تمارين محلولة

في الزمر والحلقات

أ.د فوزان إسماعيل صدقي

مقدمة

الحمد لله حمدا كثيرا طيبا مباركا فيه أن هداني ووفقني لإنجاز هذا الكتاب، وأسألة سبحانة وتعالى أن ينفعني بة في الدنيا والآخرة وأن ينفع بة الدارسين العرب لعلم الجبر المجرد (abstract algebra).

في هذا الكتاب نقدم العديد من التمارين المحلولة في مجالي الزمر والحلقات (groups and rings) باللغة العربية ليساعد الدارسين العرب على استيعاب المفاهيم الجبرية والربط بينها واستخدام المبرهنات لإستنتاج العديد من خواصها.

استخدمنا في هذا الكتاب المصطلحات العربية في مجالي الزمر والحلقات كما وردت في كتاب (الدليل إلى نظرية الزمر ، ١٤٢٨هـ - ٢٠٠٧م ، تأليف : فوزان إسماعيل صدقي مكتبة الرشد – ناشرون ، المملكة العربية السعودية – الرياض ص.ب ١٧٥٢٢) وكتاب (الدليل إلى نظرية الحلقات ونظرية الحقول ، ١٤٣٠هـ - ٢٠٠٩م ، تأليف: فوزان إسماعيل صدقي – نازك بنت عبد العزيز العيسى ، الناشر: مكتبة الملك فهد الوطنية – المملكة العربية السعودية – رقم الإيداع: ١٤٣٠\٢٦٢٤ - ردمك: ٩٧٨-٦٠٣-٠٠-٢٤٢٥-٤٠) .

على الدارس لهذا الكتاب أن يرجع إلى بعض المراجع في مجالي الزمر والحلقات والكتابين سالفي الذكر ليكون ملما بالمفاهيم والمبرهنات في مجال كل تمرين من تمارين هذا الكتاب ، وأن يحاول حل كل تمرين بمفردة أو مع آخرين قبل النظر لحلة في الكتاب.

تمنياتي أن يكون هذا الكتاب مفيدا لطلبة الرياضيات البحتة في الجامعات العربية وأن يكون إضافة مفيدة للمكتبة العربية.

فوزان إسماعيل صدقي

أستاذ الرياضيات البحتة المتفرغ بكلية العلوم جامعة الزقازيق – مصر

١٧/ ١٢/ ٢٠٢٢

أولاً: تمارين في الزمر

ملحوظة: نفرض أن الزمر في هذة التمارين زمر ضربية إلا إذا نُص على غير ذلك.

الزمر والزمر الجزئية – Groups and subgroups

١. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x^2 = 1$, $x y^4 x = y^7$. اثبت أن $y^{33} = 1$.

٢. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $y^{-1} x^2 y = x^3$, $x^{-1} y^2 x = y^3$.
اثبت أن $x = y = 1$.

٣. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x^2 y = y x$, $x^4 = 1$. اثبت أن $x = 1$.

٤. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x^{-1} y^2 x = y^3$, $x^2 = 1$. اثبت أن $y^5 = 1$.

٥. ليكن G زمرة ، وليكن $x,y,z \in G$ بحيث

$$x^2 = z^{-1} x z \quad , \quad y^2 = x^{-1} y x \quad , \quad z^2 = y^{-1} z y$$

اثبت أن $x = y = z = 1$.

٦. ليكن G زمرة بحيث $x^2 = 1$ ، لكل $x \in G$. اثبت أن G تكون ابدالية .

٧. ليكن G زمرة ، وليكن $(x y)^2 = x^2 y^2$ لكل $x,y \in G$. برهن أن G تكون ابدالية .

٨. ليكن G زمرة ، وليكن $x,y,z \in G$. أوجد عنصر $g \in G$ بحيث $x g y = z$. هل العنصر g يكون وحيداً ؟

٩. ليكن G زمرة منتهية ، وليكن $x \in G$. اثبت أنة يوجد $n \in \mathbf{N}$ بحيث $x^n = 1$.

١٠. ليكن G زمرة منتهية ، وليكن $x \in G$. اثبت أن $ord(x) \le |G|$.

١١. ليكن G زمرة منتهية ، وليكن $x,y \in G$. اثبت أن

(أ) $ord(x) = ord(x^{-1})$

(ب) $ord(y x y^{-1}) = ord(x)$

(ت) $ord(x y) = ord(y x)$

١٢. ليكن G زمرة منتهية ، وليكن $x,y\in G$.

(أ) إذا كان $x\, y = y^5 x^3$ ، فاثبت أن $ord(y\, x^{-1}) = ord(y^5 x) = ord(y^3 x^3)$

(ب) الحالة العامة لـ (أ) : إذا كان $x\, y = y^m x^n$ حيث $m - n = 2$ ، فاثبت أن

$ord(y\, x^{-1}) = ord(y^m x^{n-2}) = ord(y^n x^n)$

١٣. ليكن G زمرة منتهية ، وليكن $x\in G$ ، بحيث $ord(x) = n$. إذا كان $m\in \mathbf{N}$ بحيث $(m , n) = 1$, $1 \le m \le n$ ، فاثبت أن $ord(x^m) = n$.

١٤. ليكن G زمرة منتهية ، وليكن $x\in G$ ، بحيث $ord(x) = p$ حيث p عدد أولي . اثبت أن

(أ) $ord(x^m) = p$ لكل $1 \le m < p$ ،

(ب) لكل $n\in \mathbf{N}$ يكون $x^n= 1$ أو $ord(x^n) = p$.

١٥. اثبت أن $\mathbf{Z}_p \setminus \{\bar{0}\}$ تكون زمرة بالنسبة لعملية الضرب بقياس p ، حيث p عدد أولي .

١٦. (أ) ليكن $n\in \mathbf{N}$. اثبت أن $\mathbf{Z}^*_n = \{\bar{m} \in \mathbf{Z}_n | (m , n) = 1\}$ ، حيث $\mathbf{Z}^*_n$ هى مجموعة كل العناصر في $\mathbf{Z}_n$ التي لها معكوس بالنسبة لعملية الضرب بقياس n .

(ب) برهن أن $\mathbf{Z}^*_n$ تكون زمرة بالنسبة لعملية الضرب بقياس n .

(ت) أوجد $|\mathbf{Z}^*_{12}|$, $|\mathbf{Z}^*_{20}|$, $|\mathbf{Z}^*_{11}|$.

(ث) أوجد معكوس $\overline{19}$, $\bar{9}$ في $\mathbf{Z}^*_{20}$.

١٧. ليكن G زمرة وليكن $x,y\in G$ بحيث $ord(x) = ord(y) = 2$, $x \ne y$. برهن أن $|< x , y >| = 4$.

١٨. ليكن $G = \mathbf{R} \setminus \{-1\}$ ، وليكن $\forall\, x,y\in G$, $x * y = x + y + xy$. اثبت أن * تكون عملية ثنائية داخلية على G وأن $(G ,*)$ تكون زمرة ابدالية ، ثم أوجد $x\in G$ بحيث $5 * x * 6 = 17$.

١٩. ليكن G زمرة منتهية ، وليكن $|G| = n$. ليكن $m\in \mathbf{N}$ بحيث $(m , n) = 1$. اثبت أنة لكل $x\in G$ يوجد $y\in G$ ، بحيث $x = y^m$.

٢٠. ليكن F حقل ، وليكن $n \in \mathbf{N}$ ، $GL(n,F) = \{A \in F^{(n\times n)} \mid |A| \neq 0\}$.

(أ) اثبت أن $GL(n,F)$ تكون زمرة غير ابدالية بالنسبة لعملية ضرب المصفوفات (تسمى الزمرة الخطية العامة (general linear group) من الدرجة n فوق F) .

(ب) إذا كان $|F| = p^m$ ، حيث p عدد أولي ، فأوجد $|GL(n,F)|$.

(ت) ليكن $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \,\middle|\, a, b \in \mathbf{R} ,\ a^2 + b^2 \neq 0 \right\}$. اثبت أن G تكون زمرة جزئية ابدالية من الزمرة $GL(2,\mathbf{R})$.

٢١. (أ) ليكن F حقل . اثبت أن $SL(n,F) = \{A \in F^{(n\times n)} \mid |A| = 1\}$ ، $n \in \mathbf{N}$ تكون زمرة جزئية من الزمرة $GL(n,F)$ (الزمرة $SL(n,F)$ تسمى الزمرة الخطية الخاصة من الدرجة n فوق F) .

(ب) أوجد كل المجموعات المشاركة الشمالية المختلفة لـ $S(2,\mathbf{R})$ في $G(2,\mathbf{R})$ ، ثم أوجد $[G(2,\mathbf{R}) : S(2,\mathbf{R})]$.

٢٢. ليكن G زمرة. برهن أن G تكون منتهية إذا وفقط إذا كانت G تحتوي على عدد منتهي من الزمر الجزئية.

٢٣. ليكن G زمرة ، وليكن $I \subseteq \mathbf{N}$ بحيث $i \in I \Rightarrow i+1 \in I$. إذا كان $S = \{ S_i \mid i \in I ,\ S_i \leq G \}$ فصل زمر جزئية من G بحيث $S_i \leq S_{i+1}$ ، فاثبت أن $\bigcup S \leq G$.

٢٤. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x\,y\,x^{-1} = y^2$, $y \neq 1$, $ord(x) = 5$. أوجد $ord(y)$.

٢٥. ليكن G زمرة منتهية ، وليكن $n \in \mathbf{N} \setminus \{1,2\}$ ، $A_n = \{ x \in G \mid ord(x) = n \}$. اثبت أن $|A_n|$ (عدد عناصر المجموعة A_n) يكون عددا زوجيا (باعتبار 0 عددا زوجيا) .

٢٦. ليكن G زمرة ابدالية ، وليكن $x,y \in G$. برهن أن

$$ord(xy) = ord(x)\, ord(y) \Leftrightarrow (ord(x) , ord(y)) = 1$$

٢٧. ليكن G زمرة ابدالية منتهية ، وليكن $m = \text{Max}\{\text{ord}(a) \mid a \in G\}$. اثبت أن $\text{ord}(a) \mid m$ لكل $a \in G$.

٢٨. حلل $(\mathbf{Z}_{15})^*$ لإتحاد مجموعات مشاركة للزمرة الجزئية $\langle \overline{7} \rangle$.

٢٩. (أ) في S_5 أوجد $((1\ 2\ 3)(4\ 5))^{1202}$.

(ب) في $(\mathbf{Z}_{15})^*$ أوجد $\overline{7}^{350}$ ، $\overline{2}^{1000}$.

٣٠. ليكن H مجموعة كل التباديل في S_n التي تترك n ثابتاً . اثبت أن $H \leq S_n$ ، ثم أوجد $[S_n : H]$.

٣١. ليكن G زمرة منتهية رتبتها عدد فردي ، وليكن $x,y,z \in G$. اثبت أن

(أ) $x\,y\,z = y \Rightarrow x = 1$

(ب) $x\,y\,z\,y\,x = z \Rightarrow x\,y = 1$

٣٢. ليكن $m,n \in \mathbf{N}$ بحيث $m > 1$. اثبت أن $n \mid \phi(m^n - 1)$ ، حيث ϕ هى دالة ϕ لإويلر (Euler ϕ-function) .

٣٣. ليكن G زمرة ، وليكن $x,y \in G$ ، بحيث $xy \in C(G)$ (حيث $C(G)$ هو مركز G) . اثبت أن $x\,y = y\,x$.

التشاكلات الزمرية – Homomorphisms of groups

٣٤. اثبت أن الصورة التشاكلية للزمرة $\mathbf{Z}$ تماثل $\mathbf{Z}_n$ لكل $n \in \mathbf{N}$.

٣٥. ليكن G زمرة . برهن أن $f : G \to G$ ، حيث $f(x) = x^2$ لكل $x \in G$ يكون تشاكل زمري إذا وفقط إذا كانت G ابدالية .

٣٦. أوجد كل التشاكلات الزمرية من $\mathbf{Z}$ إلى $\mathbf{Z}$.

٣٧. أوجد كل التشاكلات الزمرية من $\mathbf{Z}_6$ إلى $\mathbf{Z}_4$.

٣٨. ليكن $f : G \to G$ تماثل زمري ، وليكن $x \in G$. اثبت أن $ord(x) = ord(f(x))$ ، ثم استخدم هذا لحل تمرين (١١) (ب ، ت) .

٣٩. أوجد $Aut(G)$ ، حيث

(أ) $G = K_4$ (K_4 هي زمرة كلين الرباعية (the klein 4-group))

(ب) $G = S_3$

(ت) $G = \mathbf{Z}_4$

٤٠. برهن أن الزمرتين $\mathbf{Z}, n\mathbf{Z}$ متماثلتين .

٤١. ليكن G زمرة . اثبت أن

(أ) إذا كان $Aut(G) = \{1\}$ ، فإن G تكون ابدالية .

(ب) إذا كان $x^2 y^2 = (x y)^2, \forall x,y \in G$ ، فإن G تكون ابدالية .

(ت) إذا كان $f : G \to G$ بحيث $f(x) = x^2 , \forall x \in G$ ، تشاكل زمري ، فإن G تكون ابدالية .

(ث) $f : G \to G$ بحيث $f(x) = x^{-1} , \forall x \in G$ يكون تماثل زمري إذا وفقط إذا كان G ابدالية .

٤٢. ليكن G زمرة وليكن $a \in G$ عنصر ثابت . ليكن $x * y = x a y$ لكل $x,y \in G$. اثبت أن $(G , *)$ تكون زمرة وتماثل G .

٤٣. ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$ ، بحيث $f(x) \neq x$ لكل $x \in G \setminus \{1\}$. اثبت أن

(أ) لكل $x \in G$ ، يوجد $y \in G$ بحيث $x = y^{-1} f(y)$.

(ب) إذا كان $f^2 = 1$ ، فإن G تكون ابدالية.

٤٤. ليكن G زمرة منتهية بحيث $|G| > 2$. اثبت أن $|Aut(G)| \geq 2$.

٤٥. ليكن G زمرة منتهية. إذا كان $|G| = n$ ، فاثبت أن $|Aut(G)| \mid (n-1)!$.

٤٦. ليكن $G = \{I_{a_1,\cdots,a_n} | a_1,\cdots,a_n \in \mathbf{R}\}$ ، حيث

$$I_{a_1,\cdots,a_n} = \begin{bmatrix} 1 & & \cdots & & a_1 \\ & & 0 & & a_2 \\ \vdots & 0 & \ddots & & \vdots \\ & & \cdots & 1 & a_n \\ & & & & 1 \end{bmatrix}$$

برهن أن $G \cong \mathbf{R}^n$.

الزمر الجزئية الناظمية – Normal subgroups

٤٧. ليكن F حقل وليكن $n \in \mathbf{N}$. اثبت أن $SL(n,F) \lhd GL(n,F)$.

٤٨. ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$ ، وليكن $S = \{x \in G \mid f(x) = x^{-1}\}$. إذا كان $|S| > 3/4\,|G|$ ، فاثبت أن $S = G$.

٤٩. أوجد كل الزمر الجزئية الناظمية من الزمر K_4 , $\mathbf{Z}_n$, S_3 , S_4
(K_4 هى زمرة كلين الرباعية (the klein 4-group)) .

٥٠. ليكن G زمرة . اثبت أن $Inn(G) \lhd Aut(G)$.

٥١. ليكن G زمرة ، وليكن $N \leq G$ بحيث رتبة N لا تساوي رتبة أي زمرة جزئية أخرى من G . اثبت أن $N \lhd G$.

٥٢. اذكرمثالا لزمرة غير ابدالية بحيث كل الزمر الجزئية الناظمية غير البديهية منها تكون ابدالية .

٥٣. ليكن G زمرة ، وليكن $N \lhd G$. إذا كان $f : G/N \to \mathbf{Z}$ تشاكل زمري شامل (epimorhism) ، فبرهن أنة لكل $n \in \mathbf{N}$ ، يوجد زمرة جزئية ناظمية S من G بحيث $[G : S] = n$.

٥٤. (أ) اثبت أن رتبة كل عنصر في الزمرة $\mathbf{Q}/\mathbf{N}$ تكون منتهية .
(ب) ليكن $n \in \mathbf{N}$ وليكن $f : \mathbf{Q}/\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ ، بحيث $f(x + \mathbf{Z}) = n\,x + \mathbf{Z}$ لكل $x + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. برهن أن f يكون تشاكل زمري وأن $Ker(f) \cong \mathbf{Z}_n$.

٥٥. ليكن $n \in \mathbf{N}$. إذا كان $n = d\,m$ ، فاثبت أن

(أ) $m\,\mathbf{Z}_n \cong \mathbf{Z}_d$

(ب) $\mathbf{Z}_n / m\,\mathbf{Z}_n \cong \mathbf{Z}_m$

٥٦. ليكن G زمرة . اثبت أن $C(G) \lhd G$

(حيث $C(G)$ هو مركز الزمرة G (center of G)) .

٥٧. ليكن G زمرة وليكن N زمرة جزئية ناظمية عظمى من G . ليكن

$G \rhd B \neq \{1\} , G \rhd A \neq \{1\}$، بحيث $A \cap N = B \cap N = \{1\}$. برهن أن $A \cong B$.

٥٨. ليكن G زمرة ، وليكن

$$N = \{x_1\, x_2 \ldots x_n\, x_n\, x_{n-1} \ldots x_2\, x_1 \mid x_1 , \ldots , x_n \in G \;\; , n \in \mathbf{N}\}$$

برهن أن $N \lhd G$ وأن $\bar{x}^{-1} = \bar{x}$ ، لكل $\bar{x} \in G / N$.

٥٩. ليكن G زمرة بحيث يوجد عدد $1 \neq n \in \mathbf{N}$ يحقق $(x\,y)^n = x^n\,y^n$ لكل $x,y \in G$ ، وليكن

$$A = \{x^n \mid x \in G\} \;\; , \;\; B = \{x \in G \mid x^n = 1\} \;\; , \;\; C = \{x^{n(n-1)} \mid x \in G\}$$

برهن أن

(أ) $A \lhd G \; . \; B \lhd G$ ،

(ب) إذا كانت الزمرة G منتهية ، فإن $|A| = |G/B|$ ،

(ت) لكل $x,y \in G$ يكون $x^{n-1}\,y^n = y^n\,x^{n-1}$, $x^{1-n}\,y^{1-n} = (x\,y)^{1-n}$ ،

(ث) C تكون زمرة جزئية ابدالية من G .

٦٠. ليكن G زمرة منتهية ، وليكن $A \lhd G \; . \; B \lhd G$ بحيث $(|A| , |B|) = 1$. اثبت أن

(أ) $A \cap B = \{1\}$ ،

(ب) $a\,b = b\,a$ لكل $a \in A , b \in B$ ،

(ت) $A\,B \cong A \times B$.

٦١. ليكن $\{G_i\}_{i \in I}$ فصل زمر . برهن أن $\bigoplus_{i \in I} G_i \lhd \prod_{i \in I} G_i$.

الزمر الدائرية – Cyclic groups

٦٢. برهن أن الزمرة $\mathbf{Q}$ غير دائرية وأن $\mathbf{Z}$ لا تماثل $\mathbf{Q}$.

٦٣. ليكن $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a.b \in \mathbf{R}.\ a^2 + b^2 \neq 0 \right\}$. أوجد زمرة جزئية دائرية من G رتبتها 4 .

٦٤. ليكن G زمرة ، وليكن $a \in G$. اثبت أن
$G = \langle a \rangle \iff f : \mathbf{Z} \to G$ ، حيث $f(n) = a^n$ لكل $n \in \mathbf{Z}$ يكون تشاكل زمري شامل .

٦٥. ليكن G زمرة دائرية منتهية . اثبت أنة لكل قاسم d لرتبة G يوجد زمرة جزئية وحيدة من G رتبتها d .

٦٦. ليكن G زمرة ابدالية منتهية بحيث تحتوي على الأكثر على عدد n حلول مختلفة للمعادلة $x^n = 1$ ، لكل $n \in \mathbf{N}$. اثبت أن G تكون دائرية .

٦٧. (أ) ليكن G زمرة ، وليكن $N \lhd G$ ، $< x > = N$. اثبت أن كل زمرة جزئية من N تكون ناظمية في G .
(ب) اعطي مثالاً للزمر G , B , A بحيث $A \lhd B \lhd G$ لكن $A \ntriangleleft G$.

٦٨. إذا كان G زمرة غير ابدالية ، فبرهن أن الزمرة $G/C(G)$ لا تكون دائرية.

٦٩. إذا كان G زمرة بحيث $|G| = p^2$ حيث p عدد أولي ، فاثبت أن G تكون ابدالية .

الضرب المباشر للزمر – Direct product of groups

٧٠. اذكر سبب صحة أو خطأ كل جملة مما يلي:

(أ) $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

(ب) $\mathbf{Z}_8 \cong \mathbf{Z}_2 \times \mathbf{Z}_4$

(ت) $\mathbf{Z}_8 \cong \mathbf{Z}_2 \times K_4$

٧١. ليكن $(\bar{x}.\bar{y}) \in \mathbf{Z}_m \times \mathbf{Z}_n$. اذكر العلاقة بين $\mathrm{ord}(\bar{x}.\bar{y}). \mathrm{ord}(\bar{x}). \mathrm{ord}(\bar{y})$ ، ثم أوجد $\mathrm{ord}(\bar{x}.\bar{y})$ عندما $m = 6 , n = 9$.

٧٢. ليكن $G = \mathbf{Z}_{p^3} \times \mathbf{Z}_{p^2} \times \mathbf{Z}_p$ ، حيث p عدد أولي . أوجد عدد العناصر في الزمرة G التي رتبها تساوي: (أ) p (ب) p^2 (ت) p^3

٧٣. ليكن p عدد أولي ، وليكن $n \in \mathbf{N}$. إذا كان $\mathbf{Z}_{p^n} \cong A \times B$ ، فبرهن أن $A = \{1\}$ أو $B = \{1\}$.

٧٤. ليكن $A = \{ z \in \mathbf{C} \mid |z| = 1\}$, $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$, $\mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$. اثبت أن $\mathbf{R}^+ , \mathbf{C}^* , A$ تكون زمر ضربية (بالنسبة لعملية ضرب الأعداد) وأن $\mathbf{C}^* \cong \mathbf{R}^+ \times A$.

٧٥. أوجد كل الزمر الجزئية من الزمرة $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ والتي رتبها تساوي:
(أ) 2 (ب) 4

٧٦. ليكن $G = \mathbf{Z}_p \times \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ (n مرة) ، حيث p عدد أولي . برهن أن $\mathrm{Aut}(G) \cong GL(n, \mathbf{Z}_p)$.

٧٧. ليكن G زمرة ، وليكن $A \lhd G$. برهن ما يلي:
يوجد $B \lhd G$ ، بحيث G تكون الضرب المباشر الداخلي لـ A , B $\Leftrightarrow$ يوجد تشاكل زمري $\phi : G \to A$ بحيث تقيدة فوق A يكون تماثل زمري
(تقيد ϕ فوق A هو التطبيق $\phi|_A : A \to A$ بحيث $\phi|_A(a) = \phi(a)$ لكل $a \in A$) .

٧٨. ليكن G زمرة ، وليكن $A \lhd G , B \lhd G$. برهن أن $G / (A \cap B)$ تماثل زمرة جزئية من الزمرة $G/A \times G/B$.

٧٩. ليكن G زمرة ابدالية منتهية ، وليكن p عدد أولي . ليكن
$$A = \{x \in G \mid \mathrm{ord}(x) = p^r , r \in \mathbf{N}\} , \quad B = \{x \in G \mid (\mathrm{ord}(x) , p) = 1\}$$
اثبت أن $A , B \leq G$ وأن G تكون الضرب المباشر الداخلي لـ A , B .

٨٠. ليكن G زمرة ابدالية منتهية . برهن أنة توجد $n_1 , n_2 , \dots , n_s \in \mathbf{N}$ ، بحيث

$G \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_s}$, $n_{i+1} \mid n_i$, $i = 1 , 2 , \dots , s-1$

٨١. ليكن $m,n \in \mathbf{N}$. اثبت أن

$\mathbf{Z}_m \times \mathbf{Z}_n \cong Z_s \times \mathbf{Z}_t$ ، حيث $s = g.c.d(m,n)$, $t = l.c.m(m,n)$

تأثير زمرة على مجموعة - An action of a group on a set

٨٢. اثبت أن زمرة كلين الرباعية K_4 (the Klein 4-group) تؤثر (شماليا) على المجموعة $I_4 = \{1,2,3,4\}$ ، ثم أوجد G_4 , G_2 , orb(4) , orb(2) ، حيث $G = K_4$ (G_x هى زمرة ثبات x (stabilizer group of x)) .

٨٣. ليكن G زمرة منتهية ، بحيث $|G| = p^r n$ حيث p عدد أولي . وليكن $X = \{M \mid M \subseteq G \ , |M| = p^r\}$. اثبت أن $* : G \times X \to X$ حيث $g * M = gM$ لكل $(g,M) \in G \times X$ ، يكون تأثير شمالي لـ G على X . اثبت كذلك أن $|orb(M)| \equiv 0 \pmod p$.

٨٤. ليكن G زمرة ، وليكن $H \leq G$, $H \neq G$. ليكن $G/H = \{aH \mid a \in G\}$.

(أ) أوجد تأثير شمالي لـ G على G/H .

(ب) ليكن G منتهية. إذا كان |G| لا يقسم ![G : H] ، فاثبت أن H تحتوي على زمرة جزئية ناظمية غير بديهية من G .

(ت) إذا كان $[G : H] = p$ ، حيث p عدد أولي يقسم |G| ، فبرهن أن $H \lhd G$.

٨٥. اثبت أن $G = SL(2,\mathbf{R})$ تؤثر شماليا على المجموعة $\mathbf{R}^2$ ، ثم أوجد $orb(x)$, G_x ، حيث $x = (0,0)$, $(1,3)$.

٨٦. ليكن $G = \mathbf{R}^* (= \mathbf{R} \setminus \{0\})$ ، وليكن $X = \mathbf{R}^2$ ، وليكن $* : \mathbf{R}^* \times \mathbf{R}^2 \to \mathbf{R}^2$ بحيث $r * (x , y) = (r x , \frac{1}{r} y)$ ، لكل $(x,y) \in \mathbf{R}^2$, $r \in \mathbf{R}^*$. برهن أن * يكون تأثير شمالي لـ G على X ، وأوجد زمر ثبات عناصر G .

٨٧. ليكن $*$ تأثير شمالي لزمرة G على مجموعة X . اثبت أن

(أ) $G_{a*x} = a\, G_x\, a^{-1}$ ، لكل $a\in G$, $x\in X$.

(ب) $G_x \cong G_y$ ، لكل $y\in orb(x)$.

(ت) لكل $y\in orb(x)$ يكون $G_x \lhd G \Leftrightarrow G_x = G_y$.

٨٨. ليكن G زمرة منتهية ، وليكن $A,B \leq G$. استخدم تأثير زمرة على مجموعة لإثبات أن

(أ) $|A\, x\, B| = \dfrac{|A|\,|B|}{|A \cap xBx^{-1}|}$. $\forall\, x \in G$

(ب) $|A \cap B| = \left|A \cap aBa^{-1}\right|$, $\forall x\in G$

٨٩. ليكن G زمرة ، وليكن $A , B \leq G$. استخدم تأثير زمرة على مجموعة لإثبات أن $|\{b\, B\, b^{-1} \mid b\in B\}| = [B : B \cap N(A)]$ ، حيث $N(A)$ هو ناظمية A في G (normalizer of N in G) .

٩٠. ليكن G زمرة منتهية ، وليكن $S \leq G$, $S \neq G$. استخدم تأثير زمرة على مجموعة لإثبات أن $G \neq \cup_{g\in G}\, g\, S\, g^{-1}$.

٩١. ليكن $A \leq S_4$ ، بحيث $|A| = 3$. برهن أن عدد الزمر الجزئية من S_4 التي تماثل A يساوي $[S_4 : N(A)]$. هل هذا يكون صحيحا أيضاً عندما $|A| = 2$ ؟

٩٢. ليكن G زمرة منتهية ، وليكن $f\in Aut(G)$. إذا كان $ord(f) = p^k$ ، حيث p عدد أولي يقسم $|G|$ ، فبرهن أن f لة عنصر ثبات لا يساوي 1 .

٩٣. ليكن F حقل ، بحيث $|F| = p^n$ و p عدد أولي . ليكن $G \leq GL(n,F)$ ، بحيث $|G| = p^r$. اثبت أنة يوجد عنصر ثبات لـ G في F لا يساوي 0 (المحايد الجمعي في F) .

٩٤. ليكن G زمرة منتهية ، وليكن X مجموعة بحيث $|X| = 18$, $|G| = 55$. ليكن G تؤثر على X . اثبت أن $|Fix_G(X)| \leq 2$.

٩٥. ليكن G زمرة منتهية و X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X و S نظام دخول للمدارات . ليكن $x,y,z\in X$, $g\in G$. برهن أن

(أ) $|G_x| = |G_y|$, $\forall\, x,y\in orb(z)$

(ب) إذا كان $Fix_g(X) = \{x\in X \mid g * x = x\}$ ، فإن

$$|\{(g,x)\in G\times X \mid x\in Fix_g(X)\}| = \sum_{g\in G} |Fix_g(X)| \quad ,$$

$$\sum_{g\in G} |Fix_g(X)| = \sum_{x\in X}|G_x| = |G||S|$$

٩٦. ليكن G زمرة منتهية و X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X وليكن S نظام دخول للمدارات. ليكن $X \supseteq Y$ بحيث $Y \supseteq S$. إذا كان $G(x,Y) = \{g\in G \mid g*x\in Y\}$, $x\in X$ ، فبرهن أن

(أ) $G(x,Y) \neq \emptyset$ ، لكل $x\in X$ ،

(ب) $|G(x,Y)| = |G_x|\,|orb(x) \cap Y|$ ،

(ت) $|Y| = \frac{1}{|G|}\sum_{x\in X}|G(x.Y)|$ ،

(ث) $|X| = |G| \sum_{x\in Y}\frac{1}{|G(x.Y)|}$.

p-زمر - p-groups

٩٧. اذكر كل الـ p-زمر غير المتماثلة والتي رتبها p^2 .

٩٨. اذكر كل الـ p-زمر غير المتماثلة والتي رتبها p^3 .

٩٩. اذكر مثالاً لـ p-زمرة غير منتهية .

١٠٠. ليكن G p-زمرة منتهية ، وليكن $N \lhd G$. برهن أن G/N تكون p-زمرة منتهية .

١٠١. ليكن G p-زمرة منتهية ، وليكن $\{1\}\neq N \lhd G$. برهن أن

(أ) $C(G) \cap N \neq \{1\}$ ،

(ب) إذا كان $|N| = p$ ، فإن $N \leq C(G)$ ،

(ت) إذا كان $|C(G)| = p$ ، $C(G) \leq N$.

١٠٢. ليكن G زمرة وليكن $N_{i+1} \lhd G$, $N_i \lhd G$ ، بحيث

$$N_1=C(G) \ , \ C(G/N_i) = N_{i+1}/N_i$$

برهن أن

(أ) $x^{-1} g^{-1} x g \in N_i$ لكل $g \in G , x \in N_{i+1}$ ،

(ب) إذا كانت G p-زمرة منتهية ، فإنة يوجد $m \in \mathbf{N}$ بحيث $N_m = G$ ،

(ت) إذا كانت G غير ابدالية ورتبتها تساوي p^3 ، حيث p عدد أولي ، فإن $N_2 = G$.

١٠٣. ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية غير بديهية من G . اثبت أن $S \neq N(S)$.

١٠٤. ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية من G بحيث $[G : S] = p$. برهن أن $S \lhd G$.

زمر سيلو والزمر البسيطة - Sylow's groups and simple groups

١٠٥. ليكن G p-زمرة بحيث $|G| = 3^4$. برهن أنة توجد زمرة جزئية ناظمية N من G ، بحيث $|N| > 3$.

١٠٦. ليكن G زمرة منتهية وليكن p عدد أولي يقسم $|G|$. إذا كان $S = \{x \in G \mid ord(x) = p^k , k \in \mathbf{N}_0\}$ ، فاثبت أن $S \leq G$.

١٠٧. ليكن G زمرة ، بحيث $|G| = 99$. برهن أن G تحتوي على زمرة جزئية ناظمية رتبتها 11.

١٠٨. أوجد زمر سيلو الجزئية من الزمرتين S_3 , $\mathbf{Z}_{4900}$.

١٠٩. ليكن G زمرة منتهية ، وليكن $S \leq N \lhd G$. وليكن p عدد أولي يقسم $|N|$. ليكن $K \leq G / N$. برهن أن

(أ) S تكون p-زمرة جزئية لسيلو من N $\Leftrightarrow$ يوجد p-زمرة جزئية لسيلو V من G بحيث $S = V \cap N$.

(ب) K تكون p-زمرة جزئية لسيلو من G/N $\Leftrightarrow$ يوجد p-زمرة جزئية لسيلو B من G بحيث $K = B N / N$.

١١٠. ليكن G زمرة منتهية ، وليكن $A \lhd G$. وليكن B p-زمرة جزئية لسيلو من A . برهن أن

(أ) $G = A\,N(B)$

(ب) يوجد p-زمرة جزئية لسيلو من G في N(B) .

١١١. ليكن G زمرة منتهية ، وليكن S زمرة جزئية من G و A p-زمرة جزئية لسيلو من G ، بحيث $N(A) \leq S$. برهن أن $[G : S] \equiv 1 \pmod p$.

١١٢. أوجد كل الـ p-زمر جزئية لسيلو من الزمرة

$$G = \{1,c,c^2,a,b,ab,ca,cb,cab,c^2a,c^2b,c^2ab\}$$

حيث $a^2 = b^2 = c^3 = 1 \;,\; a\,b = b\,a \;,\; a\,c = c\,b \;,\; b\,c = c\,a\,b$

١١٣. ليكن G زمرة بحيث $|G| = 12$. ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G . اثبت أن الأحتمال $n_2 = 3 , n_3 = 4$ غير ممكن . واثبت أنة إذا كان $n_2 = n_3 = 1$ ، فإن G تكون ابدالية .

١١٤. أوجد كل الزمر غير المتماثلة التي رتبها 12 , 8 .

١١٥. اثبت أن الزمر التي رتبها 56 , 48 , 40 تكون غير بسيطة .

١١٦. ليكن G زمرة منتهية وليكن $|G| = p^r m$ ، حيث p عدد أولي بحيث $p > m \;,\; (p , m) = 1$. اثبت أن G تكون غير بسيطة .

١١٧. اثبت أن رتبة أصغر زمرة بسيطة غير ابدالية تساوي 60 .

١١٨. ليكن G زمرة بسيطة رتبتها 60 . ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G . اثبت أن

(أ) $n_2 = 5 \text{ or } 15 \;,\; n_3 = 10 \;,\; n_5 = 6$

(ب) يوجد $H \leq G$ ، بحيث $[G : H] = 5$.

١١٩. أوجد كل الـ p-زمر جزئية لسيلو من S_5 .

١٢٠. اثبت أن كل زمرة بسيطة رتبتها 60 تماثل A_5 .

١٢١. ليكن G زمرة منتهية وليكن S p-زمرة جزئية لسيلو من G . برهن أن $p \nmid [N(S) : S]$.

الزمرة المتماثلة والزمر منتهية التولي

Symmetric group and finitely generated groups

.١٢٢ برهن أن كل دورتين في S_n لهما نفس الطول تكونان مترافقتين .

.١٢٣ اكتب عناصر S_4 باستخدام الدورات ، ثم أوجد كل الزمر الجزئية وكل الزمر الجزئية لسيلو وكل الزمر الجزئية الناظمية منها وأوجد كذلك $C(S_4)$ (مركز S_4) .

.١٢٤ برهن أن

(أ) $S_n = \langle (1\ 2), (1\ 3), \cdots, (1\ n) \rangle$.

(ب) $S_n = \langle (1\ 2), (1\ 2\ 3 \cdots n) \rangle$.

(ت) $S_n = \langle \big(f(1)\ f(2)\big), \big(f(1) \cdots f(n)\big) \rangle$ ، لكل $f \in S_n$.

.١٢٥ برهن أن كل زمرة منتهية تماثل زمرة جزئية من زمرة بسيطة .

.١٢٦ ليكن $g \in S_4$, $f \in K_4 \subset S_4$. اثبت أن $\langle f, g \rangle \neq S_4$.

.١٢٧ أوجد عدد الدورات التي طولها k في S_n ، حيث $k = 1,2,\ldots,n$.

.١٢٨ ليكن $f,g \in S_n$ ، بحيث $f = (1\ 2\ \ldots\ n)$. برهن أن: $f\,g = g\,f \Leftrightarrow g \in \langle f \rangle$.

.١٢٩ ليكن $\alpha \in Aut(S_n)$ بحيث صورة أي ناقلة بـ α تكون ناقلة أيضاً . اثبت أن α تكون تماثل ذاتي داخلي (inner automorphism) .

.١٣٠ (أ) اذكر العناصر في S_n التي رتبها 2 .

(ب) ليكن $f \in S_n$ ، بحيث $ord(f) = 2$. اثبت أن كل عناصر S_n المرافقة لـ f تكون رتبتها 2 .

.١٣١ اثبت أن الزمرة **Q** ليست منتهية التوليد .

.١٣٢ اثبت أن الزمرة $\mathbf{Q}^*$ ليست منتهية التوليد .

.١٣٣ برهن أن الزمرة **Q** ليست دائرية وأن الزمرة **Z** لا تماثل الزمرة **Q** .

.١٣٤ استخدم المبرهنة الأساسية للزمر الإبدالية منتهية التوليد لإثبات أن **Q** زمرة ليست منتهية التوليد .

١٣٥. ليكن A مجموعة جزئية منتهية من **Q** . اثبت أن $\langle A\rangle$ تكون زمرة جزئية دائرية من **Q** .

١٣٦. ليكن G زمرة ابدالية منتهية رتبتها n . إذا كانت n تساوي حاصل ضرب أعداد أولية مختلفة ، فبرهن باستخدام المبرهنة الإساسية للزمر الإبدالية منتهية التوليد أن $G \cong \mathbf{Z}_n$.

١٣٧. ليكن $f\in S_5\backslash\{1\}$ ، بحيث $ord(f) \neq 2$. اثبت أنة يوجد $g\in S_5$ ، بحيث $S_5 = \langle g , f\rangle$.

١٣٨. ليكن $G = \langle x , y \mid ord(x)=2 , ord(y)=3 , (xy)^2 = 1\rangle$. برهن أن $G \cong S_3$.

١٣٩. ليكن G زمرة بحيث لكل $x,y\in G , n\in \mathbf{N}$ يكون $x^n = y^n \Rightarrow x = y$.

(أ) برهن أن: $x^{-1} y x = y \Rightarrow x^{-m} y x^m = y$

(ب) لتكن رتبة كل تماثل زمري من G إلى G منتهية . برهن أن G تكون ابدالية ، وإذا كانت G منتهية التوليد ، فإن $G \cong \mathbf{Z}$.

١٤٠. ليكن G زمرة ابدالية منتهية التوليد . ليكن n هو عدد مولدات G . ليكن $S \leq G$. اثبت أن عدد مولدات S يكون أقل من أو يساوي n .

١٤١. اكتب كل عناصر Q_8 وأوجد كل الزمر الجزئية غير البديهية وكذلك الزمر الجزئية الناظمية غير البديهية منها ، علما بأن

$$Q_8 = \langle a , b \mid a^4=1 . \ a^2 = b^2, b\, a = a^3\, b \rangle$$

وتسمى الزمرة المرباعية (Quaternion group) .

١٤٢. أوجد الزمرة الجزئية $\langle f , g\rangle$ من الزمرة S_4 ، حيث $f = (1\ 2\ 3\ 4) , g = (2\ 4)$.

١٤٣. اذكر كل عناصر الزمرة $\langle a , b \mid a^3 = b^2 = (a\, b)^2 = 1 \rangle$ ، واذكر معكوس كل عنصر فيها ، ثم أوجد كل الزمر الجزئية غير البديهية منها .

١٤٤. ليكن G زمرة ابدالية ، وليكن $S \subseteq G$ حيث $S = \{g \in G \mid ord(g) < \infty\}$. اثبت أن $S \leq G$. وإذا كانت S منتهية التوليد ، فاثبت أن S تكون منتهية .

المتسلسلات شبة الناظمية والمتسلسلات الناظمية للزمر –

Subnormal series and normal series of groups

١٤٥. أوجد مكملتين (refinements) متماثلتين للمتسلسلتين الناظميتين

$$\{0\} \leq 60\,\mathbf{Z} \leq 15\,\mathbf{Z} \leq \mathbf{Z} \qquad (1)$$

$$\{0\} \leq 12\,\mathbf{Z} \leq \mathbf{Z} \qquad (2)$$

١٤٦. أوجد كل المتسلسلات المركبة (composition series) للزمرتين S_4 , $\mathbf{Z}_{24}$.

١٤٧. (أ) أوجد متسلسلة مركبة للزمرة $\mathbf{Z}_{p^r}$ ، حيث p عدد أولي .

(ب) أوجد متسلسلة مركبة للزمرة $\mathbf{Z}_n$ ، حيث $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ وحيث $p_1 , p_2 ,\ldots, p_r$ أعداد أولية مختلفة .

١٤٨. اثبت أن أي زمرة ابدالية لها متسلسلة مركبة تكون منتهية .

١٤٩. ليكن G زمرة رتبتها 100 . اثبت أن G تكون قابلة للحل .

١٥٠. ليكن G زمرة . برهن أن

G تكون قابلة للحل $\Leftrightarrow$ $G/C(G)$ تكون قابلة للحل

زمر المبدلات – Groups of commutators

١٥١. ليكن G زمرة ، وليكن $a,b \in G$. اثبت أن

(أ) $[ab , c] = a\,[b , c]\,a^{-1}\,[a , c]$

(ب) $[a , bc] = [a , b]\,b\,[a , c]\,b^{-1}$

(ت) $[a , b] = a\,[b , a^{-1}]\,a^{-1} = b\,[b^{-1} , a]\,b^{-1}$

(ث) $[[a , b] , bcb^{-1}]\,[[b , c] , cac^{-1}]\,[[c, a] , aba^{-1}] = 1$

١٥٢. ليكن G زمرة . أوجد متسلسلة الإشتقاق لـ G (the drive series of G) ، حيث

(أ) $|G| = 8$

(ب) $G = S_4$

١٥٣. ليكن G زمرة ، وليكن $N = \{u\,x^2 \mid x \in G , u \in G'\}$ ، حيث G' هي مشتقة G (أي أن $G' = [G , G]$) . اثبت أن $N \lhd G$.

١٥٤. ليكن G زمرة ، وليكن

$$[x_1 , x_2 , \ldots , x_n] = [x_1 , x_2\, x_3 \ldots x_n]\,[x_2 , x_3 , \ldots , x_n]$$

لكل $x_1 , x_2 , \ldots , x_n \in G , n \in \mathbf{N}$ ، حيث $[x] = 1$ لكل $x \in G$.

اثبت أن

$$G' = \{\, [x_1 , x_2 , \ldots , x_n] \mid x_1 , x_2 , \ldots , x_n \in G , n \in \mathbf{N} \,\}$$

١٥٥. ليكن G زمرة ، وليكن $x,y \in G$. إذا كان $x^3 = (x\,y)^3 = (x\,y^{-1})^3 = 1$ ، فاثبت أن $[[x , y] , y] = 1$.

١٥٦. ليكن G زمرة ، وليكن $n \in \mathbf{N}$. إذا كان

$$K^0(G) = G \;,\; K^1(G) = [G , G] \;,\; \ldots , K^{n+1}(G) = [G , K^n(G)]$$

فبرهن أن

(أ) $K^n(G) \lhd G$

(ب) $K^{n+1}(G) \leq K^n(G)$

١٥٧. ليكن G زمرة ، وليكن $m , n \in \mathbf{N}$. إذا كان

$$K^0(G) = G \;,\; K^1(G) = [G , G] \;, \ldots , K^{n+1}(G) = [G , K^n(G)]$$

فبرهن أن

$$K^m(S_n) = A_n \;, \forall\, n \geq 2 \;,\; m \geq 1$$

١٥٨. ليكن G زمرة ، وليكن $N \lhd G$. ليكن

$$K^0(G) = G \;,\; K^1(G) = [G , G] \;, \ldots ,\; K^{n+1}(G) = [G , K^n(G)] ,\; n \in \mathbf{N}$$

برهن أن $\forall n \in \mathbf{N}$, $K^n(G/N) = K^n(G)/N$.

١٥٩. ليكن G p-زمرة منتهية ، وليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \ldots , \ K^{n+1}(G) = [G , K^n(G)] \ , \ n \in \mathbf{N}$$

برهن أنة يوجد $m \in \mathbf{N}$ ، بحيث $K^m(G) = \{1\}$.

١٦٠. ليكن G , H زمرتين . وليكن لأي زمرة A

$$K^0(A) = A \ , \ K^1(A) = [A , A] \ , \ldots , \ K^{n+1}(A) = [A , K^n(A)] \ , \ n \in \mathbf{N}$$

برهن أن $K^n(G \times H) = K^n(G) \times K^n(H)$ ، لكل $n \in \mathbf{N}$.

ثانياً: تمارين في الحلقات

الحلقات والحلقات الجزئية Rings and subrings

١٦١. ليكن R حلقة بحيث $x^2 = x$ ، لكل $x \in R$. برهن أن R تكون حلقة ابدالية .

١٦٢. ليكن R حلقة ابدالية تحتوي محايد . برهن أنة لكل $n \in \mathbf{N}_0$, $x,y \in R$ يكون

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \qquad (*)$$

١٦٣. في $\mathbf{Z}_p$ ، حيث p عدد أولي ، برهن أن

$$(x+y)^p = x^p + y^p \quad , \forall\, x,y \in \mathbf{Z}_p$$

١٦٤. ليكن R حلقة .

(أ) ليكن $x^3 = x$ ، لكل $x \in R$. برهن أن $6x = 0$, $\forall\, x \in R$.

(ب) ليكن R تحتوي محايد ، وليكن $x^3 = x$ ، لكل $x \in R$. برهن أن R تكون ابدالية .

١٦٥. أوجد مركز الحلقة $\mathbf{R}^{2\times2}$.

١٦٦. ليكن R حلقة ، وليكن $n \in \mathbf{N}$. برهن أن المجموعة

$$S = \{\, x \in R \mid n\,x = 0 \,\}$$

تكون حلقة جزئية من R .

١٦٧. ليكن R حلقة ابدالية . برهن أن المجموعة

$$S = \{\, x \in R \mid \exists\, n \in \mathbf{N} \ \text{s.t.}\ x^n = 0 \,\}$$

تكون حلقة جزئية من R .

١٦٨. برهن أن

$$S = \left\{ \begin{pmatrix} x+y & y \\ -y & x \end{pmatrix} \middle|\, x,y \in \mathbf{Z} \right\}$$

تكون حلقة جزئية من الحلقة $\mathbf{Z}^{2\times2}$.

١٦٩. برهن أن

$$S = \left\{ \begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} \middle| \; x\,.\,y \in \mathbf{R} \right\}$$

تكون حلقة جزئية من الحلقة $\mathbf{R}^{2\times 2}$.

١٧٠. أوجد كل الحلقات الجزئية من الحلقة $\mathbf{Z}_{16}$ ، ثم اذكر الحلقات الجزئية التي تحتوي محايد .

١٧١. ليكن X مجموعة غير خالية ، وليكن Δ عملية الفرق المتماثل على مجموعة القوى P(X) . اثبت أن $(P(X)\,,\,\Delta\,,\,\cap)$ تكون حلقة ابدالية تحتوي محايد .

١٧٢. اذكر عناصر حلقة الزمرة (group ring) $\mathbf{Z}_2(G)$ ، حيث G هى زمرة كلين الرباعية ، ثم أوجد تأثير عملتي الجمع والضرب في هذة الحلقة على عنصرين غير المحايد الجمعي والمحايد الضربي .

١٧٣. ليكن R حلقة ، وليكن $f : R \to [0,1]$ ، بحيث

$$f(x-y) \geq \mathrm{Min}(f(x)\,,\,f(y)) \quad , \quad f(x\,y) \geq \mathrm{Min}(f(x)\,,\,f(y)) \; , \; \forall\, x,y \in R$$

اثبت أن المجموعة

$$f_t = \{x \in R \mid f(x) \geq t\} \;\; , \; t \in \mathrm{Im}(f)$$

تكون حلقة جزئية من R .

التشاكلات الحلقية - Homomorphisms of rings

١٧٤. ليكن R حلقة ، وليكن $1 \in R$.

(أ) ليكن $\oplus : R \times R \to R$ ، بحيث $x \oplus y = x + y + 1$ لكل $x,y \in R$. اثبت أن $\oplus$ تكون عملية ثنائية داخلية على R .

(ب) ليكن ليكن $\otimes : R \times R \to R$ ، بحيث $x \otimes y = x + y + x\,y$ لكل $x,y \in R$. اثبت أن $\otimes$ تكون عملية ثنائية داخلية على R .

(ت) اثبت أن $(R\,,\oplus\,,\otimes)$ تكون حلقة تحتوي عنصر محايد .

(ث) اثبت أن الحلقتان R , $(R\,,\oplus\,,\otimes)$ تكونان متماثلتين .

١٧٥. برهن أن

يوجد تشاكل حلقي $f : \mathbf{Z}_m \to \mathbf{Z}_n$ ، بحيث $n \mid m \iff m \geq n , f(\bar{1}) = \bar{1}$

١٧٦. أوجد كل التشاكلات الحلقية من $\mathbf{Z}_4$ إلى $\mathbf{Z}_4$.

١٧٧. أوجد كل التشاكلات الحلقية من $\mathbf{Z}$ إلى $\mathbf{Z}$.

١٧٨. أوجد كل التشاكلات الحلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z}$.

١٧٩. أوجد كل التشاكلات الحلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z} \times \mathbf{Z}$.

١٨٠. اذكر أمثلة لتشاكلات حلقية بحيث صورة العنصر المحايد بكل تشاكل منها تساوي العنصر محايد .

١٨١. اذكر أمثلة لتشاكلات حلقية بحيث صورة العنصر المحايد بكل تشاكل منها لا تساوي العنصر محايد .

١٨٢. اثبت أن تحصيل تشاكلات حلقية يكون تشاكل حلقي .

١٨٣. ليكن

$$R = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| \, x.y \in \mathbf{R} \right\}$$

برهن أن $\mathbf{C} \cong R$.

١٨٤. ليكن R حلقة ، وليكن

$$End(R) = \{f : R \to R \mid \text{يكون تشاكل زمري } f \}$$

(أ) برهن أن End(R) تكون حلقة .

(ب) ليكن $r \in R$ عنصر ثابت ، وليكن $_rf : R \to R$ بحيث $_rf(x) = r\,x$ لكل $x \in R$. اثبت أن $_rf \in End(R)$ ، وأن $S = \{ _rf \mid r \in R \}$ تكون حلقة جزئية من الحلقة End(R) . هل $S \cong R$ ؟

١٨٥. اثبت أن الحلقتين $\mathbf{Q} , \mathbf{R}$ غير متماثلتين .

١٨٦. اثبت أن الحلقتين $\mathbf{R} , \mathbf{C}$ غير متماثلتين .

١٨٧. هل الحلقتان $\mathbf{Z}_2 \times \mathbf{Z}_3 \;,\; \mathbf{Z}_6$ متماثلتان ؟

١٨٨. ليكن

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle| \ x.y.z \in \mathbf{R} \right\}$$

(أ) اثبت أن R تكون حلقة بالنسبة لعمليتي جمع وضرب المصفوفات .

(ب) ليكن $f : R \to \mathbf{Z}$ ، بحيث

$$f\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = x \ , \forall \ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in R$$

اثبت أن f يكون تشاكل حلقي ، ثم أوجد Ker(f) . هل f يكون شامل وهل f يكون تماثل حلقي ؟

١٨٩. هل يوجد تشاكل حلقي شامل من $\mathbf{Z}_{24}$ إلى $\mathbf{Z}_7$ ؟

١٩٠. هل يوجد تشاكل حلقي متباين من $\mathbf{Z}_6$ إلى $\mathbf{Z}_{11}$ ؟

١٩١. اثبت أن الحلقة $2\mathbf{Z}$ لا تماثل الحلقة $3\mathbf{Z}$.

١٩٢. اثبت أن الحلقة $\mathbf{Z}$ لا تماثل الحلقة $n\,\mathbf{Z}$ ، لكل $n \in \mathbf{Z} \setminus \{1\}$.

١٩٣. ليكن R حلقة بولينية (Bolean ring) لا تحتوي على مثاليات غير بديهية . اثبت أن $R \cong \mathbf{Z}_2$.

١٩٤. هل الحلقة $\mathbf{Q}[\sqrt{2}]$ تماثل الحلقة $\mathbf{Q}[\sqrt{3}]$ ؟

١٩٥. ليكن R حلقة تحتوي 1 . إذا كان $ch(R) = n > 0$ ، فاثبت أن R تحتوي على حلقة جزئية تماثل $\mathbf{Z}_n$.

١٩٦. اثبت أنة يوجد تماثل حلقي وحيد من $\mathbf{R}$ إلى $\mathbf{R}$.

بعض العناصر الخاصة في الحلقات وبعض الحلقات الخاصة

١٩٧. ليكن R حلقة ، وليكن $e \in R$ عنصر متساوي القوى (idempotent) . اثبت أن المجموعة $S = \{e\,x\,e \mid x \in R\}$ تكون حلقة جزئية من R وتحتوي محايد .

١٩٨. ليكن $m,n \in \mathbf{N} \setminus \{1\}$ ، بحيث $(m , n) = 1$. اثبت أن الحلقة $\mathbf{Z}_{mn}$ تحتوي على الأقل على أربعة عناصر متساوية القوى .

١٩٩. أوجد كل عدد طبيعي n ، بحيث $\mathbf{Z}_n$ لا يحتوي على عناصر متساوية القوى غير $0 , 1$.

٢٠٠. ليكن $f : R \to S$ تشاكل حلقي ، وليكن كل من R , S تحتوي محايد . ليكن $x \in R$.
برهن أن

(أ) إذا كان f شامل و x وحدة ، فإن $f(x)$ يكون وحدة .

(ب) إذا كان x عنصر متساوي القوى ، فإن $f(x)$ يكون عنصر متساوي القوى .

(ت) إذا كان x عنصر متلاشي القوى ، فإن $f(x)$ يكون عنصر متلاشي القوى .

(ث) إذا كان f شامل و x عنصر مركزي (أي أن $x \in C(R)$) ، فإن $f(x)$ يكون عنصر مركزي .

٢٠١. ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث

$$x\,y + y\,x = 1 \;,\quad x^2\,y + y\,x^2 = x$$

برهن أن x يكون وحدة وأن $x^{-1} = 2\,y$.

٢٠٢. ليكن R حلقة بحيث $1 \in R$ ، وليكن $x,y \in R$. برهن أن

(أ) $1 - x$ يكون وحدة ومعكوسة الضربي هو $1 + y \;\Leftrightarrow\; y - x = x\,y = y\,x$

(ب) $1 - x\,y$ يكون وحدة $\Leftrightarrow$ $1 - y\,x$ يكون وحدة

٢٠٣. ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث $y = -\,y$. برهن أن
$1 + x$ يكون وحدة ومعكوسة هو $1 + y \;\Leftrightarrow\; y - x = x\,y = y\,x$

٢٠٤. اثبت أن كل عنصر غير صفري في $\mathbf{Z}_n$ يكون وحدة أو قاسم للصفر .

٢٠٥. اذكر مع الاثبات صحة أو خطأ كل عبارة من العبارات الآتية:

(١) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر متساوي القوى ، فإن $x + y$ يكون عنصر متساوي القوى أيضاً .

(٢) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر متلاشي القوى ، فإن $x + y$ يكون عنصر متلاشي القوى أيضاً .

(٣) إذا كان R حلقة منتهية وتحتوي محايد ، فإن R يكون مجال متكامل . (integral domain)

(٤) مميز أي حلقة غير منتهية يساوي 0 .

(٥) ليكن R حلقة تحتوي محايد . إذا كان $x \in R\backslash\{0\}$ عنصر متساوي القوى وغير قاسم للصفر ، فإن $x = 1$.

(٦) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر قاسم للصفر ، فإن $x + y$ يكون عنصر قاسم للصفر أيضاً .

٢٠٦. ليكن R حلقة تحتوي محايد . برهن أنة إذا كان $x \in R$ عنصر متلاشي القوى ، فإن العنصر $1 - x$ يكون وحدة .

٢٠٧. اثبت أن عدد الوحدات في الحلقة $\mathbf{Z}[\sqrt{3}]$ يكون غير منتهي .

٢٠٨. ليكن R مجال متكامل (integral domain) ، وليكن $p \in R$ عنصر أولي (prime element) . ليكن $r_1 , r_2 , \ldots , r_n \in R$. برهن أنة إذا كان $p \mid r_1\ r_2 \ldots r_n$ ، فإنة يوجد $i \in \{1,2,\ldots,n\}$ ، بحيث $p \mid r_i$.

٢٠٩. ليكن R مجال متكامل (integral domain) ، وليكن $r_1 , r_2 ,\ldots, r_n \in R$, $n \geq 2$ عناصر ليست كلها أصفار . برهن أن

$$(r_1 , r_2 ,\ldots, r_n) \sim ((r_1 , r_2 ,\ldots, r_{n-1}) , r_n)$$

حيث $(r_1 , r_2 ,\ldots, r_n)$ يرمز للقاسم المشترك الأعظم (greatest common divisor) للعناصر $r_1 , r_2 ,\ldots, r_n$.

٢١٠. ليكن R مجال متكامل (integral domain) ، وليكن $x,y,u,v \in R$. ليكن $u = \text{l.c.m}(x , y)$. برهن أن

(أ) $v = \text{l.c.m.}(x , y) \Leftrightarrow u \sim v$

(ب) $< x > \bigcap < y > = < u >$

(ت) $(x , y)\, u \sim x\, y$

(حيث $\text{l.c.m.}(x , y)$ يرمز للمضاعف المشترك الأصغر (least common multiple)

للعنصرين x , y . كذلك (x , y) يرمز للقاسم المشترك الأعظم (greatest common divisor) للعنصرين x , y) .

٢١١. ليكن R مجال متكامل (integral domain) . نفرض أنة لكل عنصرين $x,y \in R$ يوجد قاسم مشترك أعظم (greatest common divisor) . اثبت أنة لكل عنصرين $x,y \in R$ يوجد مضاعف مشترك أصغر (least common multiple) .

٢١٢. ليكن R مجال متكامل (integral domain) . نفرض أنة لكل عنصرين $x,y \in R$ يوجد مضاعف مشترك أصغر (least common multiple) . اثبت أنة لكل عنصرين $x,y \in R$ يوجد قاسم مشترك أعظم (greatest common divisor) .

٢١٣. ليكن R مجال متكامل ، وليكن $a \in R\backslash\{0\}$ عنصر ليس وحدة وغير مختزل . إذا كان $b \in R\backslash\{0\}$ ، بحيث a لا يقسم b ، فاثبت أن $(a , b) = 1$.

٢١٤. (أ) أوجد كل قواسم العنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(ب) أوجد كل قواسم العنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(ت) أوجد كل قواسم العنصر $5+3i$ في الحلقة $\mathbf{Z}[i]$.

٢١٥. ليكن R حلقة مثاليات رئيسة (principal ideal ring) ، وليكن $a,b,c \in R \setminus \{0\}$. ليكن $d = (a , b)$. برهن أنة يوجد $r , s \in R$ ، بحيث $c = r a + s b$ إذا وفقط إذا كان $d \mid c$ (حيث (a , b) يرمز للقاسم المشترك الأعظم للعنصرين a , b في R) .

٢١٦. ليكن R حلقة ابدالية ، وليكن $1 \in R$. ليكن $p \in R \setminus \{0\}$. برهن أن p يكون عنصر غير مختزل (irreducible) $\Leftrightarrow$ $p u$ يكون عنصر غير مختزل (irreducible) لكل وحدة $u \in R$.

٢١٧. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن كل عنصر من العنصرين $2 - i\sqrt{5}$, $2 + i\sqrt{5}$ يكون غير مختزل وغير أولي .

٢١٨. أوجد كل الوحدات في الحلقة $\mathbf{Z}[i\sqrt{n}]$ ، حيث $n \in \mathbf{N}$.

٢١٩. في الحلقة $\mathbf{Z}[i]$ أوجد $(2 + 7i , 2 - 11i)$.

٢٢٠. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ أوجد $(2 , 1 + i\sqrt{5})$.

٢٢١. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن $(6 (1 - i\sqrt{5}) , 18)$ غير موجود .

٢٢٢. ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $d = (x , y)$. إذا كان $r \in R\backslash\{0\}$ ، فاثبت أن $r\,d = (r\,x , r\,y)$.

٢٢٣. ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $m = \text{l.c.m.}(x , y)$. إذا كان $r \in R\backslash\{0\}$ ، فاثبت أن $r\,m = \text{l.c.m.}(r\,x , r\,y)$.

٢٢٤. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن العنصر 3 لا يكون شريك (associate) لكل من العنصرين $2 + i\sqrt{5} , 2 - i\sqrt{5}$.

٢٢٥. في الحلقة $\mathbf{Z}[\sqrt{5}]$ اثبت أن

(أ) $2 - \sqrt{5}$ يكون وحدة .

(ب) كل من $1 - \sqrt{5} \;,\; 3 + \sqrt{5}$ لا يكون وحدة .

(ت) $1 - \sqrt{5} \sim 3 + \sqrt{5}$.

(ث) العناصر $3 - \sqrt{5} \;,\; 2 , 3 + \sqrt{5}$ تكون غير مختزلة .

٢٢٦. ليكن $n \in \mathbf{N}\backslash\{0,1\}$ ، $N : \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$ بحيث $N(a + b\sqrt{n}) = a^2 - n\,b^2$ لكل $a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$. برهن أن

(أ) N يحفظ عملية الضرب .

(ب) $N(x) = \pm 1 \Leftrightarrow x$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{n}]$.

(ت) إذا كان $N(x)$ عدد أولي ، فإن x يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{n}]$.

٢٢٧. أوجد $(\mathbf{Z}[\sqrt{-n}])^*$ ، عندما $n > 1 , n = 1$.

٢٢٨. في الحلقة $\mathbf{Z}[i]$ ، حلل كل عدد من الأعداد $2 , 3 , 5$ إلى حاصل ضرب عناصر غير مختزلة (irreducible) .

٢٢٩. في الحلقة $\mathbf{Z}[\sqrt{10}]$ اثبت أن العناصر $4 - \sqrt{10} \;,\; 4 + \sqrt{10} \;,\; 2 , 3$ تكون غير مختزلة وغير أولية .

٢٣٠. في الحلقة $\mathbf{Z}[i]$ أوجد كل العناصر الشريكة للعنصر $3 - 2i$.

٢٣١. في الحلقة $\mathbf{Z}[i\sqrt{3}]$ أوجد كل العناصر الشريكة للعنصر $2 + i\sqrt{3}$.

٢٣٢. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ أوجد كل العناصر الشريكة للعنصر $2 + i\sqrt{5}$.

٢٣٣. في الحلقة $\mathbf{Z}_{12}$ أوجد كل العناصر الشريكة للعنصر 8 .

٢٣٤. في الحلقة $\mathbf{Z}_{10}$ أوجد كل العناصر الشريكة للعنصر 6 .

٢٣٥. ليكن R حلقة متلاشية القوى (nilpotent ring) ، وليكن $f : R \to S$ تشاكل حلقي .
برهن أن

(أ) كل حلقة جزئية من R تكون متلاشية القوى .

(ب) $f(R)$ تكون حلقة متلاشية القوى .

٢٣٦. ليكن R حلقة ، وليكن I مثالي في R . إذا كان كل من $I , R / I$ حلقة متلاشية القوى (nilpotent ring) ، فبرهن أن R تكون حلقة متلاشية القوى (nilpotent ring) .

المثاليات – Ideals

٢٣٧. ليكن R حلقة خالية من قواسم الصفر . إذا كانت كل حلقة جزئية من R مثالي ، فاثبت أن R تكون حلقة ابدالية .

٢٣٨. اثبت أنة يوجد بالضبط تشاكلين حلقيين من **R** إلى **R** .

٢٣٩. ليكن R حلقة ، وليكن A,B,C مثاليات في R . إذا كان

$$A : B = \{ r \in R \mid rB \subseteq A\}$$

، فبرهن أن

(أ) $A : B$ يكون مثالي في R .

(ب) $A \subseteq A : B$.

(ت) إذا كان $\{A_i\}_{i \in I}$ فصل مثاليات في R ، فإن

$$(\cap_{i \in I} A_i) : B = \cap_{i \in I} (A_i : B)$$

(ث) إذا كان $\{B_i\}_{i \in I}$ فصل مثاليات في R ، فإن

$$A : \Sigma_{i \in I} B_i = \bigcap_{i \in I} (A : B_i)$$

(ج) $A : C\,B = (A : B) : C$.

٢٤٠. برهن أن $\mathbf{Z}[\sqrt{2}]$ يكون مثالي في الحلقة **R** مولد بالعنصرين $2+3\sqrt{2}$, $3+\sqrt{2}$.

٢٤١. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I هي مجموعة كل العناصر المتلاشية القوى (nilpotent elements) في R . برهن أن

(أ) I يكون مثالي في R .

(ب) R / I لا يحتوي على عناصر متلاشية القوى غير العنصر الصفري .

٢٤٢. ليكن R حلقة ، وليكن I , J مثاليين في R . برهن أن

$$R = I + J \iff x + I \cap y + J \neq \emptyset \;\; , \forall\, x,y \in R$$

٢٤٣. ليكن R حلقة ابدالية ، بحيث $1 \in R$. وليكن I , J مثاليين غير صفريين في R ، بحيث $I + J = R$, $I \cap J = \{0\}$. برهن أن $R \cong I \times J$.

٢٤٤. ليكن R حلقة ، وليكن $a \in R$ عنصر ثابت . ليكن $* : R \times R \to R$ بحيث $x * y = x\,a\,y$ لكل $x,y \in R$. برهن أن

(أ) $*$ تكون عملية ثنائية داخلية على R .

(ب) $R^{\wedge} = (R , + , *)$ يكون حلقة ، حيث + هي عملية الجمع على الحلقة R .

(ت) $I = \{x \in R \mid a\,x\,a = 0\}$ يكون مثالي في الحلقة $R^{\wedge}$.

(ث) ليكن $r \in R \setminus I$ ، بحيث $a\,r\,a = a$. إذن الحلقة $R^{\wedge}/ I$ تحتوي محايد .

٢٤٥. ليكن R حلقة وليكن $1 \in R$. وليكن I مثالي في حلقة المصفوفات $R^{n \times n}$. اثبت أنة يوجد مثالي J في R ، بحيث $I = J^{n \times n}$. أوجد كذلك كل المثاليات في الحلقة $(\mathbf{Z}/12\mathbf{Z})^{n \times n}$.

٢٤٦. ليكن R مجال متكامل (integral domain) ، وليكن $x,y \in R\setminus\{0\}$. برهن أن

$< x > \subset < y > \iff$ y قاسم فعلي (proper divisor) لـ x

٢٤٧. ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$\sqrt{I} = \{ x \in R \mid \exists n \in \mathbf{N} , s.t. \; x^n \in I\}$

($\sqrt{I}$ يسمى جذر I (radical of I) ويسمى أيضاً جذر تلاشي I (nil radical of I))

برهن أن

(أ) $\sqrt{I}$ يكون مثالي في R ويحتوي I .

(ب) $\sqrt{(\sqrt{I})} = \sqrt{I}$.

٢٤٨. ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي . ليكن I , J مثاليين في R , S على الترتيب . برهن أن

(أ) $f(\sqrt{I}) \subseteq \sqrt{f(I)}$ ، ويحدث التساوي إذا كان f شامل و $Ker(f) \subseteq I$.

(ب) $\sqrt{f^{-1}(J)} = f^{-1}(\sqrt{J})$.

٢٤٩. ليكن R حلقة ابدالية تحتوي محايد . برهن أن $R[x] / < x > \; \cong R$.

المثاليات العظيمة Maximal ideals

٢٥٠. اثبت أن أي مثالي غير بديهي في الحلقة $\mathbf{Z}_{15}$ يكون مثالي عظيم (maximal ideal) .

٢٥١. إذا كان p عدد أولي قاسم للعدد $n \in \mathbf{N}$ ، فاثبت أن $< \bar{p} >$ يكون مثالي عظيم في الحلقة $\mathbf{Z}_n$.

٢٥٢. أوجد كل المثاليات العظيمة في $\mathbf{Z}_n$ ، ثم أوجد تقاطعها .

٢٥٣. ليكن R مجال متكامل غير منتهي يحتوي على عدد منتهي من الوحدات . برهن أن R يحتوي على عدد غير منتهي من المثاليات العظيمة .

٢٥٤. ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$\sqrt{I} = \{ x \in R \mid \exists n \in \mathbf{N} , s.t. \; x^n \in I\}$

($\sqrt{I}$ يسمى جذر I (radical of I) ويسمى أيضاً جذر تلاشي I (nil radical of I))

برهن أن

(أ) إذا كان I مثالي عظيم في R ، فإن $\sqrt{I} = I$.

(ب) ليكن $\sqrt{I}$ مثالي عظيم في R ، وليكن $x,y \in R$ بحيث $x\,y \in I\,,\, y \notin \sqrt{I}$. إذن $x \in I$.

٢٥٥. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I , J مثاليين عظيمين مختلفين في R . برهن أن

(أ) $I + J = R$

(ب) $I \cap J = I\,J$

(ت) $R / I\,J \cong R / I \times R / J$

المثاليات الأولية Prime ideals

٢٥٦. ليكن R مجال متكامل (integral domain) . وليكن لكل مثاليين I , J في R ، بحيث $I \subseteq J$ يوجد مثالي K في R ، بحيث $I = J\,K$. برهن أن كل مثالي أولي غير صفري في R يكون مثالي عظيم .

٢٥٧. ليكن R حلقة ابدالية وتحتوي محايد ، بحيث كل عنصر في أي حلقة قسمة لـ R يكون قاسم للصفر أو وحدة . برهن أن أي مثالي أولي في R يكون مثالي عظيم .

٢٥٨. ليكن R حلقة ابدالية وتحتوي محايد . ليكن $x,y \in R\backslash\{0\}$ ، بحيث يكون x عنصر غير قاسم للصفر وبحيث $R\,x \subseteq R\,y \neq R$. إذا كان كل من $R\,x\,,\, R\,y$ مثالي أولي ، فاثبت أن $R\,x = R\,y$.

٢٥٩. ليكن R حلقة ابدالية وتحتوي محايد . ليكن $n \in \mathbf{N}\,,\, n > 2$ ، بحيث $x^n = x$ لكل $x \in R$. برهن أن كل مثالي أولي في R يكون مثالي عظيم .

٢٦٠. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I مثالي في R . إذا كان

$$J_x = \{\, r \in R \mid r\,x = 0 \,\} \;\;, x \in I$$

فبرهن أن

(أ) J_x يكون مثالي في R ، لكل $x \in I$.

(ب) كل عنصر عظيم (بالنسبة لعلاقة الإحتواء $\subseteq$) في المجموعة $S = \{\, J_x \mid x \in I \setminus \{0\} \,\}$ يكون مثالي أولي في R .

٢٦١. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S هي مجموعة كل المثاليات غير منتهية التوليد في R . برهن أن كل عنصر عظيم (maximal element) (بالنسبة لعلاقة الإحتواء $\subseteq$) في S يكون مثالي أولي في R .

٢٦٢. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S مجموعة جزئية غير خالية من R ، بحيث تكون مغلقة بالنسبة لعملية الضرب على R . ليكن I مثالي في R بحيث $I \cap S = \emptyset$. برهن أنة يوجد مثالي أولي P في R بحيث $P \cap S = \emptyset$, $I \subseteq P$.

٢٦٣. ليكن R حلقة ابدالية وتحتوي محايد . برهن أن
كل مثالي في R يكون مثالي رئيس (principal ideal) $\Leftrightarrow$ كل مثالي أولي في R يكون مثالي رئيس

٢٦٤. في الحلقة $\mathbf{Z}[x]$ اثبت أن المثالي الرئيس $< x >$ يكون أولي ولا يكون عظيم .

٢٦٥. ليكن R حلقة ابدالية تحتوي على محايد ، وليكن P مثالي أولي في R . برهن أن $\sqrt{P} = P$.

المثاليات الإبتدائية Primary ideals

٢٦٦. ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي .

(أ) ليكن Q مثالي ابتدائي في R وليكن f شامل و $Ker(f) \subseteq Q$. برهن أن $f(Q)$ يكون مثالي ابتدائي في S .

(ب) ليكن Q' مثالي ابتدائي في S . برهن أن $f^{-1}(Q')$ يكون مثالي ابتدائي في R .

٢٦٧. في الحلقة $\mathbf{Z}[x]$ برهن أن $< x^2 >$ يكون مثالي ابتدائي وأن $< x >$ هو المثالي الأولي المناظر لة (associated prime ideal) .

٢٦٨. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I , J , Q مثاليات في R بحيث Q يكون مثالي ابتدائي . برهن أن

(أ) إذا كان $I \not\subset \sqrt{Q}$, $I J \subseteq Q$ ، فإن $J \subseteq Q$.

(ب) إذا كان J منتهي التوليد و $I J \subseteq Q$ ، فإن $I \subseteq Q$ أو يوجد $n \in \mathbf{N}$ بحيث $J^n \subseteq Q$.

الحلقات النوثيرية والحلقات الأرتينية

Noetherian rings and Artinian rings

٢٦٩. ليكن R حلقة ابدالية وتحتوي محايد . برهن أن

R تكون حلقة نوثيرية (Noetherian ring) $\Leftrightarrow$ كل مثالي أولي في R يكون منتهي التوليد

٢٧٠. ليكن R حلقة نوثيرية (Noetherian ring) ، وليكن $f : R \to R$ تشاكل حلقي شامل . برهن أن f يكون متباين .

٢٧١. ليكن R حلقة نوثيرية (Noetherian ring) ابدالية . برهن أن مجموع كل المثاليات المتلاشية القوى (nilpotent ideals) في R يكون مثالي متلاشي القوى أيضاً في R .

٢٧٢. اثبت أن الحلقة الجزئية من حلقة نوثيرية (Noetherian ring) لا تكون بصفة عامة حلقة نوثيرية .

٢٧٣. ليكن R حلقة نوثيرية . إذا كان I مثالي في R ، فاثبت أن الحلقة R / I تكون حلقة نوثيرية .

