, x_n$ فإذا كان $f(x_i) = x_{i+1}$ لكل $1 \leq i \leq n-1$ وأن

$f(x_n) = x_1$ اذن نستطيع كتابة f بشكل دورة $(x_1\ x_2\ \cdots\ x_n)$ وتسمى دورة ذات طول n

مثال 1 - 11

لنفرض ان $f, g \in S_5$ حيث ان

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

اذن $(1\ 2\ 3\ 4) = f$ وهذا يعني انها دورة ذات طول 4 ، اما $(2\ 3) = g$ وهذا يعني انها دورة ذات طول 2.

تعريف 1 - 17

اي دورة طولها 2 فقط تسمى مناقلة.

ممهدة 1 - 5

معكوس اي مناقلة هي المناقلة نفسها.

مثال: $(2\ 3)^{-1} = (2\ 3)$

ممهدة 1 - 6

لتكن $(x_1\ x_2\ \cdots\ x_n)$ دورة ذات طول n فإن

$$(x_1\ x_2\ \cdots\ x_n)^{-1} == (x_1\ x_{n-1}\ x_{n-2}\ \cdots\ x_2)$$

مثال 1 - 12

معكوس الدورة $(4\ 5\ 6\ 7)$ الدورة $(4\ 7\ 6\ 5)$.

ملاحظة

نكتب العنصر المحايد في الزمرة S_n بشكل دورة ذات طول 1، ويرمز له بالرمز (1)

مبرهنة 1 - 7

كل دورة $(x_1\ x_2\ \cdots\ x_n)$ ممكن كتابتها على صورة حاصل ضرب مناقلات وهذا التعبير غير وحيد

$$(x_1\ x_2\ \cdots\ x_n) = (x_1\ x_n)(x_2\ x_n)\cdots(x_{n-1}\ x_n)$$

مثال 1 - 13

في الزمرة S_8

$$(3\ 4\ 5\ 6\ 7\ 8) = (3\ 8)(3\ 7)(3\ 6)(3\ 5)(3\ 4)$$

$$(1\ 3\ 2)(5\ 8\ 6\ 7) = (1\ 2)(1\ 3)(5\ 7)(5\ 6)(5\ 8)$$

نتيجة 1 - 8

كل تبديل نستطيع كتابته على شكل حاصل ضرب مناقلات

تعريف 1 - 18

التبديل f يسمى تبديل زوجي (فردي) اذا كان يكتب على شكل حاصل ضرب عدد زوجي (فردي) من المناقلات

مثال 1 - 14

$(1\ 2)$ تبديل فردي.

$(1\ 2\ 3) = (1\ 3)(1\ 2)$ تبديل زوجي.

ممهدة 1 - 9

الدورة (التباديل) ذات الطول n تكون تبديل فردي اذا كان الطول زوجي والعكس بالعكس.

مثال 1 - 15

$(1\ 2)$ دورة ذات طول 2 اذن تبديل فردي

$(1\ 2\ 3)$ دورة ذات طول 3 اذن تبديل زوجي.

مبرهنة 1 - 10

عند ضرب تبديلين زوجيين او فرديين فالناتج يكون تبديل زوجي ، اما عند ضرب تبديل فردي بتديل زوجي او العكس فالناتج تبديل فردي.

مثال 1 - 16

حاصل الضرب $(1\ 2\ 3)(4\ 5)(7\ 8\ 9)$ ، التبديل الاول والثالث زوجيان اما التبديل الثاني فردي ، اذن الناتج يكون تبديل زوجي.

ممهدة 1 - 11

$(S_n, \circ)$ ليست زمرة ابدالية لكل $n \geq 3$.

البرهان

لنأخذ $(1\ 2), (2\ 3) \in S_n$ نلاحظ ان ، $(1\ 2)(2\ 3) = (1\ 2\ 3)$ بينما $(2\ 3)(1\ 2) = (1\ 3\ 2)$
لذلك فإن $(2\ 3)(1\ 2) \neq (1\ 2)(2\ 3)$ بالتالي فإن $(S_n, \circ)$ ليست زمرة ابدالية. $\square$

تعريف 1 - 19

مجموعة كل التبديلات الزوجية في الزمرة S_n مع عملية التركيب $\circ$ تسمى الزمرة المتناوبة ويرمز لها بالرمز $(A_n, \circ)$ ورتبتها $O(A_n) = \dfrac{n!}{2}$.

