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

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 $e = e'$. $\square$

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 $a^n = \underbrace{a * a * \cdots * a}_{n \text{ من المرات}}$

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 $f = (1\ 2\ 3\ 4)$ وهذا يعني انها دورة ذات طول 4 ، اما $g = (2\ 3)$ 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 $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$ 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 لــ $\mathbb{Z}_n$ 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