٢٧٤. ليكن R حلقة ابدالية تحتوي محايد . إذا كانت حلقة كثيرات الحدود R[x] حلقة نوثيرية ، فبرهن أن R تكون حلقة نوثيرية .

٢٧٥. اذكر مثالاً لحلقة نوثيرية وغير أرتينية .

٢٧٦. اذكر مثالاً لحلقة أرتينية وغير نوثيرية .

٢٧٧. اذكر مثالاً لحلقة أرتينية تحتوي على حلقة جزئية غير أرتينية .

٢٧٨. اذكر مثالاً لحلقة غير أرتينية تحتوي على حلقة جزئية أرتينية .

٢٧٩. اذكر مثالاً لحلقة غير نوثيرية وغير أرتينية .

٢٨٠. اذكر مع الاثبات حلقة نوثيرية يمينية وغير نوثيرية شمالية .

حلول التمارين

أولاً: حلول تمارين الزمر

الزمر والزمر الجزئية – Groups and subgroups

١. ليكن G زمرة ، وليكن $x,y\in G$ بحيث $x^2 = 1$, $x\, y^4\, x = y^7$. اثبت أن $y^{33} = 1$.

الحل: ليكن G زمرة ، وليكن $x,y\in G$ بحيث $x^2 = 1$, $x\, y^4\, x = y^7$. بضرب المعادلة $x\, y^4\, x = y^7$ من اليمين واليسار في x نحصل على $x\, y^7\, x = y^4$. إذن $x\, y^{28}\, x = y^{49}$. كذلك $x\, y^{28}\, x = y^{16}$. إذن $y^{49} = y^{16}$. إذن $y^{-16}\, y^{49} = 1$. إذن $y^{33} = 1$.

٢. ليكن G زمرة ، وليكن $x,y\in G$ بحيث $y^{-1}\, x^2\, y = x^3$, $x^{-1}\, y^2\, x = y^3$.
اثبت أن $x = y = 1$.

الحل: ليكن G زمرة ، وليكن $x,y\in G$ بحيث

$$x^{-1}\, y^2\, x = y^3 \qquad (1)$$

$$y^{-1}\, x^2\, y = x^3 \qquad (2)$$

إذن من (2) نحصل على

$$x^{18} = (y^{-1}\, x^2\, y)^6 = y^{-1}\, x^{12}\, y = y^{-1}\, (x^3)^4\, y = y^{-1}\, (y^{-1}\, x^2\, y)^4\, y = y^{-2}\, x^8\, y^2 \quad (3)$$

كذلك نحصل من (2) على $x^{27} = (y^{-1}\, x^2\, y)^9 = y^{-1}\, x^{18}\, y$.إذن من (3) نحصل على

$$x^{27} = y^{-1}\, (y^{-2}\, x^8\, y^2)\, y = y^{-3}\, x^8\, y^3 \qquad (4)$$

أيضاً من (3) يكون $y^2\, x^{18} = x^8\, y^2$. بضرب طرفي هذة المعادلة من اليمين في x نحصل على $y^2\, x^{19} = x^8\, y^2\, x$. إذن من (1) نحصل على

$$y^2\, x^{19} = x^8\, y^2\, x = x^8\, (x\, y^3\, x^{-1})\, x = x^9\, y^3 \qquad (5)$$

لكن من (4) يكون $y^3\, x^{27} = x^8\, y^3$. وبضرب طرفي هذة المعادلة من اليسار في x نحصل على $x^9\, y^3 = x\, y^3\, x^{27}$. لكن من (1) يكون $x\, y^3 = y^2\, x$. إذن من (5) نحصل على

$$y^2\, x^{19} = x^9\, y^3 = y^2\, x\, x^{27} = y^2\, x^{28}$$

إذن $x^{19} = x^{28}$. إذن $x^9 = 1$. إذن $x^{27} = 1$. إذن ينتج من $x^9\, y^3 = x\, y^3\, x^{27}$ أن $x = 1$. بالتالي ينتج من (1) أن $y = 1$.

٣. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x^2\, y = y\, x$, $x^4 = 1$. اثبت أن $x = 1$.

الحل: بما أن $x^2\, y = y\, x$ ، فإن $x = y^{-1}\, x^2\, y$. إذن $x^2 = y^{-1}\, x^4\, y$. لكن $x^4 = 1$. إذن $x^2 = 1$. إذن $y = y\, x$. إذن $x = 1$.

٤. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x^{-1}\, y^2\, x = y^3$, $x^2 = 1$. اثبت أن $y^5 = 1$.

الحل: بما أن $x^{-1}\, y^2\, x = y^3$. فإن $y^2 = x\, y^3\, x$. إذن $y^{-2} = x\, y^{-3}\, x$. لأن $x^{-1} = x$ ، وذلك من الفرض بأن $x^2 = 1$. إذن $y = y^{-2}\, y^3 = x\, y^{-1}\, x$. إذن $y^2 = x\, y^{-2}\, x$. إذن $x\, y^3\, x = x\, y^{-2}\, x$. إذن $y^3 = y^{-2}$. إذن $y^5 = 1$.

٥. ليكن G زمرة ، وليكن $x,y,z \in G$ بحيث

$$x^2 = z^{-1}\, x\, z \quad , \quad y^2 = x^{-1}\, y\, x \quad , \quad z^2 = y^{-1}\, z\, y$$

اثبت أن $x = y = z = 1$.

الحل: ليكن $x,y,z \in G$ ، بحيث

$$x^2 = z^{-1}\, x\, z \qquad (1)$$

$$y^2 = x^{-1}\, y\, x \qquad (2)$$

$$z^2 = y^{-1}\, z\, y \qquad (3)$$

من (3) ينتج أن

$$y\, z^2 = z\, y \qquad (4)$$

ومن (4) ينتج أن

$$y\, z = z\, y\, z^{-1} \qquad (5)$$

إذن

$$(y\, z)^4 = z\, y^4\, z^{-1} \qquad (6)$$

من (2) نحصل على $y^4 = x^{-1}\, y^2\, x$. وبالتعويض في هذة المعادلة عن y من (2) نحصل على

$$y^4 = x^{-2}\, y\, x^2 \qquad (7)$$

بالتعويض من (7) في (6) نحصل على

$$(y\,z)^4 = z\,(x^{-2}\,y\,\,x^2)\,z^{-1} =^{(1)} z\,(z^{-1}\,x^{-1}\,z)\,y\,(z^{-1}\,x\,z)\,z^{-1}$$
$$= x^{-1}\,(z\,y\,z^{-1})\,x =^{(5)} x^{-1}\,y\,z\,x = (x^{-1}\,y\,x)\,(x^{-1}\,z\,x) =^{(2)} y^2\,x^{-1}\,z\,x$$
$$= y^2\,x^{-1}\,z\,x\,x\,x^{-1} = y^2\,x^{-1}(z\,x^2)\,x^{-1} =^{(1)} y^2\,x^{-1}\,(x\,z)\,x^{-1} = y^2\,z\,x^{-1}$$

إذن

$$x^{-1} = z^{-1}\,y^{-2}\,(y\,z)^4 = z^{-1}\,y^{-1}\,z\,(y\,z)^3 = z^{-1}\,y^{-1}\,(z\,y)\,z\,(y\,z)^2 =^{(4)} z^2\,(y\,z)^2$$
$$= z\,(z\,y)\,(z\,y)\,z =^{(4)} z\,(y\,z^2)\,(y\,z^2)\,z = (z\,y)\,z\,(z\,y)\,z^3$$
$$=^{(4)} (y\,z^2)\,z\,(y\,z^2)\,z^3 = y\,z^2\,(z\,y)\,z^5 = (y\,z^2)\,(y\,z^2)\,z^5 = y\,z\,(z\,y)\,z^7$$
$$=^{(4)} y\,z\,(y\,z^2)\,z^7 = y\,(z\,y)\,z^9 =^{(4)} y\,(y\,z^2)\,z^9 = y^2\,z^{11}$$

إذن $x = z^{-11}\,y^{-2}$. إذن بالتعويض عن $x\,,\,x^{-1}$ في (2) نحصل على $y^2 = y^2\,z^{11}\,y\,z^{-11}\,y^{-2}$.
وبضرب طرفي هذه المعادلة من اليمين في y^2 ومن اليسار في y^{-2} نحصل على

$$y^2 = z^{11}\,y\,z^{-11} \qquad (8)$$

من (3) يكون

$$z\,y\,z^{-1} = y\,z \qquad (9)$$

بالتعويض المتكرر من (9) في (8) نحصل على $y^2 = y\,z^{11}$. وبالتالي يكون $y = z^{11}$. إذن من (8) يكون $y^2 = z^{11}$. إذن $y = 1$. بالتالي ينتج من (3) أن $z = 1$. إذن من (1) يكون $x = 1$.

٦. ليكن G زمرة بحيث $x^2 = 1$ ، لكل $x \in G$. اثبت أن G تكون ابدالية .

الحل: ليكن G زمرة بحيث $x^2 = 1$ ، لكل $x \in G$. ليكن $x,y \in G$. إذن $x^2 = y^2 = 1$. إذن $x^{-1} = x\,,\,y^{-1} = y$. إذن $x\,y = (x\,y)^{-1} = y^{-1}\,x^{-1} = y\,x$. إذن G تكون ابدالية.

٧. ليكن G زمرة ، وليكن $(x\,y)^2 = x^2\,y^2$ لكل $x,y \in G$. برهن أن G تكون ابدالية .

الحل: ليكن G زمرة ، وليكن $(x\,y)^2 = x^2\,y^2$ لكل $x,y \in G$. إذن لكل $x,y \in G$ يكون $x\,y = (x\,y)^{-1}\,(x\,y)^2 = y^{-1}\,x^{-1}\,x^2\,y^2$. إذن $x = y^{-1}\,x\,y$. إذن $y\,x = x\,y$. إذن G تكون ابدالية.

٨. ليكن G زمرة ، وليكن $x,y,z \in G$. أوجد عنصر $g \in G$ بحيث $x\,g\,y = z$. هل العنصر g يكون وحيداً ؟

الحل: ليكن G زمرة ، وليكن $x,y,z\in G$. العنصر $g\in G$ بحيث $x\,g\,y = z$ هو $g = x^{-1} z\, y^{-1}$. وهو وحيد لأن: نفرض أن $h\in G$ ، بحيث $x\,h\,y = z$. إذن $h = x^{-1} z\, y^{-1}$. إذن $h = g$.

٩. ليكن G زمرة منتهية ، وليكن $x\in G$. اثبت أنة يوجد $n\in \mathbf{N}$ بحيث $x^n = 1$.

الحل: ليكن G زمرة منتهية ، وليكن $x\in G$. إذا كان $x = 1$ ، فإن $n = 1$. أي أن المطلوب متحقق عندما $x = 1$. نفرض أن $x \neq 1$. بما أن G مغلقة بالنسبة لعملية الضرب ، فإن $x,x^2,x^3,\ldots\in G$. لاحظ أن $x^i \neq x^{i+1}$ لكل i ، لأنة إذا كان $x^i = x^{i+1}$ ، فإن $x = 1$. وهذا يناقض الفرض بأن $x \neq 1$. بما أن G منتهية ، فإنة يوجد $m,m'\in \mathbf{N}$ بحيث $x^m = x^{m'}$, $m > m' + 1$. إذن $m = m' + n$ ، بحيث $n \geq 2$. إذن $m - m' = n$. إذن $x^n = x^{m - m'} = x^m x^{-m'} = 1$.

١٠. ليكن G زمرة منتهية ، وليكن $x\in G$. اثبت أن $\mathrm{ord}(x) \leq |G|$.

الحل: ليكن G زمرة منتهية ، وليكن $x\in G$. ليكن $\mathrm{ord}(x) = m$. إذن m هو أصغر عدد صحيح موجب بحيث $x^m = 1$. إذا كان $x = 1$ ، فإن $\mathrm{ord}(x) = 1$. وبالتالي يتحقق المطلوب . نفرض أن $x \neq 1$. إذن $1,x,x^2,\ldots,x^{m-1}\in G$. لكن $1,x,x^2,\ldots,x^{m-1}$ عناصر مختلفة وعددها m . إذن $\mathrm{ord}(x) = m \leq |G|$.

١١. ليكن G زمرة منتهية ، وليكن $x,y\in G$. اثبت أن

(أ) $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$

(ب) $\mathrm{ord}(y\,x\,y^{-1}) = \mathrm{ord}(x)$

(ت) $\mathrm{ord}(x\,y) = \mathrm{ord}(y\,x)$

الحل: ليكن G زمرة منتهية ، وليكن $x,y\in G$. ليكن $\mathrm{ord}(x) = n$.

(أ) بما أن $x^n = 1$ ، فإن $(x^{-1})^n = x^{-n} = 1$. ليكن $0 < m < n$ ، بحيث $(x^{-1})^m = 1$. إذن $x^{n-m} = x^n = 1$. لكن $n-m < n$ ، وهذا يتناقض مع الفرض $\mathrm{ord}(x) = n$. إذن لا يوجد عدد صحيح موجب m أقل من n بحيث $(x^{-1})^m = 1$. إذن $\mathrm{ord}(x^{-1}) = n$. إذن $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$.

(ب) $(y\,x\,y^{-1})^n = y\,x^n\,y^{-1} = 1$. ليكن $0 < m < n$ ، بحيث $(y\,x\,y^{-1})^m = 1$. إذن
$y\,x^m\,y^{-1} = 1$. بضرب طرفي هذة المعادلة من اليمين في y ومن اليسار في y^{-1} نحصل على
$x^m = 1$. وهذا يتناقض مع الفرض $ord(x) = n$. إذن n هو أصغر عدد صحيح موجب بحيث
$(y\,x\,y^{-1})^n = 1$. إذن $ord(y\,x\,y^{-1}) = n = ord(x)$.

(ت) ليكن $ord(x\,y) = m$. إذن $(x\,y)^m = 1$. من (أ) ينتج أن
$ord((x\,y)^{-1}) = ord(x\,y) = m$. ليكن $ord(yx) = m'$. إذن $(yx)^{m'} = 1$. من (أ) ينتج
أن $ord((y\,x)^{-1}) = ord(y\,x) = m'$.

$$(x\,y)^m = 1 \;\Rightarrow\; x\,y\,(x\,y)^{m-2}\,x\,y = 1 \;\Rightarrow\; y\,(x\,y)^{m-2}\,x = (y\,x)^{-1}$$
$$\Rightarrow\; y\,(x\,y)(x\,y)^{m-3}\,x = (y\,x)^{-1} \;\Rightarrow y\,(x\,y)^{m-3}\,x = (y\,x)^{-2}$$
$$\Rightarrow \ldots \Rightarrow\; y\,x = (y\,x)^{-(m-1)} \;\Rightarrow\; (y\,x)^{-m} = 1 \Rightarrow (y\,x)^m = 1$$
$$\Rightarrow\; m' \le m\,.$$

بنفس الطريقة نحصل على

$$(y\,x)^{m'} = 1 \;\Rightarrow\; (x\,y)^{m'} = 1 \;\Rightarrow\; m \le m'$$

إذن $m = m'$. إذن $ord(x\,y) = ord(y\,x)$.

١٢. ليكن G زمرة منتهية ، وليكن $x,y \in G$.

(أ) إذا كان $x\,y = y^5\,x^3$ ، فاثبت أن $ord(y\,x^{-1}) = ord(y^5\,x) = ord(y^3\,x^3)$

(ب) الحالة العامة لـ (أ) : إذا كان $x\,y = y^m\,x^n$ حيث $m - n = 2$ ، فاثبت أن

$$ord(y\,x^{-1}) = ord(y^m\,x^{n-2}) = ord(y^n\,x^n)$$

الحل: ليكن G زمرة منتهية ، وليكن $x,y \in G$.

(أ) ليكن $x\,y = y^5\,x^3$. إذن $y^5\,x = x\,y\,x^{-2}$. إذن ينتج من تمرين (١١) (ت) أن

$$ord(y^5\,x) = ord((x\,y\,x^{-1})\,x^{-1}) = ord(x^{-1}(x\,y\,x^{-1})) = ord(y\,x^{-1})$$

كذلك ينتج من الفرض $x\,y = y^5\,x^3$ أن $y^3\,x^3 = y^{-2}\,x\,y$. إذن ينتج من تمرين (١١) (أ) أن

$$ord(y^3\,x^3) = ord(y^{-1}\,(y^{-1}\,x\,y)) = ord((y^{-1}\,x\,y)\,y^{-1}) = ord(y^{-1}\,x) = ord(x^{-1}\,y) = ord(y\,x^{-1})$$

إذن $ord(y\,x^{-1}) = ord(y^5\,x) = ord(y^3\,x^3)$.

(ب) ليكن $x\,y = y^m x^n$ ، حيث $m - n = 2$. إذن $y^m x^{n-2} = x\,y\,x^{-2}$. إذن

$$\mathrm{ord}(y^m x^{n-2}) = \mathrm{ord}((x\,y\,x^{-1})\,x^{-1}) = \mathrm{ord}(y\,x^{-1})$$

وبما أن $x\,y = y^m x^n$ ، فإن $y^m x^n = y^{-(m-n)}\,x\,y$. إذن $y^n x^n = y^{-2}\,x\,y$. إذن

$$\begin{aligned}\mathrm{ord}(y^n x^n) &= \mathrm{ord}(y^{-2}\,x\,y) = \mathrm{ord}(y^{-1}\,(y^{-1}\,x\,y)) \\ &= \mathrm{ord}(y^{-1}\,x) = \mathrm{ord}(x\,y^{-1}) = \mathrm{ord}(y\,x^{-1})\end{aligned}$$

إذن $\mathrm{ord}(y\,x^{-1}) = \mathrm{ord}(y^m x^{n-2}) = \mathrm{ord}(y^n x^n)$.

١٣. ليكن G زمرة منتهية ، وليكن $x \in G$ ، بحيث $\mathrm{ord}(x) = n$. إذا كان $m \in \mathbf{N}$ بحيث $(m , n) = 1$ ، $1 \le m \le n$ ، فاثبت أن $\mathrm{ord}(x^m) = n$.

الحل: ليكن G زمرة منتهية ، وليكن $x \in G$ ، بحيث $\mathrm{ord}(x) = n$. ليكن $m \in \mathbf{N}$ بحيث $(m , n) = 1$ ، $1 \le m \le n$. إذن $m < n$. إذن $x^m \ne 1$. بما أن $(x^m)^n = x^{m\,n} = (x^n)^m = 1$ ، فإن $\mathrm{ord}(x^m) \le n$. نفرض أن $\mathrm{ord}(x^m) = p < n$. بما أن $(m , n) = 1$ ، فإنة يوجد $m',n' \in \mathbf{Z}$ ، بحيث $1 = m'\,m + n'\,n$. إذن $p = m'\,m\,p + n'\,n\,p$. إذن

$$x^p = x^{m'\,m\,p + n'\,n\,p} = ((x^m)^p)^{m'}\,(x^n)^{n'p} = 1$$

لكن هذا يتناقض مع الفرض بأن $\mathrm{ord}(x) = n$. إذن $\mathrm{ord}(x^m) = n$.

ملحوظة: المطلوب في هذا التمرين ينتج مباشرة بتطبيق المبرهنة التي تنص على أن

$$\mathrm{ord}(x^m) = \frac{\mathrm{ord}(x)}{(m,\mathrm{ord}(x))}$$

١٤. ليكن G زمرة منتهية ، وليكن $x \in G$ ، بحيث $\mathrm{ord}(x) = p$ حيث p عدد أولي . اثبت أن

(أ) $\mathrm{ord}(x^m) = p$ ، لكل $1 \le m < p$ ،

(ب) لكل $n \in \mathbf{N}$ يكون $x^n = 1$ أو $\mathrm{ord}(x^n) = p$.

الحل: ليكن G زمرة منتهية ، وليكن $x \in G$ ، بحيث $\mathrm{ord}(x) = p$ حيث p عدد أولي .

(أ) ليكن $m \in \mathbf{N}$ ، بحيث $1 \le m < p$. إذن $(m,p) = 1$. إذن ينتج من تمرين (١٣) أن $\mathrm{ord}(x^m) = p$ ، لكل $m \in \mathbf{N}$ ، بحيث $1 \le m < p$.

(ب) ليكن $n\in\mathbf{N}$. بما أن (مبرهنة) $ord(x^n) = \dfrac{ord(x)}{(n,ord(x))}$ ، فإن $ord(x^n) = \dfrac{p}{(n,p)}$.

لكن $(n , p) = p$ أو $(n , p) = 1$ ، لأن p عدد أولي . إذن $x^n= 1$ أو $ord(x^n) = p$.

١٥. اثبت أن $\mathbf{Z}_p \setminus \{\bar{0}\}$ تكون زمرة بالنسبة لعملية الضرب بقياس p ، حيث p عدد أولي .

الحل: ليكن p عدد أولي . ليكن $\bar{x},\bar{y} \in\mathbf{Z}_p \setminus\{\bar{0}\}$. إذن $(x,p) = 1 , (y,p) = 1$. بما أن $(x , p) = 1$ ، فإنة يوجد $a,b\in\mathbf{Z}$ ، بحيث $a x + b p = 1$. إذن $a x y + b p y = y$. نفرض أن $\bar{x}\,\bar{y} = \bar{0}$. إذن $xy \equiv 0 \pmod p$. إذن $p| x y$. لكن $a x y + b p y = y$. إذن $p | y$. وهذا يتناقض مع $(y,p) = 1$. إذن $\bar{x}\,\bar{y} \neq \bar{0}$. إذن $\bar{x}\,\bar{y} \in\mathbf{Z}_p\setminus\{\bar{0}\}$. إذن $\mathbf{Z}_p\setminus\{\bar{0}\}$ تكون مغلقة بالنسبة لعملية الضرب بقياس p . من الواضح أن $\bar{1} \in \mathbf{Z}_p\setminus\{\bar{0}\}$ ، وهو العنصر المحايد بالنسبة لعملية الضرب بقياس p . بما أن $a x + b p = 1$ ، فإن $a x - 1 = b' p$ (حيث $b' = -b$) . إذن $p | a x - 1$. إذن $a x \equiv 1 \pmod p$. إذن $\overline{a x} = \bar{1}$. إذن $\bar{a}\,\bar{x} =\bar{1}$. وبما أن عملية الضرب بقياس p ابدالية ، فإن $\bar{x}\,\bar{a} = \bar{1}$. إذن $\bar{a}$ يكون معكوس ضربي لـ $\bar{x}$. إذن $\mathbf{Z}_p\setminus\{\bar{0}\}$ تحتوي على معكوس ضربي لكل عنصر فيها . كذلك عملية الضرب بقياس p تكون دامجة . إذن $\mathbf{Z}_p\setminus\{\bar{0}\}$ تكون زمرة بالنسبة لعملية الضرب بقياس p .

١٦. (أ) ليكن $n\in\mathbf{N}$. اثبت أن $\mathbf{Z}_n^* = \{\bar{m} \in \mathbf{Z}_n | (m . n) = 1\}$ ، حيث $\mathbf{Z}_n^*$ هى مجموعة كل العناصر في $\mathbf{Z}_n$ التي لها معكوس بالنسبة لعملية الضرب بقياس n .

(ب) برهن أن $\mathbf{Z}_n^*$ تكون زمرة بالنسبة لعملية الضرب بقياس n .

(ت) أوجد $|\mathbf{Z}_{12}^*| , |\mathbf{Z}_{20}^*| , |\mathbf{Z}_{11}^*|$.

(ث) أوجد معكوس $\overline{19} , \bar{9}$ في $\mathbf{Z}_{20}^*$.

الحل: (أ) ليكن $n\in\mathbf{N}$ ، وليكن حيث $\mathbf{Z}_n^*$ هى مجموعة كل العناصر في $\mathbf{Z}_n$ التي لها معكوس بالنسبة لعملية الضرب بقياس n . إذن

$$\begin{aligned}
\bar{m} \in \mathbf{Z}_n^* &\Leftrightarrow \overline{m}\,\bar{a} = \bar{1} \ , \bar{a} \in \mathbf{Z}_n \\
&\Leftrightarrow m\,a \equiv 1 \pmod n \\
&\Leftrightarrow n \mid m\,a - 1 \\
&\Leftrightarrow m\,a - 1 = n\,b \ , a,b \in \mathbf{Z} \\
&\Leftrightarrow m\,a - n\,b = 1
\end{aligned}$$

$\Leftrightarrow\ (m,n) = 1$

$\Leftrightarrow\ \bar{m} \in \{\bar{m} \in \mathbf{Z}_n \mid (m,n)=1\}$

إذن $\mathbf{Z}_n^* = \{\bar{m} \in \mathbf{Z}_n | (m.n) = 1\}$.

(ب) ليكن $\bar{x}, \bar{y} \in \mathbf{Z}_n^*$. إذن $(x , n) = 1 , (y , n) = 1$. كما أثبتنا في التمرين السابق ، فإن $\bar{x}\,\bar{y} \neq \bar{0}$. ليكن $a \mid x\,y \;,\; a \mid n$. يوجد $a' , a'' \in \mathbf{N}$ ، بحيث $x\,y = a\,a' \;,\; n = a\,a''$. بما أن $(x , n) = 1$ ، فإنة يوجد $c,d \in \mathbf{Z}$ بحيث $c\,x + d\,n = 1$. إذن $c\,x\,y + d\,n\,y = y$. إذن $c\,a\,a' + d\,a\,a''\,y = y$. $a \mid n , a \mid y$. لكن $(y,n) = 1$. إذن $a = 1$. إذن $(xy , n) = 1$. إذن $\bar{x}\;\bar{y} \in \mathbf{Z}_n^*$. إذن $\mathbf{Z}_n^*$ تكون مغلقة بالنسبة لعملية الضرب بقياس n . من الواضح أن عملية الضرب بقياس n تكون دامجة وابدالية . بما أن $c\,x + d\,n = 1$. فإن $c\,x - 1 = d'\,n$ ، حيث $d' = -d$. إذن $n \mid c\,x - 1$. إذن $c\,x \equiv 1 \pmod n$. إذن $\bar{c}\,\bar{x} = \bar{1}$. إذن $\bar{c}$ يكون معكوس لـ $\bar{x}$ بالنسبة لعملية الضرب بقياس n . لكن $(c , n) = 1$. إذن $\bar{c} \in \mathbf{Z}_n^*$. إذن $\mathbf{Z}_n^*$ تكون زمرة ابدالية بالنسبة لعملية الضرب بقياس n .

(ت) لاحظ أن $\mathbf{Z}_p^* = \mathbf{Z}_p \backslash \{\bar{0}\}$ ، لكل عدد أولي p . إذن $|\mathbf{Z}_{11}^*| = 10$. كذلك

$$|\mathbf{Z}_{20}^*| = \phi(20) = 8 \;,\; |\mathbf{Z}_{12}^*| = \phi(12) = 4$$

حيث ϕ هي دالة ϕ لإويلر (Euler ϕ-function) ، أي أن $\phi(n) = |\{m \in \mathbf{Z} \mid (m , n) = 1\}|$.

(ث) ليكن $(\bar{9})^{-1} = \bar{x}$ في $\mathbf{Z}_{20}^*$. إذن $\bar{9}\,\bar{x} = \bar{1}$. إذن $\overline{9x} = \bar{1}$. إذن $9\,x \equiv 1 \pmod{20}$. إذن $20 \mid 9\,x - 1$. أصغر x يحقق هذا هو $x = 9$. إذن $\bar{x} = \bar{9}$.
بنفس الطريقة ينتج أن $(\overline{19})^{-1} = \overline{19}$.

١٧. ليكن G زمرة ابدالية ، وليكن $x,y \in G$ بحيث $\operatorname{ord}(x) = \operatorname{ord}(y) = 2 \;,\; x \neq y$.
برهن أن $|\langle x , y \rangle| = 4$.

الحل: ليكن G زمرة ابدالية ، وليكن $x,y \in G$ بحيث $\operatorname{ord}(x) = \operatorname{ord}(y) = 2 \;,\; x \neq y$. بما أن $\operatorname{ord}(x) = \operatorname{ord}(y) = 2$ ، فإن $1,x,y,xy \in \langle x , y \rangle$. لاحظ أن العناصر $1,x,y,xy$ مختلفة . بما أن G زمرة ابدالية ، فإن $y\,x = x\,y$. إذن $\langle x , y \rangle = \{1, x , y , x\,y\}$.
إذن $|\langle x , y \rangle| = 4$.

١٨. ليكن $G = \mathbf{R} \setminus \{-1\}$ ، وليكن $x * y = x + y + x\,y \quad , \quad \forall\, x,y\in G$. اثبت أن $*$ تكون عملية ثنائية داخلية على G وأن $(G , *)$ تكون زمرة إبدالية ، ثم أوجد $x\in G$ بحيث $5 * x * 6 = 17$.

الحل: ليكن $G = \mathbf{R} \setminus \{-1\}$ ، وليكن $x * y = x + y + x\,y , \forall\, x,y\in G$. نثبت أن $* : G \times G \to G$ حيث $*(x, y) = x * y$ ، لكل $x,y\in G$ يكون تطبيقاً (mapping) . ليكن $x,y\in G$. نبين أولاً أن $x * y\in G$. نفرض أن $x * y = -1$. إذن $(x+1)(y+1) = 0$. إذن $x = -1$ أو $y = -1$. لكن هذا يتناقض مع الفرض بأن $x,y\in G$. إذن $x * y \neq -1$. إذن $x * y\in G$. ليكن $(x,y),(x',y')\in G \times G$ ، بحيث $(x,y) = (x',y')$. إذن $x = x' , y = y'$. بالتالي $x * y = x' * y'$. إذن صورة كل عنصر في $G \times G$ بـ $*$ تكون وحيدة . إذن $*$ يكون تطبيق . إذن $*$ تكون عملية ثنائية داخلية على G . والآن نثبت أن $(G , *)$ تكون زمرة . ليكن $x,y,z\in G$. إذن

$$x * (y * z) = x + (y * z) + x\,(y * z)$$
$$= x + (y + z + y\,z) + x\,(y + z + y\,z) \qquad (1)$$
$$(x * y) * z = (x * y) + z + (x * y)\,z$$
$$= (x + y + x\,y) + z + (x + y + x\,y)\,z \qquad (2)$$

من (2) , (1) ينتج أن $(x * y) * z = x * (y * z)$. إذن $*$ تكون عملية دامجة . من الواضح أن $*$ تكون عملية ابدالية . كذلك $0\in G$ يكون عنصرا محايداً للعملية $*$ لأن $x = 0 * x = x * 0$ ، لكل $x\in G$. ليكن $x,y\in G$ ، بحيث $x * y = 0$. إذن $x + y + x\,y = 0$. إذن $x = -y/(1+y)$. إذن معكوس y في G بالنسبة للعملية $*$ هو $-y/(1+y)$ (لاحظ أن $y \neq -1$). إذن $(G , *)$ تكون زمرة إبدالية . ليكن $x\in G$ ، بحيث $5 * x * 6 = 17$. لاحظ أن $5^{-1} = -5/6 \;, 6^{-1} = -6/7$. إذن بضرب $5 * x * 6 = 17$ من الشمال في 5^{-1} ومن اليمين في 6^{-1} نحصل على

$$x = (-5/6) * 17 * (-6/7) = -4/7$$

١٩. ليكن G زمرة منتهية ، وليكن $|G| = n$. ليكن $m\in \mathbf{N}$ بحيث $(m , n) = 1$. اثبت أنة لكل $x\in G$ يوجد $y\in G$ ، بحيث $x = y^m$.

الحل: ليكن G زمرة منتهية ، وليكن $|G| = n$. ليكن $m\in\mathbf{N}$ بحيث $(m , n) = 1$. بما أن $(m , n) = 1$ ، فإنة يوجد $s,t\in\mathbf{Z}$ بحيث $m s + n t = 1$. إذن لكل $x\in G$ يكون

$$x = x^{m s + t} = x^{m s}\, x^{nt} = (x^s)^m\, (x^n)^t = (x^s)^m$$

لأن $x^{|G|} = 1$ ، لكل $x\in G$. إذن يوجد $y = x^s$ بحيث $x = y^m$.

٢٠. ليكن F حقل ، وليكن $n\in\mathbf{N}$, $GL(n,F) = \{A\in F^{(n\times n)} \mid |A| \neq 0\}$.

(أ) اثبت أن $GL(n,F)$ تكون زمرة غير ابدالية بالنسبة لعملية ضرب المصفوفات (تسمى الزمرة الخطية العامة (general linear group) من الدرجة n فوق F) .

(ب) إذا كان $|F| = p^m$ ، حيث p عدد أولي ، فأوجد $|GL(n,F)|$.

(ت) ليكن $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle|\ a.b \in \mathbf{R} ,\ a^2 + b^2 \neq 0 \right\}$. اثبت أن G تكون زمرة جزئية ابدالية من الزمرة $GL(2,\mathbf{R})$.

الحل: (أ) ليكن $A,B\in GL(n,F)$. بما أن $|AB| = |A|\,|B| \neq 0$ ، فإن $AB\in GL(n,F)$. إذن $GL(n,F)$ تكون مغلقة بالنسبة لعملية ضرب المصفوفات . بما أن $|A| \neq 0$ ، فإن A يوجد لها معكوس A^{-1} في $GL(n,F)$. ليكن I مصفوفة الوحدة من الدرجة $n\times n$ فوق F . بما أن $|I| \neq 0$ ، فإن $I\in GL(n,F)$. بما أن $|A| \neq 0$ ، فإن $|A^{-1}| \neq 0$. إذن $A^{-1}\in GL(n,F)$. كذلك ضرب المصفوفات عملية غير ابدالية ودامجة . إذن $GL(n,F)$ تكون زمرة غير ابدالية بالنسبة لعملية ضرب المصفوفات عنصرها المحايد هو I .

(ب) ليكن $A\in GL(n,F)$. إذن متجهات أعمدة A تكون مستقلة خطياً وعددها n . إذن مجموعة متجهات أعمدة (أو صفوف) A تكون أساس للفضاء المتجة F^n فوق F . وبالعكس ، كل أساس للفضاء المتجة F^n يكون مصفوفة أعمدتها (أو صفوفها) هي متجات هذا الأساس ولها معكوس ، وبالتالي تنتمي إلى $GL(n,F)$. إذن عدد عناصر الزمرة $GL(n,F)$ يساوي عدد الأساسات المختلفة للفضاء المتجة F^n . ليكن $|F| = p^m$ ، حيث p عدد أولي . نضع $|F| = q$. ليكن $\{v_1,v_2,\ldots,v_n\}$ أساس للفضاء المتجة F^n . بالتالي $v_1,v_2,\ldots,v_n$ تكون أعمدة (أو صفوف) لمصفوفة ما في $GL(n,F)$. عدد إختيارات المتجة v_1 بمتجهات غير صفرية في F^n هو $q^n - 1$. وعدد إختيارات المتجة v_2 (لأي أختيار لـ v_1) بمتجهات غير صفرية في F^n بحيث يكون v_1, v_2 مستقلين خطياً (أي $v_2 \neq av_1$, $a\in F$) هو $q^n - q$. وعدد إختيارات المتجة v_3

(لأي أختيار لـ v_1,v_2) بمتجهات غير صفرية في F^n بحيث يكون v_1, v_2, v_3 مستقلة خطياً (أي أن أي اختيار لـ v_3 لا يكون في الصورة $a_1v_1+a_2v_2$ حيث $a_1,a_2 \in F$) هو $q^n - q^2$.

بالأستمرار بهذة الطريقة نحصل على الأساسات المختلفة لـ F^n وعددها يساوي

$$(q^n - 1)(q^n\ q)(q^n - q^2) \ldots (q^n - q^{n-1})$$

إذن $|GL(n,F)| = (q^n - 1)(q^n\ q)(q^n - q^2) \ldots (q^n - q^{n-1})$

(ت) ليكن $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a.b \in \mathbf{R} .\ a^2 + b^2 \neq 0 \right\}$. نفرض أن $A,B \in G$. ليكن $A= \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B= \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$. إذن

$$AB = BA = \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix}$$

بما أن $(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2) \neq 0$ ، فإن $|AB| \neq 0$. إذن $AB \in G$.

إذن G تكون مغلقة بالنسبة لعملية ضرب المصفوفات وابدالية. من الواضح أن $I \in G$ ، حيث $I= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. وبالتالي I يكون العنصر المحايد في G بالنسبة لعملية ضرب المصفوفات . بما أن $|A| \neq 0$ ، فإن A لها المعكوس $A^{-1} = \frac{1}{|A|} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. لاحظ أن $|A^{-1}| = 1 \neq 0$. إذن $A^{-1} \in G$. أذن G تكون زمرة جزئية ابدالية من $GL(2,\mathbf{R})$.

.٢١ (أ) ليكن F حقل . اثبت أن $SL(n,F) = \{A \in F^{(n\times n)} \mid |A| = 1\}$, $n \in \mathbf{N}$ تكون زمرة جزئية من الزمرة $GL(n,F)$ (الزمرة $SL(n,F)$ تسمى الزمرة الخطية الخاصة من الدرجة n فوق F) .

(ب) أوجد كل المجموعات المشاركة الشمالية المختلفة لـ $S(2,\mathbf{R})$ في $G(2,\mathbf{R})$ ، ثم أوجد $[G(2,\mathbf{R}) : S(2,\mathbf{R})]$.

الحل: (أ) ليكن $A,B \in SL(n,F)$. $|AB| = |A|\,|B| = 1$. إذن $AB \in SL(n,F)$. كذلك $I \in SL(n,F)$ (حيث I هي مصفوفة الوحدة من الدرجة $n\times n$ فوق F) . بما أن $|A| \neq 0$ ، فإن A لها معكوس A^{-1} . وبما أن $|A^{-1}| = |A| = 1$ ، فإن $A^{-1} \in SL(n,F)$. إذن $SL(n,F) \leq GL(n,F)$.

(ب) ليكن $M \in GL(2,\mathbf{R})$. إذن $det(M) = a \in \mathbf{R}\backslash\{0\}$. نضع $G = GL(2,\mathbf{R})$, $S = SL(2,\mathbf{R})$. إذن أى مجموعة مشاركة شمالية لـ S في G تكون في

الصورة MS . بما أن $\det\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a \neq 0$ ، فإن $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G$. بالتالي $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} S$ تكون مجموعة مشاركة شمالية لـ S في G . لكن

$$\det\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} M\right) = \det\left(\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 1 \end{pmatrix} M\right) = \det\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 1 \end{pmatrix} \det(M)$$

$$= \frac{1}{a} \times a = 1$$

إذن $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} M \in S$. وبما أن S زمرة ، فإن $\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} M\right) S = S$.

إذن $MS = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} S$. إذن مجموعة كل المجموعات المشاركة الشمالية لـ S في G هي:

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} S \;\middle|\; a \in \mathbf{R} \setminus \{0\} \right\}$$

إذن $[GL(2,\mathbf{R}) : SL(2,\mathbf{R})] = \infty$.

٢٢. ليكن G زمرة . برهن أن G تكون منتهية إذا وفقط إذا كانت G تحتوي على عدد منتهي من الزمر الجزئية .

الحل: $(\Leftarrow)$ ليكن G زمرة منتهية . إذن من الواضح أن G تحتوي على عدد منتهي من الزمر الجزئية .

$(\Rightarrow)$ ليكن G زمرة بحيث تحتوي على عدد منتهي من الزمر الجزئية. نبرهن أن G تكون منتهية . ليكن $x \in G$ عنصر رتبة غير منتهية . إذن $\langle x \rangle \cong \mathbf{Z}$. لكن $\mathbf{Z}$ تحتوي على عدد غير منتهي من الزمر الجزئية (لأن لكل $n \in \mathbf{N}$ تكون $n\mathbf{Z}$ زمرة جزئية من $\mathbf{Z}$) . إذن $\langle x \rangle$ تحتوي على عدد غير منتهي من الزمر الجزئية . وهذا يتناقض مع الفرض بأن G تحتوي على عدد منتهي من الزمر الجزئية . إذن رتبة كل عنصر في G تكون منتهية . إذن رتبة $\langle x \rangle$ تكون منتهية لكل $x \in G$. لكن $G = \bigcup_{x \in G} \langle x \rangle$. إذن G تكون منتهية .

٢٣. ليكن G زمرة ، وليكن $I \subseteq \mathbf{N}$ بحيث $i \in I \Rightarrow i+1 \in I$. إذا كان $S = \{ S_i \mid i \in I , S_i \leq G \}$ فصل زمر جزئية من G بحيث $S_i \leq S_{i+1}$ ، فاثبت أن $\bigcup S \leq G$.

الحل: ليكن G زمرة ، وليكن $I \subseteq \mathbf{N}$ ، بحيث $i \in I \Rightarrow i+1 \in I$. ليكن $S = \{ S_i \mid i \in I , S_i \leq G \}$ فصل زمر جزئية من G ، بحيث $S_i \leq S_{i+1}$. ليكن $x,y \in \bigcup S$. إذن يوجد $i,j \in I$ بحيث $x \in S_i , y \in S_j$. ليكن $i \leq j$. إذن $x,y \in S_j$. لأن $S_i \leq S_j$. إذن $x\, y^{-1} \in S_j$. إذن $x\, y^{-1} \in \bigcup S$. إذن $\bigcup S \leq G$.

ملحوظة: ينتج من هذا التمرين أنة إذا كان S_1 , S_2 زمرتين جزئيتين من زمرة G ، فإن $S_1 \cup S_2 \leq G$ إذا وفقط إذا كان $S_1 \subseteq S_2$ أو $S_2 \subseteq S_1$.

٢٤. ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x\, y\, x^{-1} = y^2$, $y \neq 1$, $ord(x) = 5$. أوجد $ord(y)$.

الحل: ليكن G زمرة ، وليكن $x,y \in G$ بحيث $x\, y\, x^{-1} = y^2$, $y \neq 1$, $ord(x) = 5$. إذن

$$\begin{aligned} x\, y\, x^{-1} = y^2 &\Rightarrow x^2\, y\, x^{-2} = x\, y^2\, x^{-1} = y^4 = (y^2)^2 \\ &\Rightarrow x^3\, y\, x^{-3} = x\, y^4\, x^{-1} = y^8 = (y^2)^3 \\ &\Rightarrow \dots \\ &\Rightarrow x^n\, y\, x^{-n} = (y^2)^n \end{aligned}$$

بأخذ $n = 5$ ، نحصل على $x^5\, y\, x^{-5} = (y^2)^5$. لكن من الفرض $ord(x) = 5$ يكون $x^5 = 1$. وبما أن $ord(x) = ord(x^{-1})$ ، فإن $x^{-5} = 1$. إذن $y = y^{32}$. إذن $y^{31} = 1$. إذن $ord(y) = 1$ أو $ord(y) = 31$. لكن من الفرض $y \neq 1$. إذن $ord(y)) \neq 1$. إذن $ord(y) = 31$.

٢٥. ليكن G زمرة منتهية ، وليكن $n \in \mathbf{N} \setminus \{1,2\}$, $A_n = \{x \in G \mid ord(x) = n\}$. اثبت أن $|A_n|$ (عدد عناصر المجموعة A_n) يكون عددا زوجيا (باعتبار 0 عددا زوجيا) .

الحل: ليكن G زمرة منتهية ، وليكن $n \in \mathbf{N} \setminus \{1,2\}$, $A_n = \{x \in G \mid ord(x) = n\}$.

إذا كان n لا يقسم |G| ، فإن $A_n = \emptyset$. وذلك لأن $ord(x) \mid |G|$ لكل $x \in G$. إذن في هذة الحالة $|A_n| = 0$. ليكن $n \mid |G|$. إذا كان $x \in A_n$ ، فإن $x^{-1} \in A_n$ ، لأن $ord(x) = ord(x^{-1})$. لاحظ أن $ord(x) = 2$ إذا وفقط إذا كان $x = x^{-1}$. لكن $n > 2$. إذن A_n لا تحتوي عناصر رتبتها 2 . إذن |A| يكون عدداً زوجياً .

٢٦. ليكن G زمرة ابدالية ، وليكن $x,y \in G$. برهن أن

$$ord(x\,y) = ord(x)\;ord(y) \;\Leftrightarrow\; (ord(x)\,,\,ord(y)) = 1$$

الحل: ليكن G زمرة ابدالية ، وليكن $x,y \in G$. ليكن

$$ord(x) = m \;,\; ord(y) = n \;,\; ord(x\,y) = k$$

$(\Rightarrow)$ ليكن $k = ord(x\,y) = ord(x)\,ord(y) = m\,n$. نبرهن أن $(m,n) = 1$. نفرض أن $(m,n) = d > 1$. إذن $d \mid m \,,\, d \mid n$. إذن يوجد $m',n' \in \mathbf{N}$ ، بحيث $m = d\,m' \,,\, n = d\,n'$. بما أن G ابدالية ، فإن

$$(x\,y)^{d\,m'\,n'} = x^{d\,m'\,n'}\,y^{d\,m'\,n'} = (x^m)^{n'}\,(y^n)^{m'} = 1$$

لكن $ord(x\,y) = m\,n > d\,m'\,n'$. وهذا يتناقض مع تعريف رتبة العنصر . إذن $(m,n) = 1$.

$(\Leftarrow)$ ليكن $(m,n) = 1$. نبرهن أن $ord(x\,y) = ord(x)\,ord(y)$. أي نبرهن أن $k = m\,n$.

بما أن $(x\,y)^{m\,n} = (x^m)^n\,(y^n)^m = 1$ ، فإن $k \mid m\,n$. بما أن G ابدالية ، فإن

$$1 = (x\,y)^{k\,m} = x^{k\,m}\,y^{k\,m} = (x^m)^k\,y^{k\,m} = y^{k\,m} \;,$$

$$1 = (x\,y)^{k\,n} = x^{k\,n}\,y^{k\,n} = x^{k\,n}\,(y^n)^k = x^{k\,n} \;.$$

إذن $n \mid k\,m \;,\; m \mid k\,n$. لكن من الفرض $(m,n) = 1$. إذن $m \mid k \,,\, n \mid k$. لكن $(m\,,\,n) = 1$. إذن $m\,n \mid k$. إذن $k = m\,n$.

٢٧. ليكن G زمرة ابدالية منتهية ، وليكن $m = Max\{ord(a) \mid a \in G\}$. اثبت أن $ord(a) \mid m$ لكل $a \in G$.

الحل: ليكن G زمرة ابدالية منتهية ، وليكن $m = Max\{ord(a) \mid a\in G\}$. إذن يوجد $x\in G$ ، بحيث $ord(x) = m$. ليكن $y\in G\backslash\{1\}$. نبرهن أن $ord(y) \mid m$. نضع $ord(y) = n$. نفرض أن $(ord(x) , ord(y)) = 1$. إذن ينتج من تمرين (٢٦) أن $ord(xy) = ord(x)\, ord(y) \geq ord(x)$. لكن من الفرض بأن $m = Max\{ord(a) \mid a\in G\}$ ، يكون $ord(x) = m \geq ord(a) , \forall\ a\in G$. إذن $ord(x)\, ord(y) = ord(x)$. إذن $ord(y) = 1$. إذن $y = 1$. وهذا يتناقض مع الفرض بأن $y \neq 1$. إذن $(ord(x) , ord(y)) \neq 1$. إذن يوجد عدد أولي p يقسم m , n . إذن يوجد $i,j,s,t\in \mathbf{N}$ ، بحيث $m = ord(x) = p^i s , n = ord(y) = p^j t , (p , s) = 1 , (p , t) = 1$.

$$ord(x^{p^i}) = ord(x) / (p^i , ord(x)) = p^i s / (p^i , p^i s) = s \quad ,$$

$$ord(y^t) = ord(y) / (t , ord(y)) = p^j t / (t , p^j t) = p^j \quad .$$

وبما أن $(p , s) = 1$ ، فإن $(s , p^j) = 1$. إذن ينتج من تمرين (٢٦) أن

$$ord(x^{p^i} y^t) = ord(x^{p^i}) = p^j s$$

إذن $p^j s \leq m = p^i s$. إذن $j \leq i$. إذن العامل الأولي p لـ n يدخل في m بقوة أكبر من أو تساوي قوتة في n . وإذا كان q عدد أولي بحيث $q \neq p$, $q \mid n$. إذن $q \mid |G|$. إذن ينتج من مبرهنة كوشي أنة يوجد عنصر $z\in G$ ، بحيث $ord(z) = q$. وكما سبق إذا كان $(m , q) = 1$ ، فإن $z = 1$ وهذا تناقض . إذن $q \mid m$. بالتالي كما سبق ينتج أن q يدخل في m بقوة أكبر من أو تساوي قوتة في y . إذن $n \mid m$.

٢٨. حلل $(\mathbf{Z}_{15})^*$ لإتحاد مجموعات مشاركة للزمرة الجزئية $\langle \bar{7} \rangle$.

الحل: بما أن

$$(\mathbf{Z}_{15})^* = \{\bar{m}\in \mathbf{Z}_{15} \mid (m,15)=1\} = \{\bar{1},\bar{2},\bar{4},\bar{7},\bar{8},\overline{11},\overline{13},\overline{14}\} ,$$
$$\langle \bar{7} \rangle = \{\bar{1},\bar{4},\bar{7},\overline{13}\}$$

فإن

$$(\mathbf{Z}_{15})^* = \langle \bar{7} \rangle \cup \bar{2}\,\langle \bar{7} \rangle \cup \bar{8}\,\langle \bar{7} \rangle \cup \overline{11}\,\langle \bar{7} \rangle \cup \overline{14}\,\langle \bar{7} \rangle$$

ليكن $\bar{x},\bar{y}\in (\mathbf{Z}_{15})^* \backslash \langle \bar{7} \rangle$. إذن $\bar{x}\,\langle \bar{7} \rangle = \bar{y}\,\langle \bar{7} \rangle$ إذا وفقط إذا كان $(\bar{x})^{-1}\bar{y} \in \langle \bar{7} \rangle$. إذن

$$\bar{2}\,\langle \bar{7} \rangle = \bar{8}\,\langle \bar{7} \rangle = \overline{11}\,\langle \bar{7} \rangle = \overline{14}\,\langle \bar{7} \rangle$$

إذن $(\mathbf{Z}_{15})^* = \langle\bar{7}\rangle \cup \bar{2}\,\langle\bar{7}\rangle$.

٢٩. (أ) في S_5 أوجد $((1\ 2\ 3)(4\ 5))^{1202}$.

(ب) في $(\mathbf{Z}_{15})^*$ أوجد $\bar{2}^{1000}$. $\bar{7}^{350}$.

الحل: (أ) بما أن الدورتين $(4\ 5)$, $(1\ 2\ 3)$ منفصلتين (أي لا توجد أرقام مشتركة بينهما) ، فإن حاصل ضربهما يكون ابدالي. لاحظ أن $ord((1\ 2\ 3)) = 3$, $ord((4\ 5)) = 2$. إذن

$$((1\ 2\ 3)\ (4\ 5))^{1202} = (1\ 2\ 3)^{1202}\ (4\ 5)^{1202} = (1\ 2\ 3)^2 = (1\ 3\ 2)$$

حل آخر: نستخدم المبرهنة التي تنص على: إذا كانت G زمرة ، فإن $x^{|G|} = 1$ لكل $x \in G$.

لاحظ أن $|S_5| = 120$ وأن ضرب أي دورتين منفصلتين يكون ابدالي وأن رتبة أي ناقلة يساوي 2 . إذن

$$\begin{aligned}((1\ 2\ 3)\ (4\ 5))^{1202} &= ((1\ 2\ 3)\ (4\ 5))^{120\times 10}\ ((1\ 2\ 3)\ (4\ 5))^2\\ &= ((1\ 2\ 3)\ (4\ 5))^2\\ &= (1\ 2\ 3)^2\\ &= (1\ 3\ 2)\end{aligned}$$

(ب) $$(\mathbf{Z}_{15})^* = \{\bar{m} \in \mathbf{Z}_{15} \mid (m,15)=1\} = \{\bar{1},\bar{2},\bar{4},\bar{7},\bar{8},\overline{11},\overline{13},\overline{14}\}$$

بما أن $350 = 4\times 87+2$, $ord(\bar{7}) = 4$ ، فإن

$$(\bar{7})^{350} = (\bar{7}^4)^{87}\ \bar{7}^2 = \bar{7}^2 = \bar{4}$$

وبما أن $1000 = 4\times 250$, $ord(\bar{2}) = 4$ ، فإن $\bar{2}^{1000} = \bar{1}$.

حل آخر: كما في (أ) يمكن إيجاد المطلوب باستخدم المبرهنة التي تنص على: إذا كانت G زمرة ، فإن $x^{|G|} = 1$ لكل $x \in G$.

٣٠. ليكن H مجموعة كل التباديل في S_n التي تترك n ثابتاً . اثبت أن $H \le S_n$ ، ثم أوجد $[S_n : H]$.

الحل: ليكن H مجموعة كل التباديل في S_n التي تترك n ثابتاً . أي أن

$H = \{f \in S_n \mid f(n) = n\}$. بما أن تبديلة الوحدة 1 تترك n ثابتاً ، فإن $1 \in H$. إذن $H \neq \emptyset$.

من المبرهنة التي نصها (أي مجموعة جزئية منتهية من زمرة تكون زمرة جزئية منها إذا وفقط إذا كانت مغلقة بالنسبة لعملية هذه الزمرة) ينتج أنة يكفي إثبات أن H تكون مغلقة بالنسبة لعملية

ضرب التباديل لإثبات أن $H \leq S_n$. ليكن $f,g \in H$. إذن $f(n) = g(n) = n$. لكن $f\,g(n) = f(g(n)) = f(n) = n$. إذن $f\,g \in H$. إذن H تكون مغلقة بالنسبة لعملية ضرب التباديل . إذن $H \leq S_n$. لإيجاد الدليل $[S_n : H]$ نوجد كل المجموعات المشاركة الشمالية لـ H في S_n . ليكن $m \in \{1,2,\ldots,n\}$ بحيث $m \neq n$. ليكن $f \in S_n$ بحيث $f(n) = m$. إذن $(m\ n)f \in H$. إذن $f \in (m\ n)H$. إذن $S_n = \bigcup_{m=1}^{n}(m\ n)H$. لاحظ أن $(a\ n)H \cap (b\ n)H = \emptyset$. إذن المجموعات المشاركة الشمالية المختلفة لـ H في G هي $H\ ,\ (1\ n)H\ ,\ (2\ n)H\ ,\ \ldots\ ,\ (n\text{-}1\ n)H$. إذن $[S_n : H] = n$.

٣١. ليكن G زمرة منتهية رتبتها عدد فردي ، وليكن $x,y,z \in G$. اثبت أن

(أ) $x\,y\,z = y \;\Rightarrow\; x = 1$

(ب) $x\,y\,z\,y\,x = z \;\Rightarrow\; x\,y = 1$

الحل: ليكن G زمرة منتهية رتبتها عدد فردي ، وليكن $x,y,z \in G$.

(أ) بما أن G زمرة منتهية رتبتها عدد فردي ، فإنة يوجد $n \in \mathbf{N}$ بحيث $|G| = 2\,n + 1$. ليكن $x\,y\,x = y$. إذن بضرب الطرفين من اليمين ثم من الشمال في x^{-1} نحصل على $y\,x = x^{-1}\,y\ \ ,\ \ x\,y = y\,x^{-1}$. وبضرب $x\,y = y\,x^{-1}$ من اليمين في y نحصل على $x\,y^2 = y\,x^{-1}\,y$. وبضرب $y\,x = x^{-1}\,y$ من الشمال في y نحصل على $y^2\,x = y\,x^{-1}y$. إذن $x\,y^2 = y^2\,x$. وبضرب هذة المعادلة من اليمين في y^2 نحصل على $x\,y^4 = y^2\,x\,y^2 = y^4\,x$. وهكذا ... . إذن $x\,y^{2m} = y^{2m}\,x$ ، لكل $m \in \mathbf{N}$. بما أن

$1 = y^{|G|} = y^{2n+1} = y^{2n}\,y$

فإن $y^{-1} = y^{2n}$. وبما أن $x\,y^{2n} = y^{2n}\,x$ ، فإن $x\,y^{-1} = y^{-1}\,x$. إذن $x = y^{-1}\,x\,y$. إذن $y\,x = x\,y$. من الفرض $x\,y\,x = y$ ينتج أن $y = x\,(y\,x) = x\,(x\,y) = x^2\,y$. إذن $x^2 = 1$. إذن $ord(x) = 2$ أو $ord(x) = 1$. نفرض أن $ord(x) = 2$. بما أن $ord(a) \mid |G|$ ، لكل $a \in G$ ، فإن $2 \mid 2n+1$. لكن هذا غير ممكن . إذن $ord(x) = 1$. إذن $x = 1$.

(ب) ليكن $x\,y\,z\,y\,x = z$. بالضرب من اليمين في y ، نحصل على $(x\,y)\,(z\,y)\,(x\,y) = z\,y$. إذن ينتج من (أ) أن $x\,y = 1$.

٣٢. ليكن $m,n \in \mathbf{N}$ بحيث $m > 1$. اثبت أن $n \mid \phi(m^n - 1)$ ، حيث ϕ هى دالة ϕ لإويلر (Euler ϕ-function) .

الحل: ليكن $m,n\in\mathbf{N}$ بحيث $m > 1$. دالة ϕ لإويلر تعرف كما يلي

$$\phi(n) = |\{m\in\mathbf{Z} \mid (m,n) = 1\}| \quad , \forall\, n\in\mathbf{N}$$

لاحظ أن $(m , m^n-1) = 1$. إذن $\bar{m}\in(\mathbf{Z}_{m^n-1})^* \subset \mathbf{Z}_{m^n-1}$. بما أن $m^n \equiv 1 \pmod{m^n-1}$ ، فإن $\overline{m^n} = \bar{1}$ في $(\mathbf{Z}_{m^n-1})^*$. إذن $(\bar{m})^n = \bar{1}$ في $(\mathbf{Z}_{m^n-1})^*$.

لاحظ أن $m^k \not\equiv 1 \pmod{m^n-1}$ ، لكل $0 \le k \le n$. إذن $ord(\bar{m}) = n$. لكن

$$\left|(\mathbf{Z}_{m^n-1})^*\right| = \phi(m^n - 1) \ , \ \bar{m}\in(\mathbf{Z}_{m^n-1})^*$$

إذن ينتج من مبرهنة لاجرانج أن $n \mid \phi(m^n - 1)$.

٣٣. ليكن G زمرة ، وليكن $x,y\in G$ ، بحيث $xy\in C(G)$ (حيث $C(G)$ هو مركز G) . اثبت أن $x\,y = y\,x$.

الحل: ليكن G زمرة ، وليكن $x,y\in G$ ، بحيث $xy\in C(G)$. إذن $(x\,y)\,y = y\,(x\,y)$. إذن $(x\,y)y = (y\,x)\,y$. وبالضرب في y^{-1} من اليمين نحصل على $x\,y = y\,x$.

التشاكلات الزمرية – Homomorphisms of groups

٣٤. اثبت أن الصورة التشاكلية للزمرة $\mathbf{Z}$ تماثل $\mathbf{Z}_n$ ، حيث $n\in\mathbf{N}$.

الحل: ليكن S صورة تشاكلية للزمرة $\mathbf{Z}$. هذا يعني أنة يوجد تشاكل زمري شامل $f : \mathbf{Z} \to S$. إذن ينتج من مبرهنة التماثل الأولى في الزمر أن $\mathbf{Z}/Ker(f) \cong S$. لكن أي زمرة جزئية من $\mathbf{Z}$ تكون في الصورة $m\mathbf{Z}$ ، حيث $m\in\mathbf{N}$. لذلك يوجد $n\in\mathbf{N}$ ، بحيث $Ker(f) = n\mathbf{Z}$ لأن $Ker(f)$ زمرة جزئية من $\mathbf{Z}$. إذن $\mathbf{Z}/n\mathbf{Z} \cong S$. لكن $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$. إذن $S \cong \mathbf{Z}_n$.

٣٥. ليكن G زمرة . برهن أن $f : G \to G$ ، حيث $f(x) = x^2$ لكل $x\in G$ يكون تشاكل زمري إذا وفقط إذا كانت G ابدالية .

الحل: $(\Leftarrow)$ ليكن $f : G \to G$ تشـــاكل زمري ، بحيث $f(x) = x^2$ ، لكل $x\in G$. ليكن $x,y\in G$. إذن $(x\,y)^2 = f(x\,y) = f(x)\,f(y) = x^2\,y^2$. إذن $x\,y\,x\,y = x\,x\,y\,y$. لكن G زمرة وبالتالي يتحقق فيها قانون الحذف . إذن $x\,y = y\,x$. إذن G تكون زمرة ابدالية .

($\Rightarrow$) لتكن G زمرة ابدالية . ليكن $f : G \to G$ تطبيقاً ، بحيث $f(x) = x^2$ لكل $x \in G$. ليكن $x, y \in G$. إذاً

$$f(x\,y) = (x\,y)^2 = x\,y\,x\,y = x\,x\,y\,y = x^2\,y^2 = f(x)\,f(y)$$

إذن f يكون تشاكل زمري .

٣٦. أوجد كل التشاكلات الزمرية من **Z** إلى **Z** .

الحل: ليكن $f : \mathbf{Z} \to \mathbf{Z}$ تشاكل زمري . إذن $f(0) = 0$. لكل $n \in \mathbf{Z}$ حيث $n > 0$ يكون

$$\begin{aligned} f(n) &= f(1 + \ldots + 1) \quad (n \text{ مرة}) \\ &= f(1) + \ldots + f(1) \quad (n \text{ مرة}) \\ &= n\,f(1) \end{aligned}$$

بالمثل يكون $f(-n) = -f(n)$. إذن $f_a : \underset{n \mapsto na}{\mathbf{Z} \to \mathbf{Z}}$ لكل $a \in \mathbf{Z}$ هى كل التشاكلات الزمرية من **Z** إلى **Z** .

٣٧. أوجد كل التشاكلات الزمرية من $\mathbf{Z}_6$ إلى $\mathbf{Z}_4$.

الحل: ليكن $f : \mathbf{Z}_6 \to \mathbf{Z}_4$ تشاكل زمري . إذن $f(\bar{0}) = \bar{0}$. ليكن $\bar{n} \in \mathbf{Z}_6 \setminus \{\bar{0}\}$. إذن

$$\begin{aligned} f(\bar{n}) &= f(\bar{1} + \cdots + \bar{1}) \quad (n \text{ مرة}) \\ &= f(\bar{1}) + \cdots + f(\bar{1}) \quad (n \text{ مرة}) \end{aligned}$$

نوجد الآن الاحتمالات المختلفة لـ $f(\bar{1})$. الشروط التي يجب أن يحققها العنصر $f(\bar{1})$ هى:

(أ) رتبة $f(\bar{1})$ تقسم رتبة الزمرة $\mathbf{Z}_4$ ، أى أن $\operatorname{ord}(f(\bar{1})) \mid 4$ ،

(ب) $\operatorname{ord}(f(\bar{1})) \mid \operatorname{ord}(\bar{1})$ ، أى أن $\operatorname{ord}(f(\bar{1})) \mid 6$.

إذن $\operatorname{ord}(f(\bar{1})) \mid 4, 6$. إذن $\operatorname{ord}(f(\bar{1})) = 1$ أو $\operatorname{ord}(f(\bar{1})) = 2$.

إذا كان $\operatorname{ord}(f(\bar{1})) = 1$ ، فإن $f(\bar{1}) = \bar{0}$. وإذا كان $\operatorname{ord}(f(\bar{1})) = 2$ ، فإن $f(\bar{1}) = \bar{2}$. إذن $f(\bar{1}) = \bar{0}$ أو $f(\bar{1}) = \bar{2}$. إذن يوجد تشاكلين زمريين فقط من $\mathbf{Z}_6$ إلى $\mathbf{Z}_4$ ، هما:

$$o : \underset{\bar{n} \mapsto \bar{0}}{\mathbf{Z}_6 \to \mathbf{Z}_4} \ , \ f : \underset{\bar{n} \mapsto \overline{2n}}{\mathbf{Z}_6 \to \mathbf{Z}_4}$$

٣٨. ليكن $f : G \to G$ تماثل زمري ، وليكن $x \in G$. اثبت أن $ord(x) = ord(f(x))$ ، ثم استخدم هذا لحل تمرين (١١) (ب ، ت) .

الحل: ليكن $f : G \to G$ تماثل زمري ، وليكن $x \in G$. إذن

$ord(f(x)) \mid ord(x)$ (مبرهنة) . نضع $ord(x) = n$. إذن

$$ord(x) = n \Leftrightarrow x^n=1 \Leftrightarrow f(x^n)=1 \Leftrightarrow \left(f(x)\right)^n=1 \Leftrightarrow ord\left(f(x)\right)=n$$

إذن $ord(x) = ord(f(x))$.

<u>حل آخر لتمرين (١١) (ب ، ت) باستخدام تمرين (٣٨):</u>

(ب) ليكن $f_x : G \to G$ ، بحيث $f_x(y) = xyx^{-1}$ ، لكل $x \in G$. من السهل اثبات أن يكون f_x تماثل زمري . إذن ينتج من تمرين (٣٨) أن $ord(y) = ord(f_x(y)) = ord(x\, y\, x^{-1})$.

(ت) ليكن $f_x : G \to G$ ، بحيث $f_x(y) = xyx^{-1}$ ، لكل $x \in G$. من السهل اثبات أن يكون f_x تماثل زمري . بما أن $f_x(y\, x) = x\, y\, x\, x^{-1} = x\, y$ ، فإنة ينتج من تمرين (٣٨) أن

$ord(x\, y) = ord(f_x(y\, x)) = ord(y\, x)$

٣٩. أوجد $Aut(G)$ ، حيث

(أ) $G = K_4$ (K_4 هي زمرة كلين الرباعية (the klein 4-group))

(ب) $G = S_3$

(ت) $G = \mathbf{Z}_4$

الحل: $Aut(G)$ هي مجموعة كل التماثلات الزمرية من G إلى G .

(أ) ليكن $G = K_4 = \{1 , a , b , c\}$ ، حيث

$$a^2 = b^2 = c^2 = 1 , ab = ba = c , ac = ca = b , bc = cb = a$$

ليكن $f_i : K_4 \to K_4$ ، حيث $i = 1,2,\ldots,6$ معرفة كما يلي:

$f_1(x) = x = 1(x) , \forall\ x \in K_4$;

$f_2(1) = 1 , f_2(a) = b , f_2(b) = a , f_2(c) = c$;

$f_3(1) = 1 , f_3(a) = c , f_3(b) = b , f_3(c) = a$;

$f_4(1) = 1 , f_4(a) = a , f_4(b) = c , f_4(c) = b$;

$f_5(1) = 1 , f_5(a) = b , f_5(b) = c , f_5(c) = a$;

$f_6(1) = 1 , f_6(a) = c , f_6(b) = a , f_6(c) = b$;

من الواضح أن $f_1 ,\dots, f_6$ هي كل التماثلات الزمرية على K_4 . إذن

$$Aut(K_4) = \{f_1 , f_2 , f_3 , f_4 , f_5 , f_6\} \cong S_3$$

(ب) كما في (أ) يكون من السهل إثبات أن $Aut(S_3) \cong S_3$.

(ت) نوجد $Aut(\mathbf{Z}_n)$. ليكن $f \in Aut(\mathbf{Z}_n)$. إذن $f : \mathbf{Z}_n \to \mathbf{Z}_n$ يكون تماثل زمري . ليكن $\bar{x} \in \mathbf{Z}_n$. إذن $f(\bar{x}) = x\, f(\bar{1})$ ، لأن

$$f(\bar{x}) = f(\underbrace{\bar{1} + \cdots + \bar{1}}_{\text{مرة } x}) = \underbrace{f(\bar{1})+\cdots+f(\bar{1})}_{\text{مرة } x}$$

إذن f يتعين تعيناً كاملاً بتعين $f(\bar{1})$. أي أن لكل قيمة لـ $f(\bar{1})$ نحصل على تماثل زمري $f : \mathbf{Z}_n \to \mathbf{Z}_n$. بما أن f شامل ، فإنة يوجد $\bar{x} \in \mathbf{Z}_n$ ، بحيث $f(\bar{x}) = \bar{1}$. لاحظ أن $\bar{x}$ يكون وحيداً لأن f متباين . إذن

$$\bar{x}\, f(\bar{1}) = (\underbrace{\bar{1} + \cdots + \bar{1}}_{\text{مرة } x})\, f(\bar{1}) = \underbrace{f(\bar{1}) + \cdots + f(\bar{1})}_{\text{مرة } x} = x\, f(\bar{1}) = f(\bar{x}) = \bar{1}$$

إذن $f(\bar{1})$ يكون لة معكوس ضربي . إذن $f(\bar{1}) \in \mathbf{Z}_n^*$. إذن عدد قيم $f(\bar{1})$ يساوي $|\mathbf{Z}_n^*|$. إذن $|\mathbf{Z}_n^*| = |Aut(\mathbf{Z}_n)|$. ليكن $\phi : Aut(\mathbf{Z}_n) \to \mathbf{Z}_n^*$ ، بحيث $\phi(f) = f(\bar{1}) ,\ \forall\ f \in Aut(\mathbf{Z}_n)$. إذن ϕ يكون تطبيقاً معرفاً جيداً . ليكن $f,h \in Aut(\mathbf{Z}_n)$. وليكن $h(\bar{1}) = \bar{y}$. إذن

$$\begin{aligned}\phi(f\,h) &= f\,h(\bar{1}) = f(h(\bar{1})) = f(\bar{y}) = y\, f(\bar{1}) = \bar{y}\, f(\bar{1}) = h(\bar{1})\, f(\bar{1}) = f(\bar{1})\, h(\bar{1}) \\ &= \phi(f)\, \phi(h)\end{aligned}$$

إذن ϕ يكون تشاكل زمري .

$$\begin{aligned}Ker(\phi) &= \{f \in Aut(\mathbf{Z}_n) \mid \phi(f) = \bar{1}\} = \{f \in Aut(\mathbf{Z}_n) \mid f(\bar{1}) = \bar{1}\} \\ &= \{f \in Aut(\mathbf{Z}_n) \mid f(\bar{x}) = \bar{x} ,\ \forall\ \bar{x} \in \mathbf{Z}_n\} = \{f \in Aut(\mathbf{Z}_n) \mid f = 1\} = \{1\}\end{aligned}$$

إذن ϕ يكون متباين . ليكن $\bar{x} \in \mathbf{Z}_n^*$ ، وليكن $f \in Aut(\mathbf{Z}_n)$ ، بحيث $f(\bar{1}) = \bar{x}$. إذن $\phi(f) = f(\bar{1}) = \bar{x}$. إذن ϕ يكون شامل . إذن ϕ يكون تماثل زمري . إذن $Aut(\mathbf{Z}_n) \cong \mathbf{Z}_n^*$.

٤٠. برهن أن الزمرتين $\mathbf{Z} , n\,\mathbf{Z}$ متماثلتين .

الحل: ليكن $f : \mathbf{Z} \to n\mathbf{Z}$ ، بحيث $f(m) = nm ,\ \forall\ m \in \mathbf{Z}$. ليكن $a,b \in \mathbf{Z}$. إذن

$f(a) = f(b) \Leftrightarrow n\,a = n\,b \Leftrightarrow a = b$

إذن f يكون راسماً معرفاً جيداً ومتبايناً . من الواضح أن f يكون أيضاً شاملاً . وبما أن

$f(a + b) = n\,(a + b) = n\,a + n\,b = f(a) + f(b)$

فإن f يكون تشاكل زمري . إذن f يكون تماثل زمري . إذن $\mathbf{Z} \cong n\mathbf{Z}$.

٤١. ليكن G زمرة . اثبت أن

(أ) إذا كان $Aut(G) = \{1\}$ ، فإن G تكون ابدالية .

(ب) إذا كان $x^2\,y^2 = (x\,y)^2 ,\ \forall\ x,y \in G$ ، فإن G تكون ابدالية .

(ت) إذا كان $f : G \to G$ بحيث $f(x) = x^2 ,\ \forall\ x \in G$ ، تشاكل زمري ، فإن G تكون ابدالية .

(ث) $f : G \to G$ بحيث $f(x) = x^{-1} ,\ \forall\ x \in G$ يكون تماثل زمري إذا وفقط إذا كان G ابدالية .

الحل: ليكن G زمرة .

(أ) ليكن $x \in G$. ليكن $\alpha_x : G \to G$ ، بحيث $\alpha_x(y) = x\,y\,x^{-1}$ لكل $y \in G$. إذن α_x يكون تماثل زمري (يسمى تماثل ذاتي (inner automorphism)) . إذن $\alpha_x \in Aut(G) = \{1\}$. إذن $\alpha_x = 1$. إذن $\alpha_x(y) = y$ ، لكل $y \in G$. إذن $x\,y\,x^{-1} = y$ ، لكل $y \in G$. إذن $x\,y = y\,x$ ، لكل $y \in G$. إذن $x\,y = y\,x$ ، لكل $x,y \in G$. إذن G تكون ابدالية .

(ب) انظر تمرين (٧) .

(ت) ليكن $f : G \to G$ ، بحيث $f(x) = x^2$ لكل $x \in G$. من السهل إثبات أن f يكون تشاكل زمري . إذن لكل $x,y \in G$ ، يكون $(x\,y)^2 = f(x\,y) = f(x)\,f(y) = x^2\,y^2$. إذن ينتج من (ب) أن G تكون إبدالية .

(ث) $(\Leftarrow)$ نفرض أن $f : G \to G$ ، بحيث $f(x) = x^{-1}$ لكل $x \in G$ يكون تماثل زمري . إذن لكل $x,y \in G$ ، يكون $y^{-1}\,x^{-1} = (x\,y)^{-1} = f(x\,y) = f(x)\,f(y) = x^{-1}\,y^{-1}$. إذن G تكون إبدالية .

($\Rightarrow$) نفرض أن G تكون إبدالية وأن $f : G \to G$ ، بحيث $f(x) = x^{-1}$ لكل $x \in G$. إذن لكل $x,y \in G$ ، يكون $f(x\,y) = (xy)^{-1} = y^{-1}\,x^{-1} = x^{-1}\,y^{-1} = f(x)\,f(y)$. إذن f يكون تشاكل زمري . من الواضح أن f يكون متباين وشامل . إذن f يكون تماثل زمري .

٤٢. ليكن G زمرة وليكن $a \in G$ عنصر ثابت . ليكن $x * y = x\,a\,y$ لكل $x,y \in G$. اثبت أن $(G\,,*)$ تكون زمرة تماثل G .