1 - 4 زمرة الاعداد الصحيحة مقياس n

تعريف 1 - 20

ليكن $n \in \mathbb{Z}_+$ نعرف العلاقة $\equiv_n$ (او قياس n) على $\mathbb{Z}$ كما يلي: $a \equiv_n b$ اذا وفقط اذا $a - b$ يقبل القسمة على n او $a - b = kn$ او $a = b + kn$

مثال: $3 \equiv 1 \bmod 2$ او $3 \equiv_2 1$

مبرهنة 1 - 12

علاقة القياس n $(\equiv_n)$ لمجموعة الاعداد الصحيحة هي علاقة تكافؤ.

ملاحظة

بما ان العلاقة $\equiv_n$ هي علاقة تكافؤ على الاعداد الصحيحة (عكسية ، متناظرة ، متعدية) اذن هي تشكل تجزئة على $\mathbb{Z}$ وتوجد صفوف تكافؤ او صفوف التكافؤ، حيث نستخدم اقل عدد موجب لتمثيل صف التكافؤ بشكل عام، اذا كان $a \in \mathbb{Z}$ فإن

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid a = x \bmod n\} \\
&= \{x \mid a - x = kn, k \in \mathbb{Z}\} \\
&= \{x \mid a = x + kn, k \in \mathbb{Z}\}
\end{aligned}$$

مبرهنة 1 - 13

الزوج المرتب $(\mathbb{Z}_n, +_n)$ يشكل زمرة ابدالية التي يطلق عليها زمرة الاعداد الصحيحة مقياس n

البرهان

$\boxed{1}$ لنبرهن ان $\mathbb{Z}_n$ مغلقة تحت العملية $+_n$ ، لنفرض ان $[a], [b] \in \mathbb{Z}_n$ نجد ان

$$[a] +_n [b] = [a + b] \in \mathbb{Z}_n$$

$\boxed{2}$ لبرهان ان $+_n$ تجميعية على $\mathbb{Z}_n$ لنفرض ان $[a], [b], [c] \in \mathbb{Z}_n$ نجد

$$\begin{aligned} [a] +_n \Big([b] +_n [c]\Big) &= [a] +_n [b + c] \\ &= [a + b + c] \\ &= [a + b] +_n [c \\ &= \Big([a] +_n [b]\Big) +_n [c] \end{aligned}$$

$\boxed{3}$ $[0] \in \mathbb{Z}_n$ هو العنصر المحايد لـــ $\mathbb{Z}_n$ لأن لكل $[a] \in \mathbb{Z}_n$

$$[a] +_n [0] = [a + 0] = [a]$$

$\boxed{4}$ ليكن $[a] \in \mathbb{Z}$ فأن $[a]^{-1} = [n - a]$ لأن

$$[a] +_n [n - a] = [a + n - a] = [n] = [0]$$

$\boxed{5}$ لبرهان خاصية الابدال لنفرض ان $[a], [b] \in \mathbb{Z}_n$ فان

$$[a] +_n [b] = [a + b] = [b + a] = [b] +_n [a]$$

ملاحظة

تكتب عناصر $\mathbb{Z}_n$ بالشكل a بدل من $[a]$ و $-a$ بدل من $[n - a]$

مبرهنة 1 - 14

الزمرة $(\mathbb{Z}_n, +_n)$ تشكل زمرة دوارة مولدة بواسطة العنصر 1.

ملاحظة

اي عنصر في $\mathbb{Z}_n$ ممكن ان يكون مولد للزمرة اذا وفقط اذا $\gcd(a, n) = 1$

ملاحظة

تعرف عملية الضرب على المجموعة $\mathbb{Z}_n$ كالآتي

$$[a] \cdot_n [b] = [a \cdot b], \forall [a], [b] \in \mathbb{Z}_n$$

مثال 1 - 17

$$5 \cdot_6 4 = 2, \quad 7 \cdot_9 2 = 5, \quad 3 \cdot_4 2 = 2$$

ملاحظة

الزوج المرتب $(\mathbb{Z}_n - \{0\}, \cdot_n)$ ربما يكون زمرة اذا كان n عدد اولي. للتوضيح اكثر $(\mathbb{Z}_4 - \{0\}, \cdot_4)$ لا تمثل زمرة لان 2 لا يملك معكوس ضربي بينما $(\mathbb{Z}_5 - \{0\}, \cdot_5)$ تمثل زمرة.