الحل: ليكن G زمرة وليكن $a \in G$ عنصر ثابت ، وليكن $x * y = x\,a\,y$ لكل $x,y \in G$. من الواضح أن $* : G \times G \to G$ ، حيث $*(x,y) = x * y\ , \forall\ x,y \in G$ يكون تطبيق (راسم) معرف جيدا . إذن $*$ تكون عملية ثنائية داخلية على G . إذن G تكون مغلقة بالنسبة للعملية $*$. لكل $x \in G$ ، يكون $x * a^{-1} = a^{-1} * x = x$. إذن a^{-1} يكون عنصر محايد في G بالنسبة للعملية $*$. بما أن $x * (a^{-1}\,x^{-1}\,a^{-1}) = a^{-1}$ ، فإن $a^{-1}\,x^{-1}\,a^{-1}$ يكون معكوس للعنصر $x \in G$ ، بالنسبة للعملية $*$. ولكل $x,y,z \in G$ يكون

$$x * (y * z) = x\,a\,(y\,a\,z) = (x\,a\,y)\,a\,z = (x * y) * z$$

إذن $*$ تكون عملية دامجة . إذن $(G\,,*)$ تكون زمرة . ليكن $f_a : (G\,,*) \to G$ ، حيث $f_a(x) = a\,x\ , \forall\ x \in G$. ليكن $x,y \in G$. إذن

$$f_a(x) = f_a(y) \Leftrightarrow a\,x = a\,y \Leftrightarrow x = y$$

إذن f_a يكون معرف جيداً ومتباين . وبما أن $f_a(a^{-1}\,y) = y$ ، لكل $y \in G$ ، فإن f_a يكون شامل . لكل $x,y \in G$ يكون

$$f_a(x * y) = a\,(x * y) = a\,(x\,a\,y) = (a\,x)\,(a\,y) = f_a(x)\,f_a(y)$$

إذن f_a يكون تشاكل زمري . وبما أن f_a متباين وشامل ، فإن f_a يكون تماثل زمري .

٤٣. ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$ ، بحيث $f(x) \neq x$ لكل $x \in G \setminus \{1\}$. اثبت أن

(أ) لكل $x \in G$ ، يوجد $y \in G$ بحيث $x = y^{-1}\,f(y)$.

(ب) إذا كان $f^2 = 1$ ، فإن G تكون ابدالية .

الحل: ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$ ، بحيث $f(x) \neq x$ لكل $x \in G \setminus \{1\}$.

(أ) ليكن $\alpha : G \to G$ ، بحيث $\alpha(y) = y^{-1} f(y)$ لكل $y \in G$. ليكن $y, z \in G$. إذن

$$\alpha(y) = \alpha(z) \Leftrightarrow y^{-1} f(y) = z^{-1} f(z) \Leftrightarrow z y^{-1} f(y) = f(z) \Leftrightarrow z y^{-1} = f(z y^{-1})$$

$$\Leftrightarrow z y^{-1} = 1 \Leftrightarrow y = z$$

إذن α يكون معرف جيدا ومتباين . وبما أن G منتهية ، فمن الواضح أن α يكون شامل . إذن إذا كان $x \in G$ ، فإنة يوجد $y \in G$ ، بحيث $y^{-1} f(y) = \alpha(y) = x$.

(ب) ليكن $f^2 = 1$. إذن ينتج من (أ) أنة يوجد $y \in G$ ، بحيث $x = y^{-1} f(y)$. لكن $f^2 = 1$. إذن لكل $x \in G$ ، يكون

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

إذن ينتج من تمرين (٤١) (ث) أن G تكون ابدالية .

٤٤. ليكن G زمرة منتهية ، بحيث $|G| > 2$. اثبت أن $|Aut(G)| \geq 2$.

الحل: ليكن G زمرة منتهية ، بحيث $|G| > 2$. نفرض أن G ليست ابدالية . ليكن $x \in G \setminus \{1\}$. ليكن $\alpha_x : G \to G$ ، بحيث $\alpha_x(y) = x y x^{-1}$ لكل $y \in G$. إذن α_x يكون تماثل زمري (يسمى تماثل ذاتي (inner automorphism)) . إذن $\alpha_x \in Aut(G)$. لاحظ أن $\alpha_x \neq 1$. إذن $|Aut(G)| \geq 2$. إذن المطلوب متحقق في حالة G ليست ابدالية . لذلك نفرض الآن أن G ابدالية . ليكن $f : G \to G$ ، بحيث $f(x) = x^{-1}$ لكل $x \in G$. إذن ينتج من تمرين (٤١) (ث) أن f يكون تماثل زمري . إذن $f \in Aut(G)$. إذا كان $|G| = 3$ ، فإن $f \neq 1$, $G \cong \mathbf{Z}_3$. وبالتالي $|Aut(G)| \geq 2$. وإذا كان $|G| = 4$ ، فإن $G = \mathbf{Z}_4$ أو $G = K_4$ (حيث K_4 هي زمرة كلين الرباعية (the Klein 4-group)) . إذا كان $G = \mathbf{Z}_4$ ، فإن $f \neq 1$ وبالتالي $|Aut(G)| \geq 2$. ليكن $G = K_4 = \{1, a, b, c\}$. إذن $\phi : G \to G$ ، حيث

$$\phi(1) = 1 , \phi(a) = b , \phi(b) = a , \phi(c) = c$$

يكون تماثل زمري و $\phi \neq 1$. إذن في هذة الحالة يكون $|Aut(G)| \geq 2$. والآن نفرض أن G تحتوي على زمرة جزئية S تماثل K_4 . إذن يوجد $g_1, \ldots, g_n \in G \setminus S$ ، بحيث

$$G = S \cup g_1 S \cup \cdots \cup g_n S$$

ليكن $\alpha : G \to G$ ، بحيث $\alpha(s) = \phi(s)$, $\alpha(g_i\, s) = g_i\, \phi(s)$ لكل $i=1,2,\ldots,n$, $s\in S$.
إذن α يكون تماثل زمري ، لأن

$$\alpha((g_i\, s)\,(g_j\, s')) = \alpha((g_i\, g_j)\,(s\, s')) = (g_i\, g_j)\,\phi(s\, s') = (g_i\, g_j)\,\phi(s)\,\phi(s')$$

$$= (g_i\, \phi(s))\,(g_j\, \phi(s')) = \alpha(g_i\, s)\,\alpha(g_j\, s')$$

لاحظ أن $\text{Ker}(\alpha) = \{1\}$. إذن α يكون متباين . ومن الواضح أن α يكون شامل أيضاً . إذن $\alpha\in \text{Aut}(G)$. إذن $|\text{Aut}(G)| \geq 2$.

٤٥. ليكن G زمرة منتهية . إذا كان $|G| = n$ ، فاثبت أن $|\text{Aut}(G)| \mid (n-1)!$.

الحل: ليكن G زمرة منتهية ، وليكن $|G| = n$. لاحظ أن $f(1) = 1$ ، لكل $f\in \text{Aut}(G)$. إذن كل $f\in \text{Aut}(G)$ يناظر تبديلة على $G\backslash\{1\}$. إذن $\text{Aut}(G)$ تماثل زمرة جزئية من $S(G\backslash\{1\}) \cong S_{n-1}$ (انظر مبرهنة كايلي (Cayly's theorem)) حيث $S(X)$ ترمز لمجموعة كل التباديل على X . لكن $|S_{n-1}| = (n-1)!$. إذن ينتج من مبرهنة لاجرانج أن $|\text{Aut}(G)| \mid (n-1)!$.

٤٦. ليكن $G = \{I_{a_1,\cdots,a_n} | a_1,\cdots,a_n \in \mathbf{R}\}$ ، حيث

$$I_{a_1,\cdots,a_n} = \begin{bmatrix} 1 & & & & a_1 \\ & 1 & 0 & & a_2 \\ & 0 & \ddots & & \vdots \\ & & & 1 & a_n \\ & & & & 1 \end{bmatrix}$$

برهن أن $G \cong \mathbf{R}^n$.

الحل: ليكن $G = \{I_{a_1,\cdots,a_n} | a_1,\cdots,a_n \in \mathbf{R}\}$ ، حيث

$$I_{a_1,\cdots,a_n} = \begin{bmatrix} 1 & & & & a_1 \\ & 1 & 0 & & a_2 \\ & 0 & \ddots & & \vdots \\ & & & 1 & a_n \\ & & & & 1 \end{bmatrix}$$

نبرهن أولاً أن G تكون زمرة بالنسبة لعملية ضرب المصفوفات . من الواضح أن المجموعة G تكون مغلقة بالنسبة لعملية ضرب المصفوفات وأنها تحتوي على مصفوفة الوحدة (من الدرجة $((n+1)\times(n+1))$. معكوس المصفوفة $I_{a_1,\dots,a_n}$ هو المصفوفة $I_{-a_1,\dots,-a_n}$. إذن G تحتوي على معكوس لكل عنصر فيها (بالنسبة لعملية ضرب المصفوفات) . إذن G تكون زمرة بالنسبة لعملية ضرب المصفوفات . ليكن $\phi : G \to \mathbf{R}^n$ بحيث $\phi(I_{a_1,\dots,a_n}) = (a_1,\dots,a_n)$ ، لكل $I_{a_1,\dots,a_n} \in G$.

الزمر الجزئية الناظمية – Normal subgroups

٤٧. ليكن F حقل وليكن $n\in\mathbf{N}$. اثبت أن $SL(n,F) \lhd GL(n,F)$.

الحل: لاحظ أولاً أن $SL(n,F)$ تكون زمرة جزئية من الزمرة $GL(n,F)$ (انظر تمرين (٢١)) . ليكن $A\in GL(n,F)$, $B\in SL(n,F)$. إذن

$$|ABA^{-1}| = |A|\,|B|\,|A^{-1}| = |A|\,|B|\,|A|^{-1} = |B| = 1$$

إذن $A\,SL(n,F)\,A^{-1} \subseteq SL(n,F)$ ، لكل $A\in GL(n,F)$. إذن $SL(n,F) \lhd GL(n,F)$.

٤٨. ليكن G زمرة منتهية ، وليكن $f\in Aut(G)$ ، وليكن $S = \{x\in G \mid f(x) = x^{-1}\}$. إذا كان $|S| > 3/4\,|G|$ ، فاثبت أن $S = G$.

الحل: ليكن G زمرة منتهية ، وليكن $f\in Aut(G)$. ليكن $S = \{x\in G \mid f(x) = x^{-1}\}$ ، بحيث $|S| > 3/4\,|G|$. نفرض أن $a\in S$. إذن $|aS| =|S| > 3/4\,|G|$. إذن $|S \cap aS| > 1/2\,|G|$. ليكن $x\in S \cap aS$. إذن يوجد $y\in S$ ، بحيث $x = a\,y$. بما أن $x\in S$ ، فإن

$$f(x) = x^{-1} = (a\,y)^{-1} = y^{-1}\,a^{-1}$$

ليكن $y\in S$. إذن $f(x) = f(a\,y) =f(a)\,f(y) = a^{-1}\,y^{-1}$. إذن $x^{-1} = y^{-1}\,a^{-1} = a^{-1}\,y^{-1}$. إذن $x = a\,y = y\,a$. إذن $y\,x = y\,a\,y$, $x\,y = y\,a\,y$. إذن $x\,y = y\,x$. إذن $x\in C(y)$ ، حيث $C(y) = \{g\in G \mid g\,y = y\,g\}$ هو ممركز y في G (centeralizer of y in G) وهي زمرة جزئية من G . إذن $S \cap aS \subseteq C(y)$. إذن $(1/2)\,|G| < |S \cap aS| \le |C(y)|$. بما أن $C(y) \le G$ ، فإن $|C(y)| \mid |G|$. لكن $|C(y)| > (1/2)\,|G|$. إذن $C(y) = G$. إذن كل

عنصر في G يكون تبادلي في الضرب مع y ، أي أن $g\in G$, $\forall$ $gy = yg$. ليكن $u,v\in S$.
إذن

$$f(u v^{-1}) = f(u)\, f(v^{-1}) = u^{-1} v = v u^{-1} = (u v^{-1})^{-1}$$

إذن $u v^{-1}\in S$. إذن $S \le G$. إذن $|S| \mid |G|$. لكن $|S| > 3/4\,|G|$. إذن $|S| = |G|$. إذن $S = G$.

٤٩. أوجد كل الزمر الجزئية الناظمية من الزمر K_4 , $\mathbf{Z}_n$, S_3 , S_4
(K_4 هى زمرة كلين الرباعية (the klein 4-group)) .

الحل: بما أن K_4 , $\mathbf{Z}_n$ زمرتين ابداليتين ، فإن كل الزمر الجزئية منهما تكون ناظمية . ليكن $K_4 = \{1 , a , b , c\}$. الزمر الجزئية غير البديهية من K_4 هي $\{1,a\}$, $\{1,b\}$, $\{1,c\}$. والزمر الجزئية غير البديهية من $\mathbf{Z}_n$ هي $\langle \overline{m} \rangle$ ، حيث $0 < m < n$. الزمرة $A_3 = \{1 , (1\ 2\ 3) , (1\ 3\ 2)\}$ هي الزمرة الجزئية الناظمية الوحيدة من S_3 .

$$A_4 = \{1,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3),(2\ 3\ 4),(2\ 4\ 3),(1\ 2\ 3),(1\ 2\ 4), (1\ 3\ 2),(1\ 3\ 4),(1\ 4\ 2),(1\ 4\ 3)\}$$

هي الزمرة الجزئية الناظمية الوحيدة من S_4 . وبما أن $[S_4 : A_4] = 2$ ، فإن $A_4 \lhd S_4$.

٥٠. ليكن G زمرة . اثبت أن $Inn(G) \lhd Aut(G)$.

الحل: ليكن G زمرة . ليكن $x,y\in G$. إذن $\alpha_x : G \to G$ ، حيث $\alpha_x(g) = xgx^{-1}$ لكل $g\in G$ يكون تماثل زمري ويسمى تماثل زمري ذاتي داخلي . $Inn(G)$ هي مجموعة كل التماثلات الزمرية الذاتية الداخلية على G . ليكن $\alpha_x,\alpha_y\in Inn(G)$. إذن $\alpha_x\alpha_y = \alpha_{xy}$, $(\alpha_x)^{-1}= \alpha_{x^{-1}}$. إذن $Inn(G)$ تكون زمرة وتسمى زمرة التماثلات الزمرية الذاتية الداخلية على G . أما $Aut(G)$ فهي زمرة كل التماثلات الزمرية الذاتية على G (أي التماثلات الزمرية من G إلى G) . بالتالي يكون $Inn(G) \le Aut(G)$. من السهل اثبات أن $f\,\alpha_x = \alpha_{f(x)}\, f$ ، لكل $f\in Aut(G)$. إذن $f\, Inn(G) = Inn(G)\, f$. إذن $Inn(G) \lhd Aut(G)$.

٥١. ليكن G زمرة ، وليكن $N \le G$ بحيث رتبة N لا تساوي رتبة أي زمرة جزئية أخرى من G . اثبت أن $N \lhd G$.

الحل: ليكن G زمرة ، وليكن $N \leq G$ بحيث رتبة N لا تساوي رتبة أي زمرة جزئية أخرى من G . ليكن $x \in G$. إذن $x N x^{-1} \leq G$. إذن ينتج من الفرض بأن رتبة N لا تساوي رتبة أي زمرة جزئية أخرى من G أن $|x N x^{-1}| \neq |N|$. نفرض أن $x N x^{-1} \neq N$. لكن هذا يتناقض مع الحقيقة بأن $|x N x^{-1}| = |N|$. إذن $x N x^{-1} = N$. إذن $N \lhd G$.

٥٢. اذكرمثالا لزمرة غير ابدالية بحيث كل الزمر الجزئية الناظمية غير البديهية منها تكون ابدالية .

الحل: S_3 زمرة تحتوي على زمرة جزئية ناظمية وحيدة هي $A_3 = \{1 , (1\ 2\ 3) , (1\ 3\ 2)\}$.
لاحظ أن A_3 ناظمية في G لأن $[S_3 : A_3] = 2$ ، كذلك A_3 تكون ابدالية .

٥٣. ليكن G زمرة ، وليكن $N \lhd G$. إذا كان $f : G/N \to \mathbf{Z}$ تشاكل زمري شامل (epimorhism) ، فبرهن أنة لكل $n \in \mathbf{N}$ ، يوجد زمرة جزئية ناظمية S من G بحيث $[G : S] = n$.

الحل: ليكن G زمرة ، وليكن $N \lhd G$ وليكن $f : G/N \to \mathbf{Z}$ تشاكل زمري شامل . ليكن $n \in \mathbf{N}$. وليكن $g : G/N \to \mathbf{Z}_n$ ، بحيث $g(xN) = \overline{f(xN)}$ لكل $xN \in G/N$. من الواضح أن g يكون تطبيقاً معرفاً جيداً . ليكن $xN , yN \in G/N$. إذن

$$g((xN)(yN)) = \overline{f((xN)(yN))} = \overline{f(xN)+f(yN)} = \overline{f(xN)} + \overline{f(yN)}$$
$$= g(xN) + g(yN)$$

إذن g يكون تشاكل زمري . بما أن f شامل ، فإن g يكون كذلك شامل . بما أن $Ker(g) \lhd G / N$ ، فإنة يوجد زمرة جزئية ناظمية S من G تحتوي N بحيث $Ker(g) = S / N$. إذن ينتج من مبرهنتي التماثل الأولى والثالثة في الزمر أن $G / S \cong (G / N)/(S / N) \cong \mathbf{Z}_n$. إذن $[G : S] = |G / S| = |\mathbf{Z}_n| = n$.

٥٤. (أ) اثبت أن رتبة كل عنصر في الزمرة $\mathbf{Q}/\mathbf{Z}$ تكون منتهية .

(ب) ليكن $n \in \mathbf{N}$ ، وليكن $f : \mathbf{Q}/\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ بحيث $f(x+\mathbf{Z}) = n x + \mathbf{Z}$ لكل $x + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. برهن أن f يكون تشاكل زمري وأن $Ker(f) \cong \mathbf{Z}_n$.

الحل: بما أن $\mathbf{Q}$ زمرة ابدالية ، فإن كل زمرة جزئية منها تكون ناظمية . وبالتالي $\mathbf{Z} \lhd \mathbf{Q}$. إذن $\mathbf{Q}/\mathbf{Z}$ تكون زمرة بالنسبة لعملية جمع المجموعات المشاركة (وتسمى زمرة القسمة لـ $\mathbf{Q}$ فوق $\mathbf{Z}$) .

(أ) ليكن $a/b + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. لاحظ أن $a,b\in\mathbf{Z}$, $b \neq 0$. بما أن

$$b\,(a/b + \mathbf{Z}) = (a/b + \mathbf{Z}) + \ldots + (a/b + \mathbf{Z}) \qquad (|b| \text{ مرة})$$

$$= a + \mathbf{Z} = \mathbf{Z}$$

فإن $\operatorname{ord}(a/b + \mathbf{Z}) = b < \infty$ (لاحظ أن $0 + \mathbf{Z} = \mathbf{Z}$ هو العنصر المحايد للزمرة $\mathbf{Q}/\mathbf{Z}$) .
إذن رتبة كل عنصر في الزمرة $\mathbf{Q}/\mathbf{Z}$ تكون منتهية .

(ب) ليكن $n\in\mathbf{N}$ ، وليكن $f : \mathbf{Q}/\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ بحيث $f(x+\mathbf{Z}) = nx+\mathbf{Z}$ لكل $x+\mathbf{Z}\in\mathbf{Q}/\mathbf{Z}$. ليكن $a/b + \mathbf{Z}\,,\, c/d + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. إذن

$$f((a/b + \mathbf{Z}) + (c/d + \mathbf{Z})) = f((ad+cb)/bd + \mathbf{Z})$$

$$= n((ad+cb)/bd) + \mathbf{Z}$$

$$= (na/b + \mathbf{Z}) + (nc/d + \mathbf{Z})$$

$$= f(a/b + \mathbf{Z}) + f(c/d + \mathbf{Z})$$

إذن f يكون تشاكل زمري . لاحظ f يكون شامل لأن كل عنصر $a/b + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$ يكون صورة بـ f للعنصر $a/nb + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$.

$$\operatorname{Ker}(f) = \{a/b + \mathbf{Z} \mid f(a/b + \mathbf{Z}) = \mathbf{Z}\}$$

$$= \{a/b + \mathbf{Z} \mid na/b + \mathbf{Z} = \mathbf{Z}\}$$

$$= \{a/b + \mathbf{Z} \mid na/b\in\mathbf{Z}\}$$

$$= \{m/n + \mathbf{Z} \mid m\in\mathbf{Z}\}$$

والآن نبين أن $\operatorname{Ker}(f) \cong \mathbf{Z}_n$. ليكن $g : \mathbf{Z} \to \operatorname{Ker}(f)$ ، بحيث $g(m) = m/n + \mathbf{Z}$ لكل $m\in\mathbf{Z}$. إذن من الواضح أن g يكون تطبيقاً معرفاً جيداً وشاملاً . ليكن $m,m'\in\mathbf{Z}$. إذن

$$g(m + m') = (m + m')/n + \mathbf{Z}$$

$= (m/n + m'/n) + \mathbf{Z}$

$= (m/n + \mathbf{Z}) + (m'/n + \mathbf{Z})$

$= g(m) + g(m')$

إذن g يكون تشاكل زمري شامل . لاحظ أن $Ker(g) = n\mathbf{Z}$. إذن ينتج من مبرهنة التماثل الأولى في الزمر أن $Ker(f) \cong \mathbf{Z}/n\mathbf{Z}$. لكن $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$. إذن $Ker(f) \cong \mathbf{Z}_n$.

٥٥. ليكن $n \in \mathbf{N}$. إذا كان $n = d\,m$ ، فاثبت أن

(أ) $m\,\mathbf{Z}_n \cong \mathbf{Z}_d$

(ب) $\mathbf{Z}_n / m\,\mathbf{Z}_n \cong \mathbf{Z}_m$

الحل: ليكن $n \in \mathbf{N}$. وليكن $n = d\,m$.

(أ) ليكن $f : \mathbf{Z}_n \to \mathbf{Z}_n$ ، بحيث $f(\bar{x}) = \overline{mx}$ لكل $\bar{x} \in \mathbf{Z}_n$. من الواضح أن f معرف جيداً . ليكن $\bar{x}, \bar{y} \in \mathbf{Z}_n$. إذن

$$f(\bar{x} + \bar{y}) = f(\overline{x+y}) = \overline{m(x+y)} = \overline{mx+my} = \overline{mx} + \overline{my} = f(\bar{x}) + f(\bar{y})$$

إذن f يكون تشاكل زمري .

$$Ker(f) = \{ \bar{x} \in \mathbf{Z}_n \mid f(\bar{x}) = \bar{0} \}$$

$$= \{ \bar{x} \in \mathbf{Z}_n \mid \overline{mx} = \bar{0} \}$$

$$= \{ \bar{x} \in \mathbf{Z}_n \mid mx \equiv 0 \pmod n \}$$

$$= \{ \bar{x} \in \mathbf{Z}_n \mid n \mid mx \}$$

$$= \{ \bar{x} \in \mathbf{Z}_n \mid x = da ,\ a \in \mathbf{N} \}$$

$$= \{ \bar{0} , \bar{d} , \overline{2d} , \cdots , \overline{(m-1)d} \}$$

$$= \{ 0 + n\mathbf{Z} , d + n\mathbf{Z} , 2d + n\mathbf{Z} , \cdots , (m-1) + n\mathbf{Z} \}$$

$$= d\mathbf{Z}/n\mathbf{Z}$$

لاحظ أن $\mathbf{Z}_n \cong \mathbf{Z}/n\mathbf{Z}$. إذن ينتج من مبرهنة التماثل الأولى في الزمر أن

$$(\mathbf{Z}/n\mathbf{Z}) / (d\mathbf{Z}/n\mathbf{Z}) \cong f(\mathbf{Z}_n) = m\,\mathbf{Z}_n$$

إذن ينتج من مبرهنة التماثل الثالثة في الزمر أن $\mathbf{Z}_d \cong \mathbf{Z}/d\mathbf{Z} \cong m\,\mathbf{Z}_n$.

(ب) ليكن $g : \mathbf{Z}_n \to \mathbf{Z}_m$ ، بحيث $g(\bar{x}) = \bar{x}$ لكل $\bar{x} \in \mathbf{Z}_n$. أي أن $g(x+n\mathbf{Z}) = x+m\mathbf{Z}$ ، لكل $x+n\mathbf{Z} \in \mathbf{Z}_n$. ليكن $x+n\mathbf{Z}\,,\, y+n\mathbf{Z} \in \mathbf{Z}_n$. إذن

$$x+n\mathbf{Z} = y+n\mathbf{Z} \Leftrightarrow x-y \in n\mathbf{Z} \Leftrightarrow x-y = n\,a\,,\, a \in \mathbf{Z} \Leftrightarrow x-y = d\,a\,m$$

$$\Rightarrow x-y \in m\mathbf{Z} \Leftrightarrow x+m\mathbf{Z} = y+m\mathbf{Z}$$

$$\Leftrightarrow g(x+n\mathbf{Z}) = g(y+n\mathbf{Z})$$

إذن g يكون تطبيقاً معرفاً جيداً . من الواضح أن g يكون شامل .

$$\begin{aligned} g((x+n\mathbf{Z}) + (y+n\mathbf{Z})) &= g((x+y)+n\mathbf{Z}) \\ &= (x+y)+m\mathbf{Z} \\ &= (x+m\mathbf{Z}) + (y+m\mathbf{Z}) \\ &= g((x+n\mathbf{Z}) + g(y+n\mathbf{Z})) \end{aligned}$$

إذن g يكون تشاكل زمري .

$$\begin{aligned} Ker(g) &= \{\bar{x} \in \mathbf{Z}_n \mid g(x+n\mathbf{Z}) = 0+m\mathbf{Z}\} \\ &= \{\bar{x} \in \mathbf{Z}_n \mid x+m\mathbf{Z} = 0+m\mathbf{Z}\} \\ &= \{\bar{x} \in \mathbf{Z}_n \mid x \in m\mathbf{Z}\} \\ &= \{\bar{x} \in \mathbf{Z}_n \mid x = ma\,,\ \forall\, a \in \mathbf{Z}\} \\ &= \{m\bar{a} \mid \bar{a} \in \mathbf{Z}_n\} = m\,\mathbf{Z}_n \end{aligned}$$

إذن ينتج من مبرهنة التماثل الأولى في الزمر أن $\mathbf{Z}_n / m\mathbf{Z}_n \cong \mathbf{Z}_m$.

٥٦. ليكن G زمرة . برهن أن $C(G) \lhd G$
(حيث $C(G)$ هو مركز الزمرة G (center of G)) .

الحل: ليكن G زمرة . نبرهن أولاً أن $C(G) \le G$. ليكن $x,y \in C(G)$. بما أن

$C(G) = \{x \in G \mid x\,g = g\,x\,,\ \forall\, g \in G\}$ ، فإن لكل $g \in G$ يكون

$$(x\, y^{-1})\, g = x\, (y^{-1} g) = x\, (g^{-1} y)^{-1} = x\, (y\, g^{-1})^{-1}$$
$$= x\, (g\, y^{-1}) = (x\, g)\, y^{-1}$$
$$= (g\, x)\, y^{-1} = g\, (x\, y^{-1})$$

إذن $x\, y^{-1} \in C(G)$. إذن $C(G) \leq G$. والآن نبرهن أن $C(G) \lhd G$. لكل $g \in G\, ,\, x \in C(G)$ يكون $g\, x\, g^{-1} = g\, (g^{-1} x) = (g\, g^{-1})\, x = x$. إذن $g\, C(G)\, g^{-1} \subseteq C(G)$ ، لكل $g \in G$. إذن $C(G) \lhd G$.

٥٧. ليكن G زمرة ، وليكن N زمرة جزئية ناظمية عظمى من G . ليكن $\{1\} \neq B \lhd G\ ,\ \{1\} \neq A \lhd G$ ، بحيث $A \cap N = B \cap N = \{1\}$. برهن أن $A \cong B$.

الحل: ليكن G زمرة وليكن N زمرة جزئية ناظمية عظمى من G (maximal normal subgroup) . ليكن $\{1\} \neq A \lhd G\, ,\, \{1\} \neq B \lhd G$ ، بحيث $A \cap N = B \cap N = \{1\}$. إذن $N\, A \lhd G\ ,\ N\, B \lhd G$. إذن $N \leq N\, A \leq G$. لكن N زمرة جزئية ناظمية عظمى من G . إذن $N\, A = G$. بالمثل يكون $N\, B = G$. بالتالي من الفرض بأن $A \cap N = B \cap N = \{1\}$ ومن مبرهنة التماثل الثانية في الزمر ينتج أن

$$A \cong A / A \cap N \cong A\, N / N = G / N = B\, N / N \cong B / B \cap N \cong B$$

٥٨. ليكن G زمرة ، وليكن

$$N = \{x_1\, x_2 \ldots x_n\, x_n\, x_{n-1} \ldots x_2\, x_1 \mid x_1\, , \ldots , x_n \in G\ ,\, n \in \mathbf{N}\}$$

برهن أن $N \lhd G$ وأن $\bar{x}^{-1} = \bar{x}$ ، لكل $\bar{x} \in G / N$.

الحل: ليكن G زمرة ، وليكن

$$N = \{x_1\, x_2 \ldots x_n\, x_n\, x_{n-1} \ldots x_2\, x_1 \mid x_1\, , \ldots , x_n \in G\ ,\, n \in \mathbf{N}\}$$

بأخذ $n = 1$ ، نحصل على $(x_1)^2 \in N$ لكل $x_1 \in G$. أي أن $x^2 \in N$ لكل $x \in G$. إذن $1 \in N$. ليكن $x = x_1\, x_2 \ldots x_n\, x_n\, x_{n-1} \ldots x_2\, x_1 \in N$. إذن

$$x^{-1} = x_1^{-1}\, x_2^{-1} \ldots x_n^{-1}\, x_n^{-1}\, x_{n-1}^{-1} \ldots x_2^{-1}\, x_1^{-1} \in N$$

والآن نبين أن N تكون مغلقة بالنسبة لعملية الضرب المعرفة على G . ليكن $x,y \in G$. إذن x,y يكونان في الصورة التالية

$$x = x_1 x_2 \ldots x_n x_n x_{n-1} \ldots x_2 x_1 \quad , \quad y = y_1 y_2 \ldots y_m y_m y_{m-1} \ldots y_2 y_1$$

حيث $x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m\in G$. نضع $z = x_n \ldots x_2 x_1$. إذن

$$x\, y = x_1 x_2 \ldots x_n x_n x_{n-1} \ldots x_2 x_1 y_1 y_2 \ldots y_m y_m y_{m-1} \ldots y_2 y_1$$

$$= x_1 x_2 \ldots x_n z\, y_1 y_2 \ldots y_m y_m y_{m-1} \ldots y_2 y_1$$

$$= (x_1 x_2 \ldots x_n (z y_1 z^{-1})(z y_2 z^{-1})\ldots (z y_m z^{-1}))\ .$$

$$((z y_m z^{-1})(z y_{m-1} z^{-1})\ldots(z y_2 z^{-1})(z y_1 z^{-1})\, x_n \ldots x_2 x_1)$$

إذن $x\,y\in N$. إذن $N \le G$. والآن نبين أن $G \lhd N$. ليكن $g\in G$. إذن

$$g\, x\, g^{-1} = g\,(x_1 x_2 \ldots x_n x_n x_{n-1} \ldots x_2 x_1)\, g^{-1}$$

$$= ((g x_1 g^{-1})(g x_2 g^{-1})\ldots(g x_n g^{-1}))\ .$$

$$((g x_n g^{-1})(g x_{n-1} g^{-1})\ldots(g x_2 g^{-1})(g x_1 g^{-1}))$$

إذن $g\, x\, g^{-1}\in N$. إذن $g\, N\, g^{-1} \subseteq N$ ، لكل $g\in G$. إذن $N \lhd G$.

والآن نثبت أن $\bar{x}^{-1} = \bar{x}$ ، لكل $\bar{x}\in G/N$. ليكن $\bar{x} \in G/N$. أي أن $\bar{x} = x\,N\ ,\ x\in G$.
إذن $(\bar{x})^2 = (x\,N)\,(x\,N) = x^2 N = N$ ، لأن $x^2\in G$ لكل $x\in G$. إذن $\bar{x}^{-1} = \bar{x}$ ،
لكل $\bar{x}\in G / N$.

٥٩. ليكن G زمرة بحيث يوجد عدد $1\neq n\in \mathbf{N}$ يحقق $(x\,y)^n = x^n y^n$ لكل $x,y\in G$.
وليكن

$$A = \{x^n \mid x\in G\}\ ,\ B = \{x\in G \mid x^n = 1\}\ ,\ C = \{x^{n(n-1)} \mid x\in G\}$$

برهن أن

(أ) $B \lhd G$. $A \lhd G$ ،

(ب) إذا كانت الزمرة G منتهية ، فإن $|A| = |G/B|$ ،

(ت) لكل $x,y\in G$ يكون $x^{n-1} y^n = y^n x^{n-1}$, $x^{1-n} y^{1-n} = (x\,y)^{1-n}$ ،

(ث) C تكون زمرة جزئية ابدالية من G .

الحل: ليكن G زمرة بحيث يوجد عدد $1 \neq n \in \mathbf{N}$ يحقق $(x\,y)^n = x^n\,y^n$ لكل $x,y \in G$. وليكن
$A = \{x^n \mid x \in G\}$, $B = \{x \in G \mid x^n = 1\}$, $C = \{x^{n(n-1)} \mid x \in G\}$

(أ) ليكن $x^n, y^n \in A$. إذن من الفرض بأن $(x\,y)^n = x^n\,y^n$ لكل $x,y \in G$ ينتج أن

$$x^n\,(y^n)^{-1} = x^n\,(y^{-1})^n = (x\,y^{-1})^n \in A$$

إذن $A \leq G$. ليكن $g \in G$. إذن $g\,x^n\,g^{-1} = (g\,x\,g^{-1})^n \in A$. إذن $g\,A\,g^{-1} \subseteq A$. إذن $A \lhd G$. ليكن $x,y \in B$. إذن من الفرض بأن $(x\,y)^n = x^n\,y^n$ لكل $x,y \in G$ ينتج أن

$$(x\,y^{-1})^n = x^n\,(y^{-1})^n = x^n\,(y^n)^{-1} = 1$$

إذن $x\,y^{-1} \in B$. إذن $B \leq G$. بما أن $(g\,x\,g^{-1})^n = g\,x^n\,g^{-1} = 1$ ، فإن $g\,x\,g^{-1} \in B$. إذن $g\,B\,g^{-1} \subseteq B$. إذن $B \lhd G$.

(ب) ليكن G منتهية . إذن الزمرتين A , G/B تكونان منتهيتان . إذن لإثبات أن $|A| = |G/B|$ نثبت أن $f : A \to G/B$ ، بحيث أن $f(x^n) = x\,B$ لكل $x^n \in A$ يكون تقابل (أي متباين وشامل) . ليكن $x^n, y^n \in A$. إذن

$$x^n = y^n \iff x^n\,(y^n)^{-1} = 1 \iff x^n\,(y^{-1})^n = 1$$

$$\iff (x\,y^{-1})^n = 1 \iff x\,y^{-1} \in B$$

$$\iff x\,B = y\,B \iff f(x^n) = f(y^n)$$

إذن f يكون تطبيق معرفاً جيداً ومتباين . من الواضح أيضاً أن f يكون شامل . إذن f يكون تقابل .

(ت) ليكن $x,y \in G$. إذن $(y\,x)^n = (y\,x\,y\,y^{-1})^n = y\,(x\,y)^n\,y^{-1}$. لكن $(y\,x)^n = y^n\,x^n$. إذن $y^n\,x^n\,y = y\,(x\,y)^n$. وبالضرب من الشمال في y^{-1} نحصل على $y^{n-1}\,x^{n-1}\,x\,y = (x\,y)^n$. وبالضرب من اليمين في $(x\,y)^{-1}$ نحصل على

$$y^{n-1}\,x^{n-1} = (x\,y)^{n-1} \qquad (*)$$

إذن $(y^{n-1}\,x^{n-1})^{-1} = ((x\,y)^{n-1})^{-1}$. إذن $x^{1-n}\,y^{1-n} = (x\,y)^{1-n}$. كذلك

$$x^{1-n}\,y^n = x^{-1}\,x^n\,y^n = x^{-1}\,(x\,y)^n$$

$= x^{-1} (x y) (x y)^{n-1} = y (x y)^{n-1} =^{(*)} y y^{n-1} x^{n-1}$

$= y^n x^{n-1}$

(ث) ليكن $a = x^{n(n-1)} \in C$ ، حيث $x \in G$. إذن $a^{-1} = (x^{n(n-1)})^{-1} = (x^{-1})^{n(n-1)} \in C$. كذلك $1 = 1^{n(n-1)} \in C$. ليكن $a, b \in C$. إذن يوجد $x, y \in G$ ، بحيث $a = x^{n(n-1)} , b = y^{n(n-1)}$.
إذن C تحتوي 1 (العنصر المحايد في G) وتحتوي على معكوس لكل عنصر فيها . كذلك

$$a\, b = x^{n(n-1)} y^{n(n-1)} = (x^{n-1} y^{n-1})^n$$

$$=^{(*)} ((y\, x)^{n-1})^n = (y\, x)^{n(n-1)} \in C$$

أي أن C تكون مغلقة بالنسبة لعملية الضرب المعرفة على G . إذن $C \le G$.

٦٠. ليكن G زمرة منتهية ، وليكن $G \rhd B$. $G \rhd A$ بحيث $(|A| , |B|) = 1$. اثبت أن

(أ) $A \cap B = \{1\}$ ،

(ب) $a\, b = b\, a$ ، لكل $a \in A , b \in B$ ،

(ت) $A\, B \cong A \times B$.

الحل: ليكن G زمرة منتهية ، وليكن $G \rhd B$. $G \rhd A$ ، بحيث $(|A| , |B|) = 1$.

(أ) بما أن $A \cap B \le A , B$ ، فإنة ينتج من مبرهنة لاجرانج أن $|A \cap B| \mid |A| , |B|$. لكن $(|A| , |B|) = 1$. إذن $|A \cap B| = 1$. إذن $A \cap B = \{1\}$.

(ب) ليكن $a \in A , b \in B$. إذن $a\, b\, a^{-1} \in B$ ، لأن $G \rhd B$. إذن

$$a\, b\, a^{-1} b^{-1} = (a\, b\, a^{-1})\, b^{-1} \in B$$

كذلك $b\, a^{-1} b^{-1} \in A$ ، لأن $G \rhd A$. إذن

$$a\, b\, a^{-1} b^{-1} = a\, (b\, a^{-1} b^{-1}) \in A$$

إذن $a\, b\, a^{-1} b^{-1} \in A \cap B$. لكن من (أ) يكون $A \cap B = \{1\}$. إذن $a\, b\, a^{-1} b^{-1} = 1$. إذن $a\, b = b\, a$.

ملحوظة: نحتاج الشرط $A \cap B = \{1\}$ لبرهان (ب) ، ولكننا لا نحتاج الشرط $(|A| , |B|) = 1$.

(ت) بما أن $A \lhd G$ (أو $B \lhd G$) ، فإن $AB \le G$. كذلك $A \times B$ تكون زمرة (بالنسبة لعملية ضرب المركبات) . ليكن $f : A \times B \to A\,B$ بحيث $f((a,b)) = a\,b$ ، لكل $a \in A , b \in B$. ليكن $(a,b),(a',b') \in A \times B$. إذن

$$f((a,b)) = f((a',b')) \Leftrightarrow a\,b = a'\,b'$$

$$\Leftrightarrow (a')^{-1} a = b'\,b^{-1}$$

$$\overset{(أ)}{\Leftrightarrow} (a')^{-1} a = b'\,b^{-1} = 1$$

$$\Leftrightarrow a = a' , b = b'$$

$$\Leftrightarrow (a,b) = (a',b')$$

إذن f يكون تطبيق معرف جيداً (well define mapping) ومتباين . كذلك من الواضح أن f يكون شامل . وبما أن

$$f((a , b) (a' , b')) = f((a\,a' , b\,b')) = a\,a'\,b\,b' = a\,(a'\,b)\,b' = a\,b\,a'\,b' \quad \text{((من (ب))}$$

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

فإن f يكون تشاكل زمري . إذن f يكون تماثل زمري .

ملحوظة: (١) نحتاج الشرط $A \cap B = \{1\}$ لبرهان (ت) ، ولكننا لا نحتاج الشرط $(|A| , |B|) = 1$. الشرط $A \cap B = \{1\}$ نحتاجة لبرهان (ب) ونحتاج (ب) لبرهان (ت) .

(٢) يمكن أيضاً اثبات أن f يكون متباين كما يلي:

$$Ker(f) = \{(a,b) \in A \times B \mid f((a,b)) = 1\}$$

$$= \{(a,b) \in A \times B \mid a\,b = 1\}$$

$$= \{(a,b) \in A \times B \mid a = b^{-1}\}$$

$$= \{(a,b) \in A \times B \mid a = b = 1\} \quad \text{((من (أ))}$$

$= \{(1,1)\}$

لاحظ أن $(1,1)$ هو العنصر المحايد في $A \times B$. إذن f يكون متابين (وذلك من المبرهنة التي تنص على أن التشاكل الزمري يكون متابين إذا وفقط إذا كانت نواتة تحتوي على العنصر المحايد فقط) .

٦١. ليكن $\{G_i\}_{i\in I}$ فصل زمر . برهن أن $\bigoplus_{i\in I} G_i \lhd \prod_{i\in I} G_i$.

الحل: ليكن $\{G_i\}_{i\in I}$ فصل زمر . لاحظ أن $\prod_{i\in I} G_i$ هي زمرة الضرب المباشر الخارجي لفصل الزمر $\{G_i\}_{i\in I}$. أما $\bigoplus_{i\in I} G_i$ فهي مجموعة جزئية من الزمرة $\prod_{i\in I} G_i$ معرفة كما يلي:

$(a_i)_{i\in I} \in \bigoplus_{i\in I} G_i$ إذا وفقط إذا كان عدد مركبات العنصر $(a_i)_{i\in I}$ التي لا تساوي المحايد منتهي .

إذن $(1_i)_{i\in I} \in \bigoplus_{i\in I} G_i$ ، حيث 1_i هو العنصر المحايد في الزمرة G_i لكل $i\in I$. ليكن $(a_i)_{i\in I} , (b_i)_{i\in I} \in \bigoplus_{i\in I} G_i$. إذن عدد المركبات التي لا تساوي محايد في كل من $(a_i)_{i\in I} , (b_i)_{i\in I}$ يكون منتهي . إذن عدد العناصر $a_i b_i , i\in I$ التي لا تساوي محايد يكون منتهي . إذن $(a_i)_{i\in I} (b_i)_{i\in I} = (a_ib_i)_{i\in I} \in \bigoplus_{i\in I} G_i$. كذلك

$$((a_i)_{i\in I})^{-1} = (a_i^{-1})_{i\in I} \in \bigoplus_{i\in I} G_i$$

إذن $\bigoplus_{i\in I} G_i \leq \prod_{i\in I} G_i$. ليكن $(g_i)_{i\in I} \in \prod_{i\in I} G_i$. إذن

$$(g_i)_{i\in I} (a_i)_{i\in I} ((g_i)_{i\in I})^{-1} = (g_i)_{i\in I} (a_i)_{i\in I}(g_i^{-1})_{i\in I}$$
$$= (g_i a_i g_i^{-1})_{i\in I} \in \bigoplus_{i\in I} G_i$$

لأن عدد المركبات $g_i a_i g_i^{-1}$ التي لا تساوي محايد يكون منتهي . إذن $\bigoplus_{i\in I} G_i \lhd \prod_{i\in I} G_i$.

الزمر الدائرية – Cyclic groups

٦٢. برهن أن الزمرة **Q** غير دائرية وأن **Z** لا تماثل **Q** .

الحل: نفرض أن $\mathbf{Q}$ دائرية . إذن يوجد $q\in\mathbf{Q}$ ، بحيث $\mathbf{Q} = \langle q\rangle$. إذن يوجد تماثل زمري وحيد $f : \mathbf{Z} \to \mathbf{Q}$ ، بحيث $f(1) = q$. لاحظ أن $f(n) = n\, f(1) = n\, q \;,\; \forall\, n\in\mathbf{Z}$. لكن $\frac{q}{2} \in \mathbf{Q}$ ليست صورة لأي عنصر في $\mathbf{Z}$. بالتالي f لا يكون شامل . وهذا تناقض مع كون f تماثل . إذن $\mathbf{Q}$ ليست دائرية . وبما أن $\mathbf{Z}$ دائرية ، فإن $\mathbf{Z}$ لا تماثل $\mathbf{Q}$.

ملحوظة: في تمرين (١٣٣) نعطي برهاناً آخر لهذا التمرين .

٦٣. ليكن $G = \left\{\begin{bmatrix} a & b \\ -b & a\end{bmatrix} \middle|\, a. b \in \mathbf{R} .\; a^2 + b^2 \neq 0\right\}$. أوجد زمرة جزئية دائرية من G رتبتها 4 .

الحل: ليكن $G = \left\{\begin{bmatrix} a & b \\ -b & a\end{bmatrix} \middle|\, a. b \in \mathbf{R} .\; a^2 + b^2 \neq 0\right\}$. نفرض أن $A\in G$ ، حيث $A=\begin{bmatrix} 0 & 1 \\ -1 & 0\end{bmatrix}$. إذن

$$A^2=\begin{bmatrix} -1 & 0 \\ 0 & -1\end{bmatrix} \;,\; A^3=\begin{bmatrix} 0 & -1 \\ 1 & 0\end{bmatrix} \;,\; A^4=\begin{bmatrix} 1 & 0 \\ 0 & 1\end{bmatrix}$$

إذن $\langle A\rangle$ تكون زمرة جزئية دائرية من G رتبتها 4 .

٦٤. ليكن G زمرة ، وليكن $a\in G$. اثبت أن
$G = \langle a\rangle \;\Leftrightarrow\; f : \mathbf{Z} \to G$ ، حيث $f(n) = a^n$ لكل $n\in\mathbf{Z}$ يكون تشاكل زمري شامل .

الحل: ليكن G زمرة ، وليكن $a\in G$.

($\Leftarrow$) ليكن $G = < a >$. ليكن $f : \mathbf{Z} \to G$ ، حيث $f(n) = a^n$ لكل $n\in\mathbf{Z}$. ليكن $m,n\in\mathbf{Z}$. إذن $f(m) = a^m , f(n) = a^n$. إذن $f(m + n) = a^{m+n} = a^m a^n = f(m) f(n)$. إذن f يكون تشاكل زمري . ليكن $x\in G$. إذن يوجد $n\in\mathbf{N}$ ، بحيث $x = a^n$. إذن $f(n) = x$. إذن f يكون شامل .

($\Rightarrow$) ليكن $f : \mathbf{Z} \to G$ ، حيث $f(n) = a^n$ لكل $n\in\mathbf{Z}$ تشاكل زمري شامل . نبرهن أن $G = < a >$. ليكن $x\in G$. إذن يوجد $m\in\mathbf{N}$ ، بحيث $a^m = f(m) = x$. إذن $G = < a >$.

٦٥. ليكن G زمرة دائرية منتهية . اثبت أنة لكل قاسم d لرتبة G يوجد زمرة جزئية وحيدة من G رتبتها d .

الحل: ليكن G زمرة دائرية منتهية . ليكن $|G| = n$. إذن $ord(a) = n$, $G = < a >$. ليكن $d \mid n$. إذن يوجد $m \in \mathbf{N}$ ، بحيث $n = d\, m$. بما أن (مبرهنة) $ord(a^m) = n/(m , n)$ ، فإن $ord(a^m) = d\, m /(m , dm) = d$. إذن $< a^m >$ تكون زمرة جزئية من G رتبتها d .
والآن نبرهن أن $< a^m >$ هي الزمرة الجزئية الوحيدة من G التي رتبتها d. ليكن $S \leq G$ ، بحيث $|G| = d$. نبرهن أن $S = < a^m >$. بما أن G دائرية ، فإن S تكون دائرية أيضاً (مبرهنة) . إذن يوجد $a^t \in G$ ، بحيث $S = < a^t >$. إذن $ord(a^t) = ord(S) = d$. لكن $ord(a^t) = n /(t , n)$. إذن $d = dm/(t,n)$. إذن $(t , n) = m$. إذن $m \mid t$. إذن يوجد $k \in \mathbf{N}$ ، بحيث $t = m\, k$. إذن $a^t = a^{m\,k} = (a^m)^k \in < a^m >$. إذن $S = < a^t > \leq < a^m >$. لكن $|< a^t >| = |< a^m>| = d$. إذن $S = < a^m >$.

٦٦. ليكن G زمرة ابدالية منتهية بحيث تحتوي على الأكثر على عدد n حلول مختلفة للمعادلة $x^n = 1$ ، لكل $n \in \mathbf{N}$. اثبت أن G تكون دائرية .

الحل: ليكن G زمرة ابدالية منتهية بحيث تحتوي على الأكثر على عدد n حلول مختلفة للمعادلة $x^n = 1$ ، لكل $n \in \mathbf{N}$. ليكن $m = Max\{ord(a) \mid a \in G\}$. إذن يوجد $x \in G$ ، بحيث $ord(x) = m$. إذن ينتج من تمرين (٢٧) أن $ord(a) \mid m$ ، لكل $a \in G$. إذن $a^m = 1$ ، لكل $a \in G$. لكن من فرض التمرين G تحتوي على الأكثر على m حلول مختلفة للمعادلة $x^m = 1$. إذن $|G| \leq m$. لكن $x \in G$, $m = ord(x)$. إذن $|G| \geq m$. إذن $|G| = m = ord(x)$. إذن $G = < x >$. إذن G تكون دائرية .

٦٧. (أ) ليكن G زمرة ، وليكن $N \lhd G$. $< x > = N$. اثبت أن كل زمرة جزئية من N تكون ناظمية في G .
(ب) اعطي مثالاً للزمر A , B , G بحيث $A \lhd B \lhd G$ لكن $A \ntriangleleft G$.

الحل: (أ) ليكن G زمرة ، وليكن $N \lhd G$. حيث $N = < x >$. ليكن $S \leq N$. بالتالي $S \leq G$. بما أن N زمرة دائرية ، فإن S تكون أيضاً زمرة دائرية . إذن يوجد $m \in \mathbf{N}$ ، بحيث $S = < x^m >$. نبرهن أن $S \lhd G$. ليكن $g \in G , s \in S$. إذن يوجد $n \in \mathbf{N}$ ، بحيث

إذن $s = (x^m)^n = x^r$. إذن $g\,s\,g^{-1} = g\,x^r\,g^{-1} = (g\,x\,g^{-1})^r$. لكن $N \lhd G$. إذن

$g\,N\,g^{-1} \subseteq N$. إذن $g\,x\,g^{-1} \in N$. إذن يوجد $k \in \mathbf{N}$ ، بحيث $g\,x\,g^{-1} = x^k$. إذن

$$g\,s\,g^{-1} = (g\,x\,g^{-1})^r = (x^k)^r = (x^r)^k = s^k \in S$$

إذن $g\,S\,g^{-1} \subseteq S$. إذن $S \lhd G$.

(ب) ليكن $A = \{1 , (1\ 2)(3\ 4)\} , B = K_4 , G = A_4$. حيث

$$A_4 = \{1,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3),(2\ 3\ 4),(2\ 4\ 3),(1\ 2\ 3),(1\ 2\ 4)$$
$$,(1\ 3\ 2),(1\ 3\ 4),(1\ 4\ 2),(1\ 4\ 3)\} ,$$
$$K_4 = \{1 , (1\ 2)\ (3\ 4) , (1\ 3)\ (2\ 4) , (1\ 4)\ (2\ 3)\}$$

لاحظ أن $A \lhd K_4 \lhd A_4$ وأن $A \ntriangleleft A_4$ ، لأن

$$(1\ 2\ 3)\ ((1\ 2)(3\ 4))\ (1\ 2\ 3)^{-1} = (1\ 2\ 3)\ (1\ 2)\ (3\ 4)\ (1\ 3\ 2) = (1\ 4)\ (2\ 3) \notin A$$

إذن $A = \{1 , (1\ 2)(3\ 4)\} , B = K_4 , G = A_4$ تكون مثالاً للزمر المطلوبة .

٦٨. إذا كان G زمرة غير ابدالية ، فبرهن أن الزمرة $G/C(G)$ لا تكون دائرية .

الحل: ليكن G زمرة غير ابدالية . نبرهن أن $G/C(G)$ لا تكون دائرية . نفرض عكس المطلوب ، أي نفرض أن $G/C(G)$ تكون دائرية . نضع $C = C(G)$. إذن يوجد $a \in G \backslash C$ ، بحيث $G/C = \langle aC \rangle$. ليكن $x,y \in G$. توجد ثلاثة حالات لـ x , y هي:

(أ) $x,y \notin C$. إذن يوجد $n,m \in \mathbf{Z}$ ، بحيث $yC = a^m C$, $xC = a^n C$. إذن يوجد $c,c' \in C$ ، بحيث $x = a^n c , y = a^m c'$. إذن

$$x\,y = (a^n c)\,(a^m c') = a^n\,(c\,a^m)\,c' = a^n\,(a^m c)\,c' = a^{n+m}\,(c\,c') \quad ,$$

$$y\,x = (a^m c')\,(a^n c) = a^m\,(c'\,a^n)\,c = a^m\,(a^n c')\,c = a^{n+m}\,(c'\,c) .$$

إذن $x\,y = y\,x$.

(ب) $x \notin C , y \in C$. إذن $x\,C = a^n\,C , n \in \mathbf{Z}$. إذن كما سبق يوجد $c \in C$ ، بحيث $x = a^n c$. إذن

$$x\,y = (a^n c)\,y = a^n\,(c\,y) = a^n\,(y\,c)$$

$= (a^n y)\, c = y\, (a^n c) = y\, x$

(ت) $x,y \in C$. إذن $x\, y = y\, x$.

في هذة الحالة G تكون ابدالية . وهذا يتناقض مع الفرض بأن G غير ابدالية . إذن G/C ليست دائرية .

٦٩. إذا كان G زمرة بحيث $|G| = p^2$ حيث p عدد أولي ، فاثبت أن G تكون ابدالية .

الحل: ليكن G زمرة بحيث $|G| = p^2$ ، حيث p عدد أولي . بما أن $C(G) \leq G$ ، فإن $|C(G)|$ يساوي 1 أو p أو p^2 . من معادلة الفصول للزمرة G ينتج أن $|C(G)| \neq 1$. نفرض أن $|C(G)| = p$. إذن $|G/C(G)| = p$. إذن $G/C(G)$ تكون زمرة دائرية . إذا كانت G غير ابدالية ، فإننا نحصل على تناقض مع ما جاء في تمرين (٦٨) . إذن G تكون ابدالية أو $|C(G)| \neq p$. إذا كان $|C(G)| \neq p$ ، فإن $|C(G)| = p^2$. إذن $|G| = |C(G)|$. إذن G تكون ابدالية .

الضرب المباشر للزمر – Direct product of groups

٧٠. اذكر سبب صحة أو خطأ كل جملة مما يلي:

(أ) $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$

(ب) $\mathbf{Z}_8 \cong \mathbf{Z}_2 \times \mathbf{Z}_4$

(ت) $\mathbf{Z}_8 \cong \mathbf{Z}_2 \times K_4$

الحل: (أ) صحيحة ، بناءً على المبرهنة: ليكن $m,n \in \mathbf{N}$. إذن

$$(m,n) = 1 \iff \mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$$

(ب) خطأ ، لأن $(2,4) \neq 1$ بناءً على المبرهنة المذكورة في (أ) .

(ت) خطأ ، لأن: $K_4 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. وبالتالي $\mathbf{Z}_8 \cong \mathbf{Z}_2 \times K_4 \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. لكن $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ زمرة غير دائرية ، بينما $\mathbf{Z}_8$ زمرة دائرية .
سبب آخر لخطأ هذة العبارة: $\mathbf{Z}_2 \times K_4$ تحتوي على أكثر من زمرتين جزئيتين رتبتهما 2

($\{(\bar{0},1),(\bar{0},a)\}$, $\{(\bar{0},1),(\bar{0},b)\}$, $\{(\bar{0},1),(\bar{0}.c)\}$) ، وتحتوي ثلاثة زمر جزئية . بينما $\mathbf{Z}_8$ تحتوي على زمرة جزئية واحدة رتبتها 2 وهي $\langle\bar{4}\rangle = \{\bar{0},\bar{4}\}$.

٧١. ليكن $(\bar{x}.\bar{y}) \in \mathbf{Z}_m \times \mathbf{Z}_n$. اذكر العلاقة بين $\mathrm{ord}((\bar{x}.\bar{y})).\mathrm{ord}(\bar{x}).\mathrm{ord}(\bar{y})$ ، ثم أوجد $\mathrm{ord}((\bar{x}.\bar{y}))$ عندما $m = 6 , n = 9$.

الحل: ليكن $(\bar{x}.\bar{y}) \in \mathbf{Z}_m \times \mathbf{Z}_n$. إذن

$$\mathrm{ord}\big((\bar{x}.\bar{y})\big) = \mathrm{l.c.m}(\mathrm{ord}(\bar{x}).\mathrm{ord}(\bar{y}))$$

ليكن $(\bar{5}.\bar{3}) \in \mathbf{Z}_6 \times \mathbf{Z}_9$. إذن

$$\mathrm{ord}\left((\bar{5}.\bar{3})\right) = \mathrm{l.c.m}(\mathrm{ord}(\bar{5}).\mathrm{ord}(\bar{3})) = \mathrm{l.c.m}\ (6,3) = 6$$

٧٢. ليكن $G = \mathbf{Z}_{p^3} \times \mathbf{Z}_{p^2} \times \mathbf{Z}_p$ ، حيث p عدد أولي . أوجد عدد العناصر في الزمرة G التي رتبها تساوي: (أ) p (ب) p^2 (ت) p^3

الحل: ليكن $G = \mathbf{Z}_{p^3} \times \mathbf{Z}_{p^2} \times \mathbf{Z}_p$ ، حيث p عدد أولي .

(أ) مجموعة العناصر التي تنتمي إلى G ورتبها أقل من أو تساوي p هي

$$A = \{ (i\,\bar{p}^2, j\,\bar{p}, k\,\bar{1}) \mid 1 \le i , j , k \le p \}$$

لاحظ أن $|A| = p^3$. بما أن $|G| = p^6$ ، فإن رتبة أي عنصر في G تكون قوة للعدد الأولي p . العنصر $(\bar{0} , \bar{0} , \bar{0})$ ينتمي إلى A وهو العنصر الوحيد في A الذي رتبتة تساوي 1 . إذن عدد العناصر في G التي رتبها تساوي p هو $p^3 - 1$.

(ب) مجموعة العناصر التي تنتمي إلى G ورتبها أقل من أو تساوي p^2 هي

$$B = \{(s\,\bar{p}, t\,\bar{1} , r\,\bar{1}) | 1 \le s , t \le p^2 .\ 1 \le r \le p\}$$

وذلك لأن كل عنصر في B يحتوي على مركبة واحدة على الأقل رتبتها تساوي p^2 . لاحظ أن عدد المركبات الأولى لعناصر B يساوي p^2 ، وعدد المركبات الثانية لعناصر B يساوي p^2 ، وعدد المركبات الثالثة لعناصر B يساوي p . إذن $|B| = p^5$. لاحظ أن $A \subset B$. إذن $B \setminus A$ هي مجموعة العناصر التي تنتمي إلى G ورتبها تساوي p^2 . إذن عدد العناصر التي تنتمي إلى G ورتبها تساوي p^2 هو $p^5 - p^3$.

(ت) بما أن $|G| = p^6$ وبما أن رتبة أي عنصر في G تساوي 1 أو p أو p^2 أو p^3 ، فإن $G \setminus B$ هي مجموعة العناصر التي تنتمي إلى G ورتبها تساوي p^3 . إذن عدد العناصر التي تنتمي إلى G ورتبها تساوي p^3 هو $p^6 - p^5$.

٧٣. ليكن p عدد أولي ، وليكن $n \in \mathbf{N}$. إذا كان $\mathbf{Z}_{p^n} \cong A \times B$ ، فبرهن أن $A = \{1\}$ أو $B = \{1\}$.

الحل: ليكن p عدد أولي ، وليكن $n \in \mathbf{N}$. وليكن $\mathbf{Z}_{p^n} \cong A \times B$. إذن $A \times \{1\}$ تماثل زمرة جزئية من $\mathbf{Z}_{p^n}$. لكن $A \times \{1\} \cong A$. إذن A تماثل زمرة جزئية من $\mathbf{Z}_{p^n}$. إذن يوجد $r \in \mathbf{N}$ ، بحيث $A \cong \mathbf{Z}_{p^r}$ ، لأن أي زمرة جزئية من زمرة دائرية تكون أيضاً دائرية . بالمثل يوجد $s \in \mathbf{N}$ ، بحيث $B \cong \mathbf{Z}_{p^s}$. إذن $\mathbf{Z}_{p^n} \cong \mathbf{Z}_{p^r} \times \mathbf{Z}_{p^s}$. نفرض أن $A \neq \{1\} , B \neq \{1\}$. إذن $r,s \geq 1$. إذن $\mathbf{Z}_{p^r} \times \mathbf{Z}_{p^s}$ تحتوي على زمرتين جزئيتين مختلفتين رتبتهما تساوي p . لكن هذا يتناقض مع المبرهنة التي نصها (إذا كانت G زمرة دائرية ، فإن G تحتوي على زمرة جزئية وحيدة لكل قاسم لرتبة G بحيث تكون رتبتها تساوي هذا القاسم) . إذن $A = \{1\}$ أو $B = \{1\}$.

٧٤. ليكن $A = \{ z \in \mathbf{C} \mid |z| = 1\}$, $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$, $\mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$.
اثبت أن A , $\mathbf{C}^*$, $\mathbf{R}^+$ تكون زمر ضربية (بالنسبة لعملية ضرب الأعداد) وأن $\mathbf{C}^* \cong \mathbf{R}^+ \times A$.

الحل: من الواضح أن A , $\mathbf{C}^*$, $\mathbf{R}^+$ تكون زمر بالنسبة لعملية ضرب الأعداد . وبالتالي $\mathbf{R}^+ \times A$ تكون زمرة بالنسبة لعملية ضرب المركبات . ليكن $z \in \mathbf{C}^*$. في الصورة القطبية يكون $z = r\, e^{i\theta} = r(\cos\theta + i \sin\theta)$. ليكن $\alpha : \mathbf{C}^* \to \mathbf{R}^+ \times A$ ، بحيث $\alpha(r\, e^{i\theta}) = (r , e^{i\theta})$ لكل $r\, e^{i\theta} \in \mathbf{C}^*$. إذن من الواضح أن α يكون تماثل زمري .

٧٥. أوجد كل الزمر الجزئية من الزمرة $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ والتي رتبها تساوي:
(أ) 2 (ب) 4

الحل: نضع $G = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

(أ) ليكن $(a,b,c) \in G$ ، بحيث $ord((a,b,c)) = 2$. إذن $S = \{(0,0,0),(a,b,c)\} \leq G$ و $ord(S) = 2$. إذن نوجد كل العناصر المختلفة في G التي رتبها تساوي 2 . بما أن

$$2 = ord((a,b,c)) = l.c.m\,(ord(a)\,,\,ord(b)\,,\,ord(c))$$

الإحتمالات المختلفة لـ $(ord(a)\,,\,ord(b)\,,\,ord(c))$ هي

$$(2,1,1)\,,\,(1,2,1)\,,\,(1,1,2)\,,\,(2,2,1)\,,\,(2,1,2)\,,\,(1,2,2)\,,\,(2,2,2)$$

إذن توجد سبعة عناصر مختلفة في G رتبها تساوي 2 (أي كل عناصر G ماعدا العنصر المحايد) . إذن توجد سبعة زمر جزئية مختلفة من G رتبها تساوي 2 هي

$$\{(\bar{0},\bar{0},\bar{0}),(\bar{1},\bar{0},\bar{0})\}\;,\;\{(\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{1},\bar{0})\}\;,\;\{(\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{0},\bar{1})\}\;.$$

$$\{(\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{1},\bar{1})\}\;.\;\{(\bar{0},\bar{0},\bar{0}),(\bar{1},\bar{0},\bar{1})\}\;.\;\{(\bar{0},\bar{0},\bar{0}),(\bar{1},\bar{1},\bar{0})\}\,.$$

$$\{(\bar{0},\bar{0},\bar{0}),(\bar{1},\bar{1},\bar{1})\}$$

(ب) نوجد الزمر الجزئية المختلفة من G التي رتبها تساوي 4 . أي زمرة جزئية من G رتبتها 4 تماثل K_4 (زمرة كلين الرباعية (the Klein 4-group)) ، لأن أي زمرة رتبتها 4 تماثل $\mathbf{Z}_4$ أو K_4 ، كما أن $\mathbf{Z}_4$ زمرة دائرية و G لا تحتوي زمرة جزئية دائرية رتبتها 4 . لكن K_4 تتولد بعنصرين رتبتهما 2 . إذن أي زمرة جزئية من G رتبتها 4 تتولد بعنصرين رتبتهما 2 . لاحظ أن رتبة كل عنصر في G ماعدا العنصر المحايد تساوي 2 . ليكن $a,b,c,d \in G\backslash\{0\}$ ، حيث $(\bar{0},\bar{0},\bar{0}) = 0$. إذن $< a,b > = < c,d >$ إذا حققت العناصر a,b,c,d أحد الشروط التالية:

١- $a = c\;,\; b = d$ ، لأنة في هذة الحالة يكون $a\,b = c\,d$

٢- $a = c\,,\, ab = d$ ، لأنة في هذة الحالة يكون $a\,b = d \Rightarrow c\,b = d \Rightarrow b = c\,d$

٣- $a = d\,,\, b = c$ ، لأنة في هذة الحالة يكون $a\,b = d\,c = c\,d$ (لاحظ أن G ابدالية)

٤- $b = c\,,\, a\,b = d$ ، لأنة في هذة الحالة يكون $ab = d \Rightarrow ac = d \Rightarrow a = dc = cd$

٥- $a = d\,,\, ab = c$ ، لأنة في هذة الحالة يكون $ab = c \Rightarrow db = c \Rightarrow b = dc = cd$

٦- $b = d\,,\, ab = c$ ، لأنة في هذة الحالة يكون $ab = c \Rightarrow ad = c \Rightarrow a = cd$

ليكن $G = \{a_0\,,\,a_1\,,\,a_2\,,\,a_3\,,\,a_4\,,\,a_5\,,\,a_6\,,\,a_7\}$ ، حيث

$$a_0 = (\bar{0},\bar{0},\bar{0})\;,\;a_1 = (\bar{1},\bar{0},\bar{0})\;,\;a_2 = (\bar{0},\bar{1},\bar{0})\;,\;a_3 = (\bar{0},\bar{0},\bar{1})\;,\;a_4 = (\bar{1},\bar{1},\bar{0})$$
$$,\;a_5 = (\bar{1},\bar{0},\bar{1})\;,\;a_6 = (\bar{0},\bar{1},1)\;,\;a_7 = (\bar{1},\bar{1},\bar{1})$$

إذن الزمر $< a_1,a_2 >$, $<a_1,a_3>$, … , $< a_1,a_6 >$, $< a_2,a_3 >$ تكون زمر جزئية مختلفة من G وعددها 7 . نعتبر الزمرة الجزئية $< c,d >$ ، حيث

$$(c,d) \notin A = \{(a_1,a_2) , (a_1,a_3) , \dots ,(a_1,a_6) , (a_2,a_3)\}$$

من السهل اختبار أن c,d مع مركبتي أحد عناصر A تحقق أحد الشروط الستة السابقة . بالتالي الزمر الجزئية السبعة السابقة هي كل الزمر الجزئية من G التي رتبها 4 .

ملحوظة: (١) لاحظ أن $G \cong K_4 \times \mathbf{Z}_2 \cong \mathbf{Z}_2 \times K_4$ ، حيث $K_4 = \{1,a,b,c\}$ هي زمرة كلين الرباعية (the Klein 4-group) . إذن كل الزمر الجزئية من G التي رتبها 4 تماثل الزمر

$$\{1,a\}\times \mathbf{Z}_2 \;,\; \{1,b\}\times \mathbf{Z}_2 \;,\; \{1,c\}\times \mathbf{Z}_2 \;,\; \mathbf{Z}_2\times \{1,a\} \;,\; \mathbf{Z}_2\times \{1,b\} \;,$$

$$\mathbf{Z}_2\times \{1,c\} .$$

(٢) طريقة أخرى لإيجاد الزمر الجزئية من G التي رتبها 4 :

بما أن $G = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ ، فإن الزمر الجزئية من G التي رتبها 4 هى :

$$\{\bar{0}\} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \;,\; \mathbf{Z}_2 \times \{\bar{0}\} \times \mathbf{Z}_2 \;,\; \mathbf{Z}_2 \times \mathbf{Z}_2 \times\{\bar{0}\} \;,\; \mathbf{Z}_2 \times\{(\bar{0}.\bar{0}).(\bar{0}.\bar{1})\}$$

$$,\; \mathbf{Z}_2 \times\{(\bar{0}.\bar{0}).(\bar{1}.\bar{1})\} \;,\; \{(\bar{0}.\bar{0}).(\bar{1}.\bar{0})\}\times \mathbf{Z}_2 \;,\; \{(\bar{0}.\bar{0}).(\bar{1}.\bar{1})\}\times \mathbf{Z}_2$$

٧٦. ليكن (n مرة) $G = \mathbf{Z}_p \times \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ ، حيث p عدد أولي . برهن أن $\mathrm{Aut}(G) \cong GL(n, \mathbf{Z}_p)$.

الحل: ليكن (n مرة) $G = \mathbf{Z}_p \times \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ ، حيث p عدد أولي . بما أن p عدد أولي ، فإن $\mathbf{Z}_p$ يكون حقل (field) . وبالتالي G يكون فضاء متجة فوق $\mathbf{Z}_p$ بعدة يساوي n . ليكن $f\in \mathrm{Aut}(G)$. إذن $f : G \to G$ يكون تماثل زمري . ليكن $x,y\in G$, $\bar{r}\in \mathbf{Z}_p$. إذن

$$f(x + y) = f(x) + f(y) \;,$$

$$\begin{aligned} f(\bar{r}\, x) &= f(x + \dots + x) \quad (r \text{ times}) \\ &= f(x) + \dots + f(x) \quad (r \text{ times}) \\ &= r\, f(x) = \bar{r}\, f(x) \end{aligned}$$

إذن f يكون تطبيق خطي (linear mapping) . إذن بالنسبة لأساس (basis) ما للفضاء المتجة G ، فإن f تناظر مصفوفة (matrix) من الدرجة n×n عناصرها تنتمي إلى $\mathbf{Z}_p$. وبما

أن f تقابل (أي متباين وشامل) ، فإنة يوجد معكوس لـ f . إذن المصفوفة المناظرة لـ f يوجد لها معكوس ، وبالتالي محددها لا يساوي 0 . إذن كل تماثل زمري في $Aut(G)$ يناظر مصفوفة في $GL(n,\mathbf{Z}_p)$. إذن $Aut(G) \cong GL(n, \mathbf{Z}_p)$.

٧٧. ليكن G زمرة ، وليكن $A \lhd G$. برهن ما يلي:

يوجد $G \rhd B$ ، بحيث G تكون الضرب المباشر الداخلي لـ A , B $\Leftrightarrow$ يوجد تشاكل زمري $\phi : G \to A$ بحيث تقيدة فوق A يكون تماثل زمري

(تقيد ϕ فوق A هو التطبيق $\phi|_A : A \to A$ بحيث $\phi|_A(a) = \phi(a)$ لكل $a\in A$) .

الحل: ليكن G زمرة ، وليكن $A \lhd G$.

($\Leftarrow$) ليكن $G \rhd B$ ، بحيث G تكون الضرب المباشر الداخلي لـ A , B . إذن

$$G = A B \ , \ A \cap B = \{1\} \ , \ a b = b a , \forall a\in A , b\in B$$

إذن $G = A B \cong A \times B$ (انظر تمرين (٦٠)) . ليكن $\phi : G \to A$ بحيث $\phi(a b) = a$ ، لكل $a b\in G$ (حيث $a\in A , b\in B$) . ليكن $a b , a' b'\in G$. بما أن G تكون الضرب المباشر الداخلي لـ A , B ، فإن

$$a b = a' b' \Leftrightarrow a = a' , b = b' \Leftrightarrow \phi(a b) = \phi(a' b')$$

إذن ϕ يكون تطبيق معرف جيداً (well define mapping) . بما أن

$$\phi((a b)(a' b')) = \phi((a a')(b b')) = a a' = \phi((a b)) \phi((a' b'))$$

فإن ϕ يكون تشاكل زمري . ليكن $\phi|_A : A \to A$ هو تقيد ϕ فوق A . إذن $\phi|_A(a) = \phi(a)$ ، لكل $a\in A$. إذن $\phi|_A$ يكون تشاكل زمري . بما أن $\phi|_A(a) = \phi(a) = \phi(a 1) = a$ ، فإن $\phi|_A$ يكون تطبيق الوحدة . إذن $\phi|_A$ يكون تماثل زمري .

($\Rightarrow$) ليكن $\phi : G \to A$ تشاكل زمري ، بحيث تقيدة $\phi|_A : A \to A$ المعرف بـ $\phi|_A(a) = \phi(a)$ لكل $a\in A$ يكون تماثل زمري . نبرهن أنة يوجد $G \rhd B$ ، بحيث G تكون الضرب المباشر الداخلي لـ A,B . لاحظ أن $Ker(\phi) = \{g\in G \mid \phi(g) = 1\}\lhd G$ (مبرهنة) .

نضع $B = Ker(\phi)$. لاحظ أن الفرض بأن $\phi|_A$ يكون تماثل زمري يؤدي إلى $A\backslash\{1\} \not\subset B$.

إذن $A \cap B = \{1\}$. والآن نبرهن أن $G = A B$.

$$g\in G \Rightarrow \phi(g)\in A \Rightarrow \exists\, a\in A , \text{s.t. } \phi|_A(a) = \phi(g$$

$$\Rightarrow \phi(a) = \phi(g) \Rightarrow 1 = (\phi(a))^{-1} \phi(g) = \phi(a^{-1} g)$$

$$\Rightarrow\ a^{-1} g\in B\ \Rightarrow\ g\in a B \subseteq A B$$

إذن $A B \supseteq G$. إذن $G = A B$. إذن G تكون الضرب المباشر الداخلي لـ A , B .

٧٨. ليكن G زمرة ، وليكن $A \lhd G ,\ B \lhd G$. برهن أن $G / (A \cap B)$ تماثل زمرة جزئية من الزمرة $G/A \times G/B$.

الحل: ليكن G زمرة ، وليكن $A \lhd G ,\ B \lhd G$. وليكن $\phi : G \to G/A \times G/B$ بحيث $\phi(g) = (gA , gB)$ لكل $g\in G$. ليكن $x,y\in G$. إذن

$$\phi(xy) = ((xy)A , (xy)B) = (xA , xB)\ (yA , yB) = \phi(x)\ \phi(y)$$

إذن ϕ يكون تشاكل زمري . بما أن

$$\begin{aligned}Ker(\phi) &= \{g\in G \mid \phi(g) = 1 = (A , B)\}\\ &= \{g\in G \mid (gA , gB) = (A , B)\}\\ &= \{g\in G \mid g\in A , g\in B)\}\\ &= A \cap B\end{aligned}$$

فإنة ينتج من مبرهنة التماثل الأولى في الزمر أن $G / (A \cap B) \cong \phi(G) \leq G/A \times G/B$.

أي أن $G / (A \cap B)$ تماثل زمرة جزئية من الزمرة $G/A \times G/B$.

ملحوظة: إذا كان $A \cap B = \{1\}$ ، فإن G تماثل زمرة جزئية من الزمرة $G/A \times G/B$.

٧٩. ليكن G زمرة ابدالية منتهية ، وليكن p عدد أولي . ليكن

$$A = \{x\in G \mid ord(x) = p^r , r\in \mathbf{N}\}\ ,\ B = \{x\in G \mid (ord(x) , p) = 1\}$$

اثبت أن $A , B \leq G$ وأن G تكون الضرب المباشر الداخلي لـ A , B .

الحل: ليكن G زمرة ابدالية منتهية ، وليكن p عدد أولي . ليكن

$$A = \{x\in G \mid ord(x) = p^r , r\in \mathbf{N}\}\ ,\ B = \{x\in G \mid (ord(x) , p) = 1\}$$

ليكن $x,y\in A$. إذن يوجد $r,s\in \mathbf{N}$ ، بحيث $ord(x) = p^r\ , ord(y) = p^s$. ليكن $t = l.c.m(r , s)$. بما أن G ابدالية ، فإن $ord(x\ y) = p^t$. إذن $x\ y\in A$. لكن G منتهية . إذن $A \leq G$. ليكن $x,y\in B$. $(ord(x) , p) = (ord(y) , p) = 1$. أي أن p لا يقسم كل من $ord(x) , ord(y)$. ليكن $ord(x) = r , ord(y) = s$. إذن $(r\ s , p) = 1$. بما أن $(x\ y)^{r\ s} = 1$. فإن $ord(x\ y) \mid r\ s$. إذن $(ord(x\ y) , p) = 1$. إذن $x\ y\in B$. إذن $B \leq G$.

ليكن $|G| = p^r\ m$ ، حيث $(p , m) = 1$. إذن $(p^r , m) = 1$. إذن يوجد $a,b\in \mathbf{Z}$ ، بحيث

$p^r a + m b = 1$. إذن كل عنصر $g \in G$ يكون في الصورة

$$g = g^{p^r a+mb} = (g^{p^r})^a \, (g^m)^b$$

لكن $\;(g^{p^r})^m = g^{p^r m} = g^{|G|} = 1$. إذن $\operatorname{ord}(g^{p^r}) \mid m$. إذن

$(\operatorname{ord}(g^{p^r}), p) = 1$. إذن $g^{p^r} \in B$. بالمثل $(g^m)^{p^r} = 1$. إذن $\operatorname{ord}(g^m) \mid p^r$. إذن

$g^m \in A$. بما أن $g^{p^r} \in B$ ، فإن $(g^{p^r})^a \in B$. وبما أن $g^m \in A$ ، فإن $(g^m)^b \in A$. إذن

$g \in A\,B$. إذن $G = A\,B$. لاحظ أن $A \cap B = \{1\}$. وبما أن G ابدالية ، فإن $A, B \lhd G$.

إذن G تكون الضرب المباشر الداخلي لـ A , B .

٨٠. ليكن G زمرة ابدالية منتهية . برهن أنة يوجد $n_1 , n_2 , \ldots , n_s \in \mathbf{N}$ ، بحيث

$$G \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_s} \quad , \quad n_{i+1} \mid n_i \; , \; i = 1 , 2 , \ldots , s-1$$

الحل: ليكن G زمرة ابدالية منتهية . ليكن $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ، حيث $p_1, p_2, \ldots, p_r$ أعداد أولية مختلفة في ترتيب تصاعدي ، أي أن $p_1 < p_2 < \ldots < p_r$. ليكن

$$\alpha_1 = \alpha_{11} + \alpha_{12} + \ldots + \alpha_{1s_1} \; ,$$

$$\alpha_2 = \alpha_{21} + \alpha_{22} + \ldots + \alpha_{2s_2} \; ,$$

$$\ldots\ldots\ldots\ldots\ldots \; ,$$

$$\alpha_r = \alpha_{r1} + \alpha_{r2} + \ldots + \alpha_{rs_r} \; .$$

حيث $1 \geq \alpha_{i1} \geq \alpha_{i2} \geq \ldots \geq \alpha_{is_i}$ ، لكل $1 \leq i \leq r$.

إذن

$$G \cong (\mathbf{Z}_{p_1^{\alpha_{11}}} \times \mathbf{Z}_{p_1^{\alpha_{12}}} \times \cdots \times \mathbf{Z}_{p_1^{\alpha_{1s_1}}}) \times (\mathbf{Z}_{p_2^{\alpha_{21}}} \times \mathbf{Z}_{p_2^{\alpha_{22}}} \times \cdots \times \mathbf{Z}_{p_2^{\alpha_{2s_2}}})$$
$$\times \cdots \times (\mathbf{Z}_{p_r^{\alpha_{r1}}} \times \mathbf{Z}_{p_r^{\alpha_{r2}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{rs_r}}})$$

ليكن $s = \max(s_1, s_2, \ldots, s_r)$. وليكن $\alpha_{it} = 0$ ، لكل $t > s_i$. إذن

$$G \cong (\mathbf{Z}_{p_1^{\alpha_{11}}} \times \mathbf{Z}_{p_1^{\alpha_{12}}} \times \cdots \times \mathbf{Z}_{p_1^{\alpha_{1s}}}) \times (\mathbf{Z}_{p_2^{\alpha_{21}}} \times \mathbf{Z}_{p_2^{\alpha_{22}}} \times \cdots \times \mathbf{Z}_{p_2^{\alpha_{2s}}})$$
$$\times \cdots \times (\mathbf{Z}_{p_r^{\alpha_{r1}}} \times \mathbf{Z}_{p_r^{\alpha_{r2}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{rs}}})$$
$$\cong (\mathbf{Z}_{p_1^{\alpha_{11}}} \times \mathbf{Z}_{p_2^{\alpha_{21}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{r1}}}) \times (\mathbf{Z}_{p_1^{\alpha_{12}}} \times \mathbf{Z}_{p_2^{\alpha_{22}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{r2}}})$$
$$\times \cdots \times (\mathbf{Z}_{p_1^{\alpha_{1s}}} \times \mathbf{Z}_{p_2^{\alpha_{2s}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{rs}}})$$

$= G_1 \times G_2 \times \ldots \times G_s$

حيث

$$G_i = \mathbf{Z}_{p_1^{\alpha_{1i}}} \times \mathbf{Z}_{p_2^{\alpha_{2i}}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_{ri}}} \quad , i = 1,2,\ldots,s$$

لاحظ أن $n_i = |G_i| = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_r^{\alpha_{ri}} \quad , i = 1,2,\ldots,s$. إذن

إذن $G_i \cong \mathbf{Z}_{n_i}$, $i=1,2,\cdots,s$. لاحظ أن $n_2 \mid n_1$, $n_3 \mid n_2$, … , $n_s \mid n_{s-1}$. إذن

$$G \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_s} \quad , \quad n_{i+1} \mid n_i \ , i = 1, 2, \ldots, s-1$$

٨١. ليكن $m,n \in \mathbf{N}$. اثبت أن

$\mathbf{Z}_m \times \mathbf{Z}_n \cong Z_s \times \mathbf{Z}_t$ ، حيث $s = g.c.d(m,n)$, $t = l.c.m(m,n)$

الحل: ليكن $m,n \in \mathbf{N}$. وليكن $p_1,p_2,\ldots,p_r$ هي كل الأعداد الأولية التي تقسم m أو n . إذن

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad , \quad n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

لاحظ أنة إذا كان p_i لا يقسم m ، فإن $\alpha_i = 0$. كذلك إذا كان p_i لا يقسم n ، فإن $\beta_i = 0$. إذن

$$\mathbf{Z}_m \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_r}} \quad ,$$

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\beta_1}} \times \mathbf{Z}_{p_2^{\beta_2}} \times \cdots \times \mathbf{Z}_{p_r^{\beta_r}}$$

إذن

$$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_r^{\alpha_r}} \times \mathbf{Z}_{p_1^{\beta_1}} \times \mathbf{Z}_{p_2^{\beta_2}} \times \cdots \times \mathbf{Z}_{p_r^{\beta_r}}$$

ليكن $\gamma_i = \min(\alpha_i , \beta_i)$, $\delta_i = \max(\alpha_i , \beta_i)$, $i = 1,2,\ldots,r$. إذن

$$\mathbf{Z}_{p_i^{\alpha_i}} \times \mathbf{Z}_{p_i^{\beta_i}} \cong \mathbf{Z}_{p_i^{\gamma_i}} \times \mathbf{Z}_{p_i^{\delta_i}} \quad , i = 1,2,\ldots,r$$

إذن

$$\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\gamma_1}} \times \mathbf{Z}_{p_2^{\gamma_2}} \times \cdots \times \mathbf{Z}_{p_r^{\gamma_r}} \times \mathbf{Z}_{p_1^{\delta_1}} \times \mathbf{Z}_{p_2^{\delta_2}} \times \cdots \times \mathbf{Z}_{p_r^{\delta_r}}$$

نضع

$$s = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \quad , \quad t = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r}$$

لاحظ أن $s = g.c.d(m,n)$, $t = l.c.m(m,n)$. إذن

$$\mathbf{Z}_s \cong \mathbf{Z}_{p_1^{\gamma_1}} \times \mathbf{Z}_{p_2^{\gamma_2}} \times \cdots \times \mathbf{Z}_{p_r^{\gamma_r}} \quad ,$$

$$\mathbf{Z}_t \cong \mathbf{Z}_{p_1^{\delta_1}} \times \mathbf{Z}_{p_2^{\delta_2}} \times \cdots \times \mathbf{Z}_{p_r^{\delta_r}}$$

إذن

$\mathbf{Z}_m \times \mathbf{Z}_n \cong Z_s \times \mathbf{Z}_t$ ، حيث $s = g.c.d(m,n)$, $t = l.c.m(m,n)$.

An action of a group on a set - تأثير زمرة على مجموعة

.٨٢ اثبت أن زمرة كلين الرباعية K_4 (the Klein 4-group) تؤثر (شماليا) على المجموعة $I_4 =\{1,2,3,4\}$ ، ثم أوجد G_4 , G_2 , orb(4) , orb(2) ، حيث $G = K_4$ (G_x هى زمرة ثبات x (stabilizer group of x)) .

الحل: زمرة كلين الرباعية كزمرة تباديل هى

$$K_4 = \{1 , (1\ 2)(3\ 4) , (1\ 3)(2\ 4) , (1\ 4)(2\ 3)\}$$

ليكن $* : K_4 \times I_4 \to I_4$ بحيث $f * x = f(x)$ ، لكل $(f , x)\in K_4 \times I_4$. لاحظ أن $f * x$ ترمز لصورة (f , x) بـ $*$. من الواضح أن $*$ يكون تطبيق معرف جيداً (well define mapping) . ليكن $f,g\in K_4$, $x\in I_4$. إذن

$$1* x = 1(x) = x \ , \ (f g) * x = (f g)(x) = f(g(x)) = f(g * x) = f * (g * x)$$

إذن $*$ تكون تأثير شمالي للزمرة K_4 على المجموعة I_4 . لاحظ أن هذا التأثير يسمى التأثير الطبيعي للزمرة K_4 على المجموعة I_4 .

$$ord(2) = \{f * 2 \mid f\in K_4\} = \{f(2) \mid f\in K_4\} = \{1,2,3,4\} = I_4 \ ,$$

$$ord(4) = \{f * 4 \mid f\in K_4\} = \{f(4) \mid f\in K_4\} = \{1,2,3,4\} = I_4 \ ,$$

$$G_2 = \{f\in K_4 \mid f * 2 = 2\} = \{f\in K_4 \mid f(2) = 2\} = \{1\} ,$$

$$G_4 = \{f\in K_4 \mid f * 4 = 4\} = \{f\in K_4 \mid f(4) = 4\} = \{1\}.$$

.٨٣ ليكن G زمرة منتهية ، بحيث $|G| = p^r n$ حيث p عدد أولي . وليكن $X = \{M \mid M \subseteq G \ , |M|= p^r\}$. اثبت أن $* : G\times X \to X$ بحيث $g * M = gM$ لكل $(g,M)\in G\times X$ يكون تأثير شمالي لـ G على X . اثبت كذلك أن $|orb(M)| \equiv 0 \pmod p$.

الحل: ليكن G زمرة منتهية ، بحيث $|G| = p^r n$ حيث p عدد أولي . وليكن
$X = \{M \mid M \subseteq G \ , |M| = p^r\}$. ليكن $\ast : G\times X \to X$ بحيث $g \ast M = gM$ لكل
$(g,M)\in G\times X$. من الواضح أن $\ast$ يكون تطبيق معرف جيداً . ليكن $g,h\in G \ , M\in X$. إذن

$$1 \ast M = M \ , \ (g\,h) \ast M = (g\,h)\, M = g\,(h\,M) = g\,(h \ast M) = g \ast (h \ast M)$$

إذن $\ast$ يكون تأثير شمالي لـ G على X . لاحظ أن $g\,M = g \ast M = M \ , \forall\ g\in G_M$. إذن
$G_M\, M = \{g\,m \mid g\in G_M \ , m\in M\}$. بما أن $G_M\, M = \cup_{m\in M} G_M\, m$ ، فإن
$|M| = |\, G_M\, M| = |G_M|\, t$ ، حيث t هو عدد المجموعات المشاركة اليمينية المختلفة
$G_M\, m \ \ , m\in M$. إذن $|G_M| \mid |M|$. لكن $|M| = p^r$. إذن $|G_M| = p^{s_M}$ ، حيث $0 \le s_M \le r$.
إذا كان $s_M < r$ ، فإن $|G_M| < |M|$. بالتالي يكون

$$|orb(M)| = [G : G_M] = |G| \,/\, |G_M| = p^r\, n \,/\, p^{s_M} = p^{r-s_M}\, n = p^t\, n$$

حيث $0 < t = r - s_M$. إذن $|orb(M)| \equiv 0 \pmod p$.

٨٤. ليكن G زمرة ، وليكن $H \le G \ , H \ne G$. ليكن $G / H = \{a\,H \mid a\in G\}$.
(أ) أوجد تأثير شمالي لـ G على G / H .
(ب) ليكن G منتهية. إذا كان $|G|$ لا يقسم $[G : H]!$ ، فاثبت أن H تحتوي على زمرة جزئية ناظمية غير بديهية من G .
(ت) إذا كان $[G : H] = p$ ، حيث p عدد أولي يقسم $|G|$ ، فبرهن أن $H \lhd G$.

الحل: ليكن G زمرة ، وليكن $H \le G \ , H \ne G$. ليكن $G / H = \{a\,H \mid a\in G\}$.

(أ) ليكن $\ast : G \times G / H \to G / H$ ، بحيث $a \ast b\,H = (a\,b)\,H$ ، لكل
$(a,b\,H)\in G \times G / H$. لاحظ أن $a \ast b\,H$ ترمز لصورة $(a \,,\, b\,H)$ بـ $\ast$. من الواضح أن
$\ast$ يكون تطبيق معرف جيداً . ليكن $a,b\in G \ , c\,H\in G/H$. إذن

$$1\ast a\,H = a\,H \ ,$$

$$(a\,b) \ast c\,H = ((a\,b)\,c)\,H = (a\,(b\,c))\,H = a \ast (b\,c)\,H = a \ast (b \ast c\,H)$$

إذن $\ast$ تكون تأثير شمالي للزمرة G على المجموعة G / H .

(ب) ليكن G منتهية . وليكن $|G|$ لا يقسم $[G : H]!$. نضع $X = G/H$. لاحظ أن $S(X)$ ترمز للزمرة المتماثلة على X (أي زمرة كل التباديل على X) . ليكن $f : G \to S(X)$ بحيث $f(a)(b\,H) = (a\,b)\,H$ ، لكل $a\in G\,,\ b\,H\in X$. من الواضح أن f يكون تطبيق معرف جيداً . ليكن $a,b\in G\,,\ c\,H\in X$. إذن

$$f(a\,b)(c\,H) = ((a\,b)\,c)\,H = (a\,(b\,c))\,H = f(a)((b\,c)\,H) = f(a)(f(b)(c\,H))$$
$$= (f(a)\,f(b))(c\,H)$$

إذن $f(a\,b) = f(a)\,f(b)$. إذن f يكون تشاكل زمري . إذن ينتج من مبرهنة التماثل الأولى في الزمر أن $G / Ker(f) \cong f(G)$. ومن مبرهنة لاجرانج ينتج أن $|f(G)| \mid |S(X)|$. لاحظ أن $[G : H]$ يرمز لعدد المجموعات المشاركة (الشمالية) المختلفة لـ H في G ، ويسمى الدليل (الشمالي) لـ H في G . إذن $|X| = |G / H| = [G : H]$. إذن $|S(X)| = [G : H]!$. إذن $|f(G)| \mid [G : H]!$. نفرض أن $Ker(f) = \{1\}$. إذن f يكون متباين ، وبالتالي $|G| = |f(G)|$. إذن $|G| \mid [G : H]!$. لكن هذ يتناقض مع الفرض بأن $|G|$ لا يقسم $[G : H]!$. إذن $Ker(f) \neq \{1\}$.

$$\begin{aligned} Ker(f) &= \{a\in G \mid f(a) = 1\} \\ &= \{a\in G \mid f(a)(b\,H) = b\,H\ ,\ \forall\, b\,H\in X\} \\ &= \{a\in G \mid (a\,b)\,H = b\,H\ ,\ \forall\, b\,H\in X\} \\ &= \{a\in G \mid b^{-1}\,a\,b\in H\ ,\ \forall\, b\in G\} \\ &= \{a\in G \mid a\in b\,H\,b^{-1}\,,\ \forall\, b\in G\} \\ &= \textstyle\bigcap_{b\in G} b\,H\,b^{-1} \end{aligned}$$

لكن $b\,H\,b^{-1} \cong H$ لكل $b\in G$. إذن $Ker(f) \leq H$. لكن $Ker(f) \lhd G$. إذن $Ker(f) \lhd H$.

٨٥. اثبت أن $G = SL(2,\mathbf{R})$ تؤثر شماليا على المجموعة $\mathbf{R}^2$ ، ثم أوجد $G_x\,,\ orb(x)$ ، حيث $x = (0,0)\,,\ (1,3)$.

الحل: ليكن $X = \mathbf{R}^2\ ,\ G = SL(2,\mathbf{R})$. نضع $X = \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \middle|\ x_1 . x_2 \in \mathbf{R} \right\}$. ليكن $* : G \times X \to X$ بحيث $A * x = A\,x$ لكل $(A\,,\,x)\in G \times X$. إذن $*$ يكون تطبيق معرف

جيداً . ليكن $A,B\in G$, $x\in X$. ليكن I ترمز لمصفوفة الوحدة في G (أي العنصر المحايد في الزمرة G) . إذن

$$I * x = I\,x = x \ ,$$

$$(AB) * x = (A\,B)\,x = A\,(B\,x) = A\,(B * x) = A * (B * x)$$

إذن $*$ تكون تأثير شمالي لـ G . ليكن $o = \begin{bmatrix}0\\0\end{bmatrix} \in X$. إذن

$$G_0 = \{A\in G \mid A * o = o\} = \{A\in G \mid A\,o = o\} = G \ ,$$

$$orb(o) = \{A * o \mid A\in G\} = \left\{ \begin{bmatrix}0\\0\end{bmatrix} \right\} = \{o\}$$

ليكن $x = \begin{bmatrix}1\\3\end{bmatrix} \in X$. إذن

$$G_x = \{A\in G \mid A * x = x\} = \{A\in G \mid A \begin{bmatrix}1\\3\end{bmatrix} = \begin{bmatrix}1\\3\end{bmatrix}\}$$

ليكن $A = \begin{bmatrix}r & a\\ b & c\end{bmatrix}\in G$. إذن

$$r + 3\,a = 1 \ , \ b + 3\,c = 3 \ , \ |A| = r\,c - a\,b = 1$$

إذن $a = (1-r)/3$, $b = -3 + 3\,r$, $c = 2 - r$. إذن

$$G_x = \left\{\begin{bmatrix} r & (1-r)/3\\ -3+3r & 2-r\end{bmatrix} \middle| \, r\in\mathbf{R} \right\} \ , orb(x) = \left\{ \begin{bmatrix}a+3b\\ c+3d\end{bmatrix} \middle| \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in G \right\}$$

٨٦. ليكن $G = \mathbf{R}^* \ (= \mathbf{R}\backslash\{0\})$ ، وليكن $X = \mathbf{R}^2$ ، وليكن $* : \mathbf{R}^* \times \mathbf{R}^2 \to \mathbf{R}^2$ بحيث $r * (x\,,y) = (r\,x\,, \frac{1}{r}\,y)$ ، لكل $(x,y)\in\mathbf{R}^2$, $r\in\mathbf{R}^*$. برهن أن $*$ يكون تأثير شمالي لـ G على X ، وأوجد زمر ثبات عناصر G .

الحل: ليكن $G = \mathbf{R}^* \ (= \mathbf{R}\backslash\{0\})$ ، وليكن $X = \mathbf{R}^2$ ، وليكن $* : \mathbf{R}^* \times \mathbf{R}^2 \to \mathbf{R}^2$ بحيث $r * (x\,,y) = (r\,x\,, \frac{1}{r}\,y)$ ، لكل $(x,y)\in\mathbf{R}^2$, $r\in\mathbf{R}^*$. ليكن $a,b\in\mathbf{R}^2$, $x = (x_1\,, x_2)\in\mathbf{R}^2$. إذن

$$1 * x = 1 * (x_1\,, x_2) = (x_1\,, x_2) = x \ ,$$

$$\begin{aligned}(a\,b) * x &= (a\,b) * (x_1\,, x_2) = ((a\,b)\,x_1\,, (1/a\,b)\,x_2)\\ &= (a\,(b\,x_1)\,, (1/a)((1/b)\,x_2)) = a * (b\,x_1\,, ((1/b)\,x_2)\\ &= a * (b * (x_1\,, x_2)) = a * (b * x)\end{aligned}$$

إذن $*$ تكون تـأثير شمالي للزمرة $\mathbf{R}^*$ على المجموعة $\mathbf{R}^2$. نفرض أن $x \neq (0,0)$. إذن

$$G_x = \{a \in \mathbf{R}^* \mid a * x = x\} = \{a \in \mathbf{R}^* \mid a * (x_1 , x_2) = (x_1 , x_2)\}$$
$$= \{a \in \mathbf{R}^* \mid (ax_1 , (1/a)\, x_2) = (x_1 , x_2)\}$$
$$= \{1\}$$

أما إذا كان $x = (0,0)$ ، فإن $G_x = G = \mathbf{R}^*$.

.٨٧ ليكن $*$ تأثير شمالي لزمرة G على مجموعة X ، وليكن $x \in X$. اثبت أن

(أ) $G_{a*x} = a\, G_x\, a^{-1}$ ، لكل $a \in G$.

(ب) $G_x \cong G_y$ ، لكل $y \in orb(x)$.

(ت) لكل $y \in orb(x)$ يكون $G_x \lhd G \Leftrightarrow G_x = G_y$.

الحل: ليكن $*$ تأثير شمالي لزمرة G على مجموعة X ، وليكن $x \in X$.

(أ) ليكن $a \in G$. إذن

$$g \in G_{a*x} \Leftrightarrow g * (a * x) = a * x \Leftrightarrow a^{-1} * (g * (a * x)) = x$$
$$\Leftrightarrow a^{-1} * ((g\, a) * x)) = x \Leftrightarrow a^{-1}\, g\, a * x = x \Leftrightarrow a^{-1}\, g\, a \in G_x$$
$$\Leftrightarrow g \in a\, G_x\, a^{-1}$$

إذن $G_{a*x} = a\, G_x\, a^{-1}$ ، لكل $a \in G$.

(ب) ليكن $y \in orb(x)$. إذن يوجد $a \in G$ بحيث $y = a * x$. إذن ينتج من (أ) أن

$$G_y = G_{a*x} = a\, G_x\, a^{-1} \cong G_x .$$

(ت) لكل $a \in G$, $y \in orb(x)$. يكون

$$G_x = G_y \Leftrightarrow G_x = G_{a*x} \Leftrightarrow G_x = a\, G_x\, a^{-1} \Leftrightarrow G_x \lhd G$$

إذن لكل $y \in orb(x)$ يكون $G_x \lhd G \Leftrightarrow G_x = G_y$.

.٨٨ ليكن G زمرة منتهية ، وليكن $A,B \leq G$. استخدم تأثير زمرة على مجموعة لإثبات أن

(أ) $|A\, x\, B| = \dfrac{|A|\,|B|}{|A \cap xBx^{-1}|}$. $\forall\, x \in G$

(ب) $|A \cap B| = \left|A \cap aBa^{-1}\right|$, $\forall\, a \in A$

الحل: ليكن G زمرة منتهية ، وليكن $A,B \leq G$. ليكن $* : (A\times B) \times G \to G$ بحيث

$(a,b) * x = a\,x\,b^{-1}$ لكل $(a,b)\in A\times B$, $x\in G$. إذن لكل $(a,b),(c,d)\in A\times B$, $x\in G$ يكون

$$(1,1) * x = x \;,$$
$$((a , b) (c , d)) * x = (a c , b d) * x = (a c) x (b d)^{-1} = a (c x d^{-1}) b^{-1}$$
$$= a ((c , d) * x) b^{-1} = (a , b) * ((c , d) * x))$$

إذن $*$ يكون تأثير شمالي للزمرة $A\times B$ على المجموعة G .

$$orb(x) = \{(a , b) * x \mid (a , b)\in A\times B\} = \{a x b^{-1} \mid a\in A , b\in B\} = A x B$$

إذن $|orb(x)| = |A x B|$. لكن

$$|orb(x)| = [A\times B : (A\times B)_x] \qquad \text{(مبرهنة)}$$

إذن

$$|A x B| = [A\times B : (A\times B)_x] = |A x B| / |(A\times B)_x| = |A| |B| / |(A\times B)_x| \;,$$
$$(A\times B)_x = \{(a,b)\in A\times B \mid (a,b) * x = x\} = \{(a,b)\in A\times B \mid (a,b) * x = x\}$$
$$= \{(a,b)\in A\times B \mid a x b^{-1} = x\} = \{(a,b)\in A\times B \mid a = x b x^{-1}\}$$

إذن

$$(a,b)\in(A\times B)_x \;\Leftrightarrow\; z = a = x b x^{-1} \;, a\in A , b\in B \;\Leftrightarrow\; z\in A \cap (x B x^{-1})$$

إذن $|(A\times B)_x| = |A \cap (x B x^{-1})|$. إذن

$$|A x B| = |A| |B| / |A \cap (x B x^{-1})| \;,\; \forall\, x\in G .$$

ملحوظة: بأخذ $x = 1$ ، نحصل على

$$|A B| = |A| |B| / |A \cap B|$$

لذلك يعتبر هذا البرهان برهاناً آخر للنتيجة $|A B| = |A| |B| / |A \cap B|$.

(ب) من (أ) بأخذ $x = a \in A$ ، نحصل على

$$|A B| = |A a B| = |A| |B| / |A \cap (a B a^{-1})|$$

إذن $|A| |B| / |A \cap B| = |A| |B| / |A \cap (a B a^{-1})|$. إذن

$$|A \cap B| = |A \cap (a B a^{-1})| \;,\; \forall\, a\in A$$

ملحوظة: لاحظ أن اثبات $|A \cap B| = |A \cap (a B a^{-1})|$ لكل $a \in G$ ينتج مباشرة من $B \cong a B a^{-1}$ لكل $a \in G$.

٨٩. ليكن G زمرة ، وليكن $A , B \leq G$. استخدم تأثير زمرة على مجموعة لإثبات أن $|\{b A b^{-1} \mid b \in B\}| = [B : B \cap N(A)]$ ، حيث $N(A)$ هو ناظمية A في G (normalizer of A in G) .

الحل: ليكن G زمرة ، وليكن $A , B \leq G$. نضع $X = \{b A b^{-1} \mid b \in B\}$. ليكن $* : B \times X \to X$ بحيث $g * (b A b^{-1}) = (g b) A (g b)^{-1}$ لكل $g \in B , b A b^{-1} \in X$.

لاحظ أن $(g b) A (g b)^{-1} = g (b A b^{-1}) g^{-1}$. ليكن $g,h \in B ,\; b A b^{-1} \in X$. إذن

$$1 * b A b^{-1} = b A b^{-1} \,,$$

$$\begin{aligned}(g h) * b A b^{-1} &= ((g h) b) A ((g h) b)^{-1} = g (h b) A (b^{-1} h^{-1}) g^{-1} \\ &= g \left((h b) A (h b)^{-1}\right) g^{-1} = g \left(h * (b A b^{-1})\right) g^{-1} \\ &= g * (h * b A b^{-1})\end{aligned}$$

إذن $*$ يكون تأثير شمالي للزمرة B على المجموعة X . إذن

$$\begin{aligned}orb(b A b^{-1}) &= \{ g * b A b^{-1} \mid g \in B\} = \{(g b) A (g b)^{-1} \mid g \in B\} \\ &= \{h A h^{-1} \mid h \in B\} = X\end{aligned}$$

هذا يعني أن كل المدارات تكون متساوية وتساوي X . إذن

$$|X| = |orb((b A b^{-1})|$$

بالتالي ينتج من المبرهنة $|orb(x)| = [B : B_x]$ ، لكل $x \in X$ أن

$$|X| = [B : B_{bAb^{-1}}]$$

إذن نبرهن الآن أن $[B : B_{bAb^{-1}}] = [B : B \cap N(A)]$. أي أننا نبرهن أن

$$|B_{bAb^{-1}}| = |B \cap N(A)|$$

من تمرين (٨٨) (ب) ينتج أن

$$|B \cap N(A)| = |B \cap b\, N(A)\, b^{-1}| \quad , \forall\, b \in B$$

إذن نبرهن أن

$$|B_{bAb^{-1}}| = |B \cap b\, N(A)\, b^{-1}| \quad , \forall\, b \in B$$

لكن $b\, N(A)\, b^{-1} = N(b A b^{-1})$ ، لأن

$$g \in b\, N(A)\, b^{-1} \Leftrightarrow \exists\, h \in N(A) \text{ s.t. } g = b\, h\, b^{-1}$$
$$\Leftrightarrow g\,(b\, A\, b^{-1})\, g^{-1} = b\, h\, b^{-1}\,(b\, A\, b^{-1})\, b\, h^{-1}\, b^{-1}$$
$$= b\,(h\, A\, h^{-1})\, b^{-1} = b\, A\, b^{-1} \;,\; h \in N(A)$$
$$\Leftrightarrow g \in N(b\, A\, b^{-1})$$

إذن $b\, N(A)\, b^{-1} = N(b\, A\, b^{-1})$. ليكن $g \in B$. إذن

$$g \in B_{bAb^{-1}} \Leftrightarrow g * (b\, A\, b^{-1}) = b\, A\, b^{-1}$$
$$\Leftrightarrow (g\, b)\, A\, (g\, b)^{-1} = b\, A\, b^{-1}$$
$$\Leftrightarrow g\,(b\, A\, b^{-1})\, g^{-1} = b\, A\, b^{-1}$$
$$\Leftrightarrow g \in N(b\, A\, b^{-1}) = b\, N(A)\, b^{-1}$$

إذن $|B_{bAb^{-1}}| = |B \cap b\, N(A)\, b^{-1}| \;,\; \forall\, b \in B$

٩٠. ليكن G زمرة منتهية ، وليكن $S \leq G \,,\, S \neq G$. استخدم تأثير زمرة على مجموعة لإثبات أن $G \neq \bigcup_{g\in G} g\, S\, g^{-1}$.

الحل: ليكن G زمرة منتهية ، وليكن $S \leq G \,,\, S \neq G$. بأخذ $A = S \,,\, B = G$ في تمرين (٨٩) نحصل على

$$|\{g\, S\, g^{-1} \mid g \in G\}| = [G : N(S)]$$

أي أن عدد المجموعات $g\, S\, g^{-1}$ لكل $g \in G$ يساوي $[G : N(S)]$. لاحظ أن كل مجموعة من هذة المجموعات تحتوي على العنصر المحايد 1 للزمرة G ، كما أن هذة المجموعات ليست منفصلة . بالتالي يكون

$$\left|\bigcup_{g\in G} g\, S\, g^{-1}\right| < [G : N(S)]\, |S| \leq [G : N(S)]\, |N(S)| \leq |G|$$

إذن $G \neq \bigcup_{g\in G} g\, S\, g^{-1}$.

٩١. ليكن $A \leq S_4$ ، بحيث $|A| = 3$. برهن أن عدد الزمر الجزئية من S_4 التي تماثل A يساوي $[S_4 : N(A)]$. هل هذا يكون صحيحا أيضاً عندما $|A| = 2$ ؟

الحل: ليكن $A \leq S_4$ ، بحيث $|A| = 3$. بما أن $|S_4| = 2\times3\times4$ ، فإن S_4 تحتوي على $1+3\lambda$ 3-زمرة جزئية (لسيلو) رتبها 3 حيث $1+3\lambda \mid 24 \;,\; \lambda \geq 0$. إذن $\lambda = 0$ أو $\lambda = 1$. لكن

S_4 تحتوي على أكثر من عنصر رتبتة 3 ، وبالتالي فهي تحتوي على أكثر من زمرة جزئية رتبتها 3 . إذن $\lambda = 1$. إذن S_4 تحتوي على أربعة زمر جزئية رتبها 3 ، وهي

$A = \{1 , (1\ 2\ 3) , (1\ 3\ 2)\}$,

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

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

$(3\ 4)\ A\ (3\ 4) = \{1 , (1\ 2\ 4) , (1\ 4\ 2)\}$.

لاحظ أن كل زمرة من هذة الزمر الجزئية في الصورة $g\ S\ g^{-1}$ ، حيث $g \in S_4$. إذن عدد الزمر الجزئية من S_4 التي تماثل A يساوي 4 . لاحظ أن

$N(A) = \{f \in S_4 \mid f\ A\ f^{-1} = A\} = \{1 , (1\ 2) , (1\ 3) , (2\ 3) , (1\ 2\ 3) , (1\ 3\ 2)\}$

إذن $|N(A)| = 6$. من تمرين (٨٩) يكون

$|\{g\ A\ g^{-1} \mid g \in S_4\}| = [S_4 : N(A)] = |S_4| / |N(A)| = 24/6 = 4$

ليكن $|A| = 2$. عدد الزمر الجزئية من S_4 التي تماثل A يساوي $[S_4 : N(A)]$ إذا كانت كل زمرة جزئية من S_4 تماثل A في الصورة $g\ A\ g^{-1}$ ، حيث $g \in S_4$. لكن هذا لا يتحقق لأن الزمرة الجزئية $H = \{1 , (1\ 2)(3\ 4)\}$ من S_4 تماثل $A = \{1 , (1\ 2)\}$ ولا يوجد عنصر $g \in S_4$ ، بحيث $g\ A\ g^{-1} = H$. إذن إذا كان $|A| = 2$ ، فإن عدد الزمر الجزئية من S_4 التي تماثل A لا يساوي $[S_4 : N(A)]$.

٩٢. ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$. إذا كان $ord(f) = p^k$ ، حيث p عدد أولي يقسم $|G|$ ، فبرهن أن f لة عنصر ثبات لا يساوي 1.

الحل: ليكن G زمرة منتهية ، وليكن $f \in Aut(G)$ بحيث $ord(f) = p^k$ ، حيث p عدد أولي يقسم $|G|$. نفرض أن $H = < f >$. إذن $|H| = p^k$. ليكن $X = G \backslash \{1\}$. ليكن $*$ تأثير (شمالي) لـ H على X . من مبرهنة العناصر الثابتة (fixed elements) في تأثير زمرة على مجموعة نحصل على

$|X| \equiv |Fix_H(X)| \pmod p$

إذن $p \mid |X| - |Fix_H(X)|$. بما أن $p \mid |G|$ ، فإن $p \nmid |G| - 1$. إذن $p \nmid |X|$. إذن $|Fix_H(X)| \neq 0$. إذن $Fix_H(X) \neq \emptyset$. إذن يوجد عنصر $x \in X$ ، بحيث $h * x = x$ لكل $h \in H$ (أي أن x عنصر ثبات لـ H) . إذن x يكون عنصر ثبات بـ $f \in H$ (لاحظ أن $x \neq 1$) .

٩٣. ليكن F حقل ، بحيث $|F| = p^n$ و p عدد أولي . ليكن $G \leq GL(n,F)$ ، بحيث $|G| = p^r$. اثبت أنة يوجد عنصر ثبات لـ G في F لا يساوي 0 (المحايد الجمعي في F).

الحل: ليكن F حقل ، بحيث $|F| = p^n$ و p عدد أولي ، وليكن $G \leq GL(n,F)$ ، بحيث $|G| = p^r$. ليكن $X = F\backslash\{0\}$. إذن $|X| = p^n - 1$. ليكن $*$ تأثير (شمالي) لـ G على X . إذن من مبرهنة العناصر الثابتة (fixed elements) في تأثير زمرة على مجموعة نحصل على

$$|X| \equiv |Fix_G(X)| \pmod p$$

إذن $p \mid |X| - |Fix_G(X)|$. إذن $|Fix_G(X)| \neq 0$. إذن $Fix_G(X) \neq \emptyset$. إذن يوجد عنصر $x \in X$ ، بحيث $A * x = x$ لكل $A \in G$. إذن x يكون عنصر ثبات بـ G (لاحظ أن $x \neq 0$) .

٩٤. ليكن G زمرة منتهية ، وليكن X مجموعة بحيث $|X| = 18$, $|G| = 55$. ليكن G تؤثر على X . اثبت أن $|Fix_G(X)| \leq 2$.

الحل: ليكن G زمرة منتهية رتبتها 55 ، وليكن X مجموعة بحيث $|X| = 18$. ليكن $*$ تأثير شمالي لـ G على X . ليكن S نظام دخول للمدارات (أي أن S مجموعة جزئية من X بحيث تحتوي بالضبط على عنصر واحد فقط من كل مدار من مدارات X المختلفة) . إذن $X = \cup_{x\in S} orb(x)$. إذن $|X| = \sum_{x\in S}|orb(x)|$. لكن (مبرهنة) $|orb(x)| = [G : G_x]$. إذن $|orb(x)| = |G| / |G_x| = 55 / |G_x|$. إذن $|orb(x)|$ يساوي 1 أو 5 أو 11 أو 55 . الاحتمال $|orb(x)| = 55$ مرفوض ، لأن $orb(x) \subseteq X$, $|X| = 18$. إذن $|orb(x)|$ يساوي 1 أو 5 أو 11 . بما أن $|X| = \sum_{x\in S}|orb(x)| = 18$ ، فإنة يوجد على الأقل مدارين $orb(x)$, $orb(y)$ بحيث $|orb(x)| = |orb(y)| = 1$. لاحظ أن $x \in X$ عنصر ثابت بـ G (أي أن $x \in Fix_G(X)$) إذا وفقط إذا كان $|orb(x)| = 1$. إذن $|Fix_G(X)| \leq 2$.

٩٥. ليكن G زمرة منتهية و X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X و S نظام دخول للمدارات . ليكن $x,y,z \in X$, $g \in G$. برهن أن

(أ) $|G_x| = |G_y| \quad , \forall\ x,y \in orb(z)$

(ب) إذا كان $Fix_g(X) = \{x \in X \mid g * x = x\}$ ، فإن

$$|\{(g,x) \in G \times X \mid x \in Fix_g(X)\}| = \sum_{g\in G} |Fix_g(X)| \quad ,$$

$$\sum_{g\in G}|Fix_g(X)| = \sum_{x\in X}|G_x| = |G||S|$$

الحل: ليكن G زمرة منتهية ، وليكن X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X .
ليكن $x,y,z\in X$, $g\in G$.

(أ) ليكن $x,y\in orb(z)$. إذن يوجد $g,h\in G$ ، بحيث $x = g * z$, $y = h * z$. إذن ينتج من تمرين (٨٧) (أ) أن

$$G_x = G_{g*z} = g\,G_z\,g^{-1} \quad , \quad G_y = G_{h*z} = h\,G_z\,h^{-1}$$

إذن $|G_x| = |G_y| = |G_z|$.

(ب) ليكن $Fix_g(X) = \{x\in X \mid g * x = x\}$ ، وليكن S نظام دخول للمدارات ، أي أن S مجموعة جزئية من X بحيث تحتوي بالضبط على عنصر واحد فقط من كل مدار من مدارات X المختلفة . إذن من الواضح أن

$$|\{(g,x)\in G\times X \mid x\in Fix_g(X)\}| = \sum_{g\in G}|Fix_g(X)|$$

بما أن $x\in Fix_g(X)$ إذا وفقط إذا كان $g\in G_x$ ، فإن

$$\sum_{g\in G}|Fix_g(X)| = \sum_{x\in X}|G_x|$$

ليكن $S = \{x_1 , x_2 , \ldots , x_n\}$. إذن $X = \bigcup_{i=1}^{n} orb(x_i)$. إذن من (أ) ينتج أن

$$\begin{aligned}\sum_{x\in X}|G_x| &= \sum_{x\in orb(x_1)}|G_x| + \sum_{x\in orb(x_2)}|G_x| + \cdots + \sum_{x\in orb(x_n)}|G_x| \\ &= |orb(x_1)|\,|G_{x_1}| + |orb(x_2)|\,|G_{x_2}| + \cdots + |orb(x_n)|\,|G_{x_n}| \\ &= [G:G_{x_1}]\,|G_{x_1}| + [G:G_{x_2}]\,|G_{x_2}| + \cdots + [G:G_{x_n}]\,|G_{x_n}| \\ &= |G| + |G| + \cdots + |G| \quad (n\ times) \\ &= |G||S|\end{aligned}$$

٩٦. ليكن G زمرة منتهية و X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X وليكن S نظام دخول للمدارات . ليكن $Y \subseteq X$ بحيث $S \subseteq Y$. إذا كان
$x\in X$, $G(x,Y) = \{g\in G \mid g * x\in Y\}$ ، فبرهن أن

(أ) $G(x,Y) \neq \emptyset$ ، لكل $x\in X$ ،

(ب) $|G(x,Y)| = |G_x|\,|orb(x) \cap Y|$ ،

(ت) $|Y| = \frac{1}{|G|}\sum_{x\in X}|G(x.Y)|$ ،

(ث) $|X| = |G|\sum_{x\in Y}\frac{1}{|G(x.Y)|}$.

الحل: ليكن G زمرة منتهية و X مجموعة منتهية . ليكن $*$ تأثير شمالي لـ G على X وليكن S نظام دخول للمدارات (أي أن S مجموعة جزئية من X بحيث تحتوي بالضبط على عنصر واحد فقط من كل مدار من مدارات X المختلفة) . ليكن $Y \subseteq X$ بحيث $S \subseteq Y$. نفرض أن

$$G(x,Y) = \{g\in G \mid g * x\in Y\} , x\in X$$

(أ) بما أن $x\in X$ ، فإنة يوجد $y\in S$ بحيث $x\in orb(y)$. إذن يوجد $g\in G$ بحيث $x = g * y$.
إذن $g^{-1} * x = 1 * y = y$. إذن $g^{-1} * x\in Y$. إذن $g^{-1}\in G(x,Y)$. إذن $G(x,Y) \neq \emptyset$.

(ب) ليكن $G(x,y) = \{g\in G \mid g * x = y\} , x,y\in X$. ليكن $g\in G(x,Y)$. إذن $g * x\in Y$. إذن يوجد $y\in Y$ ، بحيث $g * x = y$. إذن $g\in G(x,y)$. إذن $G(x,Y) \subseteq \cup_{y\in Y} G(x,y)$. ليكن $g\in \cup_{y\in Y} G(x,y)$. إذن يوجد $y\in Y$ ، بحيث $g\in G(x,y)$. إذن $g * x = y\in Y$. إذن $g\in G(x,Y)$. إذن $\cup_{y\in Y} G(x,y) \subseteq G(x,Y)$. إذن $G(x,Y) = \cup_{y\in Y} G(x,y)$. لاحظ أن المجموعات $G(x,y)$ ، لكل $y\in Y$ تكون منفصلة ، أي أن $G(x,y) \cap G(x,y') = \emptyset$ ، لكل عنصرين مختلفين $y,y'\in Y$. إذن

$$|G(x,Y)| = \sum_{y\in Y}|G(x,y)| = \sum_{y\in Y\cap orb(x)}|G(x,y)| \qquad (*)$$

ليكن $y\in Y\cap orb(x)$. إذن يوجد $h\in G$ ، بحيث $y = h * x$. إذن $G(x,y) = h\, G_x$ ، لأن

$$\begin{aligned} g\in G(x,y) &\Leftrightarrow g * x = y \\ &\Leftrightarrow g * x = h * x \\ &\Leftrightarrow (h^{-1} g) * x = x \\ &\Leftrightarrow h^{-1} g\in G_x \\ &\Leftrightarrow g\in h\, G_x \end{aligned}$$

إذن $|G(x,y)| = |G_x|$. إذن ينتج من (*) أن

$$|G(x,Y)| = |Y \cap orb(x)|\, |G_x|$$

(ت) ليكن $S = \{x_1 , x_2 , \dots , x_n\}$. إذن $X = \cup_{i=1}^{n} orb(x_i)$. إذن من (ب) ينتج أن

$$\sum_{x\in X}|G(x,Y)| = \sum_{i=1}^{n}\sum_{x\in orb(x_i)}|Y\cap orb(x)|\ |G_x|$$

$$= \sum_{i=1}^{n}\left[|Y\cap orb(x_i)| \sum_{x\in orb(x_i)}|G_x|\right]$$

لاحظ أن $|orb(x)| = [G : G_x] = |G| / |G_x|$. ليكن $orb(x_i) = \{x_i , x_{i_1} , x_{i_2} ,\cdots, x_{i_{n_i}}\}$.

إذن

$$\sum_{x\in orb(x_i)}|G_x| = |G_{x_i}| + |G_{x_{i_1}}| +\cdots+ |G_{x_{i_{n_i}}}|$$

$$= \frac{|G|}{|orb(x_i)|} + \frac{|G|}{|orb(x_{i_1})|} + \cdots + \frac{|G|}{|orb(x_{i_{n_i}})|}$$

$$= |G|$$

لأن $orb(x_i) = orb(x_{i_1}) = \cdots = orb(x_{i_{n_i}})$. إذن

$$\sum_{x\in X}|G(x,Y)| = |G|\ \sum_{i=1}^{n}|Y\cap orb(x_i)| = |G||Y|$$

لأن

$$Y = \bigcup_{i=1}^{n}(Y\cap orb(x_i))$$

(ث) بما أن $Y = \bigcup_{i=1}^{n}(Y\cap orb(x_i))$ ، فإنة ينتج من (ب) أن

$$\sum_{x\in Y}\frac{|G|}{|G(x,Y)|} = \sum_{x\in Y}\frac{|orb(x)|\ |G_x|}{|Y\cap orb(x)|\ |G_x|} = \sum_{x\in Y}\frac{|orb(x)|}{|Y\cap orb(x)|}$$

$$= \sum_{i=1}^{n}\ \sum_{x\in Y\cap orb(x_i)}\frac{|orb(x)|}{|Y\cap orb(x)|}$$

$$= \sum_{i=1}^{n}|orb(x_i)| = |X|$$

p-زمر - p-groups

٩٧. اذكر كل الـ p-زمر غير المتماثلة والتي رتبها p^2 .

الحل: عدد الـ p-زمر التي رتبها p^2 يساوي 2 ، وهما $\mathbf{Z}_{p^2}$, $\mathbf{Z}_p\times\mathbf{Z}_p$

٩٨. اذكر كل الـ p-زمر غير المتماثلة والتي رتبها p^3 .

الحل: عدد الـ p-زمر التي رتبها p^3 يساوي 5 ، ثلاثة منها ابدالية وهى

$$\mathbf{Z}_{p^3}\,,\ \mathbf{Z}_{p^2}\times\mathbf{Z}_p\ .\ \mathbf{Z}_p\times\mathbf{Z}_p\times\mathbf{Z}_p$$

واثنتان غير ابداليتان . في حالة $p = 2$ ، فإن الزمرتين غير الإبداليتين هما $D_4\,,\,Q_8$.

٩٩. اذكر مثالاً لـ p-زمرة غير منتهية .

الحل: ليكن p عدد أولي ، وليكن $\mathbf{Z}(p^\infty) = \{z\in\mathbf{C} \mid z^{(p^n)}=1,\ n\in\mathbf{Z}^+\}$. لاحظ أن $\mathbf{Z}(p^\infty) = \{e^{2\pi i m/p^n} \mid 0\le m<p^n,\ n\in\mathbf{Z}^+\}$. من السهل اثبات أن $\mathbf{Z}(p^\infty)$ تكون زمرة بالنسبة لعملية ضرب الأعداد المركبة . بما أن رتبة كل عنصر في $\mathbf{Z}(p^\infty)$ تساوي قوة للعدد الأولي p ، فإن $\mathbf{Z}(p^\infty)$ تكون p-زمرة غير منتهية . (ملحوظة: الزمرة $\mathbf{Z}(p^\infty)$ تسمى بروفر p-زمرة (Prüfer p-group)).

١٠٠. ليكن G p-زمرة منتهية ، وليكن $N \lhd G$. برهن أن G/N تكون p-زمرة منتهية .

الحل: ليكن G p-زمرة منتهية ، وليكن $N \lhd G$. إذن N تكون p-زمرة جزئية من G . بما أن G p-زمرة منتهية ، فإن $|G| = p^n$. إذن يوجد $m\in\mathbf{N}$ ، بحيث $|N| = p^m$, $m\le n$. إذن $|G/N| = |G| / |N| = p^n/p^m = p^{n-m}$. إذن G/N تكون p-زمرة .

١٠١. ليكن G p-زمرة منتهية ، وليكن $\{1\}\neq N \lhd G$. برهن أن

(أ) $C(G) \cap N \neq \{1\}$ ،

(ب) إذا كان $|N| = p$ ، فإن $N \le C(G)$ ،

(ت) إذا كان $|C(G)| = p$ ، $C(G) \le N$.

الحل: ليكن G p-زمرة منتهية ، وليكن $\{1\}\neq N \lhd G$. ليكن $* : G\times N \to N$ بحيث $g * x = g^{-1}\,x\,g$ ، لكل $x\in N\,,\,g\in G$. من السهل اثبات أن $*$ يكون تأثير شمالي لـ G على N .

(أ) بما أن $\{1\}\neq N \lhd G$, $\mathrm{Fix}_G(N) = \{x\in N \mid g * x = x\,,\ \forall\, g\in G\}$ ، فإن

$$x\in\mathrm{Fix}_G(N) \Leftrightarrow g * x = x\,,\ \forall\, g\in G \Leftrightarrow g^{-1}\,x\,g = x\ ,\ \forall\, g\in G$$

$\Leftrightarrow\ x g = g x\ \ , \forall\ g\in G\ \Leftrightarrow\ x\in C(G)$

$\Leftrightarrow\ x\in C(G) \cap N$

إذن $Fix_G(N) = C(G) \cap N$. بما أن G ‎p-زمرة منتهية و $N \leq G$ ، فإن N تكون أيضاً p-زمرة منتهية . إذن يوجد $r\in \mathbf{N}$ ، بحيث $|N| = p^r$. لكن

$|N| \equiv |Fix_G(N)| \pmod p$ (مبرهنة)

إذن $p \mid |N| - |Fix_G(N)|$. إذن $|Fix_G(N)| = p^s\ \ , s \geq 1$. إذن

$|C(G) \cap N| = p^s\ \ , s \geq 1$

إذن $C(G) \cap N \neq \{1\}$.

(ب) ليكن $|N| = p$. إذن $|C(G) \cap N| = p$. إذن $N \leq C(F)$.

(ت) ليكن $|C(G)| = p$. إذن $|C(G) \cap N| = p$. إذن $C(G) \leq N$.

١٠٢. ليكن G زمرة وليكن $N_i \lhd G\ ,\ N_{i+1} \lhd G$ ، بحيث

$N_1=C(G)\ \ ,\ \ C(G/N_i) = N_{i+1}/N_i$

برهن أن

(أ) $x^{-1} g^{-1} x\ g\in N_i$ لكل $g\in G\ , x\in N_{i+1}$ ،

(ب) إذا كانت G ‎p-زمرة منتهية ، فإنة يوجد $m\in \mathbf{N}$ بحيث $N_m = G$ ،

(ت) إذا كانت G غير ابدالية ورتبتها تساوي p^3 ، حيث p عدد أولي ، فإن $N_2 = G$.

الحل: ليكن G زمرة وليكن $N_i \lhd G\ ,\ N_{i+1} \lhd G$ ، بحيث

$N_1=C(G)\ \ ,\ \ C(G/N_i) = N_{i+1}/N_i$

(أ)

$$\begin{aligned} g\in G\ , x\in N_{i+1}\ &\Rightarrow\ x\,N_i\in C(G/N_i) \\ &\Rightarrow\ x\,N_i\ g\,N_i = g\,N_i\ x\,N_i \\ &\Rightarrow\ (x\,g)\,N_i = (g\,x)\,N_i \\ &\Rightarrow\ x^{-1} g^{-1} x\ g\in N_i \end{aligned}$$

إذن $x^{-1} g^{-1} x\ g\in N_i$ لكل $g\in G\ , x\in N_{i+1}$.

(ب) ليكن G p-زمرة منتهية . نفرض أن $N_1 \neq G$. إذن G/N_1 تكون p-زمرة منتهية . إذن $p \mid |C(G / N_1)|$ ، أي أن $p \mid |N_2 / N_1|$. إذن $N_2 / N_1 \neq \{1\}$. إذن $N_1 \subsetneqq N_2$. نفرض أن $N_2 \neq G$. إذن G/N_2 تكون p-زمرة منتهية . إذن $p \mid |C(G / N_2)|$ ، أي أن $p \mid |N_3 / N_2|$. إذن $N_3 / N_2 \neq \{1\}$. إذن $N_1 \subsetneqq N_2 \subsetneqq N_3$. نفرض أن $N_2 \neq G$. نستمر بهذا الشكل ، فنحصل على السلسلة التالية من الزمر الجزئية الناظمية من G

$$N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq N_4 \subsetneqq \cdots$$

لكن G زمرة منتهية . إذن هذة السلسلة تكون منتهية . إذن يوجد $m \in \mathbf{N}$ بحيث $N_m = G$.

(ت) ليكن G غير ابدالية ورتبتها تساوي p^3 ، حيث p عدد أولي . إذن $|N_1| = |C(G)| = p$ (مبرهنة) . إذن $|G / N_1| = p^2$. إذن G/N_1 تكون p-زمرة ابدالية (مبرهنة) . إذن $C(G / N_1) = G / N_1$. إذن $N_2 / N_1 = G / N_1$. إذن $G = N_2$.

١٠٣. ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية غير بديهية من G . اثبت أن $S \neq N(S)$.

الحل: ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية غير بديهية من G . ليكن $N_i \lhd G ,\ N_{i+1} \lhd G$ ، بحيث $N_1=C(G)\ ,\ C(G/N_i) = N_{i+1}/N_i$

إذن من تمرين (١٠٢) (ب) ينتج أنة يوجد $m \in \mathbf{N}$ بحيث

$$N_0=\{1\} \subsetneqq N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq N_4 \subsetneqq \cdots \subsetneqq N_m=G$$

ليكن i هو أكبر رقم في المجموعة $\{0,1,2,\ldots,m\}$ بحيث $N_i \leq S\ ,\ N_{i+1} \nsubseteq S$. ليكن $x \in N_{i+1} \backslash S$. نبرهن أن $x \in N(S)$ ($N(S) = \{g \in G \mid g S g^{-1} = S\}$ ، وتسمى ناظمية S في G) . ليكن $g \in S$. إذن ينتج من تمرين (١٠٢) (أ) أن $x^{-1} g^{-1} x g \in N_i$. إذن $(x^{-1} g^{-1} x g)^{-1} = g^{-1} x^{-1} g x \in N_i$. إذن $x^{-1} g x = g (g^{-1} x^{-1} g x) \in S N_i$. بما أن $N_i \leq S$ ، فإن $S N_i \leq S$. إذن $x^{-1} g x \in S$ ، لكل $g \in S$. إذن $x^{-1} S x \subseteq S$. إذن $x \in N(S)$. إذن $S \neq N(S)$.

١٠٤. ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية من G بحيث $[G : S] = p$. برهن أن $S \lhd G$.

الحل: ليكن G p-زمرة منتهية ، وليكن S زمرة جزئية من G بحيث $[G : S] = p$. إذن $G \geq N(S) \rhd S$. إذن $p = [G : S] = [G : N(S)]\,[N(S) : S]$. لكن من تمرين (١٠٣) يكون $S \neq N(S)$. إذن $[N(S) : S] = |N(S)| / |S| \neq 1$. إذن $[G : N(S)] = 1$. إذن $|G| / |N(S)| = 1$. إذن $|G| = |N(S)|$. إذن $S \lhd G$.

زمر سيلو والزمر البسيطة - Sylow's groups and simple groups

١٠٥. ليكن G p-زمرة بحيث $|G| = 3^4$. برهن أنة توجد زمرة جزئية ناظمية N من G ، بحيث $|N| > 3$.

الحل: ليكن G p-زمرة بحيث $|G| = 3^4$. من مبرهنة سيلو الأولى ينتج أن G تحتوي زمر جزئية رتبها $1, 3, 3^2, 3^3, 3^4$. ليكن $N \leq G$ ، بحيث $|N| = 3^3$. إذن $N \lhd G$ (وذلك من المبرهنة التي تنص على أن: إذا كانت G p-زمرة رتبتها p^r وكان H زمرة جزئية منها رتبتها p^{r-1} ، فإن $H \lhd G$).

١٠٦. ليكن G زمرة منتهية وليكن p عدد أولي يقسم $|G|$. إذا كان $S = \{x \in G \mid ord(x) = p^k , k \in \mathbf{N}_0\}$ ، فاثبت أن $S \leq G$.

الحل: ليكن G زمرة منتهية وليكن p عدد أولي يقسم $|G|$. إذن يوجد $r , m \in \mathbf{N}$ ، بحيث $|G| = p^r m \;,\; (p,m) = 1$. إذن ينتج من مبرهنة سيلو الأولى أن G تحتوي على زمر جزئية رتبها p^s ، حيث $1 \leq s \leq r$. بما أن $ord(1) = p^0$ ، فإن $1 \in S$. وبالتالي $S \neq \emptyset$. ليكن $x,y \in S \backslash \{1\}$. إذن يوجد $s , t \in \mathbf{N}$ ، بحيث $ord(x) = p^s , ord(y) = p^t$. إذن $|< y >| = p^t \;,\; |< x >| = p^s \;,\; < x >, < y > \;\leq G$. ليكن $s \geq t$. إذن $< x >$ تحتوي على زمرة جزئية H رتبتها p^t . لكن H تكون دائرية ، لأن $< x >$ دائرية . إذن يوجد $z \in < x >$ ، بحيث $H = < z >$. إذن $H = < z > \cong < y >$. إذن $ord(yx) = ord(zx)$. لكن $ord(zx) \mid p^s$. إذن $ord(yx) \mid p^s$. إذن $ord(xy) \mid p^s$ ، لأن $ord(xy) = ord(yx)$. إذن $x\,y \in S$. لكن G منتهية . إذن $S \leq G$.

١٠٧. ليكن G زمرة ، بحيث $|G| = 99$. برهن أن G تحتوي على زمرة جزئية ناظمية رتبتها 11.

الحل: ليكن G زمرة ، بحيث $|G| = 99$. بما أن $|G| = 3^2 \times 11$ ، فإن G تحتوي على 11- زمر جزئية لسيلو (Sylow 11- subgroups) رتبها 11 وعددها يساوي $1+11\lambda$ ، بحيث $\lambda = 0,1,2,\ldots$, $1+11\lambda \mid |G|$. إذن $\lambda = 0$. إذن G تحتوي على 11- زمرة جزئية لسيلو وحيدة ولتكن H ورتبتها تساوي 11 . بالتالي $H \lhd G$.

ملحوظة: لاحظ أن هذا التمرين يعتبر مثالاً على تمرين (٨٤) (ب) لأن

$$|G| = 99 , [G : H] = |G|/|H| = 99/11 = 9 \;,\; |G| \nmid [G : H]!$$

١٠٨. أوجد زمر سيلو الجزئية من الزمرتين S_3 , $\mathbf{Z}_{4900}$.

الحل: نوجد زمر سيلو الجزئية من الزمرة $\mathbf{Z}_{4900}$. بما أن $4900 = 2^2 \times 5^2 \times 7^2$ ، فإن $\mathbf{Z}_{4900}$ تحتوي على 2-زمر جزئية لسيلو رتبها 4 و 5-زمر جزئية لسيلو رتبها 25 و 7-زمر جزئية لسيلو رتبها 49 . بما أن $\mathbf{Z}_{4900}$ زمرة ابدالية ، فإن كل زمرة جزئية منها تكون ناظمية . بالتالي $\mathbf{Z}_{4900}$ تحتوي على p-زمرة جزئية لسيلو وحيدة ، حيث $p = 2 , 5 , 7$ ، وهي :

الـ 2-زمرة جزئية لسيلو هي $\langle \bar{5}^2 \cdot \bar{7}^2 \rangle$ ، الـ 5-زمرة جزئية لسيلو هي $\langle \bar{2}^2 \cdot \bar{7}^2 \rangle$

الـ 7-زمرة جزئية لسيلو هي $\langle \bar{2}^2 \cdot \bar{5}^2 \rangle$.

والآن نوجد زمر سيلو الجزئية من الزمرة S_3 . بما أن $|S_3| = 3! = 2 \times 3$ ، فإن S_3 تحتوي على 2-زمر جزئية لسيلو رتبها 2 و 3-زمر جزئية لسيلو رتبها 3 ، وهي :

الـ 2-زمر جزئية لسيلو هي $\{1 , (2\ 3)\} , \{1 , (1\ 3)\} , \{1 , (1\ 2)\}$ ،

الـ 3-زمر جزئية لسيلو هي $\{1 , (1\ 2\ 3) , (1\ 3\ 2)\}$ (وحيدة ولذلك فهي ناظمية) .

١٠٩. ليكن G زمرة منتهية ، وليكن $S \le N \lhd G$. وليكن p عدد أولي يقسم $|N|$. ليكن $K \le G / N$. برهن أن

(أ) S تكون p-زمرة جزئية لسيلو من N $\Leftrightarrow$ يوجد p-زمرة جزئية لسيلو V من G بحيث $S = V \cap N$.

(ب) K تكون p-زمرة جزئية لسيلو من G / N $\Leftrightarrow$ يوجد p-زمرة جزئية لسيلو B من G بحيث $K = B N / N$.

الحل: ليكن G زمرة منتهية ، وليكن $S \le N \lhd G$. وليكن p عدد أولي ، بحيث $p \mid |N|$.

(أ) ($\Leftarrow$) ليكن S p-زمرة جزئية لسيلو من N . إذن S تكون أكبر p-زمرة جزئية من N . لاحظ أن S تكون أيضاً p-زمرة جزئية من G . ليكن V p-زمرة جزئية لسيلو من G . إذن V تكون أكبر p-زمرة جزئية من G . إذن $S \le V$. إذن $S = S \cap N \le V \cap N$. بما أن $|V \cap N| \mid |V|$ ، فإن $V \cap N$ تكون p-زمرة جزئية من G . لكن $V \cap N \le N$. إذن $V \cap N$ تكون p-زمرة جزئية من N . لكن S تكون أكبر p-زمرة جزئية من N . إذن $V \cap N \le S$. إذن $S = V \cap N$.

($\Rightarrow$) ليكن V p-زمرة جزئية لسيلو من G ، بحيث $S = V \cap N$. نبرهن أن S تكون p-زمرة جزئية لسيلو من N . بما أن $V \cap N \le V$ ، فإن $V \cap N$ تكون p-زمرة جزئية من N . إذن ينتج من مبرهنة سيلو الثانية أنة يوجد D p-زمرة جزئية لسيلو من N ، بحيث $V \cap N \le D \le N$. إذن يوجد p-زمرة جزئية لسيلو E من G ، بحيث $D = E \cap N$. بما أن V , E p-زمرتين جزئيتين لسيلو من G ، فإنة ينتج من مبرهنة سيلو الثانية أنة يوجد $a \in G$ ، بحيث $E = a V a^{-1}$. لكن $N \lhd G$. إذن $N = a N a^{-1}$. إذن

$$|D| = |E \cap N| = |(a V a^{-1}) \cap (a N a^{-1})| = |a (V \cap N) a^{-1}| = |V \cap N|$$

لكن $V \cap N \le D$. إذن $S = V \cap N = D$. إذن S تكون p-زمرة جزئية لسيلو من N .

(ب) ليكن $|G| = p^r m$ ، بحيث $r \ge 1 , (p , m) = 1$. نفرض أن $|G/N| = p^s n$ ، حيث $(p , n) = 1$.

($\Leftarrow$) ليكن K p-زمرة جزئية لسيلو من G/N . نبرهن أنة يوجد p-زمرة جزئية لسيلو B من G بحيث $K = BN/N$. بما أن $K \le G/N$ ، فإنة يوجد زمرة جزئية A من G تحتوي N بحيث $K = A/N$. إذن $|K| = |A / N| = p^s$. إذن $[G / N : A / N] = n$. إذن p لا يقسم $[G / N : A / N]$. بما أن

$$n = [G / N : A / N] = |G / N| / |A / N| = |G| / |A|$$

فإن $|A| = |G| / n = p^r m / n = p^r k$ ، حيث $k = m/n , (p , k) = 1$. بالتالي A تحتوي على p-زمرة جزئية لسيلو B رتبتها p^r . بالتالي B تكون p-زمرة جزئية لسيلو من G لأن $|G| = p^r m$. بما أن $B , N \le A$ ، فإن $B N \le A$. إذن $B N / N \le A / N$. من (أ) ينتج أن الزمرة $B \cap N$ تكون p-زمرة جزئية لسيلو من N . لكن $|N| = p^{r-s} k$. إذن $|B \cap N| = p^{r-s}$. إذن

$$|B N| = (|B| \, |N|) / |B \cap N| = (p^r p^{r-s} k) / p^{r-s} = p^r k = |A|$$

إذن $|B\,N / N| = |A / N|$. إذن ينتج من $B\,N / N \le A / N$ أن $B\,N / N = A / N$.

ملحوظة: اثبات آخر لـ $B\,N / N = A / N$: من مبرهنة التماثل الثانية ينتج أن $B\,N / N \cong B / B \cap N$. إذن

$$|B\,N / N| = |B / B \cap N| = |B| / |B \cap N| = p^r / p^{r-s} = p^s = |A / N|$$

إذن ينتج من $B\,N / N \le A / N$ أن $B\,N / N = A / N$.

($\Rightarrow$) ليكن B p-زمرة جزئية لسيلو B من G ، بحيث $K = B\,N / N$. نبرهن أن K تكون p-زمرة جزئية لسيلو من G / N . من (أ) ينتج أن الزمرة $B \cap N$ تكون p-زمرة جزئية لسيلو من N . إذن من الملحوظة السابقة يكون $|B\,N / N| = p^s$. إذن $K = B\,N / N$ تكون p-زمرة جزئية لسيلو من G / N .

١١٠. ليكن G زمرة منتهية ، وليكن $A \lhd G$. وليكن B p-زمرة جزئية لسيلو من A . برهن أن

(أ) $G = A\,N(B)$

(ب) يوجد p-زمرة جزئية لسيلو من G في $N(B)$.

الحل: ليكن G زمرة منتهية ، وليكن $A \lhd G$. وليكن B p-زمرة جزئية لسيلو من A .

(أ) ليكن $g \in G$. بما أن $B \le A \lhd G$ ، فإن $g\,B\,g^{-1} \le g\,A\,g^{-1} = A$. بما أن B p-زمرة جزئية لسيلو من A ، فإن $g\,B\,g^{-1}$ تكون أيضاً p-زمرة جزئية لسيلو من A . إذن من مبرهنة سيلو الثانية ينتج أنة يوجد $a \in A$ ، بحيث $B = a\,(g\,B\,g^{-1})\,a^{-1}$. إذن $B = (a\,g)\,B\,(a\,g)^{-1}$. إذن $a\,g \in N(B) = \{x \in G \mid x\,B\,x^{-1} = B\}$. إذن $g \in a^{-1}\,N(B)$. إذن $g \in A\,N(B)$. إذن $G \subseteq A\,N(B)$. إذن $G = A\,N(B)$.

(ب) ليكن $|G| = p^r\,m$ ، بحيث $r \ge 1$, $(p , m) = 1$. إذا كان $|N(B)| = p^r\,n$ ، حيث $m \mid n$ ، فإنة ينتج من مبرهنة سيلو الأولى أنة يوجد p-زمرة جزئية لسيلو S من $N(B)$ رتبتها p^r . وبالتالي S تكون p-زمرة جزئية لسيلو من G رتبتها p^r ، لأن $|G| = p^r\,m$. إذن يوجد p-زمرة جزئية لسيلو من G في $N(B)$. إذن المطلوب يتحقق إذا كان $|N(B)| = p^r\,n$ ، حيث $m \mid n$. لذلك نبرهن أن $|N(B)| = p^r\,n$ ، حيث $m \mid n$. ليكن $|A| = p^s\,k$ ، حيث $(p , k) = 1$. بما أن B p-زمرة جزئية لسيلو من A ، فإن $|B| = p^s$, $B \le A \cap N(B)$.

بالتالي $|A \cap N(B)|\ |\ |B|$. إذن $p^s\ |\ |A \cap N(B)|$. إذن يوجد $k' \in \mathbf{N}$ ، حيث $|A \cap N(B)| = p^s k'$. لكن من (أ) يكون $G = A\,N(B)$. إذن

$$\begin{aligned}(p^r m) / (p^s k) &= |G| / |A| \\ &= |A\,N(B)| / |A| \\ &= (|A|\,|N(B)|) / (|A|\,|A \cap N(B)|) \\ &= |N(B)| / |A \cap N(B)| \\ &= |N(B)| / p^s k'\end{aligned}$$

إذن $|N(B)| = p^r (m k' / k)$. نضع $m k' / k = n$. إذن $|N(B)| = p^r n$. إذن يوجد p-زمرة جزئية لسيلو من G في $N(B)$.

١١١. ليكن G زمرة منتهية ، وليكن S زمرة جزئية من G و A p-زمرة جزئية لسيلو من G ، بحيث $N(A) \leq S$. برهن أن $[G : S] \equiv 1 \pmod p$.

الحل: ليكن G زمرة منتهية ، وليكن $S \leq G$. ليكن A p-زمرة جزئية لسيلو من G ، بحيث $N(A) \leq S$. نبرهن أن $[G : S] \equiv 1 \pmod p$. نرمز لعدد الـ p-زمر جزئية لسيلو من G بالرمز $s_p(G)$ ، ونرمز لعدد الـ p-زمر جزئية لسيلو من S بالرمز $s_p(S)$. إذن من مبرهنة سيلو الثالثة ينتج أن $s_p(G) \equiv s_p(S) \equiv 1 \pmod p$. إذا كان U,V p-زمرتين جزئيتين لسيلو من G ، فإنة ينتج من مبرهنة سيلو الثانية أنة يوجد $a \in G$ ، بحيث $U = a V a^{-1}$ (أي أن U ترافق V (U is conjugate V)) . إذن $s_p(G)$ يساوي عدد الزمر الجزئية من G التي ترافق A (لأن A تكون p-زمرة جزئية لسيلو من G) . لكن عدد الزمر الجزئية من G التي ترافق A يساوي $[G : N(A)]$ (مبرهنة) ، حيث $N(A)$ هو ناظمية A في G . إذن $s_p(G) = [G : N(A)]$. بما أن $A \leq N(A) \leq S$ ، فإن A تكون أيضاً p-زمرة جزئية لسيلو من S . إذن $s_p(S) = [S : N_S(A)]$ ، حيث $N_S(A)$ هو ناظمية A في S . لكن $N(A) \leq S$. إذن $N_S(A) = N(A)$. إذن $s_p(S) = [S : N(A)]$. إذن

$$[G : N(A)] \equiv [S : N(A)] \equiv 1 \pmod p$$

إذن

$$[G : N(A)] \equiv [S : N(A)] \pmod p$$

بما أن $N(A) \leq S \leq G$ ، فإن $[G : N(A)] = [G : S]\,[S : N(A)]$. إذن

$[G : S] \equiv 1 \pmod p$

١١٢. أوجد كل الـ p-زمر جزئية لسيلو من الزمرة

$G = \{1 , c , c^2 , a , b , ab , ca , cb , cab , c^2a , c^2b , c^2ab\}$

حيث $a^2 = b^2 = c^3 = 1 \ , \ a b = b a \ , \ a c = c b \ , \ b c = c a b$

الحل: نعتبر الزمرة

$G = \{1 , c , c^2 , a , b , ab , ca , cb , cab , c^2a , c^2b , c^2ab\}$

حيث $a^2 = b^2 = c^3 = 1 \ , \ a b = b a \ , \ a c = c b \ , \ b c = c a b$

لاحظ أن $|G| = 12 = 2^2 \times 3$. إذن G تحتوي على 2-زمر جزئية لسيلو رتبها 4 و 3-زمر جزئية لسيلو رتبها 3 . عدد الـ 2-زمر جزئية لسيلو من G يساوي 1 أو 3 . بما أن $a^2 = b^2 = 1 \ , \ a b = b a$ ، فإن $< a , b>$ تكون 2-زمرة جزئية لسيلو من G . لاحظ أن G لا تحتوي على عنصر رتبتة 4 . لذلك $< a , b>$ هي الـ 2-زمرة جزئية لسيلو الوحيدة من G . عدد الـ 3-زمر جزئية لسيلو من G يساوي 1 أو 4 . بما أن

$ord(c\, a) = ord(c\, b) = ord(c\, a\, b) = ord(c^2\, a) = 3$

فإن عدد الـ 3-زمر جزئية لسيلو من G يساوي 4 ، وهي

$< c\, a > \ , \ < c\, b > \ , \ < c\, a\, b > \ , \ < c^2\, a >$

١١٣. ليكن G زمرة بحيث $|G| = 12$. ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G . اثبت أن الأحتمال $n_2 = 3 , n_3 = 4$ غير ممكن . واثبت أنة إذا كان $n_2 = n_3 = 1$ ، فإن G تكون ابدالية .