ملاحظة

العنصر a في $\mathbb{Z}_n$ يمتلك معكوس ضربي اذا وفقط اذا كان $\gcd(a, n) = 1$

1 - 5 الزمرة الجزئية

تعريف 1 - 21

لتكن $(G, *)$ زمرة و H مجموعة غير خالية جزئية من G فإن $(H, *)$ تسمى زمرة جزئية من الزمرة $(G, *)$ اذا كانت H هي زمرة كذلك ونكتب $(H, *) \leq (G, *)$

مثال 1 - 18

كل زمرة على الاقل لها زمرتان جزئيتان هما $(G, *)$ و $(\{e\}, *)$.

تعريف 1 - 22

الزمرة الجزئية $(H, *)$ تسمى زمرة جزئية فعلية من $(G, *)$ اذا كانت H هي مجموعة جزئية فعلية $H \subset G$.

تعريف 1 - 23

الزمرة الجزئية $(H, *)$ تسمى زمرة جزئية غير تافهة اذا كانت $G \neq H \neq \varnothing$.

مثال 1 - 19

$(\mathbb{R},+).(\mathbb{Z},+).(\mathbb{Q},+),(\mathbb{R}-\{0\},\cdot),(\mathbb{Q}-\{0\},\cdot)$ جميع هذه الانظمة هي زمر جزئية غير تافهة من زمرة الاعداد المركبة $(\mathbb{C},+),(\mathbb{C}-\{0\},\cdot)$ على التوالي

مبرهنة 1 - 15

لتكن $(G,*)$ زمرة و $G \subseteq H \neq \varnothing$ اذن $(H,*)$ تكون زمرة جزئية من $(G,*)$ اذا وفقط اذا حققت الشرط

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

مثال 1 - 20

$(\mathbb{Z}_e,+) \leq (\mathbb{Z},+)$

الحل

لفترض ان $a, b \in \mathbb{Z}_e$ اذن يوجد $n, m \in Z$ بحيث ان $a = 2n, b = 2m$ اذن

$$a * b^{-1} = a - b = 2n - 2m = 2\underbrace{(n-m)}_{\in\mathbb{Z}} \in \mathbb{Z}_e$$

اذن $(\mathbb{Z}_e,+) \leq (\mathbb{Z},+)$

مثال 1 - 21

وضح ان $(A_3,\circ) \leq (S_3,\circ)$

الحل

$\circ$	(1)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1)	(1 2 3)

من الجدول اعلاه نلاحظ ان $a \circ b^{-1} \in A_3$ لأي $a, b \in A_3$ اذن $(A_3,\circ) \leq (S_3,\circ)$

مثال 1 - 22

وضح ان $(A_n,\circ) \leq (S_n,\circ)$

الحل

نلاحظ ان $A_n \subseteq S_n$ و $(1) \in A_n$ اذن $A_n \neq \varnothing$ ، لنفترض ان $f, g \in A_n$ وهذا يعني كل من f, g تبديلات زوجية ، نبين ان f^{-1} تبديل زوجي ، نلاحظ ان $f \circ f^{-1} = (1)$ وهذا يعني f^{-1} تبديل زوجي وبالتالي $g \circ f^{-1}$ تبديل زوجي كذلك اي ان $g \circ f^{-1} \in A_n$ اذن $A_n \leq S_n$. $\square$

ملاحظة

كل زمرة جزئية من زمرة ابدالية تكون ابدالية.

تعريف 1 - 24

لتكن $(G, *)$ زمرة ، مجموعة كل العناصر في G التي تتبادل مع جميع عناصر G تسمى مركز الزمرة G ويرمز لها بالرمز $\operatorname{cent} G$.

$$\operatorname{cent} G = \{c \in G : x * c = c * x, \forall x \in G\}$$

مثال 1 - 23

$\operatorname{cent} S_n = (1), \quad \operatorname{cent} \mathbb{Z}_n = \mathbb{Z}_n$.

ملاحظة

$(\operatorname{cent} G, *) \leq (G, *)$.

ممهدة 1 - 16

الزمرة $(G, *)$ تكون ابدالية اذا وفقط اذا $\operatorname{cent} G = G$.

مبرهنة 1 - 17

لتكن كل من $(K, *)$ و $(H, *)$ زمرة جزئية من $(G, *)$ فإن $(K \cap H, *) \leq (G, *)$ بمعنى اخر تقاطع اي زمرتين جزئيتين هو زمرة جزئية.