الحل: ليكن G زمرة بحيث $|G| = 12$. ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G . بما أن $|G| = 12 = 2^2 \times 3$ ، فإن G تحتوي على 2-زمر جزئية لسيلو رتبها 4 و 3-زمر جزئية لسيلو رتبها 3 . عدد الـ 2-زمر جزئية لسيلو من G يساوي 1 أو 3 . من مبرهنة سيلو الثالثة يكون $n_2 = 1+2\lambda \ , \ n_3 = 1+3\lambda \ , \lambda = 0 , 1 , 2 , \ldots$ ، بحيث $n_2 \mid 12 \ , \ n_3 \mid 12$. إذن $n_2 = 1 \text{ or } 3 \ , \ n_3 = 1 \text{ or } 4$. ليكن $n_2 = 3 , n_3 = 4$. إذن G تحتوي على 4 زمر جزئية رتبها 3 (وبالتالي تكون دائرية) . عدد عناصر هذة الزمر الجزئية الأربعة غير العنصر المحايد يساوي 8 . إذن عدد كل العناصر المختلفة التي تحتويها هذة الزمر الجزئية الأربعة

يساوي 9 . إذن لا يمكن أن توجد أكثر من زمرة جزئية من G رتبتها 4 . أي إذا كان $n_3 = 4$ ، فإن $n_2 = 1$.

نفرض الآن الحالة $n_2 = n_3 = 1$. أي أن G تحتوي على 2-زمرة جزئية لسيلو وحيدة ولتكن A ، وتحتوي على 3-زمرة جزئية لسيلو وحيدة ولتكن B . إذن $A \lhd G \ , \ B \lhd G$. بما أن $|B| = 3$ ، فإن كل عنصر في B غير العنصر المحايد تكون رتبتة 3 ، وبالتالي لا ينتمي إلى A لأن $|A| = 4$. إذن $A \cap B = \{1\}$. وبما أن $|A\,B| = (|A|\,|B|) / |A \cap B| = 4 \times 3$ ، فإن $A\,B = G$. لكن $|A| = 4$. إذن A تماثل زمرة كلين الرباعية أو تماثل $\mathbf{Z}_4$. إذن A تكون ابدالية . وبما أن $|B| = 3$ ، فإن B تكون دائرية (لأن 3 عدد أولي) . إذن B تكون ابدالية . إذن $A \times B$ تكون ابدالية . لكن $A\,B \cong A \times B$ (لأن $(a,b) \mapsto a\,b$ يكون تماثل زمري). إذن $G \cong A \times B$. إذن G تكون ابدالية .

١١٤. أوجد كل الزمر غير المتماثلة التي رتبها 8 , 12 .

الحل: ليكن G زمرة ، بحيث $|G| = 8$. بما أن $|G| = 2^3$ ، فإن G تكون p-زمرة حيث $p = 2$.
إذا كانت G ابدالية ، فإن

$$G \cong \mathbf{Z}_8 \quad \text{أو} \quad G \cong \mathbf{Z}_2 \times \mathbf{Z}_4 \quad \text{أو} \quad G \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$$

وإذا كانت G غير ابدالية ، فإن

$$G \cong D_4 \quad \text{أو} \quad G \cong Q_8$$

(لاحظ أن هذا يكون صحيحاً أيضاً لأي عدد أولي p وأي زمرة G ، بحيث $|G| = p^3$)

لإثبات ذلك: نفرض أن G لا تحتوي على عنصر رتبتة 4 . إذن رتبة كل عنصر في G غير العنصر المحايد تساوي 2 (هذا ينتج من مبرهنة لاجرانج (رتبة العنصر يقسم رتبة الزمرة) . إذن عناصر G تحقق الشرط $x^2\, y^2 = (x\,y)^2$ ، لأنة في هذة الحالة يكون $x^2 = y^2 = (x\,y)^2$. إذن ينتج من تمرين (٧) أن G تكون ابدالية . لكن هذا يتناقض مع الفرض بأن G غير ابدالية . إذن G تحتوي على عنصر واحد على الأقل وليكن a بحيث رتبتة تساوي 4 . إذن
$|< a >| = 4$. إذن $[G : < a >] = 2$. إذن $< a > \lhd G$. ليكن $b \in G \setminus < a >$. إذن المجموعات المشاركة اليمينية لـ $< a >$ في G هي $< a >\, , < a > b$. إذن

$$G = < a > \cup < a > b$$

$= \{1 , a , a^2 , a^3\} \cup \{b , ab , a^2b , a^3b\}$

إذن

$$G = < a , b > = \{1 , a , a^2 , a^3 , b , ab , a^2b , a^3b\}$$

لاحظ أن $b\,a = a^3\,b$ ، لأن :

إذا كان $b\,a = b$ ، فإن $a = 1$ وهذا غير صحيح . وإذا كان $b\,a = a\,b$ ، فإن G تكون ابدالية ، وهذا يتناقض مع الفرض بأن G غير ابدالية . وإذا كان $b\,a = a^2\,b$ ، فإن $b = a^2\,b\,a$, $b = a^2\,b\,a^3$. وبالتالي $a^2 = 1$ ، وهذا غير صحيح .

بما أن $b\,a = a^3\,b$ ، فإن

$$(a\,b)^2 = b^2 \;,\; (a^2\,b)^2 = (a\,b)^2 \;,\; (a^3\,b)^2 = (a^2\,b)^2$$

إذن

$$(a\,b)^2 = (a^2\,b)^2 = (a^3\,b)^2 = b^2$$

إذا كان $b^2 = 1$ ، فإن

$$G = < a , b \mid a^4 = b^2 = (a\,b)^2 = 1 > = D_4$$

وإذا كان $a^2 = b^2$ ، فإن $b^4 = 1$. إذن

$$G = < a , b \mid a^4 = 1 , a^2 = b^2 , b\,a = a^3\,b > = Q_8$$

ليكن G زمرة ، بحيث $|G| = 12$. ليكن G ابدالية . إذن

$$G \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \quad \text{أو} \quad G \cong \mathbf{Z}_3 \times \mathbf{Z}_4 \quad \text{أو} \quad G \cong \mathbf{Z}_{12}$$

ليكن G غير ابدالية . نفرض أن n_2 هو عدد الـ 2-زمر جزئية لسيلو من G ، و n_3 هو عدد الـ 3-زمر جزئية لسيلو من G . بما أن G غير ابدالية ، فإنة ينتج من تمرين (١١٣) أن الإحتمال $n_2 = n_3 = 1$ مرفوض لأنة يؤدي إلى أن G تكون ابدالية . إذن $n_2 = 1 , n_3 = 4$ أو $n_2 = 3 , n_3 = 1$. ليكن $n_2 = 1$. أي أن G تحتوي على 2-زمرة جزئية لسيلو وحيدة رتبتها 4 ولتكن A . إذن $A \cong \mathbf{Z}_4$ أو $A \cong K_4$. إذا كان $A \cong \mathbf{Z}_4$ ، فإن $G \cong \mathbf{Z}_3 \times \mathbf{Z}_4$. وبالتالي G تكون ابدالية وهذا يتناقض مع الفرض بأن G غير ابدالية . إذن $A \cong K_4$. إذن $G \cong A_4$.

ليكن $n_2 = 3 , n_3 = 1$. في هذة الحالة G تحتوي على ثلاثة 2-زمر جزئية لسيلو رتبها 4 ولتكن A,B,C و 3-زمرة جزئية لسيلو وحيدة رتبتها 3 ولتكن N . إذن $N \lhd G$. بما أن $|G / N| = 4$ ، فإن $G / N \cong \mathbf{Z}_4$ أو $G / N \cong K_4$. لكن

$$A\,N / N \leq G / N \;,$$

$$|A\,N / N| = |A\,N| / |N| = |A| / |A \cap N| = |A| = 4$$

(لأن: $|A \cap N| \mid |A| , |B|$. أي أن $|A \cap N| \mid 3 , 4$. وبالتالي $|A \cap N| = 1$. إذن $A \cap B = \{1\}$) .

إذن ينتج من مبرهنة التماثل الثانية أن

$$A N / N \cong A / A \cap N \cong A$$

لأن $A \cap B = \{1\}$.

إذن إذا كان $G / N \cong \mathbf{Z}_4$ ، فإن $A \cong B \cong C \cong \mathbf{Z}_4$.

وإذا كان $G / N \cong K_4$ ، فإن $A \cong B \cong C \cong K_4$.

إذا كان $A \cong B \cong C \cong \mathbf{Z}_4$ ، فإن

$$G = \{1 , a , a^2 , a^3 , b , b^2 , ab , a^2b , a^3b , ab^2 , a^2b^2 , a^3b^2\}$$

حيث $n_2 = 3 , n_3 = 1$, $a^4 = b^3 = 1$.

وإذا كان $A \cong B \cong C \cong K_4$ ، فإن $G \cong D_6$ (حيث D_n هي الزمرة الزوجية النونية (n^{th} – dihedral group) ورتبتها تساوي $2n$) .

١١٥. اثبت أن الزمر التي رتبها 56 , 48 , 40 تكون غير بسيطة .

الحل: أولاً: ليكن G زمرة ، بحيث $|G| = 40$. بما أن $|G| = 2^3 \times 5$ ، فإن G تحتوي على 2-زمر جزئية لسيلو رتبها 8 و 5-زمر جزئية لسيلو رتبها 5 . نفرض أن n_2 هو عدد الـ 2-زمر جزئية لسيلو من G ، و n_5 هو عدد الـ 5-زمر جزئية لسيلو من G . من مبرهنة سيلو الثالثة يكون

$$n_2 = 1+2\lambda \quad , \quad n_5 = 1+5\lambda \quad , \quad \lambda = 0 , 1 , 2 , \ldots$$

بحيث $n_2 \mid 40 \;,\; n_3 \mid 40$.

إذن $n_5 = 1$. أي أن G تحتوي على 5-زمرة جزئية لسيلو وحيدة رتبتها تساوي 5 ولتكن N .

إذن $N \lhd G$ (مبرهنة) . لاحظ أن N ليست بديهية لأن رتبتها 5 . إذن G لا تكون بسيطة .

ثانياً: ليكن G زمرة ، بحيث $|G| = 48$. بما أن $|G| = 2^4 \times 3$ ، فإن G تحتوي على 2-زمر جزئية لسيلو رتبها 16. ليكن A 2-زمرة جزئية لسيلو من G . إذن $|A| = 16$. إذن $[G : A] = 3$. إذن $[G : A]\,! = 6$. إذن $|G| \nmid [G : A]!$. إذن ينتج من تمرين (٨٤) (ب) أن G تحتوي على زمرة جزئية ناظمية غير بديهية . إذن G لا تكون بسيطة .

حل آخر: إذا كانت G تحتوي على 2-زمرة جزئية لسيلو وحيدة ، فإنها تكون ناظمية ، وبالتالي ينتج المطلوب . لذلك نفرض أن $n_2 \geq 2$ ، حيث n_2 هو عدد الـ 2-زمر جزئية لسيلو من G .
ليكن A,B 2-زمرتين جزئيتين لسيلو من G ، بحيث $A \neq B$. إذن $|A| = |B| = 16$. بما أن $A \cap B \leq A$ ، فإن $|A \cap B|$ تساوي 1 أو 2 أو 4 أو أو 8 أو 16 . ليكن $|A \cap B| = 16$. إذن $A = B$ ، وهذا يتناقض مع الفرض بأن $A \neq B$. إذن $|A \cap B| \neq 16$. ليكن $|A \cap B| = 1$. إذن $|A B| = |A|\,|B| = 16 \times 16 > |G| = 48$ ، وهذا غير ممكن . إذن $|A \cap B| \neq 1$. ليكن $|A \cap B| = 2$. إذن

$$\begin{aligned} |A B| &= |A|\,|B| / |A \cap B| \\ &= 16 \times 16 / 2 \\ &> |G| = 48 \end{aligned}$$

وهذا غير ممكن . إذن $|A \cap B| \neq 2$. ليكن $|A \cap B| = 4$. إذن

$$\begin{aligned} |A B| &= |A|\,|B| / |A \cap B| \\ &= 16 \times 16 / 4 \\ &> |G| = 48 \end{aligned}$$

وهذا غير ممكن . إذن $|A \cap B| \neq 4$. إذن $|A \cap B| = 8$. إذن

$$A \cap B \leq A , B \quad , \quad |A| = |B| = 2^4 \quad , \quad |A \cap B| = 2^3$$

إذن $A \cap B \lhd A ,B$ (مبرهنة) . إذن $A , B \leq N(A \cap B)$. إذن $|N(A \cap B)|$ يساوي 16 أو 24 . إذا كان $|N(A \cap B)| = 16$ ، فإن $A = B$ وهذا يتناقض مع الفرض بأن $A \neq B$. إذن $|N(A \cap B)| = 24$. إذن $[G : N(A \cap B)] = 2$. إذن $N(A \cap B) \lhd G$. إذن G لا تكون بسيطة .

<u>ثالثا</u> : ليكن G زمرة ، بحيث $|G| = 56$. بما أن $|G| = 2^3 \times 7$ ، فإن G تحتوي على 2-زمر جزئية لسيلو رتبها 8 و 7-زمر جزئية لسيلو رتبها 7 . نفرض أن n_2 هو عدد الـ 2-زمر جزئية لسيلو من G وأن n_7 هو عدد الـ 7-زمر جزئية لسيلو من G . من مبرهنة سيلو الثالثة يكون

$$n_7 = 1+7\lambda \;,\; \lambda = 0 , 1 , 2 , \ldots$$

بحيث $n_7 \mid 56$.

إذن n_7 يساوي 1 أو 8 . إذا كان $n_7 = 1$ ، فإن G تحتوي على 7-زمرة جزئية لسيلو وحيدة ، وبالتالي تكون ناظمية في G . إذن G في هذة الحالة لا تكون بسيطة . نفرض أن $n_7 = 8$. ليكن A,B 7-زمرتين جزئيتين لسيلو من G . إذن $|A| = |B| = 7$. إذن $|A \cap B| = 1$. إذن $A \cap B = \{1\}$. إذن عدد العناصر المختلفة في الـ 7-زمر جزئية لسيلو من G الثمانية يساوي $(6\times8)+1$ ، أي يساوي 49 . ليكن C 2-زمر جزئية لسيلو من G . إذن $|C| = 8$. إذن $|A \cap C| = 1$. إذن إذن $A \cap C = \{1\}$. إذن يوجد فقط 7 عناصر غير موجودة في الـ 7-زمر جزئية لسيلو من G . إذن $n_2 = 1$. إذن G تحتوي على 2-زمرة جزئية لسيلو وحيدة ، وبالتالي تكون ناظمية في G . إذن G في هذة الحالة لا تكون بسيطة .

١١٦. ليكن G زمرة منتهية وليكن $|G| = p^r m$ ، حيث p عدد أولي بحيث $(p , m) = 1 ,\ p > m$. اثبت أن G تكون غير بسيطة .

الحل: ليكن G زمرة منتهية ، وليكن $|G| = p^r m$ ، حيث p عدد أولي بحيث $(p , m) = 1 ,\ p > m$. إذن G تحتوي على p-زمرة جزئية لسيلو رتبتها p^r ولتكن S . إذن $[G : S] = m$. بما أن $p > m$ ، فإن p لا يقسم $m!$ ، أي أن p لا يقسم $[G : S]!$. إذن $|G|$ لا يقسم $[G : S]!$. إذن ينتج من تمرين (٨٤) (ب) أن G تحتوي على زمرة جزئية ناظمية غير بديهية . إذن G لا تكون بسيطة .

١١٧. اثبت أن رتبة أصغر زمرة بسيطة غير ابدالية تساوي 60 .

الحل: ليكن G زمرة غير ابدالية بسيطة . ليكن $|G| = n$. إذا كان n يساوي p أو p^r أو pq أو p^2q ، حيث p,q عددين أوليين ، فإن G تكون ابدالية أو تكون غير بسيطة . وإذا كان $n = p^r m\ ,\ (p , m) = 1 , p > m$ ، حيث p عدد أولي ، فإن G تكون غير بسيطة (انظر تمرين (١١٦)) . وإذا كان n يساوي 40 أو 48 أو 56 ، فإن G تكون غير بسيطة (انظر تمرين (١١٥)) . الاحتمالات المتبقية لـ n هي n يساوي 24 أو 30 أو 36 .

<u>أولا</u>: ليكن $n = 24 = 2^3 \times 3$. إذن G تحتوي على 2-زمرة جزئية لسيلو رتبتها 8 ولتكن A . إذن $[G : A] = 3$. إذن $|G|$ لا يقسم $[G : A]!$. إذن ينتج من تمرين (٨٤) (ب) أن G تحتوي على زمرة جزئية ناظمية غير بديهية . إذن G تكون غير بسيطة .

ثانياً: ليكن $n = 30 = 2 \times 3 \times 5$. إذن G تحتوي على 2-زمر جزئية لسيلو رتبها 2 و 3-زمر جزئية لسيلو رتبها 3 و 5-زمر جزئية لسيلو رتبها 5 . نفرض أن n_2 هو عدد الـ 2-زمر جزئية لسيلو من G ، و n_3 هو عدد الـ 3-زمر جزئية لسيلو من G . و n_5 هو عدد الـ 5-زمر جزئية لسيلو من G . من مبرهنة سيلو الثالثة يكون

$$n_2 = 1+2\lambda \quad , \quad n_3 = 1+3\lambda \quad , \quad n_5 = 1+5\lambda \quad , \lambda = 0,1,2,\ldots$$

بحيث $n_2,n_3,n_5 \mid 30$.

إذن n_2 تساوي 1 أو 3 أو 15 و n_3 تساوي 1 أو 10 و n_5 تساوي 1 أو 6 . إذا كان $n_2 = 1$ أو $n_3 = 1$ أو $n_5 = 1$ ، فإن G تكون غير بسيطة ، لأنها تحتوي في هذة الحالة على زمرة جزئية ناظمية غير بديهية على الأقل (مبرهنة) . لاحظ أن تقاطع p-زمرة جزئية لسيلو من G و q-زمرة جزئية لسيلو من G ، حيث $p \neq q$ يساوي $\{1\}$. نفرض الحالة $n_3 = 10 , n_5 = 6$. إذن G تحتوي 6×4 (أي 24) عنصر رتبتة 5 (لأن أي 5-زمرة جزئية لسيلو من G رتبتها 5 (وهو عدد أولي) وبالتالي فهي دائرية ورتبة كل عنصر فيها غير المحايد تساوي 5) . كذلك G تحتوي 10×2 (أي 20) عنصر رتبتة 3 . إذن G تحتوي 44 عنصر مختلف ، وهذا غير ممكن لأن $|G| = 30 < 44$. إذن الحالة $n_3 = 10 , n_5 = 6$ تكون مرفوضة .

ثالثا: ليكن $n = 36 = 2^2 \times 3^2$. هذة الحالة مثل الحالة $n = 24$.

إذن لا يوجد زمرة بسيطة غير ابدالية رتبتها أقل من 60 . وبما أن A_5 زمرة بسيطة غير ابدالية ورتبتها 60 ، فبناءً على ما سبق تكون رتبة أصغر زمرة بسيطة غير ابدالية هي 60 .

١١٨. ليكن G زمرة بسيطة رتبتها 60 . ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G . اثبت أن

(أ) $n_2 = 5 \text{ or } 15 \;,\; n_3 = 10 \;,\; n_5 = 6$

(ب) يوجد $H \leq G$ ، بحيث $[G : H] = 5$.

الحل: ليكن G زمرة بسيطة رتبتها 60 . ليكن n_p هو عدد الـ p-زمر جزئية لسيلو من G .

(أ) بما أن ليكن $|G| = 60 = 2^2 \times 3 \times 5$ ، فإن G تحتوي على 2-زمر جزئية لسيلو رتبها 4 و 3-زمر جزئية لسيلو رتبها 3 و 5-زمر جزئية لسيلو رتبها 5 . من مبرهنة سيلو الثالثة يكون

$$n_2 = 1+2\lambda \quad , \quad n_3 = 1+3\lambda \quad , \quad n_5 = 1+5\lambda \quad , \quad \lambda = 0,1,2,\ldots$$

بحيث $n_2 , n_3 , n_5 \mid 60$.

إذن $n_5 = 1 \text{ or } 6$. لكن G بسيطة ، أي أن G لا تحتوي على زمر جزئية ناظمية غير بديهية . إذن $n_5 = 6$. وبما أن رتبة كل 5-زمرة جزئية لسيلو من G يساوي 5 (عدد أولي) ، فإن كل 5-زمرة جزئية لسيلو من G تكون دائرية وتقاطع أي إثنين منها يساوي $\{1\}$. كما أن عدد العناصر المختلفة في كل الـ 5-زمر جزئية لسيلو من G يساوي 4×6 (أي 24) . لاحظ أن رتبة كل عنصر من هذة العناصر يساوي 5 .

كذلك $n_3 = 1 \text{ or } 4 \text{ or } 10$. لكن G بسيطة ، أي أن G لا تحتوي على زمر جزئية ناظمية غير بديهية . إذن $n_3 \neq 1$. إذن $n_3 = 4 \text{ or } 10$. ليكن $n_3 = 4$. ليكن A 3-زمرة جزئية لسيلو من G . إذن ينتج من مبرهنة سيلو الثانية أن أي 3-زمرة جزئية لسيلو من G ترافق A أي تكون في الصورة $x A x^{-1}$ ، حيث $x \in G$. لكن عدد الزمر الجزئية من G التي ترافق A يساوي $[G : N(A)]$. إذن عدد الـ 3-زمر جزئية لسيلو من G يساوي $[G : N(A)]$. إذن $n_3 = [G : N(A)]$. إذن $[G : N(A)] = 4$. بما أن $|G|$ لا يقسم $4!$ ، فإنة ينتج من تمرين (٨٤) (ب) أن G تحتوي على زمرة جزئية ناظمية غير بديهية . إذن G لا تكون بسيطة . وهذا يتناقض مع الفرض بأن G تكون زمرة بسيطة . إذن $n_3 \neq 4$. إذن $n_3 = 10$. رتبة كل 3-زمرة جزئية لسيلو من G يساوي 3 (عدد أولي) . إذن كل 3-زمرة جزئية لسيلو من G تكون دائرية ، وتقاطع أي إثنين منها يساوي $\{1\}$. كما أن عدد العناصر المختلفة في كل الـ 3-زمر جزئية لسيلو من G يساوي 2×10 (أي 20) . لاحظ أن رتبة كل عنصر من هذة العناصر يساوي 3 .

أيضاً $n_2 = 1 \text{ or } 3 \text{ or } 5 \text{ or } 15$. لكن G بسيطة ، أي لا تحتوي على زمر جزئية ناظمية غير بديهية . إذن $n_2 \neq 1$. إذن $n_2 = 3 \text{ or } 5 \text{ or } 15$. ليكن $n_2 = 3$. ليكن B 2-زمرة جزئية لسيلو من G . إذن $n_2 = [G : N(B)]$. إذن $[G : N(B)] = 3$. بما أن $|G|$ لا يقسم $3!$ ، فإنة ينتج من تمرين (٨٤) (ب) أن G تحتوي على زمرة جزئية ناظمية غير بديهية . إذن G لا تكون بسيطة . وهذا يتناقض مع الفرض بأن G تكون زمرة بسيطة . إذن $n_2 \neq 3$. إذن $n_2 = 5 \text{ or } 15$.

(ب) من (أ) ينتج أن $n_2 = 5 \text{ or } 15$. نفرض أن $n_2 = 5$. ليكن C 2-زمرة جزئية لسيلو من G . إذن $n_2 = [G : N(C)]$. إذن $N(C) \leq G$ ، بحيث $[G : N(C)] = 5$. نفرض أن $n_2 = 15$. إذن يوجد 2-زمرتين جزئيتين مختلفتين لسيلو D , E من G رتبتهما 4 ، بحيث $D \cap E \neq \{1\}$. لأننا إذا فرضنا أن تقاطع كل 2-زمرتين جزئيتين لسيلو من G يساوي $\{1\}$،

فإن G تحتوي عناصر مختلفة عددها (1+24+20+15(4-1)=) 90 ، وهذا غير ممكن لأن $|G| = 60$. بما أن $|D| = |E| = 4$ ، فإن كل من D,E تماثل $\mathbf{Z}_4$ أو K_4 . إذن D,E تكونان ابداليتان . إذن كل زمرة جزئية من D أو E تكون ناظمية . ليكن $\{1\} \neq N \lhd D,E$. ليكن $H = < D , E>$. إذن $\{1\} \neq N \lhd H \leq G$. وبما أن G زمرة بسيطة ، فإن $H \neq G$. بما أن $|D| = 2^2 , D \leq H$ ، فإن D تكون 2-زمرة جزئية لسيلو من H . ليكن $n_2(H)$ هو عدد الـ 2-زمر جزئية لسيلو من H . إذن $n_2(H) = [H : N_H(D)]$. لاحظ أن كل 2-زمرة جزئية لسيلو من H تكون 2-زمرة جزئية لسيلو من G . بما أن $D \leq N_H(D) \leq H$ ، فإن

$$[H : D] = [H : N_H(D)]\ [N_H(D) : D]$$

لكن $[H : D]$ عدد فردي . إذن $[H : N_H(D)]$ يكون عدد فردي . كذلك $[H : N_H(D)] \neq 1$. بما أن

$$|H| = [H : N_H(D)]\ |N_H(D)| \ \geq\ n_2(H)\ |D|\ \geq\ 3 \times 4 = 12$$

فإن $[G : H] = |G| / |H| = 60 / |H| \leq 5$.

إذا كان $[G : H] < 5$ ، فإن $|H| > 12$. وبالتالي يكون $|H| = 15 \text{ or } 20 \text{ or } 30$. إذن من تمرين (٨٤) (ب) يكون

$$|H| = 15 \ \Rightarrow\ [G : H] = 4 \ \Rightarrow\ |G| \nmid [G : H]! \ \Rightarrow \exists\, A \lhd G \ \Rightarrow\ \text{contradiction}$$

$$|H| = 20 \Rightarrow\ [G : H] = 3 \ \Rightarrow\ |G| \nmid [G : H]! \ \Rightarrow \exists\, B \lhd G \ \Rightarrow\ \text{contradiction}$$

$$|H| = 30 \ \Rightarrow\ [G : H] = 2 \ \Rightarrow\ H \lhd G \ \Rightarrow\ \text{contradiction}$$

إذن $[G : H] = 5$.

١١٩. أوجد كل الـ p-زمر جزئية لسيلو من S_5 .

الحل: بما أن $|S_5| = 2^3 \times 3 \times 5$ ، فإن S_5 تحتوي 2-زمر جزئية لسيلو رتبها 8 وليكن عددها n_2 وتحتوي 3-زمر جزئية لسيلو رتبه 3 وليكن عددها n_3 وتحتوي 5-زمر جزئية لسيلو رتبها 5 وليكن عددها n_5 . من مبرهنة سيلو الثالثة يكون

$$n_2 = 1 + 2\lambda \ ,\ n_3 = 1 + 3\lambda \ ,\ n_5 = 1 + 5\lambda \ ,\ \lambda = 0 , 1 , 2 , \ldots$$

بحيث $n_2 , n_3 , n_5 \mid |S_5|$.

إذن

$n_2 = 1$ or 3 or 5 or 15 , $n_3 = 1$ or 4 or 10 , $n_5 = 1$ or 6

S_5 تحتوي أكثر من أربعة عناصر رتبها 5 . إذن $n_5 = 6$ ، وهي

$<(1\,2\,3\,4\,5)>$, $<(1\,2\,3\,5\,4)>$, $<(1\,2\,4\,5\,3)>$, $<(1\,2\,4\,3\,5)>$,
$<(1\,2\,5\,3\,4)>$, $<(1\,2\,5\,4\,3)>$

S_5 تحتوي 20 عنصر رتبتة 3 . وتقاطع أي 3-زمرتين جزئيتين لسيلو من S_5 يساوي $\{1\}$.
إذن يوجد عنصرين رتبتهما 3 في كل 3-زمر جزئية لسيلو من S_5 . إذن $n_3 = 10$ ، وهي

$<(1\,2\,3)>$, $<(1\,2\,4)>$, $<(1\,2\,5)>$, $<(1\,3\,4)>$, $<(1\,3\,5)>$,

$<(1\,4\,5)>$, $<(2\,3\,4)>$, $<(2\,3\,5)>$, $<(2\,4\,5)>$, $<(3\,4\,5)>$

يوجد أكثر من خمسة زمر جزئية من S_5 رتبها 8 . إذن $n_2 = 15$ ، وهي
$<(1\,3\,2\,4), (1\,2)>$, $<(1\,4\,2\,5), (1\,2)>$, $<(1\,3\,2\,5), (1\,2)>$,
$<(1\,2\,3\,4), (1\,3)>$, $<(1\,4\,3\,5), (1\,3)>$, $<(1\,2\,3\,5), (1\,3)>$,
$<(1\,2\,4\,3), (1\,4)>$, $<(1\,3\,4\,5), (1\,4)>$, $<(1\,2\,4\,5), (1\,4)>$,
$<(1\,2\,5\,3), (1\,5)>$, $<(1\,2\,5\,4), (1\,5)>$, $<(1\,3\,5\,4), (1\,5)>$,
$<(2\,4\,3\,5), (2\,3)>$, $<(2\,3\,4\,5), (2\,4)>$, $<(2\,3\,5\,4), (2\,5)>$

١٢٠. اثبت أن كل زمرة بسيطة رتبتها 60 تماثل A_5 .

الحل: ليكن G زمرة بسيطة رتبتها 60 . إذن ينتج من تمرين (١١٨) (ب) أنة يوجد $H \leq G$ ، بحيث $[G : H] = 5$. ليكن $X = \{h\,H \mid h \in G\}$. ليكن $* : G \times X \to X$ بحيث $g * h\,H = (g\,h)\,H$ ، لكل $g \in G$, $h\,H \in X$. من السهل اثبات أن $*$ يكون تأثير شمالي لـ G على X . إذن يوجد تشاكل زمري $\alpha : G \to S(X)$ بحيث $\alpha(a) = f_a$ لكل $a \in G$ ، حيث f_a تكون تبديلة على X معرفة بـ $f_a(h\,H) = a * h\,H\ (= (a\,h)\,H)$ لكل $h\,H \in X$. بما أن $[G : H] = 5$ (أي أن عدد المجموعات المشاركة الشمالية المختلفة لـ H في G يساوي 5) ، فإن $|X| = 5$. إذن $S(X) \cong S_5$. لذلك نعتبر $S(X) = S_5$. بما أن $Ker(\alpha) \lhd G$ ، فإن $Ker(\alpha) = \{1\}$ لأن G زمرة بسيطة فرضاً ولأن $Ker(\alpha) \neq G$. إذن α يكون متباين . إذن $|\alpha(G)| = 60$. لكن G بسيطة و $G \cong \alpha(G)$. إذن $\alpha(G)$ تكون زمرة بسيطة . بما أن $[S_5 : A_5] = 2$ ، فإن $A_5 \lhd S_5$. كذلك $\alpha(G) \cap A_5 \lhd \alpha(G)$. لكن $\alpha(G)$ تكون زمرة

بسيطة . إذن $\alpha(G) \cap A_5 = \{1\}$ أو $\alpha(G) \cap A_5 = \alpha(G)$. إذا كان $\alpha(G) \cap A_5 = \alpha(G)$ ، فإن $\alpha(G) \leq A_5$. لكن $|\alpha(G)| = |A_5| = 60$. إذن $\alpha(G) = A_5$. وبالتالي $\alpha : G \to A_5$ يكون تماثل زمري . والآن نثبت أن الاحتمال الثاني وهو $\alpha(G) \cap A_5 = \{1\}$ يكون مرفوضاً . نفرض أن $\alpha(G) \cap A_5 = \{1\}$. ليكن $\pi : S_5 \to S_5 / A_5$ هو التشاكل القانوني . بما أن $\alpha(G) \leq S_5$ ، فإن

$$\pi(\alpha(G)) = \alpha(G) A_5 / A_5 \leq S_5 / A_5$$

لكن

$$\begin{aligned} |\alpha(G) A_5 / A_5| &= |\alpha(G)|\, |A_5| / |\alpha(G) \cap A_5|\, |A_5| \\ &= |\alpha(G)| \\ &= |S_5| \\ &= 5! \quad , \end{aligned}$$

$$|S_5 / A_5| = |S_5| / |A_5| = 2$$

وهذا غير ممكن . إذن الاحتمال الثاني وهو $\alpha(G) \cap A_5 = \{1\}$ يكون مرفوضاً .

١٢١. ليكن G زمرة منتهية وليكن S p-زمرة جزئية لسيلو من G . برهن أن $p \nmid [N(S) : S]$.

الحل: ليكن G زمرة منتهية وليكن S p-زمرة جزئية لسيلو من G . إذن $r,m \in \mathbf{N}$ ، بحيث $|G| = p^r m \;, (p , m) = 1$. بما أن S p-زمرة جزئية لسيلو من G ، فإن $|S| = p^r$. إذن

$$\begin{aligned} [G : S] &= |G| / |S| \\ &= p^r m / p^r \\ &= m \end{aligned}$$

بما أن $S \leq N(S) \leq G$ ، فإن $\{G : S] = [G : N(S)] [N(S) : S]$. لكن $p \mid [G : N(S)] , p \nmid [G : S]$. إذن $p \nmid [N(S) : S]$.

الزمرة المتماثلة والزمر منتهية التوليد

Symmetric group and finitely generated groups

١٢٢. برهن أن كل دورتين في S_n لهما نفس الطول تكونان مترافقتين .

الحل: ليكن $f = (a_1\ a_2\ \dots\ a_r)$, $g = (b_1\ b_2\ \dots\ b_r)$ دورتان في S_n طولهما r . ليكن $h \in S_n$ ، بحيث $h(a_i) = b_i$, $i = 1,2,\dots,r$. إذن لكل $i = 1,2,\dots,r$, b_i يكون

$$h\, f\, h^{-1}(b_i) = h\, f(h^{-1}(b_i)) = h\, f(a_i) = h(a_{i+1}) = b_{i+1} = g(b_i)$$

ليكن $j \in I_n \setminus \{b_1,b_2,\dots,b_r\}$ ، حيث $I_n = \{1,2,\dots,n\}$. إذن $h^{-1}(j) \notin \{a_1,a_2,\dots,a_r\}$. إذن $f(h^{-1}(j)) = h^{-1}(j)$. إذن $h\, f\, h^{-1}(j) = j$. إذن $h\, f\, h^{-1} = g$. إذن f , g تكونان مترافقتين .

١٢٣. اكتب عناصر S_4 باستخدام الدورات ، ثم أوجد كل الزمر الجزئية وكل الزمر الجزئية لسيلو وكل الزمر الجزئية الناظمية منها وأوجد كذلك $C(S_4)$ (مركز S_4) .

الحل: عناصر S_4 هي

1 , $v_1 = (1\ 2)(3\ 4)$, $v_2 = (1\ 3)(2\ 4)$, $v_3 = (1\ 4)(2\ 3)$,

$a = (2\ 3\ 4)$, $b = (2\ 4\ 3)$, $c = (1\ 2\ 3)$, $d = (1\ 2\ 4)$,

$e = (1 3\ 2)$, $f = (1\ 3\ 4)$, $g = (1\ 4\ 2)$, $h = (1\ 4\ 3)$,

$a' = (3\ 4)$, $b' = (2\ 3)$, $c' = (2\ 4)$, $d' = (1\ 2)$,

$f' = (1\ 3)$, $g' = (1\ 4)$, $h' = (1\ 2\ 3\ 4)$, $i = (1\ 2\ 4\ 3)$,

$k = (1\ 3\ 4\ 2)$, $l = (1\ 3\ 2\ 4)$, $m = (1\ 4\ 3\ 2)$, $n = (1\ 4\ 2\ 3)$.

الزمر الجزئية من S_4 هي

زمر جزئية رتبها 12 : واحدة فقط وهي

$$A_4 = \{1 , v_1 , v_2 , v_3 , a , b , c , d , e , f , g , h\}$$

زمر جزئية رتبها 8 :

$\{1 , v_1 , v_2 , v_3 , a' , d' , l , n\}$, $\{1 , v_1 , v_2 , v_3 , c' , f' , h' , m\}$,

$\{1 , v_1 , v_2 , v_3 , b' , g' , i , k\}$

لاحظ أن هذة الزمر الجزئية الثلاثة تماثل D_4 .

زمر جزئية رتبها 6 :

$\{1 , a' , b' , c' , a , b\} , \{1 , b' , d' , f' , c , e\} , \{1 , c' , d' , g' , d , g\} ,$

$\{1 , a' , f' , g' , f , h\}$

لاحظ أن هذة الزمر الجزئية الأربعة تماثل S_3 .

زمر جزئية رتبها 4 :

$\{1 , v_1 , v_2 , v_3\} , \{1 , a' , d' , v_1\} , \{1 , c' , f' ,v_2\} , \{1 , g' , b' , v_3\} ,$

وكلٍ منها يماثل K_4

$\{1 , l , v_1 , n\} , \{1 , h' , v_2 , m\} , \{1 , i , v_3 , k\}$

وكلٍ منها يماثل $\mathbf{Z}_4$

زمر جزئية رتبها 3 :

$\{1 , a , b\} , \{1 , c , e\} , \{1 , 1 , d , g\} , \{1 , f , h\}$

زمر جزئية رتبها 2 :

$\{1 , v_1\} , \{1 , v_2\} , \{1 , v_3\} , \{1 , a'\} , \{1 , b'\} , \{1 , c'\} , \{1 , d'\} , \{1 , f'\} ,$

$\{1 , g'\}$

الزمر الجزئية الناظمية من S_4 هي:

$A_4 \ , \ \ \{1 , v_1 , v_2 , v_3\} = C(S_4)$

S_4 تحتوي 2-زمر جزئية لسيلو وهي كل الزمر الجزئية التي رتبها 8 ، وتحتوي 3-زمر جزئية لسيلو وهي كل الزمر الجزئية التي رتبها 3 .

١٢٤. برهن أن

(أ) $S_n = \langle (1\ 2). (1\ 3). \cdots . (1\ n) \rangle$.

(ب) $S_n = \langle (1\ 2),(1\ 2\ 3 \cdots n) \rangle$.

(ت) $S_n = \langle \big(f(1)\ f(2)\big),(f(1) \cdots f(n)) \rangle$ ، لكل $f \in S_n$.

الحل: (أ) ليكن $f \in S_n$. إذن f تساوي حاصل ضرب ناقلات (مبرهنة) . ليكن $i,j \in I_n = \{1,2,\ldots,n\}$. إذن $(i\ j) = (1\ i)\ (1\ j)\ (1\ i)$. لكن S_n تتولد بمجموعة كل الناقلات فيها . إذن $S_n = \langle (1\ 2).(1\ 3).\cdots.(1\ n) \rangle$.

(ب) ليكن $f = (1\ 2\ \ldots\ n)$. إذن

$$f^t\ (1\ 2)\ (f^t)^{-1} = (f^t(1)\ \ f^t(2)) = (t+1\ \ t+2) \qquad \text{(مبرهنة)}$$

لأن $f^t(1) = t+1\ ,\ f^t(2) = t+2$. ليكن $i,j \in I_n$ ، بحيث $i < j$. إذن

$$(i\ j) = (i\ \ i+1)(i+1\ \ i+2)\ \ldots\ (j-1\ \ j)(j-2\ \ j-1)\ \ldots\ (i+1\ \ i+2)(i\ \ i+1)$$
$$= \left(f^{i-1}\ (1\ 2)\ (f^{i-1})^{-1}\right)\left(f^{i}\ (1\ 2)\ (f^{i})^{-1}\right)\ \ldots\ \left(f^{j-2}\ (1\ 2)\ (f^{j-2})^{-1}\right)\ \ldots$$

إذن كل ناقلة $(i\ j)$ في S_n ، حيث $i < j$ تتولد بالتبديلتين $(1\ 2)\ ,\ f = (1\ 2\ \ldots\ n)$. لكن كل تبديلة في S_n تساوي حاصل ضرب ناقلات (مبرهنة) . إذن $S_n = \langle (1\ 2),(1\ 2\ 3\ \cdots n) \rangle$

(ت) ليكن $f,g \in S_n$. من (ب) ينتج أن $(1\ 2\ \ldots\ n)\ ,\ (1\ 2)$ تولدان التبديلة $f^{-1}\ g\ f$. لكن

$$f\ (1\ 2)\ f^{-1} = (f(1)\ \ f(2)) \qquad , \qquad f\ (1\ 2\ \ldots\ n)\ f^{-1} = (f(1)\ \ f(2)\ \ \ldots\ \ f(n))$$

إذن g تساوي حاصل ضرب منتهي من التبديلتين $(f(1)\ \ f(2))\ ,\ (f(1)\ \ f(2)\ \ \ldots\ \ f(n))$.

إذن $S_n = \langle (f(1)\ f(2)),(f(1)\cdots f(n)) \rangle$ ، لكل $f \in S_n$.

١٢٥. برهن أن كل زمرة منتهية تماثل زمرة جزئية من زمرة بسيطة .

الحل: ليكن G زمرة منتهية ، وليكن $|G| = n$. لاحظ أنة عندما $n = 1,2$ ، فإن المطلوب يكون بديهي . لذلك نفرض أن $n > 3$. من مبرهنة كايلي (Cayly's theorem) ينتج أن G تماثل زمرة جزئية من الزمرة S_n . لذلك نبرهن أن S_n تماثل زمرة جزئية من زمرة بسيطة . ليكن $f = (a_1\ a_2\ \ldots\ a_r) \in S_n$. نضع $f' = (n+a_1\ \ n+a_2\ \ldots\ n+a_r)$. إذن $f' \in S_{2n}$. وبالتالي $f\ \ f' \in S_{2n}$. لاحظ أن التبديلتين $f\ ,\ f'$ منفصلتين (أي لا توجد أرقام مشتركة بينهما) . ليكن $g \in S_n$. إذن g لها تحليلاً وحيداً كحاصل ضرب دورات منفصلة ، وليكن $g = g_1\ g_2\ \ldots\ g_k$. ليكن $\alpha : S_n \to A_{2n}$ ، بحيث $\alpha(g) = \alpha(\ g_1\ g_2\ \ldots\ g_k) = g_1\ g_1'\ g_2\ g_2'\ \ldots g_k\ g_k'$. من السهل اثبات أن α يكون تشاكل زمري متباين . إذن ينتج من مبرهنة التماثل الأولى في الزمر أن $S_n / Ker(\alpha) \cong \alpha(S_n)$. لكن α متباين . إذن $Ker(\alpha) = \{1\}$. إذن $S_n \cong \alpha(S_n)$.

إذن S_n تماثل زمرة جزئية من A_{2n} . لكن A_m تكون زمرة بسيطة لكل $m \geq 5$ (مبرهنة) . إذن

A_{2n} تكون زمرة بسيطة (لاحظ أن $n > 3$) . إذن S_n تماثل زمرة جزئية من زمرة بسيطة . إذن كل زمرة منتهية تماثل زمرة جزئية من زمرة بسيطة .

١٢٦. ليكن $g \in S_4$, $f \in K_4 \subset S_4$. اثبت أن $\langle f , g\rangle \neq S_4$.

الحل: لاحظ أنة إذا كان $f = 1$ أو $g = 1$ ، فإن $\langle f , g\rangle \neq S_4$. لذلك نفرض أن $f \neq 1 , g \neq 1$. ليكن $f \in K_4 \subset S_4 , g \in S_4$. نفرض أن $< f , g> = S_4$. إذن $g \notin K_4$. وإلا كان $<f , g> \leq K_4$. كذلك $g \notin A_4$ ، لأن $K_4 \leq A_4$ وإذا كان $g \in A_4$ ، فإن $<f , g> \leq A_4$. إذن ينتج من تمرين (١٢٣) أن

$$g \notin \{1 , v_1 , v_2 , v_3 , a , b , c , d , e , f , g , h , a' , b' , c' , d' , f' , g'\}$$

إذن $ord(g) = 4$, $ord(f) = 2$. إذن $<f , g>$ تكون زمرة جزئية من S_4 رتبتها 8 (تماثل D_4) (حيث $f \in K_4 , g \in S_4 \backslash A_4$) . إذن $\langle f , g\rangle \neq S_4$.

١٢٧. أوجد عدد الدورات التي طولها k في S_n ، حيث $k = 1,2,\ldots,n$.

الحل: ليكن $k = n$ ، وليكن $i_2,i_3,\ldots,i_n \in \{2,3,\ldots,n\}$. إذن طول الدورة $(1\ i_2\ i_3 \ldots i_n)$ يساوي n . لاحظ أن أي دورة طولها n تكون في هذة الصورة ، لأن

$$\begin{aligned}(1\ i_2\ i_3 \ldots i_n) &= (i_2\ i_3 \ldots 1)\\ &= (i_3\ i_4 \ldots i_n\ 1\ i_2)\\ &= \ldots\\ &= (i_n\ 1\ i_2 \ldots i_{n-1})\end{aligned}$$

إذن عدد الدورات التي في الصورة $(1\ i_2\ i_3 \ldots i_n)$ يساوي عدد التباديل على الأعداد $i_2,i_3,\ldots,i_n$ ، وهو $(n-1)!$.

ليكن $k < n$. وليكن $i_1,i_2,\ldots,i_k \in I_n = \{1,2,3,\ldots,n\}$. إذن عدد المجموعات الجزئية المختلفة $\{i_1,i_2,\ldots,i_k\}$ من I_n يساوي $\binom{n}{k}$. لكن كما سبق فإن عدد الدورات المختلفة التي طولها k في الزمرة المتماثلة $S(\{i_1,i_2,\ldots,i_k\})$ يساوي $(k-1)!$. إذن عدد الدورات التي طولها k في S_n حيث $k = 1,2,\ldots,n$ يساوي $(k-1)! \binom{n}{k}$.

١٢٨. ليكن $f,g\in S_n$ ، بحيث $f = (1\ 2\ \dots\ n)$. برهن أن: $f\,g = g\,f \Leftrightarrow g\in\langle f\rangle$.

الحل: ليكن $f,g\in S_n$ ، بحيث $f = (1\ 2\ \dots\ n)$. وليكن

$$\begin{aligned} H &= \{g\in S_n \mid g\,f = f\,g\} \\ &= \{g\in S_n \mid g\,f\,g^{-1} = f\} \\ &= \{g\in S_n \mid g\,(1\ 2\ \dots\ n)\,g^{-1} = (1\ 2\ \dots\ n)\} \\ &= \{g\in S_n \mid (g(1)\ \ g(2)\ \dots\ g(n)) = (1\ 2\ \dots\ n)\} \end{aligned}$$

$(\Leftarrow)$ ليكن $f\,g = g\,f$. إذن $g\in H$. إذن يوجد $r\in\{1,2,\dots,n\}$ ، بحيث $g(r) = 1$. إذن

$$\begin{aligned} (g(1)\ \ g(2)\ \dots\ g(n)) &= (g(r)\ \ g(r+1)\ \dots\ g(n)\ \ g(1)\ \ g(r-1)) \\ &= (1\ 2\ 3\ \dots\ n-r+1\ \ n-r+2\ \ \dots\ n) \end{aligned}$$

حيث

$$g(r) = 1\ ,\ g(r+1) = 2\ ,\ g(r+2) = 3\ ,\ g(n) = n-r+1\ ,$$
$$g(1) = (n-r+1)+1\ ,\ \dots\ ,\ g(r-1) = (n-r+1)+r-1 = n$$

إذن

$$g = \begin{pmatrix} r & r+1 & r+2 & \cdots & n & 1 & 2 & \cdots & r-1 \\ 1 & 2 & 3 & \cdots & n-r+1 & n-r+2 & n-r+3 & \cdots & n \end{pmatrix}$$

نضع الصف $a_1\ a_2\ \dots\ a_n$ بدلاً من الصف الأول في g . إذن

$$a_1 = r\ ,\ a_2 = r+1\ ,\ \dots, a_{n-r+1} = n\ ,\ a_{n-r+2} = 1\ ,\ a_{n-r+3} = 2\ ,\ \dots\ ,\ a_n = n$$

إذن

$$\begin{aligned} g &= \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_{(n-r+1)+1} & a_{(n-r+1)+2} & a_{(n-r+1)+3} & \cdots & a_{(n-r+1)+n} \end{pmatrix} \\ &= (a_1\ \ a_2\ \ \dots\ \ a_n)^{n-r+1} \\ &= (1\ 2\ \dots\ n)^{n-r+1} \\ &= f^{n-r+1} \in \langle f \rangle \end{aligned}$$

($\Rightarrow$) ليكن $g \in \langle f \rangle$. إذن يوجد $m \in \mathbf{N}$ ، بحيث $g = f^m$. إذن $g\,f = f^{m+1}$, $f\,g = f^{m+1}$.
إذن $f\,g = g\,f$.

١٢٩. ليكن $\alpha \in Aut(S_n)$ بحيث صورة أي ناقلة بـ α تكون ناقلة أيضاً . اثبت أن α تكون تماثل ذاتي داخلي (inner automorphism) .

الحل: ليكن $\alpha \in Aut(S_n)$ بحيث صورة أي ناقلة بـ α تكون ناقلة أيضاً . ليكن $a \in \{1,2,\ldots,n\}$ عنصر ثابت . نعتبر كل الناقلات $(a\ b)$ في S_n . ليكن $(a\ b)\ ,\ (a\ c) \in S_n$. ليكن $\alpha(a\ b) = (a'\ b')\ ,\ \alpha(a\ c) = (u\ v)$. نفرض أن $\{a'\ ,\ b'\} \cap \{u\ ,\ v\} = \emptyset$. إذن $(a'\ b')\ (u\ v) = (u\ v)\ (a'\ b')$. بما أن رتبة أي ناقلة يساوي 2 وبما أن α تماثل زمري ، وبالتالي $ord(\alpha(g)) = ord(g)$ لكل $g \in S_n$ ، فإن

$$
\begin{aligned}
2 &= ord((a'\ b')\ (u\ v)) \\
&= ord(\alpha(a\ b)\ \alpha(a\ c)) \\
&= ord(\alpha((a\ b)(a\ c)) \\
&= ord(\alpha(a\ c\ b)) \\
&= 3
\end{aligned}
$$

لكن هذا غير ممكن . إذن $\{a'\ ,\ b'\} \cap \{u\ ,\ v\} \neq \emptyset$. إذن $a' = u$ (أو $a' = v$) . إذن

$$\alpha((a\ b)) = (a'\ b')\ ,\ \ \alpha((a\ c)) = (a'\ v)$$

هذا يعني أن أي ناقلتين تحتويان رقماً مشتركاً ، تكون صورتهما ناقلتان تحتويان أيضاً رقما مشتركاً . ليكن $(a\ b),(a\ c),(a\ d) \in S_n$ ، حيث a,b,c,d أرقام مختلفة . بالتالي صورة أي ناقلتين منها تحتويان رقما مشتركاً . إذن

$$\alpha((a\ b)) = (a'\ b')\ ,\ \ \alpha((a\ c)) = (a'\ c')\ ,\ \ \alpha((a\ d)) = (c'\ b')\ \text{ or }\ (a'\ d')$$

نفرض أن $\alpha((a\ d)) = (c'\ b')$. إذن

$$
\begin{aligned}
2 &= ord((a'\ b')) \\
&= ord(\ (a'\ b')\ (b'\ c')\ (a'\ c')\ ) \\
&= ord(\ \alpha((a\ b)\ \alpha((a\ d)\ \alpha((a\ c)\ ) \\
&= ord(\ \alpha((a\ b)\ (a\ d)\ (a\ c))\ ) \\
&= ord(\ \alpha(a\ c\ d\ b)\ )
\end{aligned}
$$

$= 4$

وهذا غير ممكن . إذن $\alpha((a\ d)) = (a'\ d')$. إذن إذا كان أي ثلاثة ناقلات في S_n تحتوي رقماً مشتركاً ، فإن صورها تحتوي أيضاً رقماً مشتركاً . بالمثل أي عدد من الناقلات في S_n التي تحتوي رقماً مشتركاً ، تكون صورها محتوية أيضاً رقماً مشتركاً . إذن توجد $f \in S_n$ ، بحيث

$$\alpha((a\ b)) = (f(a)\ \ f(b)) \quad , \forall\ (a\ b) \in S_n$$

لكن $f\ (a\ b)\ f^{-1} = (f(a)\ \ f(b))$ (مبرهنة) . إذن

$$\alpha((a\ b)) = f\ (a\ b)\ f^{-1} \quad , \forall\ (a\ b) \in S_n$$

ليكن $g \in S_n$. إذن $g = (a_1\ b_1)\ (a_2\ b_2)\ \ldots\ (a_m\ b_m)$ (لأن أي تبديلة في S_n تتحلل إلى حاصل ضرب ناقلات منفصلة (مبرهنة)) . إذن

$$\begin{aligned} \alpha(g) &= \alpha((a_1\ b_1))\ \ \alpha((a_2\ b_2))\ \ldots\ \alpha((a_m\ b_m)) \\ &= f\ (a_1\ b_1)\ f^{-1}\ \ f\ (a_2\ b_2)\ f^{-1}\ \ \ldots\ f\ (a_m\ b_m)\ f^{-1} \\ &= f\ (a_1\ b_1)\ (a_2\ b_2) \ldots (a_m\ b_m)\ f^{-1} \\ &= f\ g\ f^{-1} \end{aligned}$$

إذن α يكون تماثل ذاتي داخلي .

١٣٠. (أ) اذكر العناصر في S_n التي رتبها 2 .

(ب) ليكن $f \in S_n$ ، بحيث $ord(f\ ) = 2$. اثبت أن كل عناصر S_n المرافقة لـ f تكون رتبتها 2 .

الحل: (أ) رتبة أي تبديلة f في S_n يساوي 2 إذا وفقط إذا كانت f تتحلل إلى حاصل ضرب ناقلات منفصلة . هذا يتضمن أن رتبة كل ناقلة في S_n يساوي 2 .

(ب) ليكن $f \in S_n$ ، بحيث $ord(f\ ) = 2$. بما أن f تتحلل إلى حاصل ضرب ناقلات منفصلة (مبرهنة) ، فإنة يوجد في S_n ناقلات منفصلة $f_1\ , f_2\ ,\ldots, f_m$ بحيث $f = f_1\ f_2\ \ldots\ f_m$. ليكن مجموعة كل عناصر S_n التي ترافق f هي

$$H = \{g\ f\ g^{-1} \mid g \in S_n\}$$

ليكن $f_1 = (a_1\ b_1)\ , f_2 = (a_2\ b_2)\ \ , \ldots , f_m = (a_m\ b_m)$. إذن

$$\begin{aligned} g\ f\ g^{-1} &= g\ f_1\ f_2\ \ldots\ f_m\ g^{-1} \\ &= (g\ f_1\ g^{-1})\ (g\ f_2\ g^{-1})\ \ldots\ (g\ f_m\ g^{-1}) \\ &= (g\ (a_1\ b_1)\ g^{-1})\ (g\ (a_2\ b_2)\ g^{-1})\ \ldots\ (g\ (a_m\ b_m)\ g^{-1}) \end{aligned}$$

$$= (g(a_1)\ g(b_1))\ (g(a_2)\ g(b_2))\ \ldots\ (g(a_m)\ g(b_m))$$

إذن $g\ f\ g^{-1}$ تتحلل إلى حاصل ضرب ناقات منفصلة . إذن رتبة $g\ f\ g^{-1}$ يساوي 2 .

١٣١. اثبت أن الزمرة $\mathbf{Q}$ ليست منتهية التوليد .

الحل: نفرض عكس المطلوب ، أي نفرض أن الزمرة $\mathbf{Q}$ منتهية التوليد . إذن يوجد $q_1,q_2,\ldots,q_n\in\mathbf{Q}$ ، بحيث $\mathbf{Q} = \langle q_1,q_2,\cdots,q_n\rangle$. ليكن

$$q_1 = \frac{a_1}{b_1}\ \ ,\ \ q_2=\frac{a_2}{b_2}\ \ ,\ \cdots,\ \ q_n=\frac{a_n}{b_n}$$

حيث $b_1,\ldots,b_n\in\mathbf{Z}\backslash\{0\}\ ,\ a_1,\ldots,a_n\in\mathbf{Z}$. ليكن $q\in\mathbf{Q}$.

إذن يوجد $m_1,m_2,\ldots,m_n\in\mathbf{Z}$ ، بحيث

$$q = m_1 q_1 + m_2 q_2 +\ldots+ m_n q_n$$
$$= m_1\frac{a_1}{b_1} + m_2\frac{a_2}{b_2} + \cdots + m_n\frac{a_n}{b_n}$$
$$= \frac{c}{b_1 b_2\cdots b_n}$$

حيث $c\in\mathbf{Z}$. ليكن p عدد أولي بحيث لا يقسم $b_1\ b_2\ \ldots\ b_n$. نأخذ $q=\frac{1}{p}$. إذن $\frac{c}{b_1 b_2\cdots b_n} = \frac{1}{p}$. إذن $p\ c = b_1\ b_2\ \ldots\ b_n$. إذن $p \mid b_1\ b_2\ \ldots\ b_n$. وهذا يناقض الفرض بأن p عدد أولي لا يقسم $b_1\ b_2\ \ldots\ b_n$. إذن الزمرة $\mathbf{Q}$ ليست منتهية التوليد .

١٣٢. اثبت أن الزمرة $\mathbf{Q}^*$ ليست منتهية التوليد .

الحل: نفس طريقة الحل المتبعة في تمرين (١٣١) .

١٣٣. برهن أن الزمرة $\mathbf{Q}$ ليست دائرية وأن الزمرة $\mathbf{Z}$ لا تماثل الزمرة $\mathbf{Q}$.

الحل: إذا كانت $\mathbf{Q}$ دائرية ، فإنها تكون مولدة بعنصر واحد وبالتالي تكون منتهية التوليد . لكن هذا يتناقض مع ما جاء في تمرين (١٣١) بأن $\mathbf{Q}$ ليست منتهية التوليد . إذن $\mathbf{Q}$ ليست دائرية . وبما أن $\mathbf{Z}$ دائرية ، فإن $\mathbf{Z}$ لا تماثل الزمرة $\mathbf{Q}$.

١٣٤. استخدم المبرهنة الأساسية للزمر الإبدالية منتهية التوليد لإثبات أن $\mathbf{Q}$ زمرة ليست منتهية التوليد .

الحل: نفرض عكس المطلوب ، أي نفرض أن الزمرة $\mathbf{Q}$ منتهية التوليد . لاحظ أن الزمرة $\mathbf{Q}$ ابدالية. إذن ينتج من المبرهنة الأساسية للزمر الإبدالية منتهية التوليد أنة يوجد $m_1,m_2,\ldots,m_s\in\mathbf{N}\backslash\{1\}$ ، بحيث $m_1 \mid m_2 , m_2 \mid m_3 , \ldots , m_{s-1} \mid m_s$ ، وبحيث

$$\mathbf{Q} \cong \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_s} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \quad (\text{مرة } k)$$

حيث k هو عدد عناصر المجموعة المولدة لـ $\mathbf{Q}$. بما أن رتبة كل عنصر غير المحايد في $\mathbf{Q}$ تكون غير منتهية (أي يكون عنصر عديم الفتل torsion free element) ، فإن $s = 0$. وبالتالي يكون

$$\mathbf{Q} \cong \underbrace{\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}}_{\text{مرة } k}$$

نفرض أن $k \geq 2$. إذن يوجد $x_1,x_2\in\mathbf{Q}\backslash\{0\}$ ، بحيث يكونان مستقلين خطياً فوق $\mathbf{Z}$ ، أي أن

$$n_1 x_1 + n_2 x_2 = 0 \ , n_1,n_2\in\mathbf{Z} \ \Rightarrow \ n_1 = n_2 = 0$$

ليكن $a_1,a_2,b_1,b_2\in\mathbf{Z}\backslash\{0\}$, $x_1 = a_1/b_1$, $x_2 = a_2/b_2$. بما أن $(a_2 b_1) (a_1/b_1) + (-a_1 b_2) (a_2/b_2) = 0$ ، فإن $a_1 b_2 = a_2 b_1 = 0$. إذن $a_1 = 0$ أو $b_2 = 0$ و $a_2 = 0$ أو $b_1= 0$. لكن هذا يناقض الفرض بأن $a_1,a_2,b_1,b_2\in\mathbf{Z}\backslash\{0\}$. إذن $k = 1$. إذن $\mathbf{Q} \cong \mathbf{Z}$. إذن الزمرة $\mathbf{Q}$ تكون دائرية . ليكن $\mathbf{Q} = \langle q\rangle$. لكن $q/2\notin\langle q\rangle$, $q/2 \in\mathbf{Q}$. وهذا تناقض . إذن $\mathbf{Q}$ تكون غير منتهية التوليد .

١٣٥. ليكن A مجموعة جزئية منتهية من $\mathbf{Q}$. اثبت أن $\langle A\rangle$ تكون زمرة جزئية دائرية من $\mathbf{Q}$.

الحل: ليكن $A =\{a_1/b_1 , a_2/b_2 ,\ldots, a_n/b_n\}$ مجموعة جزئية منتهي من $\mathbf{Q}$. وليكن $x\in\langle A\rangle$. إذن

$$x = m_1 (a_1/b_1) + m_2 (a_2/b_2) + \ldots + m_n (a_n/b_n)$$

حيث $m_1,m_2,\ldots,m_n\in\mathbf{Z}$. إذن

$$x = \frac{m_1a_1(b_2b_3\cdots b_n)+m_2a_2(b_1b_3\cdots b_n)+\cdots+m_na_n(b_1b_2\cdots b_{n-1})}{b_1b_2\cdots b_n}$$

$$= m\frac{1}{b_1 b_2 \cdots b_n}$$

حيث $m = m_1 a_1 (b_2 b_3 \cdots b_n) + m_2 a_2 (b_1 b_3 \cdots b_n) + \cdots + m_n a_n (b_1 b_2 \cdots b_{n-1})$

١٣٦. ليكن G زمرة ابدالية منتهية رتبتها n . إذا كانت n تساوي حاصل ضرب أعداد أولية مختلفة ، فبرهن باستخدام المبرهنة الإساسية للزمر الإبدالية منتهية التوليد أن $G \cong \mathbf{Z}_n$.

الحل: ليكن G زمرة ابدالية منتهية رتبتها n ، وليكن n تساوي حاصل ضرب أعداد أولية مختلفة . بما أن G زمرة منتهية ، فإنها تكون منتهية التوليد . إذن ينتج من المبرهنة الأساسية للزمر الإبدالية منتهية التوليد أن

$$G \cong \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_s} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \qquad (\text{k مرة})$$

بحيث $m_1 \mid m_2 \mid \ldots \mid m_s$, $m_i \geq 2$.

بما أن G منتهية ، فإن $k = 0$. إذن

$$G \cong \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_s}$$

ليكن p عدد أولي بحيث $p \mid n$. بما أن $n = m_1 m_2 \ldots m_s$ ، فإنة يوجد $i \in \{1,\ldots,s\}$ بحيث $p \mid m_i$. لكن $m_1 \mid m_2 \mid \ldots \mid m_s$. إذن إذا كان $i \neq s$ ، فإن $p^2 \mid m_s$ وبالتالي $p^2 \mid n$. لكن هذا يتناقض مع الفرض بأن n تساوي حاصل ضرب أعداد أولية مختلفة . إذن $i = s$. إذن كل قاسم أولي لـ n يقسم أيضاً m_s . إذن $n = m_s$. إذن $G \cong \mathbf{Z}_n$.

١٣٧. ليكن $f \in S_5 \backslash \{1\}$ ، بحيث $ord(f) \neq 2$. اثبت أنة يوجد $g \in S_5$ ، بحيث $S_5 = \langle g , f \rangle$.

الحل: ليكن $f \in S_5 \backslash \{1\}$ ، بحيث $ord(f) \neq 2$. بما أن f لها تحليلاً وحيداً كحاصل ضرب دورات منفصلة ، فإن f لها الإحتمالات التالية:

(أ) f تكون دورة خماسية ، أي $f = (a_1\ a_2\ a_3\ a_4\ a_5)$ ، حيث $a_1, a_2, a_3, a_4, a_5 \in \{1,2,3,4,5\}$.

ليكن $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$. إذن $f = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$. ليكن $g = (h(1)\ h(2))$. إذن ينتج من تمرين (١٢٤) (ت) أن $S_5 = \langle g , f \rangle$.

(ب) f تكون دورة رباعية ، أي $f = (a_1\ a_2\ a_3\ a_4)$ ، حيث $a_1,a_2,a_3,a_4 \in \{1,2,3,4,5\}$. ليكن $g = (a_4\ a_5)$. إذن $f\,g = (a_1\ a_2\ a_3\ a_4\ a_5) = (a_4\ a_5\ a_1\ a_2\ a_3)$. ليكن $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix}$. إذن

$f\,g = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))\ ,\ g = (h(1)\ h(2))$

إذن ينتج من تمرين (١٢٤) (ت) أن $S_5 = \langle f\,g , f \rangle = \langle g , f \rangle$.

(ت) f تكون دورة ثلاثية ، أي $f = (a_1\ a_2\ a_3)$. ليكن $g = (a_2\ a_3\ a_4\ a_5)$. إذن $f\,g = (a_1\ a_2)\ (a_3\ a_4\ a_5)$. إذن $(f\,g)^3 = (a_1\ a_2)\ ,\ (f\,g)^3\,g = (a_1\ a_2\ a_3\ a_4\ a_5)$

ليكن $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$. إذن ينتج من تمرين (١٢٤) (ت) أن

$(f\,g)^3\,g = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))\ \ ,\ \ (f\,g)^3 =(h(1)\ h(2))$

إذن $S_5 = \langle (fg)^3 ,(fg)^3 g\rangle$. لكن $\langle (fg)^3 ,(fg)^3 g\rangle \subseteq \langle g , f\rangle$. إذن $S_5 = \langle g , f \rangle$.

(ث) f تكون دورة ثنائية ، أي $f = (a_1\ a_2)$. ليكن $g = (a_2\ a_3\ a_4\ a_5)$. إذن $f\,g = (a_1\ a_2\ a_3\ a_4\ a_5)$. ليكن $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$. إذن $f = (h(1)\ h(2))\ ,\ f\,g = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$. إذن ينتج من تمرين (١٢٤) (ت) أن $S_5 = \langle f , f\,g \rangle$. لكن $\langle f , f\,g \rangle \subseteq \langle f , g \rangle$. إذن $S_5 = \langle g , f \rangle$.

(ج) $f = (a_1\ a_2)\ (a_3\ a_4\ a_5)$. ليكن $g = (a_1\ a_2\ a_3)(a_1\ a_2)$. إذن $f^3 = (a_1\ a_2)\ \ ,\ \ g\,f = (a_1\ a_2\ a_3\ a_4\ a_5)$. ليكن $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$. إذن $f^3 = (h(1)\ h(2))\ \ ,\ \ g\,f = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$. إذن ينتج من تمرين (١٢٤) (ت) أن $S_5 = \langle f^3 . g\,f \rangle = \langle g , f \rangle$.

١٣٨. ليكن $G = \langle x , y \mid ord(x)=2 , ord(y)=3 , (xy)^2 = 1\rangle$. برهن أن $G \cong S_3$.

الحل: ليكن $G = \langle x , y \mid ord(x)=2 , ord(y)=3 , (xy)^2 = 1\rangle$. أي عنصر في G يكون في صورة حاصل ضرب منتهي لعناصر في الصورة $x^m\,y^n$ ، حيث $m,n \in \mathbf{Z}$. بما أن

$(x\,y)^2 = 1$ ، فإن $x\,y = (x\,y)^{-1} = y^{-1}\,x^{-1}$. وبما أن $x^2 = 1$ ، فإن $x = x^{-1}$. كذلك $x^m = 1$ لأي عدد زوجي m و $x^n = x$ لأي عدد فردي n . إذن $y^m\,x = x^{-1}\,y^{-m}$ ، لكل $m\in\mathbf{N}$. لاحظ أنة ينتج من $y^3 = 1$ أن

$$y = y^4 = y^7 = \ldots = y^{3n+1} = \ldots \quad , n\in\mathbf{N} \;,$$
$$y^2 = y^5 = y^8 = \ldots = y^{3n+2} = \ldots \quad , n\in\mathbf{N} \;,$$
$$1 = y^3 = y^6 = \ldots = y^{3n} = \ldots \quad , n\in\mathbf{N} \,.$$

إذن أي عنصر في G يكون في الصورة $x^m\,y^n$ ، حيث $m,n\in\mathbf{Z}$. إذن

$$G = \{x^m\,y^n \mid m,n\in\mathbf{N}\}$$

بما أن $x^2 = y^3 = 1$ ، فإن $G = \{1 , x , y , y^2 , x\,y , x\,y^2\}$.لاحظ أن

$$S_3 = \{\,1 , (1\;2) , (1\;3) , (2\;3) , (1\;2\;3) , (1\;3\;2)\}$$

ليكن $f = (1\;2) , h = (1\;2\;3)$. إذن $\mathrm{ord}(h) = 3$, $\mathrm{ord}(f) = 2$. وبما أن $f\,h = (2\;3)$ ، فإن $\mathrm{ord}(f\,h) = 2$. إذن $S_3 = < f , h >$. ليكن $\phi : G \to S_3$ ، بحيث $\phi(x) = f , \phi(y) = h$. إذن من السهل إثبات أن ϕ يكون تماثل زمري .

١٣٩. ليكن G زمرة ، بحيث لكل $x,y\in G , n\in\mathbf{N}$ يكون: $x^n = y^n \Rightarrow x = y$.

(أ) برهن أن: $\quad x^{-m}\,y\,x^m = y \;\Rightarrow\; x^{-1}\,y\,x = y$

(ب) لتكن رتبة كل تماثل زمري من G إلى G منتهية . برهن أن G تكون ابدالية ، وإذا كانت G منتهية التوليد ، فإن $G \cong \mathbf{Z}$.

الحل: ليكن G زمرة بحيث لكل $x,y\in G , n\in\mathbf{N}$ يكون $x^n = y^n \;\Rightarrow\; x = y$.

(أ) ليكن $x,y\in G , m\in\mathbf{N}$. ليكن $x^{-m}\,y\,x^m = y$. بضرب الطرفين من اليسار في x^m نحصل على $y\,x^m = x^m\,y$. إذن

$$(y^{-1}\,x\,y)^m = y^{-1}\,x^m\,y = y^{-1}\,y\,x^m = x^m$$

إذن ينتج من الفرض $x^n = y^n \;\Rightarrow x = y$ لكل $n\in\mathbf{N}$ ، أن $y^{-1}\,x\,y = x$. إذن $x^{-1}\,y\,x = y$.

(ب) لتكن رتبة كل تماثل زمري من G إلى G منتهية . ليكن $y\in G$ ، وليكن $f_y : G \to G$ بحيث $f(x) = y^{-1}\,x\,y$ لكل $x\in G$. من السهل اثبات أن f يكون تماثل زمري . إذن رتبة f تكون منتهية (من الفرض) . نفرض أن $\mathrm{ord}(f\,) = m$. إذن $f^{\,m} = 1$. إذن

$f^{m}(x) = y^{-m} x y^{m} = x$. إذن ينتج من (أ) أن $y^{-1} x y = x$. إذن $x y = y x$ ، لكل $x,y \in G$. إذن G تكون زمرة ابدالية .

ليكن الآن G زمرة منتهية التوليد . بالتالي G تكون زمرة ابدالية منتهية التوليد . من المبرهنة الأساسية للزمر الأبدالية منتهية التوليد ينتج أن

$$G \cong \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus \cdots \oplus \mathbf{Z}_{m_s} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \quad (k \text{ مرة})$$

إذا كان $n \in \mathbf{N}$, $x \in G$ بحيث $x^{n} = 1$ ، فإنة ينتج من الفرض أن $x^{n} = y^{n} \Rightarrow x = y$ أن $x = 1$ (لأن $x^{n} = 1 = 1^{n}$) . إذن

$$G \cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \quad (k \text{ مرة})$$

ليكن $k = 2$. إذن $h : \mathbf{Z} \oplus \mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Z}$ ، بحيث $h(m , n) = (m + n , n)$ لكل $(m , n) \in \mathbf{Z} \oplus \mathbf{Z}$ يكون تماثل زمري ورتبتة غير منتهية . لكن هذا يتناقض مع الفرض بأن رتبة كل تماثل زمري من G إلى G تكون منتهية . إذن $k = 1$. إذن $G \cong \mathbf{Z}$.

١٤٠. ليكن G زمرة ابدالية منتهية التوليد . ليكن n هو عدد مولدات G . ليكن $S \leq G$. اثبت أن عدد مولدات S يكون أقل من أو يساوي n .

الحل: ليكن G زمرة ابدالية منتهية التوليد ، وليكن n هو عدد مولدات G . إذن يوجد $x_1,x_2,\ldots,x_n \in G$ ، بحيث $G = \langle x_1,x_2,\ldots,x_n \rangle$. ليكن $S \leq G$. نبرهن أن عدد مولدات S يكون أقل من أو يساوي n . نستخدم مبدأ الإستنتاج الرياضي على n . عندما $n = 1$ ، فإن $G = \langle x_1 \rangle$. أي أن G في هذة الحالة تكون زمرة دائرية مولدة من x_1 . إذن S تكون زمرة دائرية (وذلك من المبرهنة التي تنص على أن أي زمرة جزئية من زمرة دائربة تكون دائرية) . أي أن S في هذة الحالة تتولد من عنصر واحد . إذن المطلوب يتحقق عندما $n = 1$. نفرض أن المطلوب يتحقق عند $n - 1$ ، ونبرهن تحققة عند n . أي أننا نفرض أن أي زمرة جزئية من زمرة إبدالية مولدة من $n - 1$ عنصر تتولد على الأكثر من $n - 1$ عنصر ، ونبرهن أن أي زمرة جزئية من زمرة إبدالية مولدة من n عنصر تتولد على الأكثر من n عنصر . بما أن $G = \langle x_1,x_2,\ldots,x_n \rangle$ زمرة إبدالية منتهية التوليد (تتولد من n عنصر) ، فإن

$$G = \langle x_1,x_2,\ldots,x_n \rangle$$
$$= \langle x_1 \rangle \; \langle x_2 ,\ldots,x_n \rangle$$

وبما أن $S \leq G$ ، فإنة يوجد $B \leq < x_2 ,\ldots,x_n >$ ، $A \leq < x_1 >$ بحيث $S = A B$. من فرض الإستناج الرياضي ينتج أنة يوجد $m \leq n$ ، $b_2 ,\ldots,b_m \in < x_2 ,\ldots,x_n >$ بحيث $B = < b_2 ,\ldots,b_m >$. كذلك يوجد $a \in < x_1 >$ ، بحيث $A = < a >$. إذن

$$S = < a > < b_2 ,\ldots,b_m >$$
$$= < a , b_2 ,\ldots,b_m >$$

إذن S تتولد من n عنصرعلى الأقل .

١٤١. اكتب كل عناصر Q_8 وأوجد كل الزمر الجزئية غير البديهية وكذلك الزمر الجزئية الناظمية غير البديهية منها ، علما بأن

$$Q_8 = \langle a , b \mid a^4=1 .\ a^2 = b^2, b\, a = a^3\, b \rangle$$

وتسمى الزمرة المرباعية (Quaternion group) .

الحل: نعتبر الزمرة المرباعية

$$Q_8 = \langle a , b \mid a^4=1 .\ a^2 = b^2, b\, a = a^3\, b \rangle$$

إذن $\operatorname{ord}(a) = 4 , \operatorname{ord}(a^2) = 2 , \operatorname{ord}(a^3) = 4 , \operatorname{ord}(b) = 4$

وبما أن $(a\, b)^2 = (a\, b)\, (a\, b) = a\, a^3\, b\, b = b^2 = a^2$ ، فإن $\operatorname{ord}(a\, b) = 4$.

وبما أن $(a^2\, b)^2 = (a^2\, b)\, (a^2\, b) = a^2\, (a^3\, b)\, a\, b = a^5\, b\, a\, b = (a\, b)^2$ ، فـإن $\operatorname{ord}(a^2\, b) = 4$.

وبما أن $(a^3\, b)^2 = (a^3\, b)\, (a^3\, b) = a^3\, (a^3\, b)\, a^2\, b = (a^2\, b)^2$ ، فإن $\operatorname{ord}(a^3\, b) = 4$.

إذن

$$Q_8 = \{1 , a , a^2 , a^3 , b , a\, b , a^2 b , a^3 b\}$$

الزمر الجزئية غير البديهية من Q_8 هى:

$$H_1 = \{1 , a^2\} = < a^2 > \quad , \quad H_2 = \{1 , a , a^2 , a^3\} = < a > \quad ,$$
$$H_3 = \{1 , a\, b , a^2 , a^3\, b\} = < a\, b > \quad , \quad H_4 = \{1 , b , a^2 , a^2\, b\} = < b > .$$

بما أن

$$[Q_8 : H_2] = [Q_8 : H_3] = [Q_8 : H_4] = 2$$

فإن $H_4 \lhd Q_8$ ، $H_3 \lhd Q_8$ ، $H_2 \lhd Q_8$. كذلك $H_1 \lhd Q_8$ ، لأن

$b\,a^2\,b^{-1} = b\,a^2\,b^3 = a^3\,b\,a\,b^3 = a\,b^4 = a^2$,

$(a\,b)\,a^2\,(a\,b)^{-1} = a\,b\,a^2\,b^{-1}\,a^{-1} = a\,(b\,a^2\,b^{-1})\,a^{-1} = a\,(a^2)\,a^3 = a^2$,

$(a^2\,b)\,a^2\,(a^2\,b)^{-1} = a^2\,(b\,a^2\,b^{-1})\,a^2 = a^2\,a^2\,a^2 = a^2$

$(a^3\,b)\,a^2\,(a^3\,b)^{-1} = a^3\,(\,b\,a^2\,b^{-1})\,a = a^2$

١٤٢. أوجد الزمرة الجزئية $\langle f , g\rangle$ من الزمرة S_4 ، حيث $f = (1\,2\,3\,4)\,,\,g = (2\,4)$.

الحل: ليكن $f,g\in S_4$ ، حيث $f = (1\,2\,3\,4)\,,\,g = (2\,4)$. إذن

$ord(f) = 4$, $ord(g) = 2$,

$f\,g = (1\,2)\,(3\,4)$, $f^2\,g = (1\,3)$, $f^3\,g = (1\,4)\,(2\,3)$,

$g\,f = f^3\,g$, $g\,f^2 = f^2\,g$, $g\,f^3 = f\,g$,

$f^{-1} = f^3$, $(f^2)^{-1} = f^2$, $(f^3)^{-1} = f$, $(f\,g)^{-1} = f\,g$, $(f^2\,g)^{-1} = f^2\,g$,

$(f^3\,g)^{-1} = f^3\,g$

إذن

$$< f , g > = \{1 , f , f^2 , f^3 , g , f\,g , f^2\,g , f^3\,g\}$$

١٤٣. اذكر كل عناصر الزمرة $\langle\, a , b \mid a^3 = b^2 = (a\,b)^2 = 1\,\rangle$ ، واذكر معكوس كل عنصر فيها ، ثم أوجد كل الزمر الجزئية غير البديهية منها .

الحل: ليكن $G = \langle\, a , b \mid a^3 = b^2 = (a\,b)^2 = 1\,\rangle$. إذن

$ord(a) = 3$, $ord(b) = ord(a\,b) = 2$,

$b\,a^2 = (a\,b)^2\,b\,a^2 = a\,b\,a\,b\,b\,a^2 = a\,b\,a\,b^2\,a^2 = a\,b$,

$b\,a = b\,a^4 = (b\,a^2)\,a^2 = (a\,b)\,a^2 = a\,(b\,a^2) = a\,(a\,b) = a^2\,b$,

$a^{-1} = a^2$, $(a^2)^{-1} = a$, $b^{-1} = b$, $(a\,b)^{-1} = a\,b$, $(a^2\,b)^{-1} = b\,a = a^2\,b$.

إذن

$$G = \{1 , a , a^2 , b , a\,b , a^2\,b\}$$

كل الزمر الجزئية غير البديهية من G هي:

$< a >$, $< b >$, $< a\,b >$, $< a^2\,b >$

١٤٤. ليكن G زمرة ابدالية ، وليكن $S \subseteq G$ حيث $S = \{g\in G \mid ord(g) < \infty\}$. اثبت أن $S \leq G$. وإذا كانت S منتهية التوليد ، فاثبت أن S تكون منتهية .

الحل: ليكن G زمرة ابدالية ، وليكن $S \subseteq G$ حيث $S = \{g\in G \mid ord(g) < \infty\}$. لاحظ أن $S \neq \emptyset$ ، لأن $1\in S$. ليكن $x,y\in S$. إذن يوجد $m,n\in \mathbf{N}$ ، بحيث $ord(x) = m, ord(y) = n$. لاحظ أن $ord(y^{-1}) = n$. بما أن G زمرة إبدالية ، فإن

$$ord(x\, y^{-1}) = ord(x)\, ord(y^{-1}) = m\, n$$

إذن $x\, y^{-1}\in S$. إذن $S \leq G$. نفرض أن S منتهية التوليد . إذن يوجد $x_1,\ldots,x_r\in S$ ، بحيث $S = < x_1,\ldots,x_r >$. إذن

$$S = \{(x_1)^{t_1}(x_2)^{t_2}\cdots(x_r)^{t_r} \mid t_1,t_2,\cdots,t_r\in\mathbf{Z}\} \qquad \text{(مبرهنة)}$$

ليكن $(x_1)^{t_1}(x_2)^{t_2}\cdots(x_r)^{t_r} \in S$ ، بحيث $t_i > ord(x_i)\, , i = 1,2,\ldots,r$. إذن يوجد $a_1,a_2,\ldots,a_s\in\mathbf{N}\, , s_1,s_2,\ldots,s_r\in\mathbf{N}_0$ ، بحيث

$$t_i = a_i\, ord(x_i) + s_i \quad , \quad s_i < ord(x_i) \quad , i = 1,2,\ldots,r$$

إذن $(x_1)^{t_1}(x_2)^{t_2}\cdots(x_r)^{t_r} = (x_1)^{s_1}(x_2)^{s_2}\cdots(x_r)^{s_r}$. إذن

$$S = \{(x_1)^{t_1}(x_2)^{t_2}\cdots(x_r)^{t_r} \mid t_i \in \mathbf{Z}\, .\, 1 \leq t_i \leq ord(x_i)\, .\, i = 1.2.\cdots.r\}$$

إذن S تكون منتهية .

برهان آخر: نفرض أن G زمرة جمعية إبدالية ، ونفرض أن S منتهية التوليد . إذن S تكون زمرة (جمعية) إبدالية منتهية التوليد . نبرهن أن S تكون منتهية . بما أن S زمرة (جمعية) ابدالية منتهية التوليد ، فإنة ينتج من المبرهنة الأساسية للزمر الإبدالية منتهية التوليد أن S تماثل مجموع مباشر لعدد منتهي من الزمر الدائرية ، أي يوجد $m_1,\ldots,m_r\in\mathbf{N}$ ، بحيث

$$S \cong \mathbf{Z}_{m_1}\oplus \mathbf{Z}_{m_2} \oplus\cdots\oplus \mathbf{Z}_{m_r}\oplus \mathbf{Z} \oplus\cdots\oplus \mathbf{Z} \qquad (k \text{ مرة})$$

حيث k هو عدد العناصر المولدة لـ S وحيث $1 \leq r \leq k$. لكن رتبة كل عنصر في S تكون منتهية (فرضاً) . إذن $r = k$. إذن

$$S \cong \mathbf{Z}_{m_1}\oplus \mathbf{Z}_{m_2}\oplus\cdots\oplus \mathbf{Z}_{m_k}$$

إذن S تكون منتهية .

المتسلسلات شبة الناظمية والمتسلسلات الناظمية للزمر –

Subnormal series and normal series of groups

١٤٥. أوجد مكملتين (refinements) متماثلتين للمتسلسلتين الناظميتين

$\{0\} \leq 60\,\mathbf{Z} \leq 15\,\mathbf{Z} \leq \mathbf{Z} \qquad (1)$

$\{0\} \leq 12\,\mathbf{Z} \leq \mathbf{Z} \qquad (2)$

الحل: نعتبر المتسلسلتين الناظميتين

$\{0\} \leq 60\,\mathbf{Z} \leq 15\,\mathbf{Z} \leq \mathbf{Z} \qquad (1)$

$\{0\} \leq 12\,\mathbf{Z} \leq \mathbf{Z} \qquad (2)$

إذن المتسلسلتين الناظميتين

$\{0\} \leq 60\,\mathbf{Z} \leq 15\,\mathbf{Z} \leq 5\,\mathbf{Z} \leq \mathbf{Z} \qquad (1')$

$\{0\} \leq 60\,\mathbf{Z} \leq 12\,\mathbf{Z} \leq 3\,\mathbf{Z} \leq \mathbf{Z} \qquad (2')$

تكونان مكملتين (refinements) للمتسلسلتين الناظميتين (2) , (1) . ليكن X هي مجموعة كل زمر القسمة (لكل حدين متتاليين) للمتسلسلة (1') ، وليكن Y هي مجموعة كل زمر القسمة (لكل حدين متتاليين) للمتسلسلة (2') ، أي أن

$X = \{60\,\mathbf{Z}/\{0\}\ ,\ 15\,\mathbf{Z}/60\,\mathbf{Z}\ ,\ 5\,\mathbf{Z}/15\,\mathbf{Z}\ ,\ \mathbf{Z}/5\,\mathbf{Z}\}$,

$Y = \{60\,\mathbf{Z}/\{0\}\ ,\ 12\,\mathbf{Z}/60\,\mathbf{Z}\ ,\ 3\,\mathbf{Z}/12\,\mathbf{Z}\ ,\ \mathbf{Z}/3\mathbf{Z}\}$

من مبرهنة التماثل الثانية في الزمر يكون

$15\,\mathbf{Z}/60\,\mathbf{Z} = 15\,\mathbf{Z}/15\,\mathbf{Z} \cap 4\,\mathbf{Z} \cong 15\,\mathbf{Z}+4\,\mathbf{Z}/4\,\mathbf{Z} \cong \mathbf{Z}/4\,\mathbf{Z} \cong \mathbf{Z}_4$,

$5\,\mathbf{Z}/15\,\mathbf{Z} = 5\,\mathbf{Z}/5\,\mathbf{Z} \cap 3\,\mathbf{Z} \cong 5\,\mathbf{Z}+3\,\mathbf{Z}/3\,\mathbf{Z} \cong \mathbf{Z}/3\,\mathbf{Z} \cong \mathbf{Z}_3$,

$\mathbf{Z}/5\,\mathbf{Z} \cong \mathbf{Z}_5$,

$12\,\mathbf{Z}/60\,\mathbf{Z} = 12\,\mathbf{Z}/12\,\mathbf{Z} \cap 5\,\mathbf{Z} \cong 12\,\mathbf{Z}+5\,\mathbf{Z}/5\,\mathbf{Z} \cong \mathbf{Z}/5\,\mathbf{Z} \cong \mathbf{Z}_5$,

$3\,\mathbf{Z}/12\,\mathbf{Z} = 3\,\mathbf{Z}/3\,\mathbf{Z} \cap 4\,\mathbf{Z} \cong 3\,\mathbf{Z}+4\,\mathbf{Z}/4\,\mathbf{Z} \cong \mathbf{Z}/4\,\mathbf{Z} \cong \mathbf{Z}_4$,

$\mathbf{Z}/3\,\mathbf{Z} \cong \mathbf{Z}_3$

ليكن $\alpha : X \to Y$ ، بحيث

$\alpha(60\,\mathbf{Z}/\{0\}) = 60\,\mathbf{Z}/\{0\}$, $\alpha(15\,\mathbf{Z}/60\,\mathbf{Z}) = 3\,\mathbf{Z}/12\,\mathbf{Z}$,

$\alpha(5\,\mathbf{Z}/15\,\mathbf{Z}) = \mathbf{Z}/3\,\mathbf{Z}$, $\alpha(\mathbf{Z}/5\,\mathbf{Z}) = 12\,\mathbf{Z}/60\,\mathbf{Z}$.

إذن α يكون تقابل ويحقق $\alpha(A) \cong A\ ,\ \forall\, A \in X$ ، لأن

$\alpha(60\,\mathbf{Z}/\{0\}) = 60\,\mathbf{Z}/\{0\}$,

$\alpha(15\,\mathbf{Z}/60\,\mathbf{Z}) = 3\,\mathbf{Z}/12\,\mathbf{Z} \cong \mathbf{Z}_4 \cong 15\,\mathbf{Z}/60\,\mathbf{Z}$,

$\alpha(5\,\mathbf{Z}/15\,\mathbf{Z}) = \mathbf{Z}/3\,\mathbf{Z} \cong \mathbf{Z}_3 \cong 5\,\mathbf{Z}/15\,\mathbf{Z}$,

$\alpha(\mathbf{Z}/5\,\mathbf{Z}) = 12\,\mathbf{Z}/60\,\mathbf{Z} \cong \mathbf{Z}_5 \cong \mathbf{Z}/5\,\mathbf{Z}$.

إذن المتسلسلتان (2') , (1') تكونان متماثلتان .

١٤٦. أوجد كل المتسلسلات المركبة (composition series) للزمرتين $\mathbf{Z}_{24}$, S_4 .

الحل: **<u>أولا</u> :** المتسلسلات المركبة للزمرة $\mathbf{Z}_{24}$

المتسلسلات المركبة للزمرة $\mathbf{Z}_{24}$ هي

$$(1) \qquad \{\bar{0}\} \lhd \mathbf{Z}_3 \lhd \mathbf{Z}_6 \lhd \mathbf{Z}_{12} \lhd \mathbf{Z}_{24}$$

لأن:

(لاحظ أن $\mathbf{Z}_m \leq \mathbf{Z}_{mn}$ لا يعني أن $\mathbf{Z}_m$ تكون مجموعة جزئية من $\mathbf{Z}_{mn}$. ولكن يعني أن $\mathbf{Z}_m$ تماثل زمرة جزئية من $\mathbf{Z}_{mn}$ ، فمثلاً $< \bar{2} > \cong \mathbf{Z}_{12}$ و $< \bar{2} >$ زمرة جزئية من $\mathbf{Z}_{24}$)

لاحظ أن زمرة القسمة لمتسلسلة ناظمية أو شبة ناظمية نعني بها زمرة القسمة لحدين متتاليين من هذة المتسلسلة .

زمر القسمة للمتسلسلة (1) هي

$\mathbf{Z}_3/\{\bar{0}\} \cong \mathbf{Z}_3$, $\mathbf{Z}_6/\mathbf{Z}_3 \cong \mathbf{Z}_2$, $\mathbf{Z}_{12}/\mathbf{Z}_6 \cong \mathbf{Z}_2$, $\mathbf{Z}_{24}/\mathbf{Z}_{12} \cong \mathbf{Z}_2$

وبما أن $\mathbf{Z}_2$, $\mathbf{Z}_3$ زمرتين بسيطتين ، فإن زمر القسمة للمتسلسلة (1) تكون جميعها زمر بسيطة .

إذن المتسلسلة (1) تكون متسلسلة مركبة .

$$(2) \qquad \{\bar{0}\} \lhd \mathbf{Z}_2 \lhd \mathbf{Z}_6 \lhd \mathbf{Z}_{12} \lhd \mathbf{Z}_{24}$$

لأن:

زمر القسمة للمتسلسلة (2) هي

$\mathbf{Z}_2/\{\bar{0}\} \cong \mathbf{Z}_2$, $\mathbf{Z}_6/\mathbf{Z}_2 \cong \mathbf{Z}_3$, $\mathbf{Z}_{12}/\mathbf{Z}_6 \cong \mathbf{Z}_2$, $\mathbf{Z}_{24}/\mathbf{Z}_{12} \cong \mathbf{Z}_2$

وبما أن $\mathbf{Z}_3$, $\mathbf{Z}_2$ زمرتين بسيطتين ، فإن زمر القسمة للمتسلسلة (2) تكون جميعها زمر بسيطة .
إذن المتسلسلة (2) تكون متسلسلة مركبة .

$$(3) \quad \{\bar{0}\} \lhd \mathbf{Z}_2 \lhd \mathbf{Z}_4 \lhd \mathbf{Z}_{12} \lhd \mathbf{Z}_{24}$$

لأن:
زمر القسمة للمتسلسلة (3) هي

$$\mathbf{Z}_2 /\{\bar{0}\} \cong \mathbf{Z}_2 \ , \ \mathbf{Z}_4 / \mathbf{Z}_2 \cong \mathbf{Z}_2 \ , \ \mathbf{Z}_{12} / \mathbf{Z}_4 \cong \mathbf{Z}_3 \ , \ \mathbf{Z}_{24} / \mathbf{Z}_{12} \cong \mathbf{Z}_2$$

وبما أن $\mathbf{Z}_3$, $\mathbf{Z}_2$ زمرتين بسيطتين ، فإن زمر القسمة للمتسلسلة (3) تكون جميعها زمر بسيطة .
إذن المتسلسلة (3) تكون متسلسلة مركبة .

$$(4) \quad \{\bar{0}\} \lhd \mathbf{Z}_2 \lhd \mathbf{Z}_4 \lhd \mathbf{Z}_8 \lhd \mathbf{Z}_{24}$$

لأن:
زمر القسمة للمتسلسلة (4) هي

$$\mathbf{Z}_2 /\{\bar{0}\} \cong \mathbf{Z}_2 \ , \ \mathbf{Z}_4 / \mathbf{Z}_2 \cong \mathbf{Z}_2 \ , \ \mathbf{Z}_8 / \mathbf{Z}_4 \cong \mathbf{Z}_2 \ , \ \mathbf{Z}_{24} / \mathbf{Z}_8 \cong \mathbf{Z}_3$$

وبما أن $\mathbf{Z}_3$, $\mathbf{Z}_2$ زمرتين بسيطتين ، فإن زمر القسمة للمتسلسلة (4) تكون جميعها زمر بسيطة .
إذن المتسلسلة (4) تكون متسلسلة مركبة .

<u>ثانياً</u>: المتسلسلات المركبة للزمرة S_4

توجد متسلسلة مركبة وحيدة للزمرة S_4 هي

$$(*) \quad \{1\} \lhd \langle (1\ 2)(3\ 4) \rangle \lhd K_4 \lhd A_4 \lhd S_4$$

لأن:
زمر القسمة للمتسلسلة (*) هي

$$\langle (1\ 2)(3\ 4) \rangle /\{1\} \cong \langle (1\ 2)(3\ 4) \rangle \cong \mathbf{Z}_2 \ , \ K_4 / \langle (1\ 2)(3\ 4) \rangle \cong \mathbf{Z}_2 \ ,$$
$$A_4 / K_4 \cong \mathbf{Z}_2 \ , \ S_4 / A_4 \cong \mathbf{Z}_2$$

وبما أن $\mathbf{Z}_2$ زمرة بسيطة ، فإن زمر القسمة للمتسلسلة (*) تكون جميعها زمر بسيطة . إذن المتسلسلة (*) تكون متسلسلة مركبة .

١٤٧. (أ) أوجد متسلسلة مركبة للزمرة $\mathbf{Z}_{p^r}$ ، حيث p عدد أولي .

(ب) أوجد متسلسلة مركبة للزمرة $\mathbf{Z}_n$ ، حيث $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ وحيث $p_1 , p_2 ,\ldots, p_r$ أعداد أولية مختلفة .

الحل: (أ) المتسلسلة

$$\{\bar{0}\} \lhd \mathbf{Z}_p \lhd \mathbf{Z}_{p^2} \lhd \cdots \lhd \mathbf{Z}_{p^{r-1}} \lhd \mathbf{Z}_{p^r}$$

تكون متسلسلة مركبة للزمرة $\mathbf{Z}_{p^r}$ ، حيث p عدد أولي ، لأن كل زمرة قسمة لها تماثل $\mathbf{Z}_p$ (لاحظ أن $\mathbf{Z}_p$ تكون زمة بسيطة لأن p عدد أولي) .

(ب) ليكن $n \in \mathbf{N}$ ، وليكن $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ حيث $p_1 , p_2 ,\ldots, p_r$ أعداد أولية مختلفة . إذن

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{m_1}} \times \mathbf{Z}_{p_2^{m_2}} \times \cdots \times \mathbf{Z}_{p_r^{m_r}}$$

نضع

$$P_{1\,,\,m_1-i_1} = \mathbf{Z}_{p_1^{m_1-i_1}} \times \mathbf{Z}_{p_2^{m_2}} \times \cdots \times \mathbf{Z}_{p_r^{m_r}}$$

حيث $i_1 = 1 , 2 , \ldots , m_1$.

إذن

$$P_{1\,,\,0} \lhd P_{1\,,\,1} \lhd P_{1\,,\,2} \lhd \cdots \lhd P_{1\,,\,m_1-2} \lhd P_{1\,,\,m_1-1} \lhd \mathbf{Z}_n$$

نضع

$$P_{2\,,\,m_2-i_2} = \{\bar{0}\} \times \mathbf{Z}_{p_2^{m_2-i_2}} \times \mathbf{Z}_{p_3^{m_3}} \times \cdots \times \mathbf{Z}_{p_r^{m_r}}$$

حيث $i_2 = 1 , 2 , \ldots , m_2$.

إذن

$$P_{2\,,\,0} \lhd P_{2\,,\,1} \lhd P_{2\,,\,2} \lhd \cdots \lhd P_{2\,,\,m_2-2} \lhd P_{2\,,\,m_2-1} \lhd P_{1\,,\,0}$$

إذن

$$P_{2\,,\,0} \lhd P_{2\,,\,1} \lhd P_{2\,,\,2} \lhd \cdots \lhd P_{2\,,\,m_2-2} \lhd P_{2\,,\,m_2-1}$$
$$\lhd P_{1\,,\,0} \lhd P_{1\,,\,1} \lhd P_{1\,,\,2} \lhd \cdots \lhd P_{1\,,\,m_1-2} \lhd P_{1\,,\,m_1-1} \lhd \mathbf{Z}_n$$

نستمر بهذة الطريقة حتى الخطوة رقم r ، فنحصل على متسلسلة مركبة للزمرة $\mathbf{Z}_n$ ، لأن كل زمرة قسمة لهذة المتسلسلة (لحدين متتاليين) تماثل $\mathbf{Z}_{p_i}$ حيث $i \in \{1,2,\ldots,r\}$ وهي زمرة بسيطة لأن p_i عدد أولي .

١٤٨. اثبت أن أي زمرة ابدالية لها متسلسلة مركبة تكون منتهية .

الحل: ليكن G زمرة ابدالية . نفرض أن G لها المتسلسلة المركبة التالية

$$\{1\} = S_0 \lhd S_1 \lhd \cdots \lhd S_{m-1} \lhd S_m = G$$

بما أن هذة المتسلسلة مركبة و $S_1 \cong S/\{1\}$ ، فإن S_1 تكون زمرة بسيطة . وبما أن G ابدالية ، فإن S_1 تكون ابدالية . لذلك أي زمرة جزئية من S_1 تكون ناظمية . لكن S_1 بسيطة . إذن $|S_1| = p_1$ ، حيث p_1 عدد أولي . كذلك S_2/S_1 تكون ابدالية وبسيطة ، وبالتالي $|S_2/S_1| = p_2$ ، حيث p_2 عدد أولي . إذن $|S_2| = p_1\, p_2$. نستمر بهذة الطريقة ، فنحصل على

$$|S_m/S_{m-1}| = p_m \quad , \quad |S_m| = |G| = p_1\, p_2 \ldots p_m$$

، حيث $p_1 , p_2 , \ldots , p_m$ أعداد أولية .

أذن G تكون زمرة منتهية .

١٤٩. ليكن G زمرة رتبتها 100 . اثبت أن G تكون قابلة للحل .

الحل: ليكن G زمرة رتبتها 100 . إذن $|G| = 2^5 \times 5^2$. إذن ينتج من المبرهنة (أي زمرة رتبتها $p^m q^n$ ، حيث p , q عددين أوليين مختلفين تكون قابلة للحل) ، أن G تكون قابلة للحل .

حل آخر: بما أن $|G| = 2^5 \times 5^2$ ، فإنة ينتج من مبرهنة سيلو الأولى أن G تحتوي على 5-زمر جزئية لسيلو رتبها 25 وعددها $n_5 = 1 + 5\,\lambda$ ، حيث $\lambda = 0,1,2,\ldots$. ومن مبرهنة سيلو الثالثة يكون $n_5 \mid |G|$. إذن $n_5 = 1$. أي أن G تحتوي على 5-زمرة جزئية لسيلو رتبهتا 25 وحيدة ولتكن S . إذن $S \lhd G$. وبما أن $|S| = 5^2$ ، فإن S تكون p-زمرة منتهية حيث $p = 5$. إذن S تكون قابلة للحل (مبرهنة) . وبما أن $|G/S| = 4 = 2^2$ ، فإن G/S تكون p-زمرة منتهية حيث $p = 2$. إذن G/S تكون زمرة قابلة للحل (مبرهنة) . إذن G تكون قابلة للحل (مبرهنة) .

١٥٠. ليكن G زمرة . برهن أن

G تكون قابلة للحل $\Leftrightarrow$ G/C(G) تكون قابلة للحل

الحل: ليكن G زمرة .

($\Leftarrow$) نفرض أن الزمرة G تكون قابلة للحل . إذن G/C(G) تكون قابلة للحل (مبرهنة) .

($\Rightarrow$) نفرض أن الزمرة G/C(G) تكون قابلة للحل . بما أن C(G) زمرة ابدالية ، فإن $(C(G))' = \{1\}$. إذن C(G) تكون قابلة للحل (مبرهنة) . إذن G/C(G) , C(G) تكونان قابلتين للحل . إذن G تكون قابلة للحل .

زمر المبدلات – Groups of commutators

١٥١. ليكن G زمرة ، وليكن $a,b \in G$. اثبت أن

(أ) $[ab , c] = a [b , c] a^{-1} [a , c]$

(ب) $[a , bc] = [a , b] b [a , c] b^{-1}$

(ت) $[a , b] = a [b , a^{-1}] a^{-1} = b [b^{-1} , a] b^{-1}$

(ث) $[[a , b] ,bcb^{-1}] [[b , c] , cac^{-1}] [[c, a] , aba^{-1}] = 1$

الحل: (أ)

$$[ab , c] = a b c (a b)^{-1} c^{-1} = a b c b^{-1} a^{-1} c^{-1} ,$$

$$a [b , c] a^{-1} [a , c] = a b c b^{-1} c^{-1} a^{-1} a c a^{-1} c^{-1} = a b c b^{-1} a^{-1} c^{-1} = [ab , c]$$

(ب)

$$[a , bc] = a b c a^{-1} c^{-1} b^{-1} ,$$

$$[a , b] b [a ,c] b^{-1} = a b (a^{-1} (b^{-1} b) a) c a^{-1} c^{-1} b^{-1} , = a b c a^{-1} c^{-1} b^{-1} = [a , bc]$$

(ت)

$$a [b , a^{-1}] a^{-1} = a b a^{-1} b^{-1} a a^{-1} = a b a^{-1} b^{-1}$$

$$= [a , b] \quad ,$$

$$b\,[b^{-1} , a]\, b^{-1} = b\, b^{-1}\, a\, b\, a^{-1}\, b^{-1}$$

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

$$= [a , b]$$

(ث) نضع

$$x = [[a , b] , bcb^{-1}] \ ,$$

$$y = [[b ,c] , cac^{-1}] \ ,$$

$$z = [[c , a] , aba^{-1}]$$

إذن

$$x = a\, b\, a^{-1}\, c\, a\, b^{-1}\, a^{-1}\, b\, c^{-1}\, b^{-1} \quad ,$$

$$y = b\, c\, b^{-1}\, a\, b\, c^{-1}\, b^{-1}\, c\, a^{-1}\, c^{-1} \quad ,$$

$$z^{-1} = a\, b\, a^{-1}\, c\, a\, c^{-1}\, b^{-1}\, c\, a^{-1}\, c^{-1}$$

إذن

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

$$= z^{-1}$$

إذن $x\, y\, z = 1$.

١٥٢. ليكن G زمرة . أوجد متسلسلة الإشتقاق لـ G (the drive series of G) ، حيث

(أ) $|G| = 8$

(ب) $G = S_4$

الحل: ليكن G زمرة .

(أ) ليكن $|G| = 8$. إذا كانت G ابدالية ، فإن $G^{(1)} = G' = [G , G] = \{1\}$

(حيث $G' = < [a , b] \mid a,b \in G >$ وتسمى زمرة الإشتقاق أو زمرة المبادلة للزمرة G) .

أي زمرة غير إبدالية رتبتها 8 تماثل D_4 أو Q_8 (انظر تمرين (١١٤)) ، حيث

$$D_4 = < a , b \mid a^4 = b^2 = (a\, b)^2 = 1 > \ ,$$

$$Q_8 = < a , b \mid a^4 = 1 , a^2 = b^2 \ , b\, a = a^3\, b >$$

إذن

$$D_4^{(1)} = < a^2 > \quad , \quad D_4^{(2)} = \{1\} \ ,$$

$Q_8^{(1)} = < a^2 > \quad , \quad Q_8^{(2)} = \{1\}$.

متسلسلة الإشتقاق (أو متسلسلة زمر المبادلة) للزمرة G هي

$$G^{(n)} \lhd \ldots \lhd G^{(2)} \lhd G^{(1)} \lhd G^{(0)} = G$$

إذن متسلسلة الإشتقاق (أو متسلسلة زمر المبادلة) للزمرة D_4 هي

$$\{1\} \lhd \langle a^2 \rangle \lhd D_4{}^{(0)} = D_4$$

ومتسلسلة الإشتقاق (أو متسلسلة زمر المبادلة) للزمرة Q_8 هي

$$\{1\} \lhd \langle a^2 \rangle \lhd Q_8{}^{(0)} = Q_8$$

(ب)

$$S_4^{(3)} = (S_4^{(1)})^{(2)} = A_4^{(2)} = (A_4^{(1)})^{(1)} = K_4^{(1)} = \{1\}$$

إذن متسلسلة الإشتقاق (أو متسلسلة زمر المبادلة) للزمرة S_4 هي

$$S_4{}^{(3)} \lhd S_4{}^{(2)} \lhd S_4{}^{(1)} \lhd S_4{}^{(0)} = S_4$$

أي

$$\{1\} \lhd K_4 \lhd A_4 \lhd S_4$$

١٥٣. ليكن G زمرة ، وليكن $N = \{u\, x^2 \mid x \in G , u \in G'\}$ ، حيث 'G هي مشتقة G (أي أن $G^{(1)} = G' = [G , G]$) . اثبت أن $N \lhd G$.

الحل: ليكن G زمرة ، وليكن $N = \{u\, x^2 \mid x \in G , u \in G'\}$. بما أن $1 \in G' , 1 \in G$ ، فإن $1 \in N$. إذن $N \neq \emptyset$. ليكن $a,b \in N$. إذن يوجد $x,y \in G , u,v \in G'$ ، بحيث $a = u\, x^2 , \ b = v\, y^2$. لاحظ أن لكل $g,h \in G$ يكون $g\, h = [g , h]\, h\, g$. إذن

$$a\, b = u\, x^2\, v\, y^2 = u\, [x^2 , v]\, v\, x^2\, y^2 = u\, [x^2 , v]\, v\, x\, x\, y\, y$$
$$= u\, [x^2 , v]\, v\, [x , x\, y]\, x\, y\, x\, y = u\, [x^2 , v]\, v\, [x , x\, y]\, (x\, y)^2$$

لكن $u\, [x^2 , v]\, v\, [x , x\, y] \in G'$. إذن $a\, b \in N$. إذن N تكون مغلقة بالنسبة لعملية الضرب على G . كذلك

$$a^{-1} = (u\, x^2)^{-1} = x^{-2}\, u^{-1} = [x^{-2} , u^{-1}]\, u^{-1}\, x^{-2} = [x^{-2} , u^{-1}]\, u^{-1}\, (x^{-1})^{-2} \in N$$

إذن $N \le G$. والآن نبرهن أن $N \lhd G$. ليكن $a \in N , g \in G$. إذن يوجد $u \in G' , x \in G$ ، بحيث $a = u x^2$. إذن

$$g a g^{-1} = g (u x^2) g^{-1} = (g u g^{-1}) (g x^2 g^{-1}) = (g u g^{-1}) (g x g^{-1})^2 \in N$$

لأن $g u g^{-1} \in G'$ (لأن $G' \lhd G$) . إذن $N \lhd G$.

١٥٤. ليكن G زمرة ، وليكن

$$[x_1 , x_2 , \dots , x_n] = [x_1 , x_2 x_3 \dots x_n] [x_2 , x_3 , \dots , x_n]$$

لكل $x_1 , x_2 , \dots , x_n \in G , n \in \mathbf{N}$ ، حيث $[x] = 1$ لكل $x \in G$.

اثبت أن

$$G' = \{ [x_1 , x_2 , \dots , x_n] \mid x_1 , x_2 , \dots , x_n \in G , n \in \mathbf{N} \}$$

الحل: ليكن G زمرة ، وليكن

$$[x_1 , x_2 , \dots , x_n] = [x_1 , x_2 x_3 \dots x_n] [x_2 , x_3 , \dots , x_n]$$

لكل $x_1 , x_2 , \dots , x_n \in G , n \in \mathbf{N}$ ، حيث $[x] = 1$ لكل $x \in G$.

ليكن $x_1 , x_2 , \dots , x_n \in G , n \in \mathbf{N}$. إذن من الفرض يكون

$$[x_1 , x_2 , \dots , x_n] = [x_1 , x_2 x_3 \dots x_n] [x_2 , x_3 , \dots , x_n]$$

إذن

$$[x_1 , x_2 , \dots , x_n] = [x_1 , x_2 x_3 \dots x_n] [x_2 , x_3 , \dots , x_n] [x_3 , x_4 , \dots , x_n] \dots [x_{n-1} , x_n]$$

ليكن

$$H = \{[x_1 , x_2 , \dots , x_n] \mid x_1 , x_2 , \dots , x_n \in G , n \in \mathbf{N}\}$$

بما أن $G' = < [a,b] \mid a,b \in G >$ ، فإن $H \subseteq G'$. لكن $[a,b] \in H$. إذن $G' \subseteq H$.

إذن $G' = H$.

١٥٥. ليكن G زمرة ، وليكن $x,y \in G$. إذا كان $x^3 = (x y)^3 = (x y^{-1})^3 = 1$ ، فاثبت أن $[[x , y] , y] = 1$.

الحل: ليكن G زمرة ، وليكن $x,y \in G$ ، بحيث $x^3 = (x y)^3 = (x y^{-1})^3 = 1$. بما أن

$(x\,y)^3 = 1$ (أي أن $x\,y\,x\,y\,x\,y = 1$) ، فإن $y\,x\,y = (x\,y\,x)^{-1} = x^{-1}\,y^{-1}\,x^{-1}$. إذن
$x^{-1}\,y\,x\,y = x^{-2}\,y^{-1}\,x^{-1}$. لكن $x^3 = 1$. إذن $x^2 = x^{-1}$. إذن

$$x^{-1}\,y\,x\,y = x^{-2}\,y^{-1}\,x^2 \qquad (1)$$

وبما أن $(x\,y^{-1})^3 = 1$ ، فإن $(x\,y^{-1}\,x)\,y^{-1}\,x\,y^{-1} = 1$. إذن $x\,y^{-1}\,x = (y^{-1}\,x\,y^{-1})^{-1}$. إذن

$$x\,y^{-1}\,x = y\,x^{-1}\,y \qquad (2)$$

من (2) ينتج أن $y^{-1} = x^{-1}\,(y\,x^{-1}\,y)\,x^{-1}$. وبالتعويض في (1) ينتج أن

$$\begin{aligned} x^{-1}\,y\,x\,y &= x^{-2}\,(x^{-1}\,y\,x^{-1}\,y\,x^{-1})\,x^2 \\ &= x^{-3}\,y\,x^{-1}\,y\,x \\ &= y\,x^{-1}\,y\,x \end{aligned}$$

إذن

$$\begin{aligned} y\,x\,y\,x^{-1} &= x\,(y\,x^{-1}\,y\,x)\,x^{-1} \\ &= x\,y\,x^{-1}\,y \end{aligned}$$

أذن

$$y\,x\,y\,x^{-1} = x\,y\,x^{-1}\,y \qquad (3)$$

إذن من (3) ينتج أن

$$\begin{aligned} [[x,y]\,,y] &= [x,y]\,y\,[y,x]\,y^{-1} \\ &= x\,y\,x^{-1}\,y^{-1}\,y\,y\,x\,y^{-1}\,x^{-1}\,y^{-1} \\ &= (x\,y\,x^{-1}\,y)\,(x\,y^{-1}\,x^{-1}\,y^{-1}) \\ &= y\,x\,y\,x^{-1}\,x\,y^{-1}\,x^{-1}\,y^{-1} \\ &= 1 \end{aligned}$$

١٥٦. ليكن G زمرة ، وليكن $n \in \mathbf{N}$. إذا كان

$$K^0(G) = G\ ,\ K^1(G) = [G\,,G]\ ,\ \ldots\ ,\ K^{n+1}(G) = [G\,,K^n(G)]$$

فبرهن أن

(أ) $K^n(G) \lhd G$

(ب) $K^{n+1}(G) \leq K^n(G)$

الحل: ليكن G زمرة ، وليكن $n \in \mathbf{N}$. ليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , \ K^{n+1}(G) = [G , K^n(G)]$$

(أ) لإثبات أن $K^n(G) \lhd G$ ، نستخدم مبدأ الإستنتاج الرياضي على n . من الواضح أن المطلوب يتحقق عندما $n = 0$. كذلك يتحقق المطلوب عندما $n = 1$ ، لأن $K^1(G) = G' \lhd G$ (مبرهنة) . نفرض أن $K^n(G) \lhd G$ ، ونبرهن أن $K^{n+1}(G) \lhd G$. بما أن $K^n(G) , G \lhd G$ ، فإنة ينتج من المبرهنة $(A , B \lhd G \Rightarrow [A , B] \lhd G)$ أن

$$K^{n+1}(G) = [G , K^n(G)] \lhd G$$

(ب) من (أ) يكون $K^n(G) \lhd G$ ، لكل $n \in \mathbf{N}$. إذن $K^{n+1}(G) = [G , K^n(G)] \leq K^n(G)$ (مبرهنة) . إذن ينتج من المبرهنة

$$A \lhd G \Rightarrow [G , A] \leq A$$

أن $K^{n+1}(G) = [G , K^n(G)] \leq K^n(G) \lhd G$. إذن $K^{n+1}(G) \leq K^n(G)$ ، لكل $n \in \mathbf{N}$.

١٥٧.ليكن G زمرة ، وليكن $m , n \in \mathbf{N}$. إذا كان

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , K^{n+1}(G) = [G , K^n(G)]$$

فبرهن أن

$$K^m(S_n) = A_n \ , \forall \ n \geq 2 \ , \ m \geq 1$$

الحل: ليكن G زمرة ، وليكن $m,n \in \mathbf{N}$. ليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , \ K^{n+1}(G) = [G , K^n(G)]$$

ليكن $n \geq 2 \ , \ m \geq 1$. إذن $S_n' = S_n^{(1)} = [S_n , S_n] = A_n$ (مبرهنة) . لاحظ أن

$$K^2(S_n) = [S_n , K'(S_n)] = [S_n , S_n^{(1)}] = [S_n , A_n]$$

نبرهن أن $[S_n , A_n] = A_n$. لاحظ أن A_n تتولد من كل الدورات الثلاثية في S_n (مبرهنة) . ليكن $(i \ \ j \ \ k) \in A_n$. بما أن $(i \ \ j \ \ k) = [(i \ \ j) , (i \ \ j \ \ k)] \in [S_n , A_n]$ ، فإن $A_n \subseteq [S_n , A_n]$. وبما أن $A_n \lhd S_n$ ، فإن $[S_n , A_n] \leq A_n$ (مبرهنة) .

إذن $[S_n , A_n] = A_n$. إذن $K^2(S_n) = A_n$. إذن

$$K^3(S_n) = [S_n , K^2(S_n)] = [S_n , A_n] = A_n$$

إذن

$$K^m(S_n) = A_n \ , \forall \ n \geq 2 \ , \ m \geq 1$$

١٥٨. ليكن G زمرة ، وليكن $N \lhd G$. ليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , \ K^{n+1}(G) = [G , K^n(G)] \ , \ n \in \mathbf{N}$$

برهن أن $K^n(G/N) = K^n(G)/N \ , \forall n \in \mathbf{N}$.

الحل: ليكن G زمرة ، وليكن $N \lhd G , n \in \mathbf{N}$. لإثبات أن $K^n(G/N) = K^n(G)/N$ ، نستخدم مبدأ الإستنتاج الرياضي على n . ليكن $n = 1$. إذن

$$K^1(G/N) = [G/N , G/N] \quad , \quad K^1(G)/N = [G , G]/N$$

ليكن $a,b \in G$. إذن $[aN , bN] = [a , b] N$. إذن $K^1(G/N) = K^1(G)/N$. إذن المطلوب متحقق عندما $n = 1$. نفرض أن $K^n(G/N) = K^n(G)/N$ ، ونبرهن أن $K^{n+1}(G/N) = K^{n+1}(G)/N$. بما أن $K^n(G/N) = K^n(G)/N$ ، فإن

$$\begin{aligned} K^{n+1}(G/N) &= [G/N , K^n(G/N)] \\ &= [G/N , K^n(G)/N] \end{aligned}$$

ليكن $a \in G , b \in K^n(G)$. إذن

$$[a , b] \in [G , K^n(G)] = K^{n+1}(G) \quad , \quad [aN , bN] \in K^{n+1}(G/N)$$

لكن $[aN , bN] = [a , b] N = K^{n+1}(G)/N$. إذن $K^{n+1}(G/N) = K^{n+1}(G)/N$. إذن $K^n(G/N) = K^n(G)/N \ , \forall n \in \mathbf{N}$.

١٥٩. ليكن G p-زمرة منتهية ، وليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , \ K^{n+1}(G) = [G , K^n(G)] \ , \ n \in \mathbf{N}$$

برهن أنة يوجد $m \in \mathbf{N}$ ، بحيث $K^m(G) = \{1\}$.

الحل: ليكن G p-زمرة منتهية ، وليكن

$$K^0(G) = G \ , \ K^1(G) = [G , G] \ , \dots , \ K^{n+1}(G) = [G , K^n(G)] \ , \ n \in \mathbf{N}$$

بما أن G p-زمرة منتهية ، فإنة يوجد $n \in \mathbf{N}$ بحيث $|G| = p^n$. نبرهن أنة يوجد $m \in \mathbf{N}$ ، بحيث $K^m(G) = \{1\}$. نستخدم مبدأ الإستنتاج الرياضي على n . ليكن $n = 1$. إذن $|G| = p$. إذن ينتج من مبرهنة كوشي (Cauchy's theorem) أن G تحتوي على عنصر رتبتة p ، وليكن x . إذن $G = < x >$. إذن G تكون ابدالية . إذن $K^1(G) = G' = \{1\}$. إذن المطلوب متحقق عندما $n = 1$. نفرض أنة إذا كان G زمرة بحيث $|G| = p^n$ ، فإنة يوجد $m \in \mathbf{N}$ ، بحيث $K^m(G) = \{1\}$ ، ونبرهن أنة إذا كان $|G| = p^{n+1}$ ، فإنة يوجد $m' \in \mathbf{N}$ ، بحيث $K^{m'}(G) = \{1\}$. ليكن $|G| = p^{n+1}$. إذن G تحتوي على زمرة جزئية ناظمية رتبتها

p^n ولتكن N . إذن ينتج من فرض الإستنتاج الرياضي أنة يوجد $m \in \mathbf{N}$ ، بحيث $K^m(N) = \{1\}$. بما أن $|G/N| = p$ ، فإن الزمرة G/N تكون ابدالية . إذن $(G/N)' = \{1\} = \{N\}$. إذن

$$K^1(G/N) = [G/N , G/N] = (G/N)' = \{1\}$$

إذن ينتج من تمرين (١٥٨) أن $K^1(G)/N = \{1\}$. إذن $K^1(G) \leq N$. إذن ينتج من تمرين (١٥٦) (ب) أن $K^{m+1}(G) \leq K^m(N) = \{1\}$. إذن $K^{m+1}(G) = \{1\}$.

١٦٠. ليكن G , H زمرتين ، وليكن لأي زمرة A

$$K^0(A) = A \ , \ K^1(A) = [A , A] \ , \dots , \ K^{n+1}(A) = [A , K^n(A)] \ , \ n \in \mathbf{N}$$

برهن أن $K^n(G \times H) = K^n(G) \times K^n(H)$ ، لكل $n \in \mathbf{N}$.

الحل: ليكن G , H زمرتين ، وليكن

$$K^0(A) = A \ , \ K^1(A) = [A , A] \ , \dots , \ K^{n+1}(A) = [A , K^n(A)] \ , \ n \in \mathbf{N}$$

لأي زمرة A . نستخدم مبدأ الإستنتاج الرياضي على n . ليكن $n = 1$. إذن

$$K^1(G \times H) = (G \times H)^{(1)} = G^{(1)} \times H^{(1)} = K^1(G) \times K^1(H)$$

إذن المطلوب متحقق عندما $n = 1$. نفرض أن $K^n(G \times H) = K^n(G) \times K^n(H)$ ، ونبرهن أن $K^{n+1}(G \times H) = K^{n+1}(G) \times K^{n+1}(H)$. بما أن

$$K^{n+1}(G \times H) = [G \times H , K^n(G \times H)] = [G \times H , K^n(G) \times K^n(H)] \ ,$$

$$K^{n+1}(G) \times K^{n+1}(H) = [G , K^n(G)] \times [H , K^n(H)]$$

فإن كل عنصر في $K^{n+1}(G \times H)$ يتولد من مبدلات في الصورة $[(g,h) , (a,b)]$ ، حيث $g \in G , h \in H \ , \ a \in K^n(G) \ , \ b \in K^n(H)$. وكل عنصر في $K^{n+1}(G) \times K^{n+1}(H)$ مركبتة الأولى تتولد من مبدلات في الصورة $[g , a]$ ، حيث $g \in G , a \in K^n(G)$ ، ومركبتة الثانية تتولد من مبدلات في الصورة $[h , b]$ ، حيث $h \in H , b \in K^n(H)$. لكن

$$[(g,h) , (a,b)] = (g,h)(a,b)(g,h)^{-1}(a,b)^{-1} = (g,h)(a,b)(g^{-1},h^{-1})(a^{-1},b^{-1})$$
$$= (gag^{-1}a^{-1} , hbh^{-1}b^{-1}) = ([g , a] , [h , b])$$

إذن

$$K^{n+1}(G \times H) = K^{n+1}(G) \times K^{n+1}(H)$$

إذن

$$K^n(G \times H) = K^n(G) \times K^n(H) \ , \ \forall \ n \in \mathbf{N}$$

ثانياً: حلول تمارين الحلقات

الحلقات والحلقات الجزئية Rings and subrings

١٦١. ليكن R حلقة بحيث $x^2 = x$ ، لكل $x \in R$. برهن أن R تكون حلقة ابدالية .

الحل: ليكن R حلقة بحيث $x^2 = x$ ، لكل $x \in R$. ليكن $x \in R$. إذن

$$\begin{aligned} x + x &= (x + x)^2 \\ &= (x + x)(x + x) \\ &= x^2 + x^2 + x^2 + x^2 \\ &= x + x + x + x \end{aligned}$$

إذن $x + x = 0$ ، لكل $x \in R$. أي أن كل عنصر في R يكون معكوساً لنفسة بالنسبة لعملية الجمع . ولكل $x,y \in R$ يكون

$$\begin{aligned} x + y &= (x + y)^2 \\ &= (x + y)(x + y) \\ &= x^2 + x\,y + y\,x + y^2 \\ &= x + x\,y + y\,x + y \\ &= (x + y) + (x\,y + y\,x) \end{aligned}$$

إذن $x\,y + y\,x = 0$. إذن $x\,y + x\,y + y\,x = x\,y$. إذن $x\,y = y\,x$ ، لكل $x,y \in R$. إذن R تكون حلقة ابدالية .

١٦٢. ليكن R حلقة ابدالية تحتوي محايد . اثبت أنة لكل $n \in \mathbf{N}_0$, $x,y \in R$ يكون

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}\, y^i \qquad (*)$$

الحل: ليكن R حلقة ابدالية تحتوي محايد . لإثبات (*) نستخدم مبدأ الإستنتاج الرياضي على n . من الواضح أن (*) تتحقق عندما $n = 0 , 1 , 2$. نفرض أن (*) تتحقق عند n . أي نفرض أن

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}\, y^i$$

ونثبت أن (*) تتحقق عند $n + 1$ ، أي نثبت أن

$$(x+y)^{n+1}=\sum_{i=0}^{n+1}\binom{n+1}{i}x^{n+1-i}\,y^{i}$$

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^{n}\\ &= (x+y)\left(\sum_{i=0}^{n}\binom{n}{i}x^{n-I}\,y^{I}\right)\\ &= \sum_{i=0}^{n}\binom{n}{i}x^{n+1-i}\,y^{i}+\sum_{i=0}^{n}\binom{n}{i}x^{n-i}\,y^{i+1}\end{aligned}$$

لكن $\binom{n}{i-1}-\binom{n+1}{i}=\binom{n}{i}$. إذن

$$\begin{aligned}(x+y)^{n+1} &= \sum_{i=0}^{n}\left[\binom{n+1}{i}-\binom{n}{i-1}\right]x^{n+1-i}\,y^{i}+\sum_{i=0}^{n}\binom{n}{i}x^{n-i}\,y^{i+1}\\ &= \sum_{i=0}^{n}\binom{n+1}{i}x^{n+1-i}\,y^{i}-\sum_{i=0}^{n}\binom{n}{i-1}x^{n+1-i}\,y^{i}+\\ &\quad \sum_{i=0}^{n}\binom{n}{i}x^{n-i}\,y^{i+1}\\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}x^{n+1-i}\,y^{i}-\sum_{i=0}^{n}\binom{n}{i-1}x^{n+1-i}\,y^{i}+\sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}\,y^{i+1}\\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}x^{n+1-i}\,y^{i}\end{aligned}$$

لأن

$$-\sum_{i=0}^{n}\binom{n}{i-1}x^{n+1-i}\,y^{i}+\sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}\,y^{i+1}=0$$

إذن

$$(x+y)^{n}=\sum_{i=0}^{n}\binom{n}{i}x^{n-i}\,y^{i}\qquad .\forall\, n\in\mathbf{N}_0$$

١٦٣. في $\mathbf{Z}_p$ ، حيث p عدد أولي ، برهن أن

$$(x+y)^{p}=x^{p}+y^{p}\quad ,\forall\, x,y\in\mathbf{Z}_p$$

الحل: نعتبر الحلقة $\mathbf{Z}_p$. ليكن $x,y\in\mathbf{Z}_p$. إذن

$$(x+y)^{p}=x^{p}+\sum_{i=0}^{p-1}\binom{p}{i}x^{p-i}\,y^{i}+y^{p}$$

لاحظ أن p يقسم $\binom{p}{i}$ ، وأن $p\,z=0$ ، لكل $z\in\mathbf{Z}_p$. إذن

$$\sum_{i=0}^{p-1}\binom{p}{i}x^{p-i}\,y^{i}=0$$

إذن

$$(x + y)^p = x^p + y^p \quad , \forall\, x,y \in \mathbf{Z}_p$$

١٦٤. ليكن R حلقة .

(أ) ليكن $x^3 = x$ ، لكل $x \in R$. برهن أن $6\,x = 0 \;, \forall\, x \in R$.

(ب) ليكن R تحتوي محايد ، وليكن $x^3 = x$ ، لكل $x \in R$. برهن أن R تكون ابدالية .

الحل: ليكن R حلقة .

(أ) ليكن $x^3 = x$ ، لكل $x \in R$. ليكن $x \in R$. إذن

$$\begin{aligned} x + x &= (x + x)^3 = (x + x)\,(x^2 + x^2 + x^2 + x^2) \\ &= x^3 + \ldots + x^3 \qquad (\text{8 مرة}) \\ &= x + \ldots + x \qquad (\text{8 مرة}) \end{aligned}$$

إذن

$$\underbrace{x + \cdots + x}_{\text{6 مرة}} = 0$$

إذن $6\,x = 0$.

(ب) ليكن R تحتوي محايد ، وليكن $x^3 = x$ ، لكل $x \in R$. ليكن $x,y \in R$. إذن

$$\begin{aligned} x + y &= (x + y)^3 \\ &= (x + y)\,(x^2 + x\,y + y\,x + y^3) \\ &= x + x^2\,y + x\,y\,x + x\,y^2 + y\,x^2 + y\,x\,y + y^2\,x + y \end{aligned}$$

إذن

$$x^2\,y + x\,y\,x + x\,y^2 + y\,x^2 + y\,x\,y + y^2\,x = 0 \qquad (1)$$

بوضع $-x$ بدلاً من x في (1) نحصل على

$$x^2\,y + x\,y\,x - x\,y^2 + y\,x^2 - y\,x\,y - y^2\,x = 0 \qquad (2)$$

لاحظ أن

$$(-x)\,y\,(-x) = -(x\,y)\,(-x) = x\,y\,x \quad ,$$

$$y\,(-x)\,y = -(y\,x)\,y = -(y\,x\,y)$$

بجمع (2) , (1) نحصل على

$$2\,x^2\,y + 2\,x\,y\,x + 2\,y\,x^2 = 0 \qquad (3)$$

بضرب (3) من الشمال في x ، ثم من اليمين في x أيضاً نحصل على

$$2\,x\,y + 2\,x^2\,y\,x + 2\,x\,y\,x^2 = 0 \qquad (4)$$

$$2\,x^2\,y\,x + 2\,x\,y\,x^2 + 2\,y\,x = 0 \qquad (5)$$

بجمع (5) والمعكوس الجمعي لـ (4) نحصل على

$$2\,x\,y = 2\,y\,x \quad , \forall\ x,y \in R$$

وبوضع $y = 1$ في (2) نحصل على

$$3\,x^2 = 3\,x \quad , \forall\ x \in R$$

إذن

$$3\,(x + y)^2 = 3\,(x + y)$$

إذن

$$3\,(x^2 + x\,y + y\,x + y^3) = 3\,x + 3\,y$$

إذن

$$3\,x\,y + 3\,y\,x = 0$$

إذن

$$3\,x\,y = -\,3\,y\,x$$

لكن من (أ) يكون $3\,y\,x + 3\,y\,x = 0$ ، وبالتالي $-\,3\,y\,x = 3\,y\,x$. إذن $3\,x\,y = 3\,y\,x$.
لكن $2\,x\,y = 2\,y\,x$. إذن

$$x\,y = y\,x \quad , \quad \forall\ \ x,y \in R$$

إذن R تكون حلقة ابدالية .

١٦٥. أوجد مركز الحلقة $\mathbf{R}^{2\times2}$.

الحل: ليكن $A = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \in C(\mathbf{R}^{2\times2})$. إذن لكل $\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathbf{R}^{2\times2}$ يكون

$$A\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} A$$

إذن

$$r_1\,x_1 + r_2\,x_3 = x_1\,r_1 + x_2\,r_3 \quad , \quad r_1\,x_2 + r_2\,x_4 = x_1\,r_2 + x_2\,r_4 \quad ,$$

$$r_3\,x_1 + r_4\,x_3 = x_3\,r_1 + x_4\,r_3 \quad , \quad r_3\,x_2 + r_4\,x_4 = x_3\,r_2 + x_4\,r_4 \ .$$

ينتج من هذة المعادلات أن $r_1 = r_4$, $r_2 = r_3 = 0$. إذن المصفوفة A تكون في الصورة

$$A=\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \ . \ r \in \mathbf{R}$$

إذن

$$C(\mathbf{R}^{2\times 2}) = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \middle| r \in \mathbf{R} \right\}$$

١٦٦. ليكن R حلقة ، وليكن $n \in \mathbf{N}$. برهن أن المجموعة

$$S = \{ x \in R \mid n x = 0 \}$$

تكون حلقة جزئية من R .

الحل: ليكن R حلقة ، وليكن $n \in \mathbf{N}$. ليكن $S = \{ x \in R \mid n x = 0 \}$. لاحظ أن $n x = x + x + \dots + x$ (n مرة) ، لكل $x \in R$. لاحظ أن $S \subseteq R$. ليكن $x,y \in S$.
إذن $n x = 0 , n y = 0$. لكن

$$n (x y) = \underbrace{x y + \cdots + x y}_{\text{مرة } n}$$

$$= \underbrace{(x + \cdots + x)}_{\text{مرة } n} \ y$$

$$= (n x) y = 0 y = 0$$

إذن $x y \in S$. كذلك

$$n (x - y) = (x - y) + (x - y) + \dots + (x - y) \quad (\text{مرة } n)$$

$$= \underbrace{(x + \cdots + x)}_{\text{مرة } n} - \underbrace{(y + \cdots + y)}_{\text{مرة } n}$$

$$= n x - n y = 0$$

إذن $x - y \in S$. إذن S تكون حلقة جزئية من R .

١٦٧. ليكن R حلقة ابدالية ، برهن أن المجموعة

$$S = \{ x \in R \mid \exists\, n \in \mathbf{N} \ \text{s. t.} \ x^n = 0 \}$$

تكون حلقة جزئية من R .

الحل: لاحظ أن $0 \in S$. إذن $S \neq \emptyset$. لاحظ كذلك أن $S \subseteq R$. إذا كان $S = \{0\}$ ، فإن S تكون حلقة جزئية من R . لذلك نفرض أن $|S| > 1$. ليكن $x \in S$ ، وليكن $n \in \mathbf{N}$ هو أصغر عدد طبيعي بحيث $x^n = 0$. إذن $x , x^2 , x^3 , \dots , x^n \in S$. ليكن $x,y \in S$. إذن يوجد

$m,n \in \mathbf{N}$ بحيث $x^m = 0 , y^n = 0$. نفرض أن m هو أصغر عدد طبيعي بحيث $x^m = 0$ ، وأن n هو أصغر عدد طبيعي بحيث $y^n = 0$. إذن

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} \binom{n+m}{i} x^{m+n-i} (-y)^i$$

لكن $x^{m+n-i} = 0$ ، لكل $i = 0 , 1 , 2 , \ldots , n$. كذلك $(-y)^i = 0$ ، لكل $i = n+1 , n+2 , \ldots , n+m$. إذن $(x-y)^{m+n} = 0$. إذن $x - y \in S$. ليكن $k = \text{l.c.m.}\,(m,n)$. إذن يوجد $a,b \in \mathbf{N}$ ، بحيث $k = n\,b \;,\; k = m\,a$. إذن

$$\begin{aligned} (x\,y)^k &= x^k y^k \qquad (\text{لأن } R \text{ حلقة ابدالية}) \\ &= x^{m a}\, y^{n b} \\ &= (x^m)^a (y^n)^b \\ &= 0 \end{aligned}$$

إذن $x\,y \in S$. إذن S تكون حلقة جزئية من R .

١٦٨. برهن أن

$$S = \left\{ \begin{pmatrix} x+y & y \\ -y & x \end{pmatrix} \middle| x,y \in \mathbf{Z} \right\}$$

تكون حلقة جزئية من الحلقة $\mathbf{Z}^{2\times 2}$.

الحل: ليكن

$$S = \left\{ \begin{pmatrix} x+y & y \\ -y & x \end{pmatrix} \middle| x,y \in \mathbf{Z} \right\}$$

ليكن $A , B \in S$ حيث

$$A = \begin{pmatrix} x+y & y \\ -y & x \end{pmatrix} \;,\; B = \begin{pmatrix} a+b & b \\ -b & a \end{pmatrix}$$

إذن من الواضح أن $A - B , A\,B \in S$. إذن S تكون حلقة جزئية من الحلقة $\mathbf{Z}^{2\times 2}$.

١٦٩. برهن أن

$$S = \left\{ \begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} \middle| x.y \in \mathbf{R} \right\}$$

تكون حلقة جزئية من الحلقة $\mathbf{R}^{2\times2}$.

الحل: ليكن

$$S = \left\{ \begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} \middle| \; x.y \in \mathbf{R} \right\}$$

ليكن

$$\begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} , \begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} \in S$$

نضع

$$A = \begin{pmatrix} x & y\sqrt{3} \\ -y\sqrt{3} & x \end{pmatrix} . \; B = \begin{pmatrix} x' & y'\sqrt{3} \\ -y'\sqrt{3} & x' \end{pmatrix}$$

إذن

$$A - B = \begin{pmatrix} x - x' & (y-y')\sqrt{3} \\ -(y-y')\sqrt{3} & x - x' \end{pmatrix} \in S \quad ,$$

$$A\,B = \begin{pmatrix} x\,x' - 3y\,y' & (x\,y' + x'\,y)\sqrt{3} \\ -(x\,y' + x'\,y)\sqrt{3} & x\,x' - 3y\,y') \end{pmatrix} \in S$$

إذن S تكون حلقة جزئية من الحلقة $\mathbf{R}^{2\times2}$.

١٧٠. أوجد كل الحلقات الجزئية من الحلقة $\mathbf{Z}_{16}$ ، ثم اذكر الحلقات الجزئية التي تحتوي محايد .

الحل: كل زمرة جزئية من $\mathbf{Z}_n$ تكون حلقة جزئية ، وكل زمرة جزئية من $\mathbf{Z}_n$ تكون دائرية لأن $\mathbf{Z}_n$ زمرة دائرية (مولدة بـ $\bar{1}$) . إذن الحلقات الجزئية من الحلقة $\mathbf{Z}_{16}$ هي :

$$\{\bar{0}\} . Z_{16} = \langle\bar{1}\rangle = \langle\bar{3}\rangle = \langle\bar{5}\rangle = \langle\bar{7}\rangle = \langle\bar{9}\rangle = \langle\overline{11}\rangle = \langle\overline{13}\rangle = \langle\overline{15}\rangle .$$

$$\langle\bar{2}\rangle = \{\bar{0}.\bar{2}.\bar{4}.\bar{6}.\bar{8}.\overline{10}.\overline{12}.\overline{14}\} .$$

$$\langle\bar{4}\rangle = \{\bar{0}.\bar{4}.\bar{8}.\overline{12}\} .$$

$$\langle\bar{6}\rangle = \{\bar{0}.\bar{6}.\overline{12}.\bar{2}.\bar{8}.\overline{14}.\bar{4}.\overline{10}\} .$$

$$\langle\bar{8}\rangle = \{\bar{0}.\bar{8}\} .$$

$$\langle\overline{10}\rangle = \{\bar{0}.\overline{10}.\bar{4}.\overline{14}.\bar{8}.\bar{2}.\overline{12}.\bar{6}\} .$$

$\langle\overline{12}\rangle = \{\bar{0}\,.\,\overline{12}\,.\,\bar{8}\,.\,\bar{4}\}$.

$\langle\overline{14}\rangle = \{\bar{0}\,.\,\overline{14}\,.\,\overline{12}\,.\,\overline{10}\,.\,\bar{8}\,.\,\bar{6}\,.\,\bar{4}\,.\,\bar{2}\}$

بالتالي يتضح أن $\mathbf{Z}_{16}$ هي الحلقة الجزئية الوحيدة التي تحتوي محايد (ضربي) وهو $\bar{1}$.

١٧١. ليكن X مجموعة غير خالية ، وليكن Δ عملية الفرق المتماثل على مجموعة القوى P(X) . اثبت أن $(P(X) , \Delta , \cap)$ تكون حلقة ابدالية تحتوي محايد .

الحل: عملية الفرق المتماثل على مجموعة القوى P(X) تعرف كما يلي:

$$A \,\Delta\, B = (A \setminus B) \cup (B \setminus A) \quad , \forall\, A,B \in P(X)$$

من السهل اثبات أن Δ تكون عملية دامجة . ليكن $A \in P(X)$. بما أن

$$A \,\Delta\, \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A \ ,$$

$$\emptyset \,\Delta\, A = (\emptyset \setminus A) \cup (A \setminus \emptyset) = \emptyset \cup A = A$$

فإن $\emptyset$ يكون عنصر محايد للعملية Δ . وبما أن

$$A \,\Delta\, A = (A \setminus A) \cup (A \setminus A) = \emptyset$$

، فإن A يكون معكوساً لنفسة ، أي أن A لة معكوس بالنسبة للعملية Δ هو A . إذن $(P(X) , \Delta)$ تكون زمرة . لاحظ أن $\forall\, A,B \in P(X) \ , \ A \,\Delta\, B = B \,\Delta\, A$. إذن $(P(X) , \Delta)$ تكون زمرة ابدالية . من السهل اثبات أن $\cap$ تكون عملية دامجة على المجموعة P(X) . ليكن $A,B,C \in P(X)$. إذن

$$A \cap (B \,\Delta\, C) = A \cap ((B \setminus C) \cup (C \setminus B))$$
$$= (A \cap (B \setminus C)) \cup (A \cap (C \setminus B)) \ ,$$

$$(A \cap B) \,\Delta\, (A \cap C) = ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B))$$

لكن

$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C) \ ,$$
$$A \cap (C \setminus B) = (A \cap C) \setminus (A \cap B)$$

إذن

$$A \cap (B \,\Delta\, C) = (A \cap B) \,\Delta\, (A \cap C)$$

إذن العملية $\cap$ تكون موزعة شمالياً بالنسبة للعملية Δ . وبما أن $\cap$ عملية ابدالية ، فإن العملية $\cap$ تكون موزعة أيضاً يمينياً بالنسبة للعملية Δ . إذن $(P(X) , \Delta , \cap)$ تكون حلقة ابدالية . وبما أن

$X \cap A = A \cap X = A$

، فإن $(P(X) , \Delta , \cap)$ تكون حلقة ابدالية تحتوي على محايد بالنسبة للعملية $\cap$ هو X .

١٧٢. اذكر عناصر حلقة الزمرة (group ring) $\mathbf{Z}_2(G)$ ، حيث G هى زمرة كلين الرباعية ، ثم أوجد تأثير عملتي الجمع والضرب في هذة الحلقة على عنصرين غير المحايد الجمعي والمحايد الضربي .

الحل: ليكن $G = \{e , a , b , c\}$ هى زمرة كلين الرباعية ، حيث e هو العنصر المحايد . بما أن $\mathbf{Z}_2 = \{0 , 1\}$ ، فإن

$$\begin{aligned}\mathbf{Z}_2(G) = \{&0 , 1e + 1a + 1b + 1c , 1a + 1b + 1c , 1e + 1a + 1b ,\\ &1e + 1a + 1c , 1e + 1b + 1c , 1e + 1a , 1e + 1b , 1e + 1c ,\\ &1a + 1b , 1a + 1c , 1b + 1c , 1e , 1a , 1b , 1c\}\end{aligned}$$

$$\begin{aligned}(1b + 1c) + (1e + 1a + 1c) &= 1e + 1a + 1b + (1 + 1) c\\ &= 1e + 1a + 1b + 0c\\ &= 1e + 1a + 1b\end{aligned}$$

$$\begin{aligned}(1b + 1c) (1e + 1a + 1c) &= (1b)(1e) + (1b)(1a) + (1b)(1c) +\\ &\quad (1c)(1e) + (1c)(1a) + (1c)(1c)\\ &= (1.1)(be) + (1.1)(ba) + (1.1)(bc) +\\ &\quad (1.1)(ce) + (1.1)(ca) + (1.1)(cc)\\ &= 1b + 1c + 1a + 1c + 1b + 1e\\ &= 1e + 1a + (1 + 1)b + (1 + 1)c\\ &= 1e + 1a + 0b + 0c\\ &= 1e + 1a\end{aligned}$$

١٧٣. ليكن R حلقة ، وليكن $f : R \to [0,1]$ ، بحيث

$$f(x - y) \geq \mathrm{Min}(f(x) , f(y)) \quad , \quad f(x\, y) \geq \mathrm{Min}(f(x) , f(y)) \quad , \quad \forall\, x,y \in R$$

اثبت أن المجموعة

$$f_t = \{x \in R \mid f(x) \geq t\} \quad , t \in \mathrm{Im}(f)$$

تكون حلقة جزئية من R .

الحل: ليكن R حلقة ، وليكن $f : R \to [0,1]$ ، بحيث

$$f(x-y) \geq \mathrm{Min}(f(x), f(y)) \quad , \quad f(x\,y) \geq \mathrm{Min}(f(x), f(y)) \quad , \quad \forall\, x,y \in R$$

وليكن $t \in \mathrm{Im}(f)$. نبرهن أن المجموعة $f_t = \{x \in R \mid f(x) \geq t\}$ تكون حلقة جزئية من R .
بما أن $t \in \mathrm{Im}(f)$ ، فإنة يوجد $x \in R$ بحيث $f(x) = t$. إذن $x \in f_t$. إذن $f_t \neq \emptyset$. ليكن $x,y \in f_t$. إذن

$$f(x-y) \geq \mathrm{Min}(f(x), f(y)) \geq t \quad , \quad f(x\,y) \geq \mathrm{Min}(f(x), f(y)) \geq t$$

إذن $x-y \, , \, x\,y \in f_t$. إذن f_t تكون حلقة جزئية من R .

التشاكلات الحلقية - Homomorphisms of rings

١٧٤. ليكن R حلقة ، وليكن $1 \in R$.

(أ) ليكن $\oplus : R \times R \to R$ ، بحيث $x \oplus y = x + y + 1$ لكل $x,y \in R$. اثبت أن $\oplus$ تكون عملية ثنائية داخلية على R .

(ب) ليكن $\otimes : R \times R \to R$ ، بحيث $x \otimes y = x + y + x\,y$ لكل $x,y \in R$. اثبت أن $\otimes$ تكون عملية ثنائية داخلية على R .

(ت) اثبت أن $(R , \oplus , \otimes)$ تكون حلقة تحتوي عنصر محايد .

(ث) اثبت أن الحلقتان $R \, , \, (R , \oplus , \otimes)$ تكونان متماثلتين .

الحل: ليكن $R = (R , + , .)$ حلقة ، وليكن $1 \in R$.

(أ) واضح

(ب) واضح

(ت) ليكن $\oplus : R \times R \to R$ ، بحيث $x \oplus y = x + y + 1$ لكل $x,y \in R$. من (أ) ينتج أن $\oplus$ تكون عملية ثنائية داخلية على R . وبما أن العملية + عملية ابدالية ودامجة ، فإنة ينتج مباشرة أن $\oplus$ تكون عملية ابدالية ودامجة . بما أن $1 \in R$ ، فإن $-1 \in R$. ليكن $x,y,z \in R$. إذن $x \oplus -1 = x$. إذن -1 هو المحايد الجمعي للعملية $\oplus$. نضع $0' = -1$. ليكن $x \oplus y = 0'$. إذن $x + y + 1 = -1$. إذن $y = -x - 1 - 1$. إذن $x \oplus (-x - 1 - 1) = 0'$. إذن العنصر $-x - 1 - 1$ هو المعكوس الجمعي للعنصر x بالنسبة للعملية $\oplus$. إذن $(R , \oplus)$ تكون زمرة جمعية (أي بالنسبة للعملية $\oplus$) ابدالية . ليكن

$\otimes : R \times R \to R$ ، بحيث $x \otimes y = x + y + x\,y$ لكل $x,y \in R$. من (ب) ينتج أن $\otimes$ تكون عملية ثنائية داخلية على R .

$$x \otimes (y \otimes z) = x \otimes (y + z + + y\,z) = x + (y + z + + y\,z) + x\,(y + z + + y\,z)\ ,$$

$$(x \otimes y) \otimes z = (x + y + x\,y) \otimes z = (x + y + x\,y) + z + (x + y + x\,y)\,z$$

إذن $x \otimes (y \otimes z) = (x \otimes y) \otimes z$. إذن العملية $\otimes$ تكون دامجة . إذن $(R , \otimes)$ تكون شبة زمرة ضربية (أي بالنسبة للعملية $\otimes$) . كذلك

$$x \otimes (y \oplus z) = x + (y \oplus z) + x\,(y \oplus z)$$
$$= x + y + z + 1 + x\,(y + z + 1)\ ,$$
$$(x \otimes y) \oplus (x \otimes z) = (x + y + x\,y) \oplus (x + z + x\,z)$$
$$= x + y + x\,y + x + z + x\,z + 1$$

إذن

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$

بالمثل يمكن اثبات أن

$$(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$$

إذن عملية الضرب $\otimes$ تكون موزعة شمالياً ويمينياً بالنسبة لعملية الجمع $\oplus$. إذن $(R , \oplus , \otimes)$ تكون حلقة . وبما أن $x \otimes 0 = 0 \otimes x = x$ لكل $x \in R$ ، فإن العنصر 0 يكون العنصر المحايد الضربي (أي بالنسبة للعملية $\otimes$) في الحلقة $(R , \oplus , \otimes)$.