البرهان

لتكن $a, b \in K \cap H$ اذن $a, b \in H$ و $a, b \in K$ ولأن كل منهما زمرة جزئية ، فإن $a * b^{-1} \in H$ و $a * b^{-1} \in G$ لذلك فإن $a * b^{-1} \in K \cap H$ وبالتالي $(K \cap H, *) \leq (G, *)$. $\square$

ملاحظة

اذا كان كل من $(K,*)$ و $(H,*)$ زمرة جزئية من $(G,*)$ فليس من الضروري ان يكـــــــــون $(K\cup H,*)\le(G,*)$ ، بمعنى آخر اتحاد اي زمرتين جزئيتين لا يعطي بالضرورة زمرة جزئية.

مبرهنة 1 - 18

لتكن كل من $(K,*)$ و $(H,*)$ زمرة جزئية من $(G,*)$ فإن $(K\cup H,*)\le(G,*)$ اذا وفقط اذا كان اما $H\subseteq K$ أو $K\subseteq H$.

تعريف 1 - 25

لتكن $(G,*)$ زمرة و $\varnothing\ne S\subseteq G$ ولتكن $(S)=\{H: S\subseteq H, (H,*)\le(G,*)\}$ تسمى $((S),*)$ زمرة جزئية مولدة بواسطة المجموعة S.

ملاحظة

الزمرة الجزئية $((S),*)$ هي اصغر زمرة تحتوي على المجموعة S.

تعريف 1 - 26

لتكن $(G,*)$ زمرة وليكن $a\in G$ فإن الزمرة الجزئية $\big((\{a\}),*\big)$ وتكتب بالصيغة $((a),*)$ وهي الزمرة الجزئية المولدة بواسطة العنصر a.

ملاحظة

1. لتكن $(G,*)$ زمرة ، اذا كان $a\in G$ يمتلك رتبة منتهية فإن $O(a)=O\Big((a)\Big)$
2. لتكن $(G,*)$ زمرة ، اذا كان $a\in G$ فإن $(a)=\{a^n: n\in\mathbb{Z}\}$.

مثال 1 - 24

جد (3) في $(\mathbb{Z},+)$

الحل

$(3)=\{3^n: n\in\mathbb{Z}\}=\{3n: n\in\mathbb{Z}\}$.

مثال 1 - 25

اوجد (2) فـــي $(\mathbb{Z}_8,+_8)$.

الحل

$(2) = \{2^n : n \in \mathbb{Z}\} = \{2n : n \in \mathbb{Z}\} = \{0, 2, 4, 6\}$.

تعريف 1 - 27

لتكن كل من $(K, *)$ و $(H, *)$ زمرة جزئية من $(G, *)$ فإن حاصل ضرب الزمرتان الجزئيتيان يعرف بالشكل $H * K = \{h * k : h \in H, k \in K\}$.

مثال 1 - 26

ليكن $H = (2)$ و $K = (3)$ زمرتان جزئيتيان من الزمرة $(\mathbb{Z}_{12}, +_{12})$ اوجد $H_{12}K$

الحل

$H = \{0, 2, 4, 6, 8, 10\}$ ، $K = \{0, 3, 6, 9\}$ اذن

$H +_{12} K = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \mathbb{Z}_{12}$

ملاحظة

لتكن كل من $(K, *)$ و $(H, *)$ زمرة جزئية من $(G, *)$ فإن حاصل ضرب الزمرتان الجزئيتيان $H * K$ ربما لا يكون زمرة جزئية من $(G, *)$.

مبرهنة 1 - 19

لتكن كل من $(K, *)$ و $(H, *)$ زمرة جزئية من $(G, *)$ فإن حاصل ضرب الزمرتان الجزئيتيان $(H * K, *)$ يكون زمرة اذا كان $H * K = K * H$.

ملاحظة

لتكن كل من $(K, *)$ و $(H, *)$ زمرة جزئية من $(G, *)$ فإن $(H \cup K, *) = (H * K, *)$.

مثال 1 - 27

لتكن $H = \{3\}$ و $K = \{4\}$ زمرتان جزئيتيان من الزمرة $(\mathbb{Z}_{12}, +_{12})$ اوجد $(H \cup K, +_{12})$

الحل

$H = \{0, 3, 6, 9\}$ ، $K = \{0, 4, 8\}$ اذن

$H \cup K = H +_{12} K = \{0, 4, 8, 3, 7, 11, 6, 10, 2, 9, 1, 5\} = \mathbb{Z}_{12}$

مبرهنة 1 - 20

لتكن $(G,*)$ زمرة ابدالية و لتكن كل من $(K,*)$ و $(H,*)$ زمرة جزئية من $(G,*)$ فإن $(H*K,*)\leq(G,*)$.

مبرهنة 1 - 21

لتكن $((a),*)$ زمرة دائرية تمتلك رتبة منتهية n فإن $(a)=\{a^0=e,a,a^2,\dots,a^{n-1}\}$.

مثال 1 - 28

اوجد $\big((1\ 2\ 3)\big)$ فـــــي $(S_3,\circ)$.

الحل

$$O\big((1\ 2\ 3)\big)=3 \Leftarrow \big((1\ 2\ 3)\big)=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$$

تعريف 1 - 28

لتكن $(H,*)$ زمرة جزئية من الزمرة $(G,*)$ وأن $a\in G$ ،تسمى المجموعة المعرفة بالشكل التالي $a*H=\{a*h : h\in G\}$ بالمجموعة المشاركة (المصاحبة) اليسارية لــ H في G ، وتسمى $H*a=\{h*a : h\in G\}$ بالمجموعة المشاركة (المصاحبة) اليمينية.

مثال 1 - 29

ليكن $H=\{0,2,4\}$ اوجد $1+_6H, 2+_6H, 3+_6H, 4+_6H, 5+_6H$

الحل

$$\begin{aligned}
1+_6H&=\{1+_60,1+_62,1+_64\}=\{1,3,5\}\\
2+_6H&=\{2+_60,2+_62,2+_64\}=\{2,4,0\}\\
3+_6H&=\{3+_60,3+_62,3+_64\}=\{3,5,1\}\\
4+_6H&=\{4+_60,4+_62,4+_64\}=\{4,0,2\}\\
5+_6H&=\{5+_60,5+_62,5+_64\}=\{5,1,3\}
\end{aligned}$$

مبرهنة 1 - 22

لتكن $(H,*)$ زمرة جزئية من الزمرة $(G,*)$ فإن

1. $a \in H \iff a * H = H$.
2. $a \in H \iff H * a = H$

البرهان

ليكن $a * H = H$ اذن $a \in G$ و $e \in H$ نحصل على $a = a * e \in a * H = H$ اذن $a \in H$.

لنفترض $a \in H$ وليكن $x \in a * H$ يوجد $h \in H$ بحيث $x = a * h$ اذن $a * H \subseteq H$ ، الآن نفترض $y \in H$ فإن $y = a * (a^{-1} * y) \in a * H$ اذن $H \subseteq a * H$ وبالتالي $a * H = H$ □

تعريف 1 - 29

لتكن $(H, *)$ زمرة جزئية من الزمرة $(G, *)$ ، يسمى عدد كل من المجموعات المشتركة اليمنى او اليسرى بدليل الزمرة الجزئية H في G ويرمز له بالرمز $[G : H]$.

مثال 1 - 30

$[A_n : S_n] = 2$.

مبرهنة 1 - 23 (مبرهنة لاكرانج)

لتكن $(G, *)$ زمرة منتهية ، فإن كل من رتبة ودليل اي زمرة جزئية H منها تقسم رتبتها $O(G)$.

البرهان

بما ان $(G, *)$ زمرة منتهية و $(H, *)$ زمرة جزئية منها ، اذن مجموعة كل المجموعات المشاركة تشكل تجزئة للزمرة G وكذلك يوجد عدد منتهي من المجموعات المشاركة المختلفة كالآتي $H, a_1 * H, a_2 * H, \ldots, a_k * H \Leftarrow G = H \cup a_1 * H \cup a_2 * H \cup \cdots \cup a_k * H$ اذن $O(G) = O(H) + O(a_1 * H) + O(a_2 * H) + \cdots + O(a_k * H)$ ولكن يوجد تقابل بين اي اثنين من المجموعات المشاركة المختلفة لذلك $O(G) = \underbrace{O(H) + O(H) + \cdots + O(h)}_{k \text{ من المرات}}$

ومنه نحصل على $O(G) = k \cdot O(H)$ بالتالي $O(G) = [G : H]O(H)$. □

ملاحظة

عكس مبرهنة لاكرانج ربما لا يكون صحيح دائماً لأي زمرة منتهية (لأي قاسم من قواسم رتبة الزمرة المنتهية توجد هنالك زمرة جزئية رتبتها ذلك القاسم).

مثال 1 - 31

الزمرة A_4 رتبتها 12 لكن لا توجد زمرة جزئية منها رتبتها 6.

نتيجة 1 - 24

لتكن $(G,*)$ زمرة منتهية وليكن $a \in G$ فإن رتبة العنصر $O(a)$ عامل من عوامل رتبة الزمرة ، هذا يعني $a^{O(G)} = e$.

البرهان

الزمرة الجزئية $\big((a),*\big)$ رتبتها تساوي رتبة العنصر a اي $O\big((a)\big) = O(a)$ هو عامل من عوامل $O(G)$.