(ث) ليكن $f : (R , + , .) \to (R , \oplus , \otimes)$ ، بحيث $f(x) = x - 1$ لكل $x \in R$. ليكن $x,y \in R$. إذن

$$f(x) = f(y) \ \Leftrightarrow\ x - 1 = y - 1 \ \Leftrightarrow\ x = y$$

إذن f يكون تطبيق معرفاً جيداً ومتباين . وبما أن $f(x + 1) = x$ ، لكل $x \in R$ ، فإن f يكون شامل . ليكن $x,y \in R$. إذن

$$f(x + y) = x + y - 1\ ,\quad f(x) \oplus f(y) = f(x) + f(y) + 1 = x + y - 1$$

إذن $f(x + y) = f(x) \oplus f(y)$ ، لكل $x,y \in R$. كذلك

$$f(x\,y) = x\,y - 1\ ,$$
$$f(x) \otimes f(y) = f(x) + f(y) + f(x)\,f(y)$$
$$= x - 1 + y - 1 + (x - 1)(y - 1)$$

$= x\,y - 1$

إذن $f(x\,y) = f(x) \otimes f(y)$ ، لكل $x,y \in R$. إذن f يكون تشاكل حلقي . وبما أن f تقابل (أي متباين وشامل) ، فإن f يكون تماثل حلقي .

١٧٥. برهن أن

يوجد تشاكل حلقي $f : \mathbf{Z}_m \to \mathbf{Z}_n$ ، بحيث $f(\bar{1}) = \bar{1}$ ، $m \geq n$ $\Leftrightarrow$ $n \mid m$

الحل: ($\Leftarrow$) نفرض أن $f : \mathbf{Z}_m \to \mathbf{Z}_n$ يكون تشاكل حلقي وأن $f(\bar{1}) = \bar{1}$ ، $m \geq n$. إذن $f(\bar{0}) = \bar{0}$. إذن في $\mathbf{Z}_n$ يكون $\bar{m} = f(\bar{m}) = \bar{0}$. إذن $m \equiv 0 \pmod n$. إذن $n \mid m$.

($\Rightarrow$) نفرض أن $n \mid m$. ليكن $f : \mathbf{Z}_m \to \mathbf{Z}_n$ ، بحيث $f(\bar{x}) = \bar{x}$ لكل $\bar{x} \in \mathbf{Z}_m$. إذن $f(\bar{1}) = \bar{1}$. ليكن $\bar{x} . \bar{y} \in \mathbf{Z}_m$. بما أن $n \mid m$ ، فإنة يوجد $a \in \mathbf{N}$ بحيث $m = n\,a$. ليكن $\bar{x} = \bar{y}$. إذن $x \equiv y \pmod m$. إذن $m \mid x - y$. إذن $n \mid x - y$. إذن $x \equiv y \pmod n$. إذن في $\mathbf{Z}_n$ يكون $f(\bar{x}) = \bar{x} = \bar{y} = f(\bar{y})$. إذن f يكون تطبيق معرف جيداً . ولكل $\bar{x} . \bar{y} \in \mathbf{Z}_m$ يكون

$$f(\bar{x} + \bar{y}) = \bar{x} + \bar{y} = f(\bar{x}) + f(\bar{y}) \; .$$
$$f(\bar{x}\,\bar{y}) = \bar{x}\;\bar{y} = f(\bar{x})\,f(\bar{y})$$

إذن f يكون تشاكل حلقي .

١٧٦. أوجد كل التشاكلات الحلقية من $\mathbf{Z}_4$ إلى $\mathbf{Z}_4$.

الحل: ليكن $f : \mathbf{Z}_4 \to \mathbf{Z}_4$ تطبيق . لكي يكون f تشاكل حلقي يجب أن يحقق الشرطين

$$f(\bar{m} + \bar{n}) = f(\bar{m}) + f(\bar{n}) \quad , \quad f(\bar{m}\,\bar{n}) = f(\bar{m})\,f(\bar{n}) \quad , \forall\, \bar{m}, \bar{n} \in \mathbf{Z}_4$$

لذلك نفرض أن f يحقق هذين الشرطين . ليكن $\bar{n} \in \mathbf{Z}_4$. ليكن $ord(f(\bar{1})) = 4$. إذن $f(\bar{1}) = \bar{1}$. إذن $f(\bar{n}) = \bar{n}$ ، لكل $\bar{n} \in \mathbf{Z}_4$. في هذة الحالة f يحقق الشرطين السابقين ، وبالتالي يكون تشاكل حلقي . إذن يوجد تشاكلين حلقيين فقط من $\mathbf{Z}_4$ إلى $\mathbf{Z}_4$ هما f , g ، حيث $f(\bar{n}) = \bar{0}$ ، $g(\bar{n}) = \bar{n}$ لكل $\bar{n} \in \mathbf{Z}_4$.

١٧٧. أوجد كل التشاكلات الحلقية من $\mathbf{Z}$ إلى $\mathbf{Z}$.

الحل: ليكن $f : \mathbf{Z} \to \mathbf{Z}$ تشاكل حلقي . إذن لكل $m,n \in \mathbf{Z}$ يكون

$$f(m) = f(1 + \ldots + 1) \qquad (\text{مرة } m)$$
$$= f(1) + \ldots + f(1) \qquad (\text{مرة } m)$$
$$= m\, f(1) \quad ,$$
$$f(m\, n) = f(m)\, f(n) = (m\, f(1))\, (n\, f(1)) = m\, n\, f(1)\, f(1)$$

إذن $m\, n\, f(1) = m\, n\, f(1)\, f(1)$. إذن $f(1) = f(1)\, f(1)$. لكن $f(1) \in \mathbf{Z}$. إذن $f(1) = 0$ أو $f(1) = 1$. إذن يوجد تشاكلين حلقيين فقط من $\mathbf{Z}$ إلى $\mathbf{Z}$ هما f , g ، حيث $f(n) = 0 \;,\; g(n) = n$ ، لكل $n \in \mathbf{Z}$.

١٧٨. أوجد كل التشاكلات الحلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z}$.

الحل: ليكن $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ تشاكل حلقي . إذن لكل $(m , n) \in \mathbf{Z} \times \mathbf{Z}$ يكون

$$f((m , n)) = f(m\,(1 , 0) + n\,(0 , 1))$$
$$= f((1 , 0)) + \ldots + f((1 , 0)) \qquad (\text{مرة } m)$$
$$+ f((0 , 1)) + \ldots + f((0 , 1)) \qquad (\text{مرة } n)$$
$$= m\, f(1 , 0) + n\, f(0 , 1)$$

كذلك لكل $(m , n),(a , b) \in \mathbf{Z} \times \mathbf{Z}$ ، يكون

$$f((m , n)\,(a , b)) = f((m , n))\, f((a , b))$$

إذن $f((m\, a , n\, b)) = f((m , n))\, f((a , b))$. إذن

$$m\, a\, f((1 , 0)) + n\, b\, f((0 , 1))$$
$$= (m\, f((1 , 0)) + n\, f((0 , 1))\, (a\, f((1 , 0)) + b\, f(0 , 1))$$

نضع $f((1 , 0)) = x \;,\; f((0 , 1)) = y$. إذن

$$(m\, a)\, x + (n\, b)\, y = (m\, x + n\, y)\, (\, a\, x + b\, y)$$

لاحظ أن $x\, y = 0$ ، لأن $f((0 , 0)) = 0$. إذن

$$(m\, a)\, x + (n\, b)\, y = (m\, a)\, x^2 + (n\, b)\, y^2$$

إذن $x = 0$ أو $x = 1$ كذلك $y = 0$ أو $y = 1$ ، بحيث $x\, y = 0$. أي أن

$$(x , y) = (0 , 0) \;\text{ or }\; (0 , 1) \;\text{ or }\; (1 , 0)$$

إذن توجد ثلاثة تشاكلات حلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z}$ هي o , p_1 , p_2 ، حيث

$o((m,n)) = 0 \quad , \quad p_1((m,n)) = m \quad , \quad p_2((m,n)) = n \quad , \forall (m,n) \in \mathbf{Z} \times \mathbf{Z}$

١٧٩. أوجد كل التشاكلات الحلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z} \times \mathbf{Z}$.

الحل: ليكن $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}$ تشاكل حلقي . إذن لكل $(m , n) , (a , b) \in \mathbf{Z} \times \mathbf{Z}$ يكون

$$f((m,n)) = f(m(1,0) + n(0,1)) = m\, f((1,0)) + n\, f((0,1))$$
$$= m\,x + n\,y$$

حيث $x = f((1,0)) \ , \ y = f((0,1))$.

بما أن $f((m,n)(a,b)) = f((m,n))\, f((a,b))$ ، فإن

$$f((m\,a , n\,b)) = (m\,x + n\,y)(a\,x + b\,y)$$

إذن

$$(m\,a)\,x + (n\,b)\,y = (m\,a)\,x^2 + (n\,b)\,y^2 + (m\,b + n\,a)\,x\,y$$

لكن

$$x\,y = f((1,0))\, f((0,1)) = f((1,0)(0,1)) = f((0,0)) = (0,0)$$

إذن

$$(m\,b + n\,a)\,x\,y = (0,0)$$

إذن

$$(m\,a)\,x + (n\,b)\,y = (m\,a)\,x^2 + (n\,b)\,y^2$$

إذن :

$$x = (0,0) \ \Rightarrow \ y = (0,0) \text{ or } (0,1) \text{ or } (1,0) \text{ or } (1,1) \ ,$$
$$x = (0,1) \ \Rightarrow \ y = (0,0) \text{ or } (1,0) \ ,$$
$$x = (1,0) \ \Rightarrow \ y = (0,0) \text{ or } (0,1) \ ,$$
$$x = (1,1) \ \Rightarrow \ y = (0,0) \ .$$

إذن يوجد تسعة تشاكلات حلقية من $\mathbf{Z} \times \mathbf{Z}$ إلى $\mathbf{Z} \times \mathbf{Z}$ هي $f_0 , f_1 , f_2 , \ldots , f_8$ ، حيث

$$f_0((m,n)) = (0,0) \quad , \quad f_1((m,n)) = (0,n) \quad , \quad f_2((m,n)) = (n,0) \quad ,$$
$$f_3((m,n)) = (n,n) \quad , \quad f_4((m,n)) = (0,m) \quad , \quad f_5((m,n)) = (n,m) \quad ,$$
$$f_6((m,n)) = (m,0) \quad , \quad f_7((m,n)) = (m,n) \quad , \quad f_8((m,n)) = (m,m) \quad ,$$

لكل $(m , n) \in \mathbf{Z} \times \mathbf{Z}$.

١٨٠. اذكر أمثلة لتشاكلات حلقية بحيث صورة العنصر المحايد بكل تشاكل منها تساوي العنصر محايد .

الحل: التشاكلات الحلقية f_3 , f_5 , f_7 , f_8 في التمرين السابق ترسم العنصر المحايد إلى العنصر المحايد .

١٨١. اذكر أمثلة لتشاكلات حلقية بحيث صورة العنصر المحايد بكل تشاكل منها لا تساوي العنصر محايد .

الحل: التشاكلات الحلقية f_1 , f_2 , f_4 , f_6 في التمرين قبل السابق لا ترسم العنصر المحايد إلى العنصر المحايد .

١٨٢. اثبت أن تحصيل تشاكلات حلقية يكون تشاكل حلقي .

الحل: ليكن $g : S \to H$, $f : R \to S$ تشاكلين حلقيين . إذن لكل $a,b \in R$ يكون

$$gf(a + b) = g(f(a + b)) = g(f(a) + f(b)) = gf(a) + gf(b) \quad ,$$
$$gf(a\, b) = g(f(a\, b)) = g(f(a)\, f(b)) = g(f(a))\, g(f(b)) \, .$$

إذن $gf : R \to H$ يكون تشاكل حلقي .

١٨٣. ليكن

$$R = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| \, x.y \in \mathbf{R} \right\}$$

برهن أن $\mathbf{C} \cong R$.

الحل: لاحظ أن $\mathbf{C}$ (مجموعة الأعداد المركبة) تكون حلقة ابدالية غير منتهية وتحتوي محايد (وهو العدد الصحيح 1) بالنسبة لعمليتي جمع وضرب الأعداد المركبة . كما في حل تمرين (١٦٨) يمكن اثبات أن المجموعة R تكون حلقة (جزئية من الحلقة $\mathbf{R}^{2\times2}$) ابدالية غير منتهية وتحتوي عنصر محايد (وهو مصفوفة الوحدة من الدرجة 2×2) بالنسبة لعمليتي جمع وضرب المصفوفات من الدرجة 2 × 2 . والآن نبرهن أن الحلقتين $\mathbf{C}$, R تكونان متماثلتين . ليكن

$f : \mathbf{C} \to R$ ، بحيث

$$f(x+iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \quad , \forall \; x+iy \in \mathbf{C}$$

ليكن $a+ib\ ,\ x+iy \in \mathbf{C}$. إذن

$$f((a+ib)+(x+iy)) = f((a+x)+i(b+y))$$
$$= \begin{pmatrix} a+x & b+y \\ -(b+y) & a+x \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$
$$= f(a+ib) + f(x+iy) \quad ,$$
$$f((a+ib)(x+iy)) = f((ax-by)+i(bx+ay))$$
$$= \begin{pmatrix} ax-by & bx+ay \\ -(bx+ay) & ax-by \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$
$$= f(a+ib)\, f(x+iy) \quad .$$

إذن f يكون تشاكل حلقي . من الواضح أن f يكون متباين وشامل (أي تقابل) إذن f يكون تماثل حلقي . أي أن $\mathbf{C} \cong R$.

١٨٤. ليكن R حلقة ، وليكن

$$End(R) = \{f : R \to R \mid \text{يكون تشاكل زمري } f\}$$

(أ) برهن أن End(R) تكون حلقة .

(ب) ليكن $r \in R$ عنصر ثابت ، وليكن $_rf : R \to R$ بحيث $_rf(x) = r\,x$ لكل $x \in R$. اثبت أن $_rf \in End(R)$ ، وأن $S = \{\,_rf \mid r \in R\,\}$ تكون حلقة جزئية من الحلقة End(R) . هل $S \cong R$ ؟

الحل: نعرف عملية جمع + وعملية ضرب . على المجموعة End(R) كما يلي . ليكن $f,g \in End(R)$ ، وليكن

$$(f+g)(x) = f(x)+g(x) \quad , \quad (f\,.\,g)(x) = f(g(x)) \quad , \quad \forall\, x \in R\,.$$

من السهل اثبات أن هاتين العمليتين معرفتين جيداً على المجموعة End(R) . للسهولة نكتب عادة f g بدلاً من f . g .

(أ) نبرهن أن End(R) تكون حلقة بالنسبة لهاتين العمليتين . ليكن $f,g,h \in End(R)$ ، وليكن $x,y \in R$. إذن

$$(f + g)(x + y) = f(x + y) + g(x + y)$$
$$= f(x) + f(y) + g(x) + g(y)$$
$$= (f(x) + g(x)) + (f(y) + g(y))$$
$$= (f + g)(x) + (f + g)(y)$$

إذن $f + g \in End(R)$. إذن $End(R)$ تكون مغلقة بالنسبة للعملية + . كذلك

$$(f + (g + h))(x) = f(x) + (g + h)(x) = f(x) + (g(x) + h(x))$$
$$= (f(x) + g(x)) + h(x) = (f + g)(x) + h(x)$$
$$= ((f + g) + h)(x)$$

إذن عملية الجمع + على $End(R)$ تكون عملية دامجة . وبما أن عملية الجمع + على R تكون ابدالية ، فإن

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$$

إذن $f + g = g + f$ ، لكل $f , g \in End(R)$. إذن عملية الجمع + على $End(R)$ تكون عملية ابدالية . ليكن $o \in End(R)$ ، معرف بـ $o(x) = 0$ لكل $x \in R$ ، حيث 0 هو العنصر المحايد الجمعي في R . إذن لكل $x \in R$, $f \in End(R)$ يكون

$$(o + f)(x) = o(x) + f(x) = 0 + f(x) = f(x)$$

إذن $o + f = f + o = f$ ، لكل $f \in End(R)$. إذن o يكون العنصر المحايد الجمعي في $End(R)$. لكل $f \in End(R)$ نعرف $-f : R \to R$ ، بـ $-f(x) = -(f(x))$ لكل $x \in R$. من السهل اثبات أن $-f \in End(R)$. بما أن

$$(-f + f)(x) = (-f)(x) + f(x) = -(f(x)) + f(x) = 0 = o(x)$$

، فإن $(-f) + f = f + (-f) = o$ (لأن + عملية ابدالية) . إذن $-f$ هو المعكوس الجمعي لـ f بالنسبة لعملية الجمع + على $End(R)$. إذن $End(R)$ تكون زمرة جمعية ابدالية . كذلك لكل $f,g \in End(R)$ ، ولكل $x,y \in R$ يكون

$$f\,g(x + y) = f(g(x + y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y))$$
$$= f\,g(x) + f\,g(y)$$

إذن $f\,g \in End(R)$. إذن $End(R)$ تكون مغلقة بالنسبة لعملية الضرب . على $End(R)$. ولكل $f,g,h \in End(R)$ ، ولكل $x \in R$ يكون

$$(f(g\,h))(x) = f(g\,h(x)) = f(g(h(x)) = (f\,g)(h(x)) = ((f\,g)\,h)(x)$$

إذن $f(g\,h) = (f\,g)\,h$. إذن عملية الضرب . على $End(R)$ تكون دامجة . إذن $End(R)$ تكون شبة زمرة ضربية . كذلك لكل $f,g,h \in End(R)$ ، ولكل $x \in R$ يكون

$$(f\,(g + h))(x) = f\,((g + h)(x)) = f\,(g(x) + h(x)) = f\,(g(x)) + f\,(h(x))$$
$$= f\,g(x) + f\,h(x) = (f\,g + f\,h)(x)$$

إذن $f\,(g + h) = f\,g + f\,h$. بالمثل يكون $(g + h)\,f = g\,f + h\,f$. إذن في $End(R)$ تكون عملية الضرب موزعة شمالياً ويمينياً بالنسبة لعملية الجمع . إذن $End(R)$ تكون حلقة بالنسبة لعمليتي الجمع والضرب السابق تعريفهما علية . لاحظ أن $End(R)$ تحتوي على عنصر محايد (ضربي) وهو تطبيق الوحدة $i : R \to R$ ، حيث $i(r) = r$ لكل $r \in R$.

(ب) ليكن $r \in R$ عنصر ثابت ، وليكن ${}_rf : R \to R$ بحيث ${}_rf(x) = r\,x$ لكل $x \in R$. نبرهن أن المجموعة $S = \{\,{}_rf \mid r \in R\,\}$ تكون حلقة جزئية من الحلقة $End(R)$. ليكن ${}_rf \in S$ ، وليكن $x,y \in R$. إذن

$${}_rf\,(x + y) = r\,(x + y) = r\,x + r\,y = r\,f(x) + r\,f(y)$$

إذن ${}_rf$ يكون تشاكل زمري من R إلى R . إذن ${}_rf \in End(R)$. إذن $S \subseteq End(R)$.

والآن نبرهن أن المجموعة $S = \{\,{}_rf \mid r \in R\,\}$ تكون حلقة جزئية من الحلقة $End(R)$. ليكن ${}_rf\,,\,{}_sf \in S$. إذن

$$({}_rf - {}_sf\,)(x) = {}_rf(x) + (-\,{}_sf\,)(x) = r\,x + (-\,s\,x) = (r - s)\,x = {}_{(r-s)}f\,(x)$$

إذن ${}_rf - {}_sf = {}_{(r-s)}f$. إذن ${}_rf - {}_sf \in End(R)$. كذلك

$$({}_rf\ {}_sf)(x) = {}_rf\,({}_sf\,(x)) = {}_rf\,(s\,x) = r\,(s\,x) = (r\,s)\,x = {}_{r\,s}f\,(x)$$

إذن ${}_rf\ {}_sf = {}_{r\,s}f$. إذن ${}_rf\ {}_sf \in End(R)$. إذن S تكون حلقة جزئية من الحلقة $End(R)$. وبما أن ${}_1f\ {}_rf = {}_rf\ {}_1f = {}_rf$ ، فإن ${}_1f$ يكون عنصر محايد ضربي في S . لاحظ أن ${}_1f = i$ ، أي أن العنصر المحايد في S يساوي العنصر المحايد في $End(R)$. ليكن $\theta : R \to S$ بحيث $\theta(r) = {}_rf$ ، لكل $r \in R$. إذن

$$r = s \iff {}_rf = {}_sf \iff \theta(r) = \theta(s)$$

إذن θ يكون تطبيق معرف جيدا ومتباين . ومن الواضح أن θ يكون شامل أيضاً . إذن θ يكون تقابل . نبين فيما يلي أن θ يكون تشاكل حلقي . ليكن $r,s \in R$. إذن

$$\theta(r + s) = {}_{r+s}f = {}_rf + {}_sf = \theta(r) + \theta(s)\ ,\ \theta(r\,s) = {}_{r\,s}f = {}_rf\ {}_sf = \theta(r)\ \theta(s)$$

إذن θ يكون تشاكل حلقي وتقابل . إذن θ يكون تماثل حلقي . أي أن $R \cong S$.

١٨٥. اثبت أن الحلقتين **Q** , **R** غير متماثلتين .

الحل: ليكن $\phi : \mathbf{Q} \to \mathbf{R}$ تماثل حلقي . بما أن $\sqrt{3} \in \mathbf{R}$ ، فإنة يوجد $x \in \mathbf{Q}$ ، بحيث $\phi(x) = \sqrt{3}$ (لأن ϕ شامل) . إذن $\phi(x^2) = 3$ (لأن ϕ تشاكل حلقي) . وبما أن ϕ تشاكل حلقي شامل ، فإن $\phi(1) = 1$. إذن $\phi(3) = 3$. إذن $\phi(x^2) = \phi(3)$. ولكن ϕ متباين . إذن $x^2 = 3$ في **Q** . لكن لا يوجد $x \in \mathbf{Q}$ ، بحيث $x^2 = 3$. إذن ϕ لا يمكن أن يكون تماثل حلقي . إذن الحلقتان **R** , **Q** غير متماثلتين . فيما يلي نثبت أنة لا يوجد $x \in \mathbf{Q}$ ، بحيث $x^2 = 3$. نفرض العكس ، أي نفرض أنة يوجد $a / b \in \mathbf{Q}$ ، بحيث $a^2 / b^2 = 3$. نفرض أن الكسر a / b في أبسط صورة ، أي أن 1 هو القاسم المشترك الوحيد لـ a , b . إذن $a^2 = 3\,b^2$. إذن $3 \mid a^2$. إذن $3 \mid a$. إذن يوجد $c \in \mathbf{Z}$ ، بحيث $a = 3\,c$. إذن $3\,b^2 = 9\,c^2$. إذن $b^2 = 3\,c^2$. إذن $3 \mid b^2$. إذن $3 \mid b$. إذن $3 \mid a , 3 \mid b$ ، أي أن 3 قاسم مشترك لـ a , b . لكن هذا يتناقض مع الفرض بأن a / b في أبسط صورة . إذن لا يوجد $x \in \mathbf{Q}$ ، بحيث $x^2 = 3$.

١٨٦. اثبت أن الحلقتين **C** , **R** غير متماثلتين .

الحل: ليكن $\phi : \mathbf{R} \to \mathbf{C}$ تماثل حلقي . إذن ϕ يكون شامل . إذن يوجد $x \in \mathbf{R}$ ، بحيث $\phi(x) = i$ (حيث $i = \sqrt{-1}$) . إذن $\phi(x^2) = -1$ (لأن ϕ تشاكل حلقي) . وبما أن ϕ تشاكل حلقي شامل ، فإن $\phi(1) = 1$. وبالتالي $\phi(-1) = -1$. إذن $\phi(x^2) = \phi(-1)$. لكن ϕ يكون متباين أيضاً . إذن $x^2 = -1$ في **R** . لكن لا يوجد $x \in \mathbf{R}$ ، بحيث $x^2 = -1$. إذن ϕ لا يمكن أن يكون تماثل حلقي . إذن الحلقتان **C** , **R** غير متماثلتين .

حل آخر: ليكن $\phi : \mathbf{C} \to \mathbf{R} \times \mathbf{R}$ ، بحيث $\phi(x+iy) = (x,y)$ لكل $x+iy \in \mathbf{C}$. من السهل اثبات أن ϕ يكون تماثل حلقي . إذن $\mathbf{C} \cong \mathbf{R} \times \mathbf{R}$. لكن $\mathbf{R} \times \mathbf{R}$ لا تماثل **R** . إذن **C** لا تماثل **R** . وفيما يلي نثبت أن $\mathbf{R} \times \mathbf{R}$ لا تماثل **R** . ليكن $\theta : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ تماثل حلقي . إذن $\theta(1,1) = 1$. إذن

$$1 = \theta(1,1) = \theta((0,1) + (1,0)) = \theta((0,1)) + \theta((1,0))$$

نضع $b = \theta((1,0))$, $a = \theta((0,1))$. إذن $a + b = 1$. لكن

$$a\,b = \theta((0,1))\ \ \theta((1,0)) = \theta((0,1)\ (1,0)) = \theta((0,0)) = 0$$

إذن أحد العددين a , b يساوي 0 والآخر يساوي 1 . ليكن $b = 1$, $a = 0$. إذن
$(= 1)\ \theta((1,1)) = \theta((1,0))$. لكن θ متباين . إذن $(1,1) = (1,0)$. وهذا غير ممكن . إذن θ
لا يكون تماثل حلقي . إذن $\mathbf{R} \times \mathbf{R}$ لا تماثل $\mathbf{R}$.

١٨٧. هل الحلقتان $\mathbf{Z}_2 \times \mathbf{Z}_3$, $\mathbf{Z}_6$ متماثلتان ؟

الحل: من المبرهنة التي تنص على ($\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n \Leftrightarrow (m,n) = 1$) ينتج مباشرة أن
الحلقتان $\mathbf{Z}_2 \times \mathbf{Z}_3$, $\mathbf{Z}_6$ متماثلتان .

ملحوظة: (١) يمكن أيضاً اثبات أن الحلقتان $\mathbf{Z}_2 \times \mathbf{Z}_3$, $\mathbf{Z}_6$ متماثلتان بدون استخدام
المبرهنة ($\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n \Leftrightarrow (m,n) = 1$) كما يلي :

ليكن $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ ، بحيث $\phi(\bar{x}) = x\,((\bar{1}\,.\,\bar{1}))\ ,\ \forall\ \bar{x} \in \mathbf{Z_6}$. من السهل اثبات أن
ϕ يكون تماثل حلقي .

(٢) لاحظ أنة ليس كل تشاكل زمري من $\mathbf{Z}_6$ إلى $\mathbf{Z}_2 \times \mathbf{Z}_3$ يكون تشاكل حلقي ، فمثلاً
$\theta : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ ، حيث $\theta(\bar{x}) = x\,((\bar{1}\,.\,\bar{2}))\ ,\ \forall\ \bar{x} \in \mathbf{Z_6}$ لا يكون تشاكل حلقي
بالرغم من أنة تشاكل زمري .

١٨٨. ليكن

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle|\ x\,.\,y.\,z \in \mathbf{R} \right\}$$

(أ) اثبت أن R تكون حلقة بالنسبة لعمليتي جمع وضرب المصفوفات .

(ب) ليكن $f : R \to \mathbf{Z}$ ، بحيث

$$f\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = x\ ,\forall\ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in R$$

اثبت أن f يكون تشاكل حلقي ، ثم أوجد Ker(f) . هل f يكون شامل وهل f يكون تماثل حلقي ؟

الحل: ليكن

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle|\ x\,.\,y.\,z \in \mathbf{R} \right\}$$

(أ) من السهل اثبات أن R تكون مغلقة بالنسبة لعمليتي جمع وضرب المصفوفات . لاحظ أن R
تكون مجموعة جزئية من الحلقة $\mathbf{Z}^{2 \times 2}$. ليكن

$$A=\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\in R\ ,\ B=\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\in R$$

إذن $A\ B \in R$, $A - B$. إذن R تكون حلقة جزئية من الحلقة $\mathbf{Z}^{2\times 2}$. إذن R تكون حلقة .

(ب) ليكن $f : R \to \mathbf{Z}$ ، بحيث

$$f\left(\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\right)=x\ ,\forall\ \begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\in R$$

لاحظ أن f يكون تطبيق معرف جيداً . ليكن

$$A=\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\in R\ ,\ B=\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\in R$$

إذن $f(A) + f(B) = x + a$, $f(A + B) = x + a$. إذن $f(A + B) = f(A) + f(B)$.

كذلك $f(A)\ f(B) = x\ a$, $f(A\ B) = x\ a$. إذن $f(A\ B) = f(A)\ f(B)$. إذن f يكون تشاكل حلقي . بما أن

$$A \in Ker(f\,) \ \Leftrightarrow\ f(A) = 0 \ \Leftrightarrow\ x = 0$$

فإن

$$Ker(f\,) = \left\{\begin{pmatrix}0 & y\\ 0 & z\end{pmatrix}\middle|\ y.z \in \mathbf{R}\right\}$$

إذن

$$Ker(f\,) \neq \left\{\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\right\}$$

إذن f لا يكون متباين . وبالتالي f لا يكون تماثل حلقي . ليكن $x \in \mathbf{Z}$. إذن $f(C) = x$ ، لكل $C = [c_{ij}] \in R$ بحيث $c_{11} = x$. إذن f يكون شامل .

١٨٩. هل يوجد تشاكل حلقي شامل من $\mathbf{Z}_{24}$ إلى $\mathbf{Z}_7$ ؟

الحل: نفرض أن $f : \mathbf{Z}_{24} \to \mathbf{Z}_7$ تشاكل حلقي شامل . إذن $f(1) = 1$. إذن

$$\begin{aligned}
f(0) = f(24) &= f(1+\ldots+1) && (\text{٢٤ مرة})\\
&= f(1) + \ldots + f(1) && (\text{٢٤ مرة})\\
&= 1 + \ldots + 1 && (\text{٢٤ مرة})\\
&= 24\\
&= 3
\end{aligned}$$

لكن $f(0) = 0$ ، لأن f تشاكل زمري . إذن $3 = 0$ في $\mathbf{Z}_7$. وهذا غير ممكن . إذن لا يوجد تشاكل حلقي شامل من $\mathbf{Z}_{24}$ إلى $\mathbf{Z}_7$.

١٩٠. هل يوجد تشاكل حلقي متباين من $\mathbf{Z}_6$ إلى $\mathbf{Z}_{11}$ ؟

الحل: نفرض أن $f : \mathbf{Z}_6 \to \mathbf{Z}_{11}$ تشاكل حلقي متباين . بما أن f تشاكل زمري ، فإن $f(0) = 0$. وبما أن f متباين ، فإنة يوجد $a \in \mathbf{Z}_{11}\ , a \neq 0$ ، بحيث $f(1) = a$. إذن

$$f(6) = f(1 + \ldots + 1) \qquad (\text{٦ مرة})$$
$$= f(1) + \ldots + f(1) \qquad (\text{٦ مرة})$$
$$= a + \ldots + a = 6a \qquad (\text{٦ مرة})$$

إذن $6a = f(6) = f(0) = 0$. إذن $6a = 0$ في $\mathbf{Z}_{11}$. إذن $\text{ord}(a) = 6$. إذن $6 \mid 11$. وهذا غير ممكن . إذن لا يوجد تشاكل حلقي متباين من $\mathbf{Z}_6$ إلى $\mathbf{Z}_{11}$.

١٩١. اثبت أن الحلقة $2\mathbf{Z}$ لا تماثل الحلقة $3\mathbf{Z}$.

الحل: نفرض أن $f : 2\mathbf{Z} \to 3\mathbf{Z}$ تماثل حلقي . ليكن $f(2) = 3a$ ، حيث $a \in \mathbf{Z}$. بما أن f تشاكل زمري ، فإن

$$f(4) = f(2 + 2) = f(2) + f(2) = 3a + 3a = 3(2a)$$

بالمثل يكون

$$f(6) = 3(3a) \quad , \quad f(8) = 3(4a) \quad , \quad \ldots$$

أي أن $f(2x) = 3(xa)$ ، لكل $x \in \mathbf{Z}$. بما أن f شامل ، فإن العنصر $3 \in 3\mathbf{Z}$ يكون صورة لعنصر ما في في $2\mathbf{Z}$. إذن $3 = 3(xa)$. إذن $a = 1$. وبما أن f تشاكل حلقي ، فهو يحفظ عملية الضرب . إذن لكل $x,y \in \mathbf{Z}$ يكون $f((2x)\,(2y)) = f(2x)\,f(2y)$. إذن $f(2(2xy)) = f(2x)\,f(2y)$. إذن $3(2xy) = 3x \times 3y$. إذن $2 = 3$. وهذا غير ممكن . إذن لا يوجد تماثل حلقي من $2\mathbf{Z}$ إلى $3\mathbf{Z}$.

١٩٢. اثبت أن الحلقة $\mathbf{Z}$ لا تماثل الحلقة $n\,\mathbf{Z}$ ، لكل $n \in \mathbf{Z} \setminus \{1\}$.

الحل: ليكن $n \in \mathbf{Z} \setminus \{1\}$. نفرض أن $f : \mathbf{Z} \to n\,\mathbf{Z}$ تشاكل زمري . إذن $f(m) = m\,f(1)$ ، لكل $m \in \mathbf{Z}$. بما أن $f(1) \in n\,\mathbf{Z}$ ، فإنة يوجد $a \in \mathbf{Z}$ بحيث $f(1) = n\,a$. ليكن $x \in \mathbf{Z}$ بحيث a لا يقسم x . ليكن $m \in \mathbf{Z}$ ، بحيث $f(m) = n\,x$. إذن

$n\,x = f(m) = m\,f(1) = m\,n\,a$

إذن a يقسم x . لكن هذا يتناقض مع الفرض بأن a لا يقسم x . إذن العنصر $n\,x \in n\,\mathbf{Z}$ لا يكون صورة لأي عنصر في $\mathbf{Z}$. بالتالي f لا يكون شامل . ولكي يكون f شامل يجب أن يقسم a كل عنصر $x \in \mathbf{Z}$. إذن $a = 1$. وبالتالي $f(1) = n$ و f يكون تشاكل زمري شامل . إذن $f(m) = m\,n$ ، لكل $m \in \mathbf{Z}$. إذن f يكون متباين . إذن f يكون تقابل . إذن f يكون تماثل زمري . لكن f لا يكون تشاكل حلقي ، لأنة لا يحفظ عملية الضرب لأن:

إذا كان $m,m' \in \mathbf{Z}$ ، فإن

$$f(m\,m') = m\,m'\,n \quad , \quad f(m) = m\,n \quad , \quad f(m') = m'\,n$$

وبالتالي $f(m\,m') \neq f(m)\,f(m')\ ,\ \forall\, m , m' \in \mathbf{Z} \setminus \{0\}$.

إذن الحلقة $\mathbf{Z}$ لا تماثل الحلقة $n\,\mathbf{Z}$ ، لكل $n \in \mathbf{Z} \setminus \{1\}$.

١٩٣. ليكن R حلقة بولينية (Boolean ring) لا تحتوي على مثاليات غير بديهية . اثبت أن $R \cong \mathbf{Z}_2$.

الحل: لاحظ أولاً أن $\mathbf{Z}_2$ تكون حلقة بولينية . بما أن R حلقة بولينية ، فإن R تكون حلقة ابدالية وتحتوي محايد . ليكن $x \in R$ ، بحيث $x \neq 1$, $x \neq 0$. إذن $< x >$ (المثالي الرئيس المولد بـ x) يكون مثالي في R . بما أن R ابدالية و $1 \in R$ ، فإن $< x > = R\,x$. إذن ينتج من الفرض بأن R لا تحتوي على مثاليات غير بديهية ، أن $R\,x = \{0\}$ أو $R\,x = R$. إذا كان $R\,x = \{0\}$ ، فإن $x = 0$. وهذا يتناقض مع الفرض بأن $x \neq 0$. وإذا كان $R\,x = R$ ، فإنة يوجد $y \in R$ ، بحيث $y\,x = 1$. إذن $y^2\,x = y$ و y لة معكوس ضربي . وبما أن R حلقة بولينية ، فإن $y^2 = y$. إذن $y\,x = y$. إذن $x = 1$. وهذا يتناقض مع الفرض بأن $x \neq 1$. إذن $R = \{0 , 1\}$. إذن $R \cong \mathbf{Z}_2$.

١٩٤. هل الحلقة $\mathbf{Q}[\sqrt{2}]$ تماثل الحلقة $\mathbf{Q}[\sqrt{3}]$ ؟

الحل : نفرض أن $f : \mathbf{Q}[\sqrt{2}] \to \mathbf{Q}[\sqrt{3}]$ تشاكل حلقي شامل . إذن $f(1) = 1$. وبالتالي $f(2) = 2$. إذن $f(\sqrt{2})\,f(\sqrt{2}) = f(2) = 2$. بما أن $f(\sqrt{2}) \in \mathbf{Q}[\sqrt{3}]$ ، فإنة يوجد $a,b \in \mathbf{Q}$ بحيث $f(\sqrt{2}) = a + b\,\sqrt{3}$. إذن

$$\begin{aligned} 2 = f(\sqrt{2})\,f(\sqrt{2}) &= (a + b\,\sqrt{3})^2 \\ &= a^2 + 3\,b^2 + 2\,a\,b\,\sqrt{3} \end{aligned}$$

إذا كان $a\,b = 0$ ، فإن $a^2 + 3\,b^2 = 2$. لكن هذا غير ممكن . إذن $a\,b \neq 0$. إذن

$$\sqrt{3} = (2 - a^2 - 3\,b^2) / (2\,a\,b) \in \mathbf{Q}$$

لكن هذا يتناقض مع كون $\sqrt{3} \notin \mathbf{Q}$. إذن لا يوجد تشاكل حلقي شامل من الحلقة $\mathbf{Q}[\sqrt{2}]$ إلى الحلقة $\mathbf{Q}[\sqrt{3}]$. إذن الحلقة $\mathbf{Q}[\sqrt{2}]$ لا تماثل الحلقة $\mathbf{Q}[\sqrt{3}]$.

١٩٥. ليكن R حلقة تحتوي 1. إذا كان $ch(R) = n > 0$ ، فاثبت أن R تحتوي على حلقة جزئية تماثل $\mathbf{Z}_n$.

الحل: ليكن R حلقة تحتوي 1 ، وليكن $ch(R) = n > 0$. إذن n هو أصغر عدد صحيح موجب بحيث $n\,1 = 0$ في R . ليكن $S = \{\, m\,1 \mid m \in \mathbf{Z} \,\}$. من الواضح أن S تكون حلقة جزئية من الحلقة R . إذن S هي أصغر حلقة جزئية من الحلقة R تحتوي العنصر المحايد 1 .
ليكن $\phi : \mathbf{Z}_n \to S$ ، بحيث $\phi(\bar{m}) = m\,1$ لكل $\bar{m} \in \mathbf{Z}_n$. ليكن $\bar{a}, \bar{b} \in \mathbf{Z}_n$. إذن

$$\begin{aligned}
\bar{a} = \bar{b} &\Leftrightarrow a \equiv b \pmod{n} \\
&\Leftrightarrow n \mid a - b \Leftrightarrow a - b = c\,n \ , c \in \mathbf{Z} \\
&\Leftrightarrow (a - b)\,1 = 0 \\
&\Leftrightarrow a\,1 = b\,1 \\
&\Leftrightarrow \phi(\bar{a}) = \phi(\bar{b})
\end{aligned}$$

إذن ϕ يكون تطبيق معرف جيداً ومتباين . ومن الواضح أن ϕ يكون شامل . كذلك لكل $\bar{a}, \bar{b} \in \mathbf{Z}_n$ يكون

$$\phi(\bar{a}+\bar{b}) = \phi(\overline{a+b}) = (a+b)\,1 = a\,1 + b\,1 = \phi(\bar{a}) + \phi(\bar{b}) \ ,$$

$$\phi(\bar{a}\,\bar{b}) = \phi(\overline{ab}) = (a\,b)\,1 = (a\,1)\,(b\,1) = \phi(\bar{a})\ \phi(\bar{b}) \ .$$

إذن ϕ يكون تماثل حلقي . إذن R تحتوي على حلقة جزئية تماثل $\mathbf{Z}_n$ (وهى S) .

حل آخر: ليكن $f : \mathbf{Z} \to R$ بحيث $f(m) = m\,1$ لكل $m \in \mathbf{Z}$. من الواضح أن f يكون تطبيق معرف جيداً . ليكن $m, m' \in \mathbf{Z}$. إذن

$$f(m + m') = (m + m')\,1 = m\,1 + m'\,1 = f(m) + f(m') \ ,$$

$$f(m\,m') = (m\,m')\,1 = (m\,1)\,(m'\,1) = f(m)\ f(m') \ .$$

إذن f يكون تشاكل حلقي .

$$Ker(f) = \{\, m \in \mathbf{Z} \mid f(m) = 0 \,\}$$

$= \{ m \in \mathbf{Z} \mid m\,1 = 0 \}$

بما أن $ch(R) = n$ ، فإن $n\,1 = 0$. إذن $n \in Ker(f)$. لكن n هو أصغر عدد صحيح موجب بحيث $n\,1 = 0$. إذن إذا كان $m\,1 = 0$ ، فإن m يساوي مضاعف ما لـ n ، أي أنة يوجد $c \in \mathbf{Z}$ بحيث $m = c\,n$. إذن $Ker(f) = n\,\mathbf{Z}$. إذن ينتج من مبرهنة التماثل الأولى (مبرهنة التشاكل) في الحلقات أن $\mathbf{Z} / n\,\mathbf{Z} \cong f(\mathbf{Z})$. لكن $\mathbf{Z} / n\,\mathbf{Z} \cong \mathbf{Z}_n$. إذن $f(\mathbf{Z}) \cong \mathbf{Z}_n$. لاحظ أن $f(\mathbf{Z})$ تكون حلقة جزئية من R (مبرهنة) ، وأن $f(\mathbf{Z}) = \{ m\,1 \mid m \in \mathbf{Z} \}$. إذن R تحتوي على حلقة جزئية تماثل $\mathbf{Z}_n$ (وهى $\{ m\,1 \mid m \in \mathbf{Z} \}$) .

١٩٦. اثبت أنة يوجد تماثل حلقي وحيد من **R** إلى **R** .

الحل: ليكن $f : \mathbf{R} \to \mathbf{R}$ تماثل حلقي . ليكن $m,n \in \mathbf{Z}$. بما أن f تشاكل زمري ، فإن $f(m) = m\,f(1)$. وبما أن f يحفظ عملية الضرب ، فإن

$$(m\,n)\,f(1) = f(m\,n)$$
$$= f(m)\,f(n)$$
$$= (m\,f(1))\,(n\,f(1))$$

إذن $(f(1))^2 = f(1)$. إذن $f(1) = 0$ أو $f(1) = 1$. الإحتمال $f(1) = 0$ مرفوض ، لأن $f(0) = 0$ (لأن f تشاكل زمري) ولأن f متباين . إذن $f(1) = 1$. إذن $f(m) = m$ ، لكل $m \in \mathbf{Z}$. ليكن $a / b \in \mathbf{Q}$. بما أن $a,b \in \mathbf{Z}$ ، فإن

$$f(a / b) = f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,(f(b))^{-1}$$
$$= a\,b^{-1} = a / b$$

إذن $f(x) = x$ ، لكل $x \in \mathbf{Q}$. ليكن $x \in \mathbf{R}$ ، بحيث $x \geq 0$. إذن يوجد $y \in \mathbf{R}$ ، بحيث $x = y^2$. إذن

$$f(x) = f(y^2) = f(y)\,f(y) = (f(y))^2 \geq 0$$

إذن

$$x \geq 0 \implies f(x) \geq 0$$

كذلك إذا كان $x,y \in \mathbf{R}$ بحيث $x \geq y$ ، فإن $f(x) \geq f(y)$ لأن :

بما أن $x \geq y$ ، فإن $x - y \geq 0$. إذن $f(x - y) \geq 0$. إذن $f(x) - f(y) \geq 0$. إذن $f(x) \geq f(y)$. هذا يعني أن f يحفظ الترتيب . والآن نبين أن f يكون متصل أيضاً . ليكن $\varepsilon > 0$. إذن $\varepsilon \in \mathbf{R}$. لكن f شامل . إذن يوجد $\delta \in \mathbf{R}$ ، بحيث $f(\delta) = \varepsilon$. ليكن $x,y \in \mathbf{R}$ ،

بحيث $|x - y| < \delta$. إذن $-\delta < x - y < \delta$. وبما أن f يحفظ الترتيب ، فإن $f(-\delta) < f(x - y) < f(\delta)$. أي أن $-\varepsilon < (f(x) - f(y)) < \varepsilon$. إذن $|f(x) - f(y)| < \varepsilon$.
إذن f يكون متصل (continuous) . أخيراً نثبت أن $f(x) = x$ ، لكل $x \in \mathbf{R} \setminus \mathbf{Q}$. لاحظ أن $\mathbf{Q}$ تكون مكثفة في كل $\mathbf{R}$ ، وبالتالي يوجد متسلسلة (sequence) لأعداد كسرية $\{x_i\}$ بحيث $\lim_{i\to\infty} x_i = x$. بما أن f متصل ، فإن

$$f(\lim_{i\to\infty} x_i) = \lim_{i\to\infty} f(x_i) = \lim_{i\to\infty} x_i = x$$

إذن $f(x) = x$ ، لكل $x \in \mathbf{R}$.

بعض العناصر الخاصة في الحلقات وبعض الحلقات الخاصة

١٩٧. ليكن R حلقة ، وليكن $e \in R$ عنصر متساوي القوى (idempotent) . اثبت أن المجموعة $S = \{e\,x\,e \mid x \in R\}$ تكون حلقة جزئية من R وتحتوي محايد .

الحل: ليكن R حلقة ، وليكن $e \in R$ عنصر متساوي القوى (idempotent) . ليكن $S = \{e\,x\,e \mid x \in R\}$. نفرض أن $a,b \in S$. إذن يوجد $x,y \in R$ بحيث $a = e\,x\,e$, $b = e\,y\,e$. إذن

$$a - b = e\,x\,e - e\,y\,e = e\,(x - y)\,e \in S$$

لأن $x - y \in R$. كذلك

$$a\,b = (e\,x\,e)\,(e\,y\,e) = (e\,x)\,e^2\,(y\,e) = e\,(x\,e\,y)\,e \in S$$

لأن $x\,e\,y \in R$, $e^2 = e$.
إذن S تكون حلقة جزئية من R . وبما أن

$$e\,a = e\,(e\,x\,e) = e\,x\,e = a \quad , \quad a\,e = (e\,x\,e)\,e = e\,x\,e = a$$

فإن $e \in S$ يكون عنصر محايد ضربي . إذن S تكون حلقة جزئية من R وتحتوي محايد .

١٩٨. ليكن $m,n \in \mathbf{N} \setminus \{1\}$ ، بحيث $(m , n) = 1$. اثبت أن الحلقة $\mathbf{Z}_{mn}$ تحتوي على الأقل على أربعة عناصر متساوية القوى .

الحل: ليكن $m,n \in \mathbf{N} \setminus \{1\}$ ، بحيث $(m , n) = 1$. لاحظ أولاً أن العنصران $\bar{0},\bar{1} \in \mathbf{Z}_{mn}$ يكونان متساويان القوي . لذلك نثبت فيما يلي أن $\mathbf{Z}_{mn}$ تحتوي عنصران آخران متساويان القوى .

بما أن $(m , n) = 1$ ، فإنة يوجد $x,y \in \mathbf{Z}$ بحيث $m x + n y = 1$. لكن

$$m x + n y = 1 \implies 1 - m x = n y \implies m - m^2 x = m n y$$
$$\implies m n \mid m - m^2 x \implies m \equiv m^2 x \pmod{m n}$$
$$\implies \overline{m} = \overline{m^2 x} \implies \overline{m x} = (\overline{m x})^2$$

إذن $\overline{m x} \in \mathbf{Z}_{mn}$ يكون عنصر متساوي القوى . لاحظ أن $\overline{m x} \neq \overline{0}$ ، لأن :

نفرض أن $\overline{m x} = \overline{0}$. إذن $m x \equiv 0 \pmod{m n}$. إذن $m n \mid m x$. إذن $n \mid x$. إذن يوجد $x' \in \mathbf{Z}$ بحيث $x = n x'$. إذن

$$1 = m x + n y = m n x' + n y = n (m x' + y)$$

إذن $n = 1$. لكن هذا يتناقض مع الفرض بأن $n \neq 1$. إذن $\overline{m x} \neq \overline{0}$.

كذلك $\overline{m x} \neq \overline{1}$. لأن :

نفرض أن $\overline{m x} = \overline{1}$. إذن $m x \equiv 1 \pmod{m n}$. إذن $m n \mid m x - 1$. إذن يوجد $a \in \mathbf{Z}$ ، بحيث $m x - 1 = m n a$. إذن $m x - m n a = 1$. إذن $m (x - n a) = 1$.

إذن $m = 1$. لكن هذا يتناقض مع الفرض بأن $m \neq 1$. إذن $\overline{m x} \neq \overline{1}$.

كذلك

$$m x + n y = 1 \implies 1 - n y = m x \implies n - n^2 y = m n x$$
$$\implies m n \mid n - n^2 y \implies n \equiv n^2 y \pmod{m n}$$
$$\implies \overline{n} = \overline{n^2 y} \implies \overline{n y} = (\overline{n y})^2$$

إذن $\overline{n y} \in \mathbf{Z}_{mn}$ يكون عنصر متساوي القوى . لاحظ أن $\overline{n y} \neq \overline{0}$ ، لأن :

نفرض أن $\overline{n y} = \overline{0}$. إذن $n y \equiv 0 \pmod{m n}$. إذن $m n \mid n y$. إذن $m \mid y$. إذن يوجد $y' \in \mathbf{Z}$ بحيث $y = m y'$. إذن

$$1 = m x + n y = m x + m n y' = m (x + n y')$$

إذن $m = 1$. لكن هذا يتناقض مع الفرض بأن $m \neq 1$. إذن $\overline{n y} \neq \overline{0}$.

كذلك $\overline{n y} \neq \overline{1}$. لأن :

نفرض أن $\overline{n y} = \overline{1}$. إذن $n y \equiv 1 \pmod{m n}$. إذن $m n \mid n y - 1$. إذن يوجد $b \in \mathbf{Z}$ ، بحيث $n y - 1 = m n b$. إذن $n y - m n b = 1$. إذن $n (y - m b) = 1$.

إذن $n = 1$. لكن هذا يتناقض مع الفرض بأن $n \neq 1$. إذن $\overline{n y} \neq \overline{1}$. إذن الحلقة $\mathbf{Z}_{mn}$ تحتوي على الأقل على أربعة عناصر متساوية القوى .

١٩٩. أوجد كل عدد طبيعي n ، بحيث $\mathbf{Z}_n$ لا يحتوي على عناصر متساوية القوى غير $0 , 1$.

الحل: ليكن $n > 3$, $n \in \mathbf{N}$. نضع $n = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ ، حيث $p_1 , p_2 , \ldots , p_s$ أعداد أولية مختلفة ، وحيث $r_1 , r_2 , \ldots , r_s \in \mathbf{N}$. نفرض أن $s > 1$. نضع $a = p_1^{r_1}$, $b = p_2^{r_2} \ldots p_s^{r_s}$. وبالتالي $n = a\,b$, $(a , b) = 1$. إذن ينتج من تمرين (١٩٨) أن $\mathbf{Z}_n$ $(= \mathbf{Z}_{ab})$ تحتوي على عناصر متساوية القوى غير $\bar{0} , \bar{1}$. إذن $s = 1$. إذن $n = p^r$ ، حيث p عدد أولي و $r \in \mathbf{N}$. والآن نبين أن الحلقة $\mathbf{Z}_{p^r}$ لا تحتوي على عناصر متساوية القوى غير $\bar{0} , \bar{1}$. ليكن $\bar{x} \in \mathbf{Z}_{p^r}$ عنصر متساوي القوى . إذن $x^2 \equiv x \pmod{p^r}$. إذن $p^r \mid x\,(x-1)$. لكن $(x , x-1) = 1$. إذن $p^r \mid x$ أو $p^r \mid x - 1$. إذا كان $p^r \mid x$ ، فإن $x \equiv 0 \pmod{p^r}$. إذن $\bar{x} = \bar{0}$. وإذا كان $p^r \mid x - 1$ ، فإن $x \equiv 1 \pmod{p^r}$. إذن $\bar{x} = \bar{1}$. إذن الحلقة $\mathbf{Z}_{p^r}$ لا تحتوي على عناصر متساوية القوى غير $\bar{0} , \bar{1}$.

٢٠٠. ليكن $f : R \to S$ تشاكل حلقي ، وليكن كل من R , S تحتوي محايد . ليكن $x \in R$. برهن أن

(أ) إذا كان f شامل و x وحدة ، فإن $f(x)$ يكون وحدة .

(ب) إذا كان x عنصر متساوي القوى ، فإن $f(x)$ يكون عنصر متساوي القوى .

(ت) إذا كان x عنصر متلاشي القوى ، فإن $f(x)$ يكون عنصر متلاشي القوى .

(ث) إذا كان f شامل و x عنصر مركزي (أي أن $x \in C(R)$) ، فإن $f(x)$ يكون عنصر مركزي .

الحل: ليكن $f : R \to S$ تشاكل حلقي ، وليكن كل من R , S تحتوي محايد . ليكن $x \in R$.

(أ) ليكن f شامل و x وحدة . بما أن f تشاكل حلقي شامل ، فإن $f(1) = 1$. وبما أن x وحدة ، فإنة يوجد معكوس ضربي x^{-1} للعنصر x . إذن

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

إذن $f(x)$ لة معكوس ضربي (وهو $f(x^{-1})$) . إذن $f(x)$ يكون وحدة .

(ب) ليكن x عنصر متساوي القوى . إذن $x^2 = x$. إذن $(f(x))^2 = f(x)\,f(x) = f(x^2) = f(x)$.
إذن $f(x)$ يكون عنصر متساوي القوى .

(ت) ليكن x عنصر متلاشي القوى . إذن يوجد $n \in \mathbf{N}$ ، بحيث $x^n = 0$. إذن

$$0 = f(0) = f(x^n) = (f(x))^n$$

إذن $f(x)$ يكون عنصر متلاشي القوى .

(ث) ليكن f شامل ، وليكن x عنصر مركزي . إذن $x \in C(R)$. إذن $x\, r = r\, x$ ، لكل $r \in R$. ليكن $s \in S$. بما أن f شامل ، فإنة يوجد $r \in R$ بحيث $f(r) = s$. إذن

$$f(x)\, s = f(x)\, f(r) = f(x\, r) = f(r\, x) = f(r)\, f(x) = s\, f(x)$$

إذن $f(x)\, s = s\, f(x)$ ، لكل $s \in S$. إذن $f(x) \in C(S)$. إذن $f(x)$ يكون عنصر مركزي .

٢٠١. ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث

$$x\, y + y\, x = 1 \;\;,\;\; x^2\, y + y\, x^2 = x$$

برهن أن x يكون وحدة وأن $x^{-1} = 2\, y$.

الحل: ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث

$$x\, y + y\, x = 1 \qquad (1)$$

$$x^2\, y + y\, x^2 = x \qquad (2)$$

بضرب (1) من الشمال في x نحصل على $x^2\, y + x\, y\, x = x$. وبضرب (1) من اليمين في x نحصل على $x\, y\, x + y\, x^2 = x$. إذن $x^2\, y = y\, x^2$. وبضرب (2) من اليمين في y نحصل على $(x^2\, y)\, y + y\, x^2\, y = x\, y$. وبضرب (2) من الشمال في y نحصل على $y\, x^2\, y + y\, (y\, x^2) = y\, x$. لكن $x^2\, y = y\, x^2$. إذن

$$(x^2\, y)\, y = (y\, x^2)\, y = y\, (x^2\, y) = y\, (y\, x^2)$$

إذن $x\, y = y\, x$. إذن

$$1 = x\, y + y\, x = x\, y + x\, y = x\, (2\, y) \;\;,$$

$$1 = x\, y + y\, x = y\, x + y\, x = (2\, y)\, x$$

لاحظ أن $2\, y$ يرمز للعنصر $y + y$. إذن $2y$ يكون معوس ضربي لـ x . أي أن $x^{-1} = 2\, y$. وبالتالي x يكون وحدة .

٢٠٢. ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$. برهن أن

(أ) $1 - x$ يكون وحدة ومعكوسة الضربي هو $1 + y$ $\Leftrightarrow$ $y - x = x\, y = y\, x$

(ب) $1 - x\, y$ يكون وحدة $\Leftrightarrow$ $1 - y\, x$ يكون وحدة

الحل: ليكن R حلقة بحيث $1 \in R$ ، وليكن $x,y \in R$.

(أ) ($\Leftarrow$) ليكن $1 - x$ وحدة ومعكوسة الضربي هو $1 + y$. إذن

$$1 = (1 - x)(1 + y) = 1 + y - x - x\,y \quad ,$$
$$1 = (1 + y)(1 - x) = 1 + y - x - y\,x$$

إذن $y - x = x\,y = y\,x$.

($\Rightarrow$) ليكن $y - x = x\,y = y\,x$. إذن

$$(1 - x)(1 + y) = 1 + (y - x) - x\,y = 1 \quad ,$$
$$(1 + y)(1 - x) = 1 + (y - x) - y\,x = 1$$

إذن $1 - x$ يكون وحدة ومعكوسة الضربي هو $1 + y$.

(ب) ($\Leftarrow$) ليكن $1 - x\,y$ وحدة . إذن يوجد معكوس ضربي للعنصر $1 - x\,y$ في R ، وليكن z . إذن

$$(1 - x\,y)\,z = 1 \qquad (1)$$

بضرب (1) من اليمين في x نحصل على

$$z\,x - x\,y\,z\,x = x \qquad (2)$$

وبضرب (2) من الشمال في y نحصل على $y\,x = y\,z\,x - y\,x\,y\,z\,x$. إذن

$(1 - y\,x)\,y\,z\,x = y\,x$. إذن $(1 - y\,x)\,y\,z\,x = 1 - 1 + y\,x$. إذن

$$(1 - y\,x)(1 + y\,z\,x) = 1 \qquad (3)$$

كذلك

$$z\,(1 - x\,y) = 1 \qquad (1')$$

بضرب (1') من الشمال في y نحصل على

$$y\,z - y\,z\,x\,y = y \qquad (2')$$

بضرب (2') من اليمين في x نحصل على,

$$y\,z\,x - y\,z\,x\,y\,x = y\,x$$

إذن $y\,z\,x\,(1 - y\,x) = y\,x$. إذن $- y\,x + y\,z\,x\,(1 - y\,x) = 0$. إذن

$(1 - y\,x) + y\,z\,x\,(1 - y\,x) = 1$. إذن

$$(1 + y\,z\,x)(1 - y\,x) = 1 \qquad (3')$$

إذن ينتج من (3') , (3) أن العنصر $(1 + y z x)$ يكون معكوس ضربي للعنصر $(1 - y x)$.
إذن العنصر $(1 - y x)$ يكون وحدة .

$(\Longleftarrow)$ مثل برهان الإتجاة السابق .

٢٠٣. ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث $y = -y$. برهن أن
$1 + x$ يكون وحدة ومعكوسة هو $1 + y \Leftrightarrow y - x = x y = y x$

الحل: ليكن R حلقة ، بحيث $1 \in R$. وليكن $x,y \in R$ بحيث $y = -y$.

$(\Longrightarrow)$ نفرض أن $1 + x$ يكون وحدة ومعكوسة هو $1 + y$. إذن

$$1 = (1 + x)(1 + y) = 1 + x + y + x y \ ,$$
$$1 = (1 + y)(1 + x) = 1 + x + y + y x$$

إذن $x y = y x$.

بما أن $1 + x + y + x y = 1$ ، فإن $x + y + x y = 0$. إذن $y + x + y + x y = y$. لكن $y + y = 0$ (من الفرض) . إذن $x + x y = y$. إذن $y - x = x y$.

$(\Longleftarrow)$ نفرض أن $y - x = x y = y x$. إذن

$$(1 + x)(1 + y) = 1 + x + y + x y = 1 + x + y + y x = (1 + y)(1 + x)$$

لكن

$$(1 + x)(1 + y) = 1 + x + y + x y = 1 + x + y + y - x = 1$$

إذن العنصر $1 + y$ يكون معكوس ضربي للعنصر $1 + x$. إذن $1 + x$ يكون وحدة .

٢٠٤. اثبت أن كل عنصر غير صفري في $\mathbf{Z}_n$ يكون وحدة أو قاسم للصفر .

الحل: ليكن $\bar{x} \in \mathbf{Z}_n$ ، بحيث $\bar{x} \neq \bar{0}$. نفرض أن $\bar{x}$ ليس قاسم للصفر ، ونبرهن أنة وحدة .
لاحظ أن $\bar{x}$ يكون وحدة (أي لة معكوس ضربي) إذا وفقط إذا كان $(x , n) = 1$. نفرض عكس المطلوب ، أي نفرض أن $\bar{x}$ ليس وحدة . إذن $(x , n) \neq 1$. ليكن $(x , n) = a > 1$. إذن $a \mid x \ , \ a \mid n$. إذن يوجد $b , c \in \mathbf{N}$ ، بحيث $n = a c \ , \ x = a b$. إذن $x c = a b c$. إذن $x c = b n$. إذن $\bar{x}\,\bar{c} = \bar{0}$. لكن $\bar{c} \neq \bar{0}$. إذن $\bar{x}$ يكون قاسم للصفر ، وهذا يتناقض مع الفرض بأن $\bar{x}$ ليس قاسم للصفر . إذن $\bar{x}$ يكون وحدة .

٢٠٥. اذكر مع الاثبات صحة أو خطأ كل عبارة من العبارات الآتية:

(١) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر متساوي القوى ، فإن $x + y$ يكون عنصر متساوي القوى أيضاً .

(٢) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر متلاشي القوى ، فإن $x + y$ يكون عنصر متلاشي القوى أيضاً .

(٣) إذا كان R حلقة منتهية وتحتوي محايد ، فإن R يكون مجال متكامل (integral domain) .

(٤) مميز أي حلقة غير منتهية يساوي 0 .

(٥) ليكن R حلقة تحتوي محايد . إذا كان $x \in R\setminus\{0\}$ عنصر متساوي القوى وغير قاسم للصفر ، فإن $x = 1$.

(٦) ليكن R حلقة ، وليكن $x,y \in R$. إذا كان كل من x , y عنصر قاسم للصفر ، فإن $x + y$ يكون عنصر قاسم للصفر أيضاً .

الحل: لاحظ أولاً أن اثبات خطأ عبارة ما يكون بإعطاء مثال لا يحقق هذة العبارة .

(١) العبارة خطأ . مثال : في الحلقة $\mathbf{Z}_{12}$ يكون كل من 4 , 1 عنصر متساوي القوى ، بينما العنصر $(5 =)\ 4 + 1$ لا يكون متساوي القوى .

(٢) العبارة خطأ . مثال : في الحلقة $\mathbf{Z}_{16}$ يكون كل من 4 , 6 عنصر متلاشي القوى (لأن $6^4 = 0$, $4^2 = 0$) ، بينما العنصر $(10 =)\ 6 + 4$ لا يكون متلاشي القوى ، لأنة لا يوجد $m \in \mathbf{N}$ ، بحيث $10^m = 0$ في $\mathbf{Z}_{16}$.

(٣) العبارة خطأ . مثال : الحلقة $\mathbf{Z}_6$ تكون حلقة منتهية وتحتوي محايد ، لكنها ليست مجال متكامل لأنها غير خالية من قواسم الصفر (لاحظ أن المجال المتكامل يكون خالي من قواسم الصفر) ، لأن كل من 3 , 2 يكون قاسم للصفر في $\mathbf{Z}_6$ (لأن $2 \cdot 3 = 0$ في $\mathbf{Z}_6$) .

(٤) العبارة خطأ . مثال : ليكن X مجموعة غير منتهية . إذن مجموعة القوى لـ X ونرمز لها بالرمز $P(X)$ تكون مجموعة غير منتهية . ليكن Δ عملية الفرق المتماثل على $P(X)$. إذن ينتج من تمرين (١٧١) أن $(P(X) , \Delta , \cap)$ تكون حلقة غير منتهية (ابدالية وتحتوي محايد بالنسبة للعملية $\cap$ هو X) . إذن $2\,A = A \,\Delta\, A = \emptyset$ ، لكل $A \in P(X)$. إذن مميز الحلقة $P(X)$ يساوي 2 .

(٥) العبارة صحيحة . البرهان : ليكن R حلقة ، وليكن $1 \in R$. ليكن $x \in R\setminus\{0\}$ عنصر متساوي القوى وغير قاسم للصفر . إذن $x^2 = x$. إذن $x\,(x - 1) = x^2 - x = 0$. لكن x عنصر غير قاسم للصفر و $x \neq 0$. إذن $x - 1 = 0$. إذن $x = 1$.

(٦) العبارة خطأ . مثال: في الحلقة $\mathbf{Z}_{12}$ كل من العنصران 3 , 2 يكون قاسم للصفر (لأن في $\mathbf{Z}_{12}$ يكون $3 . 4 = 0$, $2 . 6 = 0$) . لكن في $\mathbf{Z}_{12}$ العنصر $2 + 3 (= 5)$ لا يكون قاسم للصفر .

٢٠٦. ليكن R حلقة تحتوي محايد . برهن أنة إذا كان $x \in R$ عنصر متلاشي القوى ، فإن العنصر $1 - x$ يكون وحدة .

الحل: ليكن R حلقة تحتوي محايد ، وليكن $x \in R$ عنصر متلاشي . إذن يوجد $n \in \mathbf{N}$ ، بحيث $x^n = 0$. ليكن $y = 1 + x + x^2 + x^3 + \ldots + x^{n-1}$. إذن

$$(1 - x)\, y = 1 + x + x^2 + x^3 + \ldots + x^{n-1} - x - x^2 - x^3 - \ \ldots - \ x^{n-1} - x^n$$
$$= 1$$

بالمثل يكون $y (1 - x) = 1$. إذن y يكون معكوس ضربي للعنصر $1 - x$. إذن العنصر $1 - x$ يكون وحدة .

٢٠٧. اثبت أن عدد الوحدات في الحلقة $\mathbf{Z}[\sqrt{3}]$ يكون غير منتهي .

الحل: ليكن $a + b\sqrt{3} , x + y\sqrt{3} \in \mathbf{Z}[\sqrt{3}]$ ، بحيث $(a + b\sqrt{3})(x + y\sqrt{3}) = 1$. إذن $(a + 3by) + (ay + bx)\sqrt{3} = 1$. إذن $ay + bx = 0$, $a + 3by = 1$. بحل هاتين المعادلتين نحصل على

$$x = a / (a^2 - 3b^2) \quad , \quad y = (- b) / (a^2 - 3b^2)$$

نختار قيمة كل من a , b بحيث يكون $x , y \in \mathbf{Z}$. لذلك نأخذ $b = 1$, $a = 2$ ، لأنة في هذة الحالة يكون $y = - 1$, $x = 2$ ، وبالتالي ينتميان لـ $\mathbf{Z}$. إذن العنصر $2 - \sqrt{3}$ يكون معكوس ضربي للعنصر $2 + \sqrt{3}$ (لاحظ أنة بصفة عامة يكون $a^2 - nb^2 = 1$ إذا وفقط إذا كان $(a + b\sqrt{n})(a - b\sqrt{n}) = 1$) . إذن العنصر $2 + \sqrt{3}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{3}]$. كذلك في الحلقة $\mathbf{Z}[\sqrt{3}]$ العنصر $(2 - \sqrt{3})^m$ يكون معكوس للعنصر $(2 + \sqrt{3})^m$ ، لكل $m \in \mathbf{N}$ ، لأن

$$(2 + \sqrt{3})^m \ (2 - \sqrt{3})^m = ((2 + \sqrt{3})(2 - \sqrt{3}))^m = 1$$

إذن في الحلقة $\mathbf{Z}[\sqrt{3}]$ العنصر $(2 + \sqrt{3})^m$ يكون وحدة لكل $m \in \mathbf{N}$. إذن عدد الوحدات في الحلقة $\mathbf{Z}[\sqrt{3}]$ يكون غير منتهي .

٢٠٨. ليكن R مجال متكامل (integral domain) ، وليكن $p \in R$ عنصر أولي (prime element) . ليكن $r_1 , r_2 , \dots , r_n \in R$. برهن أنة إذا كان $p \mid r_1 \; r_2 \dots r_n$ ، فإنة يوجد $i \in \{1,2,\dots,n\}$ ، بحيث $p \mid r_i$.

الحل: ليكن R مجال متكامل (integral domain) ، وليكن $p \in R$ عنصر أولي (prime element) . إذن $p \neq 0$ وكذلك p لا يكون وحدة ، أي أن $p \notin R^*$ (حيث R^* هي مجموعة الوحدات في R) . ليكن $r_1 , r_2 ,\dots, r_n \in R$ ، بحيث $p \mid r_1 \; r_2 \dots r_n$. نستخدم مبدأ الإستنتاج الرياضي على n . من الواضح أن المطلوب متحقق عندما $n = 1$. ليكن $n = 2$. إذن $p \mid r_1 \, r_2$. لكن p عنصر أولي في المجال المتكامل R . إذن $p \mid r_1$ أو $p \mid r_2$. وبالتالي المطلوب يكون متحقق عندما $n = 2$. نفرض أن المطلوب متحقق عندما $n = m$ ، ونبرهن أنة متحقق عندما $n = m+1$. بما أن المطلوب متحقق عندما $n = m$ ، فإن $p \mid r_1 \; r_2 \dots r_m$ ، يؤدي إلى أنة يوجد $i \in \{1,2,\dots,m\}$ ، بحيث $p \mid r_i$. ليكن $p \mid r_1 \; r_2 \dots r_{m+1}$. إذن $p \mid (r_1 \; r_2 \dots r_m) \, r_{m+1}$. لكن p عنصر أولي في المجال المتكامل R . إذن $p \mid r_1 \; r_2 \dots r_m$ أو $p \mid r_{m+1}$. إذا كان $p \mid r_{m+1}$ ، فإن المطلوب يكون متحقق عندما $n = m+1$. وإذا كان $p \mid r_1 \; r_2 \dots r_m$ ، فإنة ينتج من فرض الإستنتاج الرياضي أنة يوجد $i \in \{1,2,\dots,m\}$ ، بحيث $p \mid r_i$. وبالتالي المطلوب يكون متحقق أيضاً عندما $n = m+1$. إذن المطلوب يكون متحقق لجميع قيم n .

٢٠٩. ليكن R مجال متكامل (integral domain) ، وليكن $r_1 , r_2 ,\dots, r_n \in R , n \geq 2$ عناصر ليست كلها أصفار . برهن أن

$$(r_1 , r_2 ,\dots, r_n) \sim ((r_1 , r_2 ,\dots, r_{n-1}) , r_n)$$

حيث $(r_1 , r_2 ,\dots, r_n)$ يرمز للقاسم المشترك الأعظم (greatest common divisor) للعناصر $r_1 , r_2 ,\dots, r_n$.

الحل: ليكن R مجال متكامل (integral domain) ، وليكن $r_1 , r_2 ,\dots, r_n \in R , n \geq 2$ عناصر ليست كلها أصفار . نضع

$$a = (r_1 , r_2 ,\dots, r_n) \;\; , \;\; b = (r_1 , r_2 ,\dots, r_{n-1}) \;\; , \;\; c = (b , r_n)$$

نبرهن أن $a \sim c$ ، أي نبرهن أن a شريك لـ c (a associate to c) . أي نبرهن أنة يوجد وحدة $u \in R$ بحيث $a = c\,u$. لاحظ أن $c \neq 0 \;\; , \;\; b \neq 0 \;\; , \;\; a \neq 0$. بما أن

$a = (r_1 , r_2 ,\dots, r_n)$ ، فإن $a \mid r_1 , r_2 ,\dots, r_n$. إذن $a \mid b$. وبالتالي $a \mid c$. وبما أن $c \mid b$ ، فإن $c \mid r_1 , r_2 , \dots , r_{n-1}$. كذلك $c \mid r_n$. إذن $c \mid a$. إذن ينتج من $a \mid c \;,\; c \mid a$ ، أنة يوجد $u , e \in R$ بحيث $c = a\,e \;,\; a = c\,u$. إذن $a = (a\,e)\,u = a\,(e\,u)$. إذن $a\,(1 - e\,u) = 0$. لكن R مجال متكامل (وبالتالي يكون خالي من قواسم الصفر) و $a \neq 0$. إذن $1 - e\,u = 0$. إذن $e\,u = 1$. إذن u يكون وحدة في R . إذن $a \sim c$.

٢١٠. ليكن R مجال متكامل (integral domain) ، وليكن $x,y,u,v \in R$. ليكن $u = \text{l.c.m.}(x , y)$. برهن أن

(أ) $v = \text{l.c.m}(x , y) \;\Leftrightarrow\; u \sim v$

(ب) $< x > \cap < y > = < u >$

(ت) $(x , y)\, u \sim x\, y$

(حيث $\text{l.c.m.}(x , y)$ يرمز للمضاعف المشترك الأصغر (least common multiple) للعنصرين x , y . كذلك (x , y) يرمز للقاسم المشترك الأعظم (greatest common divisor) للعنصرين x , y) .

الحل: ليكن R مجال متكامل (integral domain) ، وليكن $x,y,u,v \in R$. ليكن $u = \text{l.c.m.}(x , y)$.

(أ) $(\Leftarrow)$ ليكن $u \sim v$. إذن $v \mid u \;,\; u \mid v$. بما أن $u = \text{l.c.m.}(x , y)$ ، فإن $x \mid u , y \mid u$. إذن $x \mid v , y \mid v$. إذن $v = \text{l.c.m.}(x , y)$.

$(\Rightarrow)$ ليكن $v = \text{l.c.m}(x , y)$. وبما أن $u = \text{l.c.m}(x , y)$ ، فإن إذن $v \mid u \;,\; u \mid v$. إذن يوجد $a,b \in R$ ، بحيث $v = u\,b \;,\; u = v\,a$. إذن $u = u\,(b\,a)$. إذن $u\,(1 - b\,a) = 0$. لكن R مجال متكامل (وبالتالي يكون خالي من قواسم الصفر) و $u \neq 0$. إذن $1 - b\,a = 0$. إذن $b\,a = 1$. إذن a يكون وحدة في R . إذن $u \sim v$.