نتيجة 1 - 25

لتكن $(G,*)$ زمرة منتهية رتبتها مركبة (قابلة للتحليل الى عوامل) فإن $(G,*)$ تمتلك زمرة جزئية غير تافهة.

البرهان

اذا كانت $(G,*)$ زمرة ليست دائرية فإنه يوجد عنصر $a \in G$ بحيث يولد زمرة جزئية $\big((a),*\big)$ غير تافهة.

اما اذا كانت $(G,*)$ زمرة دائرية مولدة بواسطة العنصر a ، بما ان رتبة الزمرة قابلة للتحليل فأن $O(G) = mn$ حيث $m,n \in \mathbb{Z}$ ان كل من $m,n \neq 1$ اذن $a^{mn} = (a^n)^m = e$ ولكن $(a^n)^{m_1} = e$ حيث ان $0 < m_1 < m$ ، اذن $\big((a),*\big)$ رتبتها تساوي m_1 وبالتالي فإنها زمرة جزئية غير تافهة. $\square$

نتيجة 1 - 26

كل زمرة منتهية ذات رتبة اولية تكون دائرية.

1 - 6 الزمر الجزئية الناظمية

تعريف 1 - 30

لتكن $(H,*)$ زمرة جزئية من $(G,*)$ فإن $(H,*)$ تسمى زمرة جزئية ناظمية (سوية) اذا وفقط اذا كان $a * H = H * a$ لكل $a \in G$ ونكتب $H \trianglelefteq G$.

مثال 1 - 32

كل زمرة جزئية دليلها 2 تكون زمرة ناظمية.

البرهان

لتكن $(H,*) \leq (G,*)$ بما ان $[G:H]=2$ اذن G تمتلك مجموعتين مشاركتين يسرى هما $H, a*H$ وكذلك مجموعتين مشاركتين يمنى $H, H*a$

ليكن $b \in G$. اذا كان $b \in H$ نحصل على $H = H*b$ و $H = b*H \Leftarrow H*a = a*H$

اما اذا كان $b \notin H$ فإن $b*H \neq H$ اذن $H*b = a*H$ كذلك $H*b \neq H$ ومنه $H*b = H*a = a*H$ اذن $H \trianglelefteq G$. $\square$

مثال 1 - 33

اثبت ان $(A_n, \circ) \trianglelefteq (S_n, \circ)$

البرهان

بما ان $2 = \frac{n!}{\frac{n!}{2}} = \frac{O(S_n)}{O(A_n)} = [S_n : A_n]$ ، اذن $(A_n, \circ) \trianglelefteq (S_n, \circ)$ $\square$

مبرهنة 1 - 27

كل زمرة جزئية من زمرة ابدالية تكون زمرة سوية.

البرهان

نفترض ان $(H,*) \leq (G,*)$ ، لبرهان $a*H = H*a$ لكل $a \in G$ ، ليكن $a*h \in a*H$ ، وبما ان $(G,*)$ زمرة ابدالية ، اذن $a*h = h*a \in H*a$ ، اذن $a*H \subseteq H*a$ ، وبنفس الطريقة نبرهن $H*a \subseteq a*H$ وبالتالي $a*H = H*a$ ومنه $(H,*) \trianglelefteq (G,*)$. $\square$

تعريف 1 - 31

الزمرة $(G,*)$ تسمى زمرة بسيطة اذا كانت تحوي فقط زمرتين سويتين هما $(\{e\},*), (G,*)$.

1 - 7 زمرة القسمة

تعريف 1 - 32

لتكن $(H,*)$ زمرة جزئية من $(G,*)$ نعرف المجموعة $G/H = \{a*H : a \in G\}$ او $G/H = \{H*a : a \in G\}$ ، بأنها مجموعة القسمة لــ G على H وتمثل مجموعة كل المجموعات المصاحبة اليمنى او اليسرى للزمرة الجزئية H في الزمرة G.

تعريف 1 - 33

لتكن $(H,*)$ زمرة جزئية من $(G,*)$ ، نعرف العملية الثنائية $\circledast$ على G/H بالشكل التالي $(a*H) \circledast (b*H) = (a*b)*H, \forall a,b \in G$ ويسمى الزوج المرتب $(G/H, \circledast)$ بزمرة القسمة.

مبرهنة 1 - 28

لتكن $(G,*)$ زمرة و $(H,*)$ زمرة جزئية سوية منها فإن الثنائي $(G/H, \circledast)$ يشكل زمرة.

مبرهنة 1 - 29

لتكن $(G,*)$ زمرة ابدالية ، فإن $(G/H, \circledast)$ زمرة ابدالية لأي زمرة جزئية سوية $(H,*)$.

مبرهنة 1 - 30

لتكن $(G,*)$ زمرة دائرية ، فإن $(G/H, \circledast)$ زمرة دائرية لأي زمرة جزئية سوية $(H,*)$.

الفصل الثاني

نظرية الحلقات

2 - 1 تعريف الحلقة

تعريف 2 - 1

الحلقة هي ثلاثي مرتب $(R, +, \cdot)$ مكون من مجموعة غير خالية R وعمليتي الجمع والضرب بحيث

$\boxed{1}$ $(R, +)$ زمرة ابدالية.

$\boxed{2}$ $(R, \cdot)$ شبه زمرة.

$\boxed{3}$ العملية $\cdot$ تتوزع على العملية $+$ ، أي أن:

(التوزيع من اليسار) $$a \cdot (b + c) = a \cdot b + a \cdot c$$

(التوزيع من اليمين) $$(b + c) \cdot a = b \cdot a + c \cdot a$$

لكل $a, b, c \in R$

مثال 2 - 1

الانظمة التالية تمثل حلقات $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$
بينما الانظمة $(\mathbb{N}, +, \cdot), (\mathbb{R}, \cdot, +)$ لا تمثل حلقات

تعريف 2 - 2

يقال ان حلقة $(R, +, \cdot)$ تحتوي على قواسم الصفر ، اذا كان هناك عنصرين $a, b \in R$ بحيث $a \neq 0$ ، $b \neq 0$ مع ذلك فأن $a \cdot b = 0$ ، يطلق على العناصر a, b قواسم الصفر

مثال 2 - 2

الحلقة $(\mathbb{Z}_6, +_6, \cdot_6)$ تمتلك قواسم للصفر ، لأن $2 \cdot_6 3 = 0$ بينما الحلقة $(\mathbb{Z}_7, +_7, \cdot_7)$ لا تمتلك قواسم للصفر.

مبرهنة 2 - 1

لتكن $(R, +, \cdot)$ حلقة بحيث $R \neq \{0\}$ ، عندئذٍ تكون العناصر 0 و 1 مختلفة $(1 \neq 0)$.

مبرهنة 2 - 2

لتكن $(R, +, \cdot)$ حلقة و $a, b \in R$ فإن $-(a \cdot b) = a \cdot (-b) = (-a) \cdot b$.

نتيجة 2 - 3

لكل $a, b \in R$ فإن $a \cdot (b-c) = a \cdot b - a \cdot c$ و $(b-c) \cdot a = b \cdot a - c \cdot a$
اي ان عملية الضرب تتوزع على الطرح.

مبرهنة 2 - 4

الحلقة $(R, +, \cdot)$ لا تحتوي على قواسم صفرية اذا وفقط اذا كان قانون الاختصار ينطبق على عملية الضرب.

نتيجة 2 - 5

لتكن $(R, +, \cdot)$ حلقة لا تحتوي على قواسم صفرية فإن الحلول الوحيدة للمعادلة $a^2 = a$ هي $a = 0, a = 1$

البرهان

$a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a \cdot (a-1) = 0$ ، وبما ان R ليس لها قواسم صفرية فإن $a = 0$ او $a - 1 = 0$ وبالتالي $a = 0$ أو $a = 1$. □

تعريف 2 - 3 (الساحة التامة)

لتكن $(R, +, \cdot)$ حلقة مع عنصر محايد لعملية الضرب ، نقول ان $(R, +, \cdot)$ ساحة تامة اذا لم تحوي على قواسم الصفر وكانت ابدالية بالنسبة لعملية الضرب.

مثال 2 - 3

الحلقة $(\mathbb{Z}, +, \cdot)$ هي ساحة تامة لتحقيقها الشروط ، ولكن الحلقة $\mathbb{Z}_6, +_6, \cdot_6$ ليست ساحة تامة لأحتوائها على قواسم الصفر.

2 - 2 الحلقة الجزئية

تعريف 2 - 4

لتكن $(R, +, \cdot)$ حلقة و أن $R \supseteq S \neq \varnothing$ ، اذا كانت $(S, +, \cdot)$ حلقة بحد ذاتها نقول بأنها حلقة جزئية من $(R, +, \cdot)$ و اختصاراً نقول S حلقة جزئية من R.

ملاحظة

نقول ان S حلقة جزئية من R اذا تحقق الآتي

$\boxed{1}$ $S \neq \varnothing$.

$\boxed{2}$ $\forall a, b \in S \Rightarrow a - b \in S$.

$\boxed{3}$ $\forall a, b \in S \Rightarrow a \cdot b \in S$.

مثال 2 - 4

لتكن $S = \{a + b\sqrt{3} : a, b \in \mathbb{R}\}$ فإن S حلقة جزئية من $\mathbb{R}$.

تعريف 2 - 5

لنفرض ان R حلقة ، اذا كان هناك عدد صحيح موجب n بحيث يكون $na = 0$ لكل $a \in R$ ، فإن اقل عدد صحيح موجب يحقق هذه الخاصية يسمى المميز للحلقة R و نكتب $\operatorname{char} R = n$ ، اذا لم يوجد عدد صحيح موجب يحقق هذه الخاصية لجميع عناصر R ، فإننا نقول R ليست لها مميز او يكون المميز للحلقة يساوي 0 $(\operatorname{char} R = 0)$

مثال 2 - 5

الحلقة $(\mathbb{Z}_4, +_4, \cdot_4)$ تمتلك المميز 4. اي ان $\operatorname{char} \mathbb{Z}_4 = 4$

مبرهنة 2 - 6

لتكن R حلقة ذات محايد ، فأن $\operatorname{char} R = n > 0$ اذا وفقط اذا كان n هو اقل عدد صحيح موجب بحيث $n1 = 0$.

2 - 3 المثاليات

تعريف 2 - 6

لتكن R حلقة و I مجموعة جزئية من R ، نقول ان I هي مثالية في R اذا تحققت الشروط

$\boxed{1}$ $a-b \in I, \forall a,b \in I$.

$\boxed{2}$ $r \cdot a \in I$ و $a \cdot r \in I$ لكل $r \in R, a \in I$.

مثال 2 - 6

المجموعة $I = \{3k : k \in \mathbb{Z}\}$ تمثل مثالية في الحلقة $\mathbb{Z}$.

الحل

$$\boxed{1}\ \forall n,m \in I \Rightarrow n = 3r, m = 3s, \exists r,s \in \mathbb{Z} \Rightarrow n-m = 3\underbrace{(r-s)}_{\in \mathbb{Z}} \in I.$$

$$\boxed{2}\ \forall n \in I, \forall r \in \mathbb{Z} \Rightarrow rn = r(3m) = 3\underbrace{(rm)}_{\in \mathbb{Z}} \in I.$$

2 - 4 بعض الانواع الخاصة للمثاليات

تعريف 2 - 7 (المثالية الاعظمية)

لتكن R حلقة و I مثالية فيها ، تسمى I مثالية اعظمية في R ، اذا كانت $R \neq I$ و عندما توجد مثالية J بحيث $R \subseteq J \subseteq I$ فإن $J = R$.

ملاحظة

لتكن R حلقة و ان I مثالية في R بحيث $R \neq I$ و $a \in R - I$ فإن

1. $\subset (I,a) \subseteq R$.
2. اذا كانت I مثالية اعظمية فإن $(I,a) = R$.

مبرهنة 2 - 7

في الحلقة $\mathbb{Z}$ و حيث $n > 1$ ، فأن (n) مثالية اعظمية اذا وفقط اذا كان n عدد أولي.

البرهان

($\Leftarrow$) نفرض (n) مثالية اعظمية في $\mathbb{Z}$ ونفرض ان n ليس عدد اولي ، اي يمكن كتابته بالشكل $n = a \cdot b$ لبعض $a, b \in \mathbb{Z}$ ، من الواضح ان $(n) \subset (a)$ لأن $n = a \cdot b$ و لكن $(a) \neq \mathbb{Z}$ وبالتالي حصلنا على $(n) \subset (a) \subset \mathbb{Z}$ وهذا تناقض مع كون (n) مثالية اعظمية.

($\Rightarrow$) اذا كان n عدداً اولياً ، نفترض وجود مثالية I في $\mathbb{Z}$ بحيث $(n) \subset I \subset \mathbb{Z}$ ، لنأخذ $a \in I$ حيث $a \notin (n)$ ، بما أن n عدد أولي فأن $\gcd(a, n) = 1$ ، وبالتالي يوجد $x, y \in \mathbb{Z}$ بحيث $ax + ny = 1$ وبما ان I مثالية فأن $ax, ny \in I$ وبالتالي $1 \in I$ اذن $I = \mathbb{Z}$ وبالتالي (n) مثالية اعظمية. $\square$