(ب) ليكن $z \in < u >$. بما أن R مجال متكامل ، فإن R تكون حلقة ابدالية وتحتوي محايد . إذن $< u > = R\,u$. إذن يوجد $r \in R$ ، بحيث $z = r\,u$. لكن $y \mid u \;,\; x \mid u$. إذن يوجد $a , b \in R$ ، بحيث $u = a\,x = b\,y$. إذن $u = b\,y \in < y > \;,\; u = a\,x \in < x >$. إذن $z = r\,u \in < x > \cap < y >$. إذن $< u > \subseteq < x > \cap < y >$. ليكن $z \in < x > \cap < y >$. إذن يوجد $a,b \in R$ بحيث $z = a\,x = b\,y$. إذن $y \mid z \;,\; x \mid z$. إذن

z يكون مضاعف مشترك للعنصرين x , y في R . إذن $u | z$. إذن يوجد $c \in R$ بحيث $z = u c$. إذن $z \in \langle u \rangle$. إذن $\langle x \rangle \cap \langle y \rangle \subseteq \langle u \rangle$. إذن $\langle x \rangle \cap \langle y \rangle = \langle u \rangle$.

(ت) ليكن $v = (x , y)$. نبرهن أن $x y \sim v u$. يوجد $a,b,c,d \in R$ ، بحيث $x = a v \;,\; y = b v \;,\; u = c x = d y$. إذن $u = c a v = d b v$. إذن $(c a - d b) v = 0$. لكن R خالي من قواسم الصفر لأنة مجال متكامل و $v \neq 0$. إذن $c a - d b = 0$. إذن $c a = d b$. إذن $a | d b$. ليكن $(a , b) = e$. إذن $e | a \;,\; e | b$. إذن يوجد $a' , b' \in R$ ، بحيث $a = e a' , b = e b'$. إذن $x = a' (e v) \;,\; y = b' (e v)$. إذن $e v | x \;,\; e v | y$. إذن $e v | v$. إذن $v = e' e v , e' \in R$. إذن $(1 - e' e) v = 0$. إذن $e e' = 1$. إذن e يكون وحدة . لكن $a | d b$. إذن $a | d$. إذن $d = a d' \;,\; d' \in R$. إذن $u = d b v = d' (a b v)$. إذن $a b v | u$. لكن $x = a v \;,\; y = b v$. إذن $b x = a b v , a y = a b v$. إذن $x | a b v \;,\; y | a b v$. إذن $a b v = l.c.m.(x , y)$. إذن ينتج من (أ) أن $u \sim a b v$. إذن $u v \sim a b v v = (a v) (b v) = x y$.

٢١١. ليكن R مجال متكامل (integral domain) . إذا كان لكل عنصرين $x,y \in R$ يوجد قاسم مشترك أعظم (greatest common divisor) ، فاثبت أنة لكل عنصرين $x,y \in R$ يوجد مضاعف مشترك أصغر (least common multiple) .

الحل: ليكن R مجال متكامل (integral domain) . نفرض أنة لكل عنصرين $x,y \in R$ يوجد قاسم مشترك أعظم (greatest common divisor) . ليكن $x,y \in R$. لاحظ أولاً أن $l.c.m.(x , 0) = l.c.m.(0 , 0) = 0$. لذلك نفرض أن $x \neq 0 , y \neq 0$. ليكن $v = (x , y)$. إذن يوجد $a , b \in R$ ، بحيث $x = a v \;,\; y = b v$. إذن

$$b x = a y = a b v := k \qquad (1)$$

إذن $x | k \;,\; y | k$. إذن k يكون مضاعف مشترك لـ x , y . ليكن $k' \in R$ مضاعف مشترك آخر لـ x , y . نفرض أن $(k , k') = c$. بما أن $x | k \;,\; x | k'$ ، فإن $x | c$. إذن يوجد $r \in R$ ، بحيث $c = r x$. كذلك بما أن بما أن $y | k \;,\; y | k'$ ، فإن $y | c$. إذن يوجد $s \in R$ ، بحيث $c = s y$. إذن

$$c = r x = s y \qquad (2)$$

وبما أن $c | k$ ، فإنة يوجد $d \in R$ بحيث

$$k = d\,c \qquad (3)$$

إذن ينتج من (3) , (2) , (1) أن

$$a\,y = k = d\,c = d\,s\,y$$

إذن $d\,s = a$.

كذلك ينتج من (3) , (2) , (1) أن

$$b\,x = k = d\,c = d\,r\,x$$

إذن $d\,r = b$.

لكن a , b يكونان أوليان نسبياً (relatively prime – coprime) . إذن أي قاسم مشترك لـ a , b يكون وحدة . إذن d يكون وحدة . إذن ينتج من (3) أن $k \sim c$. إذن $(k , k') = k$. إذن $k \mid k'$. إذن k هو أصغر مضاعف مشترك لـ x , y . أي أن $k = \text{l.c.m.}(x , y)$.

٢١٢. ليكن R مجال متكامل (integral domain) . نفرض أنة لكل عنصرين $x,y \in R$ يوجد مضاعف مشترك أصغر (least common multiple) . اثبت أنة لكل عنصرين $x,y \in R$ يوجد قاسم مشترك أعظم (greatest common divisor) .

الحل: لاحظ أولاً أن هذا التمرين هو عكس التمرين السابق . ليكن $x,y \in R$. نرمز للقاسم المشترك الأعظم للعنصرين x , y بالرمز (x , y) . لاحظ أن

$$(x , 0) = (0 , x) = x \;\; , (0 , 0) = 0$$

لذلك نفرض أن $x \neq 0 , y \neq 0$. ليكن $u = \text{l.c.m.}(x , y)$. بما أن $x\,y$ مضاعف مشترك للعنصرين x , y (لأن $x \mid x\,y \;\; , \;\; y \mid x\,y$) ، فإن $u \mid x\,y$. إذن يوجد $a \in R$ ، بحيث $x\,y = a\,u$. نبرهن أن $a = (x , y)$. بما أن $x \mid u \;\; , \;\; y \mid u$ ، فإنة يوجد $b , c \in R$ بحيث $u = b\,x = c\,y$. إذن $x\,y = a\,u = a\,b\,x = a\,c\,y$. إذن $x\,y = a\,c\,y \;\; , \;\; x\,y = a\,b\,x$. لكن R مجال متكامل . إذن $x = a\,c \;\; , \;\; y = a\,b$. إذن $a \mid y \;\; , \;\; a \mid x$. إذن a يكون قاسم مشترك للعنصرين x , y . ليكن $d \in R$ قاسم مشترك آخر لـلعنصرين x , y . إذن يوجد $x' , y' \in R$ بحيث $y = d\,y' \;\; , \;\; x = d\,x'$. إذن $y \mid d\,x'\,y' \;\; , \;\; x \mid d\,x'\,y'$. أي أن $d\,x'\,y'$ يكون مضاعف مشترك للعنصرين x , y . نضع $e = d\,x'\,y'$. إذن $u \mid e$. إذن يوجد $k \in R$ بحيث $e = u\,k$. إذن $x\,y = e\,d = u\,k\,d \;\; , \;\; x\,y = a\,u$. إذن $a\,u = u\,k\,d$. لكن R مجال متكامل . إذن $a = k\,d$. إذن $d \mid a$. إذن a هو القاسم المشترك الأعظم للعنصرين x , y . أي أن $a = (x , y)$.

٢١٣. ليكن R مجال متكامل ، وليكن $a \in R\backslash\{0\}$ عنصر ليس وحدة وغير مختزل . إذا كان $b \in R\backslash\{0\}$ ، بحيث a لا يقسم b ، فاثبت أن $(a , b) = 1$.

الحل: ليكن R مجال متكامل ، وليكن $a \in R\backslash\{0\}$ عنصر ليس وحدة وغير مختزل . نفرض أن $b \in R\backslash\{0\}$ ، بحيث a لا يقسم b . ليكن c قاسم مشترك للعنصرين a , b في R . نفرض أن c ليس وحدة . إذن يوجد $x,y \in R$ ، بحيث $b = c\, y \;,\; a = c\, x$. لكن a عنصر غير مختزل في R . إذن c أو x يكون وحدة في R . لكن c ليس وحدة فرضا . إذن x يكون وحدة . إذن $c = a\, x^{-1}$. إذن $b = a\,(x^{-1} y)$. إذن $a \mid b$. لكن هذا يتناقض مع الفرض بأن a لا يقسم b . إذن c يكون وحدة . إذن أي قاسم مشترك للعنصرين a , b يكون وحدة . إذن $(a , b) = 1$

(لاحظ أن هذا ينتج مباشرة من المبرهنة : ليكن R مجال متكامل ، وليكن $a,b \in R\backslash\{0\}$. إذن $(a , b) = 1$ إذا وفقط إذا كان كل قاسم مشترك للعنصرين a , b وحدة) .

٢١٤. (أ) أوجد كل قواسم العنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(ب) أوجد كل قواسم العنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(ت) أوجد كل قواسم العنصر $5+3i$ في الحلقة $\mathbf{Z}[i]$.

الحل: (أ) لاحظ أولاً أن الحلقة $\mathbf{Z}[i\sqrt{6}]$ تكون ابدالية وتحتوي على عنصر محايد وهو العدد الصحيح 1 . ليكن $a + bi\sqrt{6} \in \mathbf{Z}[i\sqrt{6}]$ ، بحيث $a + bi\sqrt{6} \mid 6$. إذن يوجد $c + di\sqrt{6} \in \mathbf{Z}[i\sqrt{6}]$ ، بحيث

$$6 = (a + bi\sqrt{6})\,(c + di\sqrt{6}) \qquad (1)$$

إذن

$$\overline{6} = 6 = (a - bi\sqrt{6})\,(c - di\sqrt{6}) \qquad (2)$$

إذن بضرب (2) , (1) نحصل على

$$(a^2 + 6\, b^2)\,(c^2 + 6\, d^2) = 36$$

بالتالي توجد الإحتمالات التالية:

(١) $a^2 + 6\, b^2 = 1$

في هذه الحالة يكون $b = 0 \;,\; a = \pm 1$. إذن $1 , -1$ يكونان قاسمان للعنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(٢) $a^2 + 6\, b^2 = 2$

هذا الإحتمال مرفوض ، لأنة لا يوجد $a,b \in \mathbf{Z}$ يحققان المعادلة $a^2 + 6b^2 = 2$.

(٣) $a^2 + 6b^2 = 3$

هذا الإحتمال مرفوض أيضاً كما جاء في الإحتمال السابق .

(٤) $a^2 + 6b^2 = 4$

في هذة الحالة يكون $b = 0$, $a = \pm 2$. إذن $2 , -2$ يكونان قاسمان للعنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(٥) $a^2 + 6b^2 = 6$

في هذة الحالة يكون $b = \pm 1$, $a = 0$. إذن $i\sqrt{6} , -i\sqrt{6}$ يكونان قاسمان لـ 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(٦) $a^2 + 6b^2 = 9$

في هذة الحالة يكون $b = 0$, $a = \pm 3$. إذن $3 , -3$ يكونان قاسمان للعنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

(٧) $a^2 + 6b^2 = 12$

هذا الإحتمال مرفوض ، لأن المعادلة $a^2 + 6b^2 = 12$ ليس لها حل في $\mathbf{Z}$.

(٨) $a^2 + 6b^2 = 18$

هذا الإحتمال مرفوض أيضاً ، لأن المعادلة $a^2 + 6b^2 = 18$ ليس لها حل في $\mathbf{Z}$.

(٩) $a^2 + 6b^2 = 36$

في هذة الحالة يكون $b = 0$, $a = \pm 6$. إذن $6 , -6$ يكونان قاسمان للعنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$.

ينتج مما سبق أن كل قواسم العنصر 6 في الحلقة $\mathbf{Z}[i\sqrt{6}]$ هي:

$\pm 1 \;,\; \pm 2 \;,\; \pm 3 \;,\; \pm 6 \;,\; \pm i\sqrt{6}$

(ب) لاحظ أولاً أن الحلقة $\mathbf{Z}[i\sqrt{5}]$ تكون ابدالية وتحتوي على محايد وهو العدد الصحيح 1 .

ليكن $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $a + bi\sqrt{5} \mid 21$. إذن يوجد $c + di\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث

$$21 = (a + bi\sqrt{5})(c + di\sqrt{5}) \qquad (1)$$

إذن

$$21 = (a - bi\sqrt{5})(c - di\sqrt{5}) \qquad (2)$$

إذن بضرب (2) , (1) نحصل على

$$(a^2 + 5\,b^2)\,(c^2 + 5\,d^2) = 441$$

بالتالي توجد الإحتمالات التالية:

(١) $a^2 + 5\,b^2 = 1$

في هذة الحالة يكون $a = \pm 1 \;,\; b = 0$. إذن $1 \,, -1$ يكونان قاسمان للعنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(٢) $a^2 + 5\,b^2 = 3$

هذا الإحتمال مرفوض ، لأن المعادلة $a^2 + 5\,b^2 = 3$ ليس لها حل في $\mathbf{Z}$.

(٣) $a^2 + 5\,b^2 = 7$

هذا الإحتمال مرفوض أيضاً كما جاء في الإحتمال السابق .

(٤) $a^2 + 5\,b^2 = 9$

في هذة الحالة يكون $(a = \pm 3 \;,\; b = 0)$. أما $(a = \pm 2 \;,\; b = \pm 1)$ فهو مرفوض .

إذن $3 \,, -3$ يكونان قاسمان للعنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(٥) $a^2 + 5\,b^2 = 21$

في هذة الحالة يكون $(a = \pm 1 \;,\; b = \pm 2)$ و $(a = \pm 4,\; b = \pm 1)$. إذن $(\pm 4 \pm i\sqrt{5})\,,\,(\pm 1 \pm 2i\sqrt{5})$ تكون قواسم للعنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(٦) $a^2 + 5\,b^2 = 49$

في هذة الحالة يكون $(a = \pm 7 \;,\; b = 0)$ و $(a = \pm 2,\; b = \pm 3)$. إذا كان $(a = \pm 7 \;,\; b = 0)$ ، فإن $(a + bi\sqrt{5} = 7 \;,\; c + di\sqrt{5} = 3)$ و $(a + bi\sqrt{5} = -7 \;,\; c + di\sqrt{5} = -3)$. وإذا كان $(a = \pm 2,\; b = \pm 3)$ ، فإن $c^2 + 5\,d^2 = 9$. وبالتالي $(c = \pm 3 \;,\; d = 0)$ أو $(c = \pm 2 \;,\; d = \pm 1)$. لكن $(\pm 2 \pm 3i\sqrt{5})\,(\pm 3) \neq 21$. إذن $(c = \pm 3 \;,\; d = 0)$ يكون مرفوض . كذلك $(\pm 2 \pm 3i\sqrt{5})\,(\pm 2 \pm i\sqrt{5}) \neq 21$. إذن $(c = \pm 2,\; d = \pm 1)$ يكون مرفوض . إذن $(a = \pm 2,\; b = \pm 3)$ يكون مرفوض . إذن $7 \,, -7$ يكونان قاسمان للعنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(٧) $a^2 + 5\,b^2 = 63$

هذا الإحتمال مرفوض ، لأن المعادلة $a^2 + 5\,b^2 = 63$ ليس لها حل في $\mathbf{Z}$.

(٨) $a^2 + 5\,b^2 = 147$

هذا الإحتمال مرفوض أيضاً ، لأن المعادلة $a^2 + 5b^2 = 147$ ليس لها حل في $\mathbf{Z}$.

(٩) $a^2 + 5b^2 = 441$

في هذة الحالة يكون $b = 0$, $a = \pm 21$. إذن -21 , 21 يكونان قاسمان للعنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

ينتج مما سبق أن كل قواسم العنصر 21 في الحلقة $\mathbf{Z}[i\sqrt{5}]$ هي:

$$\pm 1 \;,\; \pm 3 \;,\; \pm 7 \;,\; \pm 21 \;,\; (\pm 1 \pm 2i\sqrt{5}) \,,\, (\pm 4 \pm i\sqrt{5})$$

(ت) لاحظ أولاً أن الحلقة $\mathbf{Z}[i]$ تكون ابدالية وتحتوي على محايد وهو العدد الصحيح 1. ليكن $a + bi \in \mathbf{Z}[i]$ ، بحيث $a + bi \mid 5 + 3i$. إذن يوجد $c + di \in \mathbf{Z}[i]$ ، بحيث

$$5 + 3i = (a + bi)(c + di) \qquad (1)$$

إذن

$$5 - 3i = (a - bi)(c - di) \qquad (2)$$

إذن بضرب (2) , (1) نحصل على

$$(a^2 + b^2)(c^2 + d^2) = 34 \qquad (3)$$

بالتالي توجد الإحتمالات التالية:

(١) $a^2 + b^2 = 1$

في هذة الحالة يكون $(a = \pm 1 \;,\; b = 0)$ و $(a = 0 \;,\; b = \pm 1)$. إذن $\pm 1 , \pm i$ تكون قواسم للعنصر $5 + 3i$ في الحلقة $\mathbf{Z}[i]$.

(٢) $a^2 + b^2 = 2$

في هذة الحالة يكون $(a = \pm 1 \;,\; b = \pm 1)$. في هذة الحالة يكون $c^2 + d^2 = 17$. وبالتالي احتمالات قيم c , d هي

$$(c , d) = (\pm 4 , \pm 1) , (\pm 1, \pm 4)$$

الإحتمالات

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

تكون مرفوضة لأنها لا تحقق (3) . إذن

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

إذن $-1 - i$, $1 + i$ يكونان قاسمان للعنصر $5 + 3i$ في الحلقة $\mathbf{Z}[i]$.

(٣) $a^2 + b^2 = 17$

في هذة الحالة يكون $c^2 + d^2 = 2$. بالتالي احتمالات قيم a , b , c , d هى

$(a , b) = (\pm 4 , \pm 1) \;,\; (\pm 1 , \pm 4)$

$(c , d) = (\pm 1 , \pm 1)$

إذن قيم a , b التي تحقق (3) هى

$(a , b) = (1, 4) , (-1, -4) , (4 , -1) , (-4 , 1)$

إذن $-4 + i \;,\; 4 - i \;,\; -1 - 4i \;,\; 1 + 4i$ تكون قواسم للعنصر $5 + 3i$ في الحلقة **Z**[i] .

(٤) $a^2 + b^2 = 34$

في هذة الحالة يكون $c^2 + d^2 = 1$. بالتالي احتمالات قيم a , b , c , d هى

$(a , b) = (\pm 3 , \pm 5) \;,\; (\pm 5 , \pm 3)$

$(c , d) = (\pm 1 , 0) \;,\; (0 , \pm 1)$

إذن قيم a , b التي تحقق (3) هى

$(a , b) = (3, -5) , (-3 , 5) , (5 , 3) , (-5 , -3)$

إذن $-5 - 3i \;,\; 5 + 3i \;,\; -3 + 5i \;,\; 3 - 5i$ تكون قواسم للعنصر $5 + 3i$ في الحلقة **Z**[i] . إذن كل قواسم $5 + 3i$ غير الصفرية في الحلقة **Z**[i] هي

$\pm 1 , \pm i , 1 + i \;,\; -1 - i \;,\; 1 + 4i \;,\; -1 - 4i \;,\; 4 - i \;,\; -4 + i \;,\; 3 - 5i \;,$
$-3 + 5i \;,\; 5 + 3i \;,\; -5 - 3i$

٢١٥. ليكن R حلقة مثاليات رئيسة (principal ideal ring) ، وليكن $a,b,c \in R \setminus \{0\}$. ليكن $d = (a , b)$. برهن أنة يوجد $r , s \in R$ ، بحيث $c = r a + s b$ إذا وفقط إذا كان $d \mid c$ (حيث (a , b) يرمز للقاسم المشترك الأعظم للعنصرين a , b في R) .

الحل: ليكن R حلقة مثاليات رئيسة (principal ideal ring) ، وليكن $a,b,c \in R \setminus \{0\}$. ليكن $d = (a , b)$. نفرض أنة يوجد $r , s \in R$ ، بحيث $c = r a + s b$. بما أن $d = (a , b)$ ، فإن $d \mid r a + s b = c$.

بالعكس ، نفرض أن $d \mid c$. إذن يوجد $k \in R$ ، بحيث $c = d k$. بما أن $d = (a , b)$ ، وبما أن R حلقة مثاليات رئيسة ، فإنة يوجد $a' , b' \in R$ بحيث $d = a' a + b' b$. إذن

$$c = k d = (k a') a + (k b') b$$

وذلك لأن R حلقة مثاليات رئيسة ، وبالتالي R تكون حلقة ابدالية وتحتوي محايد . نضع $r = k a' ,\; s = k b'$. إذن $c = r a + s b$.

٢١٦. ليكن R حلقة ابدالية ، وليكن $1 \in R$. ليكن $p \in R \setminus \{0\}$. برهن أن p يكون عنصر غير مختزل (irreducible) $\Leftrightarrow$ $p\,u$ يكون عنصر غير مختزل (irreducible) لكل وحدة $u \in R$.

الحل: ليكن R حلقة ابدالية ، وليكن $1 \in R$. ليكن $p \in R \setminus \{0\}$. ليكن $u \in R$ وحدة .

($\Leftarrow$) ليكن p عنصر غير مختزل (irreducible) في R . لاحظ أن $p\,u$ لا يكون وحدة ، لأنة إذا كان $p\,u = e$ وحدة في R ، فإن $p = e\,u^{-1}$ يكون وحدة ، وهذا يتناقض مع الفرض بأن p عنصر غير مختزل . ليكن $a,b \in R$ ، بحيث $p\,u = a\,b$. إذن $p = a\,(b\,u^{-1})$. لكن p عنصر غير مختزل في R . إذن a أو $b\,u^{-1}$ يكون وحدة . إذا كان $b\,u^{-1}$ وحدة ، فإن b يكون وحدة . إذن a أو b يكون وحدة . إذن $p\,u$ يكون عنصر غير مختزل .

($\Rightarrow$) ليكن $p\,u$ عنصر غير مختزل في R . إذا كان p وحدة ، فإن $p\,u$ يكون وحدة ، وهذا يتناقض مع الفرض بأن $p\,u$ يكون عنصر غير مختزل في R . إذن p لا يكون وحدة . ليكن $a,b \in R$ بحيث $p = a\,b$. إذن $p\,u = a\,(b\,u)$. بما أن $p\,u$ عنصر غير مختزل ، فإن a أو $b\,u$ يكون وحدة . إذا كان $b\,u$ وحدة ، فإن b يكون وحدة . إذن a أو b يكون وحدة . إذن p يكون عنصر غير مختزل .

٢١٧. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن كل عنصر من العنصرين $2 - i\sqrt{5}$, $2 + i\sqrt{5}$ يكون غير مختزل وغير أولي .

الحل: لاحظ أولاً أن الحلقة $\mathbf{Z}[i\sqrt{5}]$ تكون مجال متكامل . نبين الآن أن العنصر $2 + i\sqrt{5}$ يكون غير مختزل في الحلقة $\mathbf{Z}[i\sqrt{5}]$. ليكن $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث

$$(a + bi\sqrt{5})\,(2 + i\sqrt{5}) = 1$$

إذن $-4a - 5b = 1$. لكن هذة المعادلة ليس لها حل في $\mathbf{Z}$. إذن العنصر $2 + i\sqrt{5}$ ليس وحدة في الحلقة $\mathbf{Z}[i\sqrt{5}]$. ليكن $a + bi\sqrt{5}\,,\, c + di\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث

$$2 + i\sqrt{5} = (a + bi\sqrt{5})\,(c + di\sqrt{5}) \qquad (1)$$

إذن

$$2 - i\sqrt{5} = (a - bi\sqrt{5})\,(c - di\sqrt{5}) \qquad (2)$$

بضرب (1) في (2) نحصل على

$$(a^2 + 5\,b^2)\,(c^2 + 5\,d^2) = 9$$

إذن توجد الإحتمالات التالية:

(أ) $c^2 + 5\,d^2 = 9 \quad , \quad a^2 + 5\,b^2 = 1$

إذن $b = 0 \;,\; a = \pm 1$. إذن $a + bi\sqrt{5} = \pm 1$. إذن في هذة الحالة العنصر $a + bi\sqrt{5}$ يكون وحدة الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(ب) $c^2 + 5\,d^2 = 1 \quad , \quad a^2 + 5\,b^2 = 9$

إذن $d = 0 \;,\; c = \pm 1 \;,\; a = \pm 2 \;,\; b = \pm 1$. إذن $c + di\sqrt{5} = \pm 1$. إذن في هذة الحالة العنصر $c + di\sqrt{5}$ يكون وحدة الحلقة $\mathbf{Z}[i\sqrt{5}]$.

(ت) $c^2 + 5\,d^2 = 3 \quad , \quad a^2 + 5\,b^2 = 3$

هذا الإحتمال مرفوض ، لأنة لا يوجد عناصر $a,b,c,d \in \mathbf{Z}$ تحققة .

إذن العنصر $2 + i\sqrt{5}$ يكون غير مختزل في الحلقة $\mathbf{Z}[i\sqrt{5}]$. بالمثل العنصر $2 - i\sqrt{5}$ يكون غير مختزل في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

والآن نبين أن العنصر $2 + i\sqrt{5}$ لا يكون عنصر أولي في الحلقة $\mathbf{Z}[i\sqrt{5}]$. بما أن العنصر $2 + i\sqrt{5}$ ليس وحدة في الحلقة $\mathbf{Z}[i\sqrt{5}]$ ، فإننا نبين أنة يوجد عنصرين في الحلقة $\mathbf{Z}[i\sqrt{5}]$ بحيث $2 + i\sqrt{5}$ يقسم حاصل ضربهما ولا يقسم كل منهما . بما أن $9 = (2 + i\sqrt{5})\,(2 - i\sqrt{5})$ ، فإن $2 + i\sqrt{5} \mid 3 \times 3$. لكن $2 + i\sqrt{5}$ لا يقسم 3 . (لأن: نفرض العكس ، أي نفرض أن $2 + i\sqrt{5} \mid 3$. إذن يوجد $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث

$$3 = (2 + i\sqrt{5})\,(a + bi\sqrt{5})$$

إذن

$$3 = (2 - i\sqrt{5})\,(a - bi\sqrt{5})$$

إذن $a^2 + 5\,b^2 = 1$. إذن $b = 0 \;,\; a = \pm 1$. إذن $a + bi\sqrt{5} = \pm 1$. إذا كان $a + bi\sqrt{5} = 1$ ، فإن $3 = 2 + i\sqrt{5}$. إذن $3 = 2$ ، وهذا غير ممكن . إذن $a + bi\sqrt{5} \neq 1$. وإذا كان $a + bi\sqrt{5} = -1$ ، فإن $3 = -\;2 -\; i\sqrt{5}$. إذن $3 = -2$ ، وهذا غير ممكن . إذن $a + bi\sqrt{5} \neq -1$) . إذن العنصر $2 + i\sqrt{5}$ لا يكون عنصر أولي في الحلقة $\mathbf{Z}[i\sqrt{5}]$. بالمثل العنصر $2 - i\sqrt{5}$ يكون غير أولي في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

٢١٨. أوجد كل الوحدات في الحلقة $\mathbf{Z}[i\sqrt{n}]$ ، حيث $n \in \mathbf{N}$.

الحل: ليكن $n \in \mathbf{N}$, $a + bi\sqrt{n} \in \mathbf{Z}[i\sqrt{n}]$ ، بحيث $a + bi\sqrt{n} \neq 0$. المعكوس الضربي للعنصر $a + bi\sqrt{n}$ (إن وُجد) يكون في الصورة التالية

$$1/(a + bi\sqrt{n}) = 1/(a + bi\sqrt{n}) \times (a - bi\sqrt{n}) / (a - bi\sqrt{n})$$
$$= (a/(a^2 + nb^2)) - (b / (a^2 + nb^2))\, i\sqrt{n}$$

إذن يوجد معكوس ضربي للعنصر $a + bi\sqrt{n}$ في الحلقة $\mathbf{Z}[i\sqrt{n}]$ إذا وفقط إذا كان $a^2 + nb^2 = 1$. بالتالي توجد الحالتين التاليتين:

(١) $n = 1$

في هذه الحالة يكون:

$a^2 + b^2 = 1$ إذا وفقط إذا كان $(a = \pm 1 \;,\; b = 0)$ أو $(a = 0 \;,\; b = \pm 1)$

إذن $\pm i$, ± 1 هي كل الوحدات في $\mathbf{Z}[i]$ (ملحوظة: حل تمرين (٢٢٧) يتضمن حل آخر لهذة النتيجة) .

(٢) $n > 1$

في هذه الحالة يكون:

$a^2 + nb^2 = 1$ إذا وفقط إذا كان $b = 0 \;,\; a = \pm 1$.

إذن ± 1 هي كل الوحدات في $\mathbf{Z}[i\sqrt{n}]$ (انظر حل آخر لهذة النتيجة في تمرين (٢٢٧)) .

٢١٩. في الحلقة $\mathbf{Z}[i]$ أوجد $(2 + 7i , 2 - 11i)$.

الحل: بما أن $-i$, i , -1 , 1 هى كل الوحدات في الحلقة $\mathbf{Z}[i]$ (انظر حل تمرين (٢١٨)) ، فإن كل من العنصرين $2 - 11i$, $2 + 7i$ لا يكون وحدة في الحلقة $\mathbf{Z}[i]$. نفرض أن $2 + 7i \mid 2 - 11i$. إذن يوجد $a + bi \in \mathbf{Z}[i]$ ، بحيث $2 - 11i = (2 + 7i)(a + bi)$. إذن $125 = 53 (a^2 + b^2)$. لكن هذة المعادلة ليس لها حل في $\mathbf{Z}$ ، لأن 53 لا يقسم 125 . إذن $2 + 7i$ لا يقسم $2 - 11i$. ليكن $a + bi , c + di \in \mathbf{Z}[i]$ ، بحيث $2 + 7i = (a + bi)(c + di)$. إذن $2 - 7i = (a - bi)(c - di)$. إذن $53 = (a^2 + b^2)(c^2 + d^2)$. إذن توجد الإحتمالات التالية:

(أ) $a^2 + b^2 = 1 \;,\; c^2 + d^2 = 53$

في هذه الحالة يكون

$(a = 0 , b = \pm 1)$ أو $(a = \pm 1 , b = 0)$ ،

$(c = \pm 7 , d = \pm 2)$ أو $(c = \pm 2 , d = \pm 7)$

(ب) $a^2 + b^2 = 53 \;,\; c^2 + d^2 = 1$

في هذة الحالة يكون

$(a = \pm 2 , b = \pm 7)$ أو $(a = \pm 7, b = \pm 2)$ ،

$(c = 0 , d = \pm 1)$ أو $(c = \pm 1 , d = 0)$

إذن $a + bi = \pm 1$ أو $a + bi = \pm i$ و $c + di = \pm 1$ أو $c + di = \pm i$. إذن $a + bi$ أو $c + di$ يكون وحدة في الحلقة $\mathbf{Z}[i]$. إذن العنصر $2 + 7i$ يكون غير مختزل في الحلقة $\mathbf{Z}[i]$.

إذن ينتج من تمرين (٢١٣) أن $(2 + 7i , 2 - 11i) = 1$.

٢٢٠. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ أوجد $(2 , 1 + i\sqrt{5})$.

الحل: بما أن $1 , -1$ هى كل الوحدات في الحلقة $\mathbf{Z}[i\sqrt{5}]$ (انظر تمرين (٢١٨)) ، فإن كل من العنصرين $2 , 1 + i\sqrt{5}$ لا يكون وحدة في الحلقة $\mathbf{Z}[i\sqrt{5}]$. نفرض أن $2 \mid 1 + i\sqrt{5}$. إذن يوجد $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $1 + i\sqrt{5} = 2\,(a + bi\sqrt{5})$. إذن $2a = 1 , 2b = 1$. لكن هاتين المعادلتين ليس لهما حل في $\mathbf{Z}$. إذن 2 لا يقسم $1 + i\sqrt{5}$.

ليكن $a + bi\sqrt{5} , c + di\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $2 = (a + bi\sqrt{5})\,(c + di\sqrt{5})$. إذن $2 = (a - bi\sqrt{5})\,(c - di\sqrt{5})$. إذن $4 = (a^2 + 5b^2)\,(c^2 + 5d^2)$. إذن توجد الإحتمالات التالية:

(أ) $a^2 + 5b^2 = 1 \;,\; c^2 + 5d^2 = 4$

في هذة الحالة يكون

$(a = \pm 1 , b = 0)$ و $(c = \pm 2 , d = 0)$ ،

(ب) $a^2 + 5b^2 = 4 \;,\; c^2 + 5d^2 = 1$

في هذة الحالة يكون

$(a = \pm 2 , b = 0)$ و $(c = \pm 1 , d = 0)$

(ت) $a^2 + 5b^2 = 2 \;,\; c^2 + 5d^2 = 2$

لكن هاتين المعادلتين ليس لهما حل في $\mathbf{Z}$ ، وبالتالي هذا الإحتمال مرفوض .

إذن $a + bi\sqrt{5} = \pm 1$ أو $c + di\sqrt{5} = \pm 1$. إذن $a + bi\sqrt{5}$ أو $c + di\sqrt{5}$ يكون وحدة في الحلقة $\mathbf{Z}[i\sqrt{5}]$. إذن 2 يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[i\sqrt{5}]$. إذن ينتج من تمرين (٢١٣) أن $(2 , 1+ i\sqrt{5}) = 1$.

٢٢١. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن $(6\,(1 - i\sqrt{5}) , 18)$ غير موجود .

الحل: نفرض أن $d = (6\,(1 - i\sqrt{5}) , 18)$ موجود في الحلقة $\mathbf{Z}[i\sqrt{5}]$. لاحظ أن

$$18 = 3 \times 6 = 3\,(1 + i\sqrt{5})\,(1 - i\sqrt{5})$$

إذن $d = 3\,(1 - i\sqrt{5})\,(2 , 1 + i\sqrt{5})$. لكن من التمرين السابق يكون $(2 , 1+ i\sqrt{5}) = 1$. إذن $d = 3\,(1 - i\sqrt{5})$. لكن $6 \mid 18$, $6 \mid 6\,(1 - i\sqrt{5})$. إذن $6 \mid d$. أي أن $6 \mid 3\,(1 - i\sqrt{5})$. إذن $2 \mid (1 - i\sqrt{5})$. إذن يوجد $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $1 - i\sqrt{5} = 2\,(a + bi\sqrt{5})$. إذن $2a = 1$ في $\mathbf{Z}$. لكن هذا غير ممكن . إذن الفرض بوجود قاسم مشترك أعظم للعنصرين 18 , $6\,(1 - i\sqrt{5})$ في الحلقة $\mathbf{Z}[i\sqrt{5}]$ غير صحيح . إذن لا يوجد قاسم مشترك أعظم للعنصرين 18 , $6\,(1 - i\sqrt{5})$ في الحلقة $\mathbf{Z}[i\sqrt{5}]$.

٢٢٢. ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $d = (x , y)$. إذا كان $r \in R\backslash\{0\}$ ، فاثبت أن $r\,d = (r\,x , r\,y)$.

الحل: ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $d = (x , y)$. ليكن $r \in R\backslash\{0\}$. نضع $e = (r\,x , r\,y)$. بما أن $d = (x , y)$ ، فإن $d \mid x , d \mid y$. إذن $r\,d \mid r\,y$, $r\,d \mid r\,x$ ، لكل $r \in R\backslash\{0\}$. إذن $r\,d \mid e$. إذن يوجد $a \in R$ ، بحيث $e = r\,d\,a$. وبما أن $r \mid r\,y$, $r \mid r\,x$ ، فإن $r \mid e$. إذن يوجد $b \in R$ ، بحيث $e = r\,b$. إذن $b = d\,a$ (لأن R خالي من قواسم الصفر ، لأنة مجال متكامل) . لكن $e \mid r\,y$, $e \mid r\,x$. إذن $r\,b \mid r\,y$, $r\,b \mid r\,x$. إذن $b \mid y$, $b \mid x$. إذن $b \mid d$. إذن $d\,a \mid d$. إذن $a \mid 1$. إذن a يكون وحدة في R . إذن ينتج من $e = r\,d\,a$ أن $r\,d \sim e$. إذن $r\,d = (r\,x , r\,y)$.

٢٢٣. ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $m = \mathrm{l.c.m.}(x , y)$. إذا كان $r \in R\backslash\{0\}$ ، فاثبت أن $r\,m = \mathrm{l.c.m.}(r\,x , r\,y)$.

الحل: ليكن R مجال متكامل ، وليكن $x,y \in R$ بحيث يوجد $m = \mathrm{l.c.m.}(x , y)$. ليكن $r \in R\backslash\{0\}$. نضع $k = \mathrm{l.c.m.}(r\,x , r\,y)$. بما أن $m = \mathrm{l.c.m.}(x , y)$ ، فإن

$x \mid m \;,\; y \mid m$. إذن $r\,x \mid r\,m \;,\; r\,y \mid r\,m$. إذن $r\,m$ يكون مضاعف مشترك للعنصرين $r\,x , r\,y$ في R . إذن $k \mid r\,m$. إذن يوجد $a \in R$ ، بحيث $r\,m = k\,a$. لكن $r \mid k$ ، لأن $r \mid r\,x \;,\; r \mid r\,y$. إذن يوجد $b \in R$ ، بحيث $k = r\,b$. إذن $r\,m = r\,a\,b$. إذن $m = a\,b$ (لأن R خالي من قواسم الصفر ، لأنة مجال متكامل) . وبما أن $r\,x \mid k \;,\; r\,y \mid k$ ، فإن $r\,x \mid r\,b \;,\; r\,y \mid r\,b$. إذن $x \mid b \;,\; y \mid b$. إذن $m \mid b$. لكن $m = a\,b$. إذن $a \mid 1$. إذن a يكون وحدة في R . إذن ينتج من $r\,m = k\,a$ أن $r\,m \sim k$. إذن $r\,m = \text{l.c.m.}(r\,x , r\,y)$.

٢٢٤. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ اثبت أن العنصر 3 لا يكون شريك (associate) لكل من العنصرين $2 + i\sqrt{5} , 2 - i\sqrt{5}$.

الحل: في الحلقة $\mathbf{Z}[i\sqrt{5}]$ يكون $3 \sim 2 + i\sqrt{5}$ إذا وفقط إذا كان $3 = (2 + i\sqrt{5})\,u$ ، حيث u وحدة في الحلقة $\mathbf{Z}[i\sqrt{5}]$. لكن من تمرين (٢١٨) ينتج أن الحلقة $\mathbf{Z}[i\sqrt{5}]$ تحتوي على وحدتين فقط هما $1 , -1$. إذن $u = \pm 1$. لكن $3 \neq (2 + i\sqrt{5})\,u$. إذن في الحلقة $\mathbf{Z}[i\sqrt{5}]$ العنصر 3 لا يكون شريك للعنصر $2 + i\sqrt{5}$. بالمثل في الحلقة $\mathbf{Z}[i\sqrt{5}]$ العنصر 3 لا يكون شريك للعنصر $2 - i\sqrt{5}$.

٢٢٥. في الحلقة $\mathbf{Z}[\sqrt{5}]$ اثبت أن

(أ) $2 - \sqrt{5}$ يكون وحدة .

(ب) كل من $1 - \sqrt{5} \;,\; 3 + \sqrt{5}$ لا يكون وحدة .

(ت) $3 + \sqrt{5} \sim 1 - \sqrt{5}$.

(ث) العناصر $3 - \sqrt{5} \;,\; 2 , 3 + \sqrt{5}$ تكون غير مختزلة .

الحل: (أ)

$$1 / (2 - \sqrt{5}) = 1/(2 - \sqrt{5}) \times (2 + \sqrt{5})/(2 + \sqrt{5}) = -2 - \sqrt{5} \in \mathbf{Z}[\sqrt{5}]$$

إذن $1 = (2 - \sqrt{5})\,(-2 - \sqrt{5})$. إذن العنصر $2 - \sqrt{5}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$.

(ب)

$$1 / (3 + \sqrt{5}) = 1/(3 + \sqrt{5}) \times (3 - \sqrt{5})/(3 - \sqrt{5}) = (3/4) - (1/4)\sqrt{5} \notin \mathbf{Z}[\sqrt{5}]$$

إذن العنصر $3 + \sqrt{5}$ ليس وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$. كذلك

$$1 / (1 - \sqrt{5}) = 1/(1 - \sqrt{5}) \times (1 + \sqrt{5})/(1 + \sqrt{5}) = (-1/4) - (1/4)\sqrt{5} \notin \mathbf{Z}[\sqrt{5}]$$

إذن العنصر $1 - \sqrt{5}$ ليس وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$.

(ت) ليكن $a + b\sqrt{5} \in \mathbf{Z}[\sqrt{5}]$ ، بحيث $1 - \sqrt{5} = (3 + \sqrt{5})(a + b\sqrt{5})$. إذن

$$3a + 5b = 1 \quad , \quad a + 3b = -1$$

إذن $b = -1 \; , \; a = 2$. إذن $1 - \sqrt{5} = (3 + \sqrt{5})(2 - \sqrt{5})$. لكن من (أ) العنصر $2 - \sqrt{5}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$ ، ومن (ب) كل من العنصران $1 - \sqrt{5} , 3 + \sqrt{5}$ ليس وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$. إذن $3 + \sqrt{5} \sim 1 - \sqrt{5}$.

(ث) ليكن $a + b\sqrt{5} \in \mathbf{Z}[\sqrt{5}]$ ، بحيث $2(a + b\sqrt{5}) = 1$. إذن $2a = 1 \; , \; 2b = 0$. لكن $2a = 1$ ليس لها حل في $\mathbf{Z}$. إذن العنصر 2 ليس لة معكوس ضربي في الحلقة $\mathbf{Z}[\sqrt{5}]$. إذن 2 ليس وحدة في الحلقة $\mathbf{Z}[\sqrt{5}]$. ليكن $a + b\sqrt{5} , c + d\sqrt{5} \in \mathbf{Z}[\sqrt{5}]$ ، بحيث

$$2 = (a + b\sqrt{5})(c + d\sqrt{5}) \qquad (1)$$

إذن

$$2 = (a - b\sqrt{5})(c - d\sqrt{5}) \qquad (2)$$

بضرب (1) في (2) نحصل على

$$(a^2 - 5b^2)(c^2 - 5d^2) = 4$$

إذن توجد الإحتمالات التالية:

(١) $a^2 - 5b^2 = 1 \quad , \quad c^2 - 5d^2 = 4$

إذن

$$a = \pm 1 \; , \; b = 0 \; , \; (c, d) = (\pm 2, 0) \; , \; (\pm 3, \pm 1) \; , \; (\pm 7, \pm 3)$$

الإحتمالات $(c, d) = (\pm 3, \pm 1) \; , \; (\pm 7, \pm 3)$ مرفوضة لأنها لا تحقق (1) . إذن

$$a + b\sqrt{5} = 1 \; , \; c + d\sqrt{5} = 2$$

أو

$$a + b\sqrt{5} = -1 \; , \; c + d\sqrt{5} = -2$$

(٢) $a^2 - 5b^2 = 4 \quad , \quad c^2 - 5d^2 = 1$

هذة الحالة مثل الإحتمال (١)

(٣) $a^2 - 5b^2 = 2 \quad , \quad c^2 - 5d^2 = 2$

هذا الإحتمال مرفوض ، لأنة لا يوجد $a,b,c,d \in \mathbf{Z}$ تحققة .

إذن العنصر 2 يكون غير مختزل في الحلقة $\mathbf{Z}[\sqrt{5}]$.

ليكن $a + b\sqrt{5} , c + d\sqrt{5} \in \mathbf{Z}[\sqrt{5}]$ ، بحيث

$$3 + \sqrt{5} = (a + b\sqrt{5})(c + d\sqrt{5}) \qquad (1)$$

إذن

$$3 - \sqrt{5} = (a - b\sqrt{5})(c - d\sqrt{5}) \qquad (2)$$

بضرب (1) في (2) نحصل على

$$(a^2 - 5b^2)(c^2 - 5d^2) = 4$$

إذن بالمثل كما في حالة العنصر 2 ، فإن كل من العنصرين $3 + \sqrt{5}\ ,\ 3 - \sqrt{5}$ يكون غير مختزل في الحلقة $\mathbf{Z}[\sqrt{5}]$.

٢٢٦. ليكن $n \in \mathbf{N}\backslash\{0,1\}$ ، $N : \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$ ، بحيث $N(a + b\sqrt{n}) = a^2 - n b^2$ لكل $a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$. برهن أن

(أ) N يحفظ عملية الضرب .

(ب) $N(x) = \pm 1 \Leftrightarrow x$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{n}]$.

(ت) إذا كان $N(x)$ عدد أولي ، فإن x يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{n}]$.

الحل: ليكن $n \in \mathbf{N}\backslash\{0,1\}$ ، $N : \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$ ، بحيث $N(a + b\sqrt{n}) = a^2 - n b^2$ لكل $a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$.

(أ) ليكن $a + b\sqrt{n} , c + d\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$. نضع $x = a + b\sqrt{n} , y = c + d\sqrt{n}$. إذن $\bar{x} = a - b\sqrt{n}\ ,\ \bar{y} = c - d\sqrt{n}$. إذن $x\bar{x} = a^2 - n b^2\ ,\ y\bar{y} = c^2 - n d^2$. إذن

$$N(x) = N(a + b\sqrt{n}) = a^2 - n b^2 = x\bar{x} ,$$

$$N(y) = N(c + d\sqrt{n}) = c^2 - n d^2 = y\bar{y}$$

إذن

$$N(xy) = (xy)(\bar{x}\bar{y}) = (x\bar{x})(y\bar{y}) = N(x)N(y)$$

إذن N يحفظ عملية الضرب .

(ب) $(\Leftarrow)$ ليكن $x = a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$ ، بحيث $N(x) = \pm 1$. إذن $x\bar{x} = \pm 1$. أي أن $a^2 - n b^2 = \pm 1$. إذن

$$1/(a + b\sqrt{n}) = 1/(a + b\sqrt{n}) \times (a - b\sqrt{n})/(a - b\sqrt{n})$$

$$= (a - b\sqrt{n})/(a^2 - n b^2)$$

$$= \pm (a - b\sqrt{n}) \in \mathbf{Z}[\sqrt{n}]$$

إذن $a + b\sqrt{n}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{n}]$.

($\Rightarrow$) ليكن $x \in \mathbf{Z}[\sqrt{n}]$ وحدة . إذن يوجد $y \in \mathbf{Z}[\sqrt{n}]$ ، بحيث $x\, y = 1$. إذن $N(x\, y) = N(1) = 1$. إذن ينتج من (أ) أن $N(x)\, N(y) = 1$. إذن $N(x) = \pm 1$.

(ت) ليكن $x \in \mathbf{Z}[\sqrt{n}]$ ، بحيث $N(x)$ يكون عدد أولي . إذن $N(x)$ لا يكون وحدة (من تعريف العنصر الأولي) . إذن $N(x) \neq \pm 1$ (لأن $1 , -1$ هي كل الوحدات في الحلقة $\mathbf{Z}$) . إذن ينتج من (ب) أن x لا يكون وحدة . ليكن $y,z \in \mathbf{Z}[\sqrt{n}]$ ، بحيث $x = y\, z$. إذن ينتج من (أ) أن $N(x) = N(y)\, N(z)$. لكن $N(x)$ يكون عدد أولي في $\mathbf{Z}$. إذن $N(y) = \pm 1$ أو $N(z) = \pm 1$. إذن ينتج من (ب) أن y أو z يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{n}]$. إذن x يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{n}]$.

ملحوظة: التمرين السابق يظل صحيحاً إذا استبدلنا n بـ n - ، أي إذا كان $n \in \mathbf{N}\backslash\{0,1\}$, $N : \mathbf{Z}[\sqrt{-n}] \to \mathbf{Z}$ ، بحيث $N(a + b\sqrt{-n}) = a^2 + n b^2$ لكل $a + b\sqrt{-n} \in \mathbf{Z}[\sqrt{-n}]$ ، فإن

(أ) N يحفظ عملية الضرب .

(ب) $N(x) = \pm 1 \Leftrightarrow x$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{-n}]$.

(ت) إذا كان $N(x)$ عدد أولي ، فإن x يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{-n}]$.

٢٢٧. أوجد $(\mathbf{Z}[\sqrt{-n}])^*$ ، عندما $n = 1 , n > 1$.

الحل: لاحظ أولاً أنة إذا كان R حلقة ، فإن R^* هي مجموعة كل عناصر R التي لها معكوس ضربي في R أي مجموعة كل الوحدات (units) في R .

ليكن $f : \mathbf{Z}[\sqrt{-n}] \to \mathbf{Z}$ بحيث $f(a+b\sqrt{-n}) = a^2 + n b^2$ ، لكل $a+b\sqrt{-n} \in \mathbf{Z}[\sqrt{-n}]$ (لاحظ أن f هو التطبيق N المعرف في تمرين (٢٢٦) بوضع n– بدلاً من n ، حيث n عدد موجب) . ليكن $a+b\sqrt{-n} \in \mathbf{Z}[\sqrt{-n}]$. إذن ينتج من تمرين (٢٢٦) (ب) أن العنصر $a+b\sqrt{-n}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{-n}]$ إذا وفقط إذا كان $f(a+b\sqrt{-n}) = \pm 1$. لكن n عدد موجب . إذن العنصر $a+b\sqrt{-n}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{-n}]$ إذا وفقط إذا كان $a^2 + n b^2 = 1$.

ليكن $n = 1$. إذن العنصر $a+ib$ يكون وحدة في الحلقة $\mathbf{Z}[i]$ إذا وفقط إذا كان $a^2 + b^2 = 1$ (حيث $i = \sqrt{-1}$) . لذلك نفرض أن $a^2 + b^2 = 1$. إذن $a = 0 , b = \pm 1$ أو $a = \pm 1 , b = 0$. إذن في هذة الحالة يوجد في الحلقة $\mathbf{Z}[i]$ أربع وحدات فقط هى $1 , -1 , i , -i$. إذن $(\mathbf{Z}[i])^* = \{1 , -1 , i , -i\}$ (انظر حل آخر لهذة النتيجة في تمرين (٢١٨)) .

ليكن $n > 1$. إذن العنصر $a+b\sqrt{-n}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{-n}]$ إذا وفقط إذا كان $a^2 + n\,b^2 = 1$. لذلك نفرض أن $a^2 + n\,b^2 = 1$. إذن $a = \pm 1 , b = 0$. إذن في هذة الحالة يوجد في الحلقة $\mathbf{Z}[\sqrt{-n}]$ وحدتين فقط هما $1 , -1$. إذن $(\mathbf{Z}[\sqrt{-n}])^* = \{1 , -1\}$ (انظر حل أخر لهذة النتيجة في تمرين (٢١٨)) .

٢٢٨. في الحلقة $\mathbf{Z}[i]$ ، حلل كل عدد من الأعداد $2 , 3 , 5$ إلى حاصل ضرب عناصر غير مختزلة (irreducible) .

الحل: ليكن N هو التطبيق المعرف في تمرين (٢٢٦) بوضع $n = -1$.

<u>أولاً</u> : العدد 2

$2 = (1 + i)\,(1 - i)$ في الحلقة $\mathbf{Z}[i]$. بما أن $N(1 + i) = N(1 - i) = 2$ وبما أن 2 عنصر (عدد) أولي في الحلقة $\mathbf{Z}$ ، فإنة ينتج من تمرين (٢٢٦) (ت) أن كل من $1 + i , 1 - i$ يكون عنصر غير مختزل (irreducible) في الحلقة $\mathbf{Z}[i]$.

<u>ثانياً</u> : العدد 3

نفرض أن $a+bi , c+di \in \mathbf{Z}[i]$ ، بحيث $3 = (a+bi)\,(c+di)$. من تمرين (٢٢٦) (أ) ينتج أن $N(3) = N(a+bi)\,N(c+di)$. لكن $N(3) = 9$. إذن $N(a+bi)\,N(c+di) = 9$. الإحتمال $N(a+bi) = 3 , N(c+di) = 3$ مرفوض ، لأنة في هذة الحالة يكون $a^2 + b^2 = 3$ وهذا غير ممكن . إذن $N(a+bi) = 1 , N(c+di) = 9$ أو $N(a+bi) = 9 , N(c+di) = 1$. إذن ينتج من تمرين (٢٢٦) (ب) أن $a+bi$ يكون وحدة أو $c+di$ يكون وحدة . إذن 3 يكون عنصر غير مختزل .

<u>ثالثاً</u> : العدد 5

$5 = (2 + i)\ (2 - i)$ في الحلقة $\mathbf{Z}[i]$. بما أن $N(2 + i) = N(2 - i) = 5$ وبما أن 5 عنصر (عدد) أولي في الحلقة $\mathbf{Z}$ ، فإنة ينتج من تمرين (٢٢٦) (ت) أن كل من $2 + i\ ,\ 2 - i$ يكون عنصر غير مختزل (irreducible) في الحلقة $\mathbf{Z}[i]$.

٢٢٩. في الحلقة $\mathbf{Z}[\sqrt{10}]$ اثبت أن العناصر $2\ ,\ 3\ ,\ 4 + \sqrt{10}\ ,\ 4 - \sqrt{10}$ تكون غير مختزلة وغير أولية .

الحل: ليكن $a + b\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ عنصر غير صفري . المعكوس الضربي لهذا العنصر (إن وُجد) يكون في الصورة التالية

$$1/(a + b\sqrt{10}) = 1/(a + b\sqrt{10}) \times (a - b\sqrt{10}) / (a - b\sqrt{10})$$
$$= (a - b\sqrt{10}) / (a^2 - 10\,b^2)$$

إذن يوجد معكوس ضربي للعنصر $a + b\sqrt{10}$ في الحلقة $\mathbf{Z}[\sqrt{10}]$ إذا وفقط إذا كان $a^2 - 10\,b^2 = \pm 1$. لاحظ أنة ينتج من تمرين (٢٢٦) (ب) أن $a + b\sqrt{10}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{10}]$ إذا وفقط إذا كان $N(a + b\sqrt{10}) = \pm 1$ ، أي إذا وفقط إذا كان $a^2 - 10\,b^2 = \pm 1$. إذن العناصر $2\ ,\ 3\ ,\ 4 + \sqrt{10}\ ,\ 4 - \sqrt{10}$ لا تكون وحدات في الحلقة $\mathbf{Z}[\sqrt{10}]$ ، لأن $a^2 - 10\,b^2 \neq \pm 1$ أو لأن $N(a + b\sqrt{10}) \neq \pm 1$ لكل

$$a + b\sqrt{10} \in \{2\ ,\ 3\ ,\ 4 + \sqrt{10}\ ,\ 4 - \sqrt{10}\}$$

نفرض الآن أن $a + b\sqrt{10}\ ,\ c + d\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ ، بحيث

$$2 = (a + b\sqrt{10})\ (c + d\sqrt{10})$$

إذن

$$2 = (a - b\sqrt{10})\ (c - d\sqrt{10})$$

إذن

$$(a^2 - 10\,b^2)\ (c^2 - 10\,d^2) = 4$$

نضع $x = a + b\sqrt{10}\ ,\ y = c + d\sqrt{10}$. إذن $N(x)\ N(y) = 4$.

توجد الإحتمالات التالية:

(١) $N(x) = \pm 1\ ,\ N(y) = \pm 4$

في هذة الحالة x يكون وحدة (انظر تمرين (٢٢٦) (ب)) .

(٢) $N(x) = \pm 4\ ,\ N(y) = \pm 1$

في هذة الحالة y يكون وحدة (انظر تمرين (٢٢٦) (ب)) .

(٣) $N(x) = \pm 2 \;,\; N(y) = \pm 2$

إذن في هذة الحالة يكون $c^2 - 10\, d^2 = \pm 2 \;,\; a^2 - 10\, b^2 = \pm 2$. لكن هذا لا يتحقق في $\mathbf{Z}$. إذن هذا الإحتمال مرفوض .

إذن $a + b\sqrt{10}$ أو $c + d\sqrt{10}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{10}]$. إذن 2 يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{10}]$. بالمثل يمكن اثبات أن 3 يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{10}]$. والآن نبين أن العنصر $4 + \sqrt{10}$ يكون غير مختزل في الحلقة $\mathbf{Z}[\sqrt{10}]$. نفرض أن $a + b\sqrt{10} , c + d\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ ، بحيث

$$4 + \sqrt{10} = (a + b\sqrt{10})\,(c + d\sqrt{10})$$

إذن

$$4 - \sqrt{10} = (a - b\sqrt{10})\,(c - d\sqrt{10})$$

إذن

$$(a^2 - 10\, b^2)\,(c^2 - 10\, d^2) = 6$$

نضع $y = c + d\sqrt{10} \;,\; x = a + b\sqrt{10}$. إذن $N(x)\; N(y) = 6$.

توجد الإحتمالات التالية:

(١) $N(x) = \pm 1 \;,\; N(y) = \pm 6$

في هذة الحالة x يكون وحدة (انظر تمرين (٢٢٦) (ب)) .

(٢) $N(x) = \pm 6 \;,\; N(y) = \pm 1$

في هذة الحالة y يكون وحدة (انظر تمرين (٢٢٦) (ب)) .

(٣) $N(x) = \pm 2 \;,\; N(y) = \pm 3$

إذن في هذة الحالة يكون $a^2 - 10\, b^2 = \pm 2$. لكن هذة المعادلة ليس لها حل في $\mathbf{Z}$. إذن هذا الإحتمال مرفوض .

(٤) $N(x) = \pm 3 \;,\; N(y) = \pm 2$

إذن في هذة الحالة يكون $c^2 - 10\, d^2 = \pm 2$. لكن هذة المعادلة ليس لها حل في $\mathbf{Z}$. إذن هذا الإحتمال مرفوض .

إذن $x = a + b\sqrt{10}$ أو $y = c + d\sqrt{10}$ يكون وحدة في الحلقة $\mathbf{Z}[\sqrt{10}]$. إذن $4 + \sqrt{10}$ يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{10}]$. بالمثل يمكن اثبات أن $4 - \sqrt{10}$ يكون عنصر غير مختزل في الحلقة $\mathbf{Z}[\sqrt{10}]$.

والآن نثبت أن العناصر $4-\sqrt{10}\ ,\ 4+\sqrt{10}\ ,\ 3\ ,\ 2$ تكون غير أولية في الحلقة $\mathbf{Z}[\sqrt{10}]$.
بما أن $6 = (4+\sqrt{10})\,(4-\sqrt{10})$ ، فإن $2 \mid (4+\sqrt{10})\,(4-\sqrt{10})$. نفرض أن $2 \mid 4+\sqrt{10}$. إذن يوجد $a+b\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ ، بحيث $4+\sqrt{10} = 2\,(a+b\sqrt{10})$. إذن $1 = 2\,b$. لكن هذه المعادلة ليس لها حل في $\mathbf{Z}$. إذن 2 لا يقسم $4+\sqrt{10}$ في الحلقة $\mathbf{Z}[\sqrt{10}]$. بالمثل 2 لا يقسم $4-\sqrt{10}$ في الحلقة $\mathbf{Z}[\sqrt{10}]$. إذن 2 يكون عنصر غير أولي في الحلقة $\mathbf{Z}[\sqrt{10}]$. أيضاً $3 \mid (4+\sqrt{10})\,(4-\sqrt{10})$. نفرض أن $3 \mid 4+\sqrt{10}$. إذن يوجد $a+b\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ ، بحيث $4+\sqrt{10} = 3\,(a+b\sqrt{10})$. إذن $3\,b = 1$. لكن هذه المعادلة ليس لها حل في $\mathbf{Z}$. إذن 3 لا يقسم $4+\sqrt{10}$ في الحلقة $\mathbf{Z}[\sqrt{10}]$. بالمثل 3 لا يقسم $4-\sqrt{10}$ في الحلقة $\mathbf{Z}[\sqrt{10}]$. إذن 3 يكون عنصر غير أولي في الحلقة $\mathbf{Z}[\sqrt{10}]$.
كذلك $4+\sqrt{10} \mid (4+\sqrt{10})\,(4-\sqrt{10})$. إذن $4+\sqrt{10} \mid 6$. إذن $4+\sqrt{10} \mid 2\times 3$.
نفرض أن $4+\sqrt{10} \mid 2$. إذن يوجد $a+b\sqrt{10} \in \mathbf{Z}[\sqrt{10}]$ ، بحيث $2 = (4+\sqrt{10})\,(a+b\sqrt{10})$. إذن $N(2) = N(4+\sqrt{10})\ \ N(a+b\sqrt{10})$ (لأن N يحفظ عملية الضرب (انظر تمرين (٢٢٦) (أ)) . إذن $3\,a^2 = 30\,b^2 + 2$. لكن هذه المعادلة ليس لها حل في $\mathbf{Z}$. إذن $4+\sqrt{10}$ لا يقسم 2 في الحلقة $\mathbf{Z}[\sqrt{10}]$. بنفس الطريقة ينتج أن $4+\sqrt{10}$ لا يقسم 3 في الحلقة $\mathbf{Z}[\sqrt{10}]$. إذن $4+\sqrt{10}$ يكون عنصر غير أولي في الحلقة $\mathbf{Z}[\sqrt{10}]$. بالمثل يمكن اثبات أن $4-\sqrt{10}$ يكون عنصر غير أولي في الحلقة $\mathbf{Z}[\sqrt{10}]$.

٢٣٠. في الحلقة $\mathbf{Z}[i]$ أوجد كل العناصر الشريكة للعنصر $3-2\,i$.

الحل: ليكن $a+bi \in \mathbf{Z}[i]$ ، بحيث $a+bi \sim 3-2i$. إذن يوجد وحدة $u \in \mathbf{Z}[i]$ ، بحيث $3-2\,i = u\,(a+bi)$. لكن من تمرين (٢١٨) أو تمرين (٢٢٧) ينتج أن $1\ ,\ -1\ ,\ i\ .\ -i$ هي كل الوحدات في الحلقة $\mathbf{Z}[i]$. إذن $u \in \{1\ ,-1\ ,\ i\ ,-i\}$.

عندما $u = 1$ يكون $a+bi = 3-2\,i$.
وعندما $u = -1$ يكون $a+bi = -3+2\,i$.
وعندما $u = i$ يكون $a+bi = -2-3\,i$.
وعندما $u = -i$ يكون $a+bi = 2+3\,i$.
إذن العناصر الشريكة للعنصر $3-2\,i$ في الحلقة $\mathbf{Z}[i]$ هى

$$3-2\,i\ ,\ -3+2\,i\ ,\ -2-3\,i\ ,\ 2+3\,i$$

٢٣١. في الحلقة $\mathbf{Z}[i\sqrt{3}]$ أوجد كل العناصر الشريكة للعنصر $2 + i\sqrt{3}$.

الحل: ليكن $a + bi\sqrt{3} \in \mathbf{Z}[i\sqrt{3}]$ ، بحيث $a + bi\sqrt{3} \sim 2 + i\sqrt{3}$. إذن يوجد وحدة $u \in \mathbf{Z}[i\sqrt{3}]$ ، بحيث $2 + i\sqrt{3} = u\,(a + bi\sqrt{3})$. لكن من تمرين (٢١٨) أو تمرين (٢٢٧) ينتج أن $1 , 1 -$ هى كل الوحدات في الحلقة $\mathbf{Z}[i\sqrt{3}]$. إذن $u \in \{1 , -1\}$.

عندما $u = 1$ يكون $a + bi\sqrt{3} = 2 + i\sqrt{3}$.

وعندما $u = -1$ يكون $a + bi\sqrt{3} = -2 - i\sqrt{3}$.

إذن العناصر الشريكة للعنصر $2+ i\sqrt{3}$ في الحلقة $\mathbf{Z}[i\sqrt{3}]$ هى

$$2 + i\sqrt{3} \;\; , -2 - i\sqrt{3}$$

٢٣٢. في الحلقة $\mathbf{Z}[i\sqrt{5}]$ أوجد كل العناصر الشريكة للعنصر $2 + i\sqrt{5}$.

الحل: ليكن $a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $a + bi\sqrt{5} \sim 2 + i\sqrt{5}$. إذن يوجد وحدة $u \in \mathbf{Z}[i\sqrt{5}]$ ، بحيث $2 + i\sqrt{5} = u\,(a + bi\sqrt{5})$. لكن من تمرين (٢١٨) أو تمرين (٢٢٧) ينتج أن $1 , 1 -$ هى كل الوحدات في الحلقة $\mathbf{Z}[i\sqrt{5}]$. إذن $u \in \{1 , -1\}$.

عندما $u = 1$ يكون $a + bi\sqrt{5} = 2 + i\sqrt{5}$.

وعندما $u = -1$ يكون $a + bi\sqrt{5} = -2 - i\sqrt{5}$.

إذن العناصر الشريكة للعنصر $2+ i\sqrt{5}$ في الحلقة $\mathbf{Z}[i\sqrt{5}]$ هى

$$2 + i\sqrt{5} \, , -2 - i\sqrt{5}$$

٢٣٣. في الحلقة $\mathbf{Z}_{12}$ أوجد كل العناصر الشريكة للعنصر 8 .

الحل: ليكن $x \in \mathbf{Z}_{12}$ ، بحيث $x \sim 8$. إذن يوجد وحدة $u \in \mathbf{Z}_{12}$ ، بحيث $8 = u\,x$. لكن $1 , 5 , 7 , 11$ هي كل الوحدات في الحلقة $\mathbf{Z}_{12}$.

عندما $u = 1$ ، فإن $x = 8$.

وعندما $u = 5$ ، فإن $x = 4$.

وعندما $u = 7$ ، فإن $x = 8$.

وعندما $u = 11$ ، فإن $x = 4$.

إذن $4 , 8 \in \mathbf{Z}_{12}$ هى كل العناصر الشريكة للعنصر 8 في الحلقة $\mathbf{Z}_{12}$.

٢٣٤. في الحلقة $\mathbf{Z}_{10}$ أوجد كل العناصر الشريكة للعنصر 6 .

الحل: ليكن $x \in \mathbf{Z}_{10}$ ، بحيث $x \sim 6$. إذن يوجد وحدة $u \in \mathbf{Z}_{10}$ ، بحيث $6 = u\,x$. لكن 9 , 7 , 3 , 1 هي كل الوحدات في الحلقة $\mathbf{Z}_{10}$. إذن

عندما $u = 1$ ، فإن $x = 6$.

وعندما $u = 3$ ، فإن $x = 2$.

وعندما $u = 7$ ، فإن $x = 8$.

وعندما $u = 9$ ، فإن $x = 4$.

إذن $2 , 4 , 6 , 8 \in \mathbf{Z}_{10}$ هى كل العناصر الشريكة للعنصر 6 في الحلقة $\mathbf{Z}_{10}$.

٢٣٥. ليكن R حلقة متلاشية القوى (nilpotent ring) ، وليكن $f : R \to S$ تشاكل حلقي . برهن أن

(أ) كل حلقة جزئية من R تكون متلاشية القوى .

(ب) $f(R)$ تكون حلقة متلاشية القوى .

الحل: ليكن R حلقة متلاشية القوى (nilpotent ring) ، وليكن $f : R \to S$ تشاكل حلقي . بما أن R متلاشية القوى ، فإنة يوجد $n \in \mathbf{N}$ ، بحيث يكون ضرب أي عناصر من R عددها n يساوي 0 .

(أ) ليكن S حلقة جزئية من R ، وليكن $x_1 , x_2 ,\ldots, x_n \in S$. إذن $x_1 x_2 \ldots x_n \in S \subseteq R$. إذن $x_1 x_2 \ldots x_n = 0$. إذن S تكون متلاشية القوى .

(ب) بما أن $f : R \to S$ تشاكل حلقي ، فإن $f(R)$ تكون حلقة جزئية من R . ليكن $x_1 , x_2 , \ldots , x_n \in f(R)$. إذن يوجد $y_1, y_2 ,\ldots, y_n \in R$ ، بحيث $x_1 = f(y_1) , x_2 = f(y_2) , \ldots , x_n = f(y_n)$. إذن

$$x_1 x_2 \ldots x_n = f(y_1) f(y_2) \ldots f(y_n) = f(y_1 y_2 \ldots y_n) = f(0) = 0$$

إذن $f(R)$ تكون متلاشية القوى .

٢٣٦. ليكن R حلقة ، وليكن I مثالي في R . إذا كان كل من $I , R / I$ حلقة متلاشية القوى (nilpotent ring) ، فبرهن أن R تكون حلقة متلاشية القوى (nilpotent ring) .

الحل: ليكن R حلقة ، وليكن I مثالي في R . نفرض أن كل من I , R / I تكون حلقة متلاشية القوى . إذن يوجد $m,n \in \mathbf{N}$ ، بحيث $(R / I)^n = \{0\} = \{I\}$, $I^m = \{0\}$. ليكن $x_1 , x_2 ,\ldots, x_n \in R$. إذن $x_1 + I ,\ldots, x_n + I \in R / I$. إذن

$$(x_1\, x_2 \ldots x_n) + I = (x_1 + I) \ldots (x_n + I) = I$$

إذن $x_1\, x_2 \ldots x_n \in I$. هذا يعني أن ضرب أي عناصر في R عددها n يكون عنصر في I .

ليكن $a_1 , a_2 ,\ldots, a_{mn} \in R$. إذن

$$(a_1\, a_2 \ldots a_n) , (a_{n+1}\, a_{n+2} \ldots a_{2n}) , \ldots , (a_{(m-1)n+1}\;\; a_{(m-1)n+1}\; \ldots a_{mn}) \in I$$

لكن $I^m = \{0\}$. إذن

$$a_1\, a_2 \ldots a_{mn} = (a_1\, a_2 \ldots a_n)\, (a_{n+1}\, a_{n+2} \ldots a_{2n}) \ldots (a_{(m-1)n+1}\;\; a_{(m-1)n+1} \ldots a_{mn})$$
$$= 0$$

إذن ضرب أي عناصر في R عددها mn يساوي 0 . إذن R تكون حلقة متلاشية القوى .

المثاليات – Ideals

٢٣٧. ليكن R حلقة خالية من قواسم الصفر . إذا كانت كل حلقة جزئية من R مثالي ، فاثبت أن R تكون حلقة ابدالية .

الحل: ليكن R حلقة خالية من قواسم الصفر . نفرض أن كل حلقة جزئية من R تكون مثالي . ليكن $r \in R\backslash\{0\}$ ، وليكن $C(r) = \{\, s \in R \mid s\, r = r\, s \,\}$. من الواضح أن C(r) تكون حلقة جزئية من R . إذن من الفرض بأن كل حلقة جزئية من R تكون مثالي ينتج أن C(r) يكون مثالي في R . إذن $R\, C(r) \subseteq C(r)$. ليكن $s \in R$. إذن $s\, r \in C(r)$. إذن $(s\, r)\, r = r\, (s\, r)$. إذن $(s\, r)\, r - r\, (s\, r) = 0$. إذن $(s\, r - r\, s)\, r = 0$. لكن $r \neq 0$. إذن من الفرض بأن R خالية من قواسم الصفر ينتج أن $s\, r - r\, s = 0$. إذن $s\, r = r\, s$. إذن $s \in C(r)$. إذن $R \subseteq C(r)$. إذن $R = C(r)$. إذن R تكون حلقة ابدالية .

٢٣٨. اثبت أنة يوجد بالضبط تشاكلين حلقيين من **R** إلى **R** .

الحل: ليكن $f : \mathbf{R} \to \mathbf{R}$ تشاكل حلقي . إذن $Ker(f\,)$ يكون مثالي في **R** . لكن **R** يكون حقل . إذن **R** لا يحتوي على مثاليات غير بديهية . إذن $Ker(f\,) = \{0\}$ أو $Ker(f\,) = \mathbf{R}$. إذا كان $Ker(f\,) = \mathbf{R}$ ، فإن $f(x) = 0$ ، لكل $x \in \mathbf{R}$. وبالتالي f في هذة الحالة هو التشاكل الحلقي

الصفري . وإذا كان $Ker(f) = \{0\}$ ، فإنة ينتج من مبرهنة التماثل الأولى (مبرهنة التشاكل في الحلقات أن $\mathbf{R} \cong \mathbf{R} / Ker(f) \cong f(\mathbf{R})$. إذن $f(\mathbf{R}) = \mathbf{R}$. إذن f يكون شامل . إذن f يكون تماثل حلقي . إذن ينتج من تمرين (١٩٦) أن $f(x) = x$ لكل $x \in \mathbf{R}$. إذن يوجد بالضبط تشاكليين حلقيين من $\mathbf{R}$ إلى $\mathbf{R}$ هما التشاكل الصفري وتشاكل الوحدة (أي الذي يرسم كل عنصر إلى نفسة) .

٢٣٩. ليكن R حلقة ، وليكن A,B,C مثاليات في R . إذا كان

$$A : B = \{ r \in R \mid r B \subseteq A\}$$

، فبرهن أن

(أ) $A : B$ يكون مثالي في R .

(ب) $A \subseteq A : B$.

(ت) إذا كان $\{A_i\}_{i \in I}$ فصل مثاليات في R ، فإن

$$\left(\bigcap_{i \in I} A_i\right) : B = \bigcap_{i \in I} (A_i : B)$$

(ث) إذا كان $\{B_i\}_{i \in I}$ فصل مثاليات في R ، فإن

$$A : \Sigma_{i \in I} B_i = \bigcap_{i \in I} (A : B_i)$$

(ج) $A : C B = (A : B) : C$.

الحل: ليكن R حلقة ، وليكن A,B,C مثاليات في R . نفرض أن

$$A : B = \{ r \in R \mid r B \subseteq A\}$$

(أ) ليكن $r,s \in A : B$. إذن $s B \subseteq A$, $r B \subseteq A$. إذن $(r - s) B = r B - s B \subseteq A$ ، لأن A تكون زمرة جزئية جمعية من R . إذن $r - s \in A : B$. إذن $A : B$ تكون زمرة جزئية جمعية من R . ليكن $r \in R , s \in A : B$. إذن $s B \subseteq A$. إذن $(r s) B = r (s B) \subseteq A$ ، لأن A مثالي في R وبالتالي $R A \subseteq A$. إذن $R (A : B) \subseteq A : B$. إذن $A : B$ يكون مثالي في R .

(ب) بما أن A مثالي في R ، فإن $A R \subseteq A$. إذن $A B \subseteq A$. إذن $a B \subseteq A$ ، لكل $a \in A$. إذن $a \in A : B$ ، لكل $a \in A$. إذن $A \subseteq A : B$.

(ت) ليكن $\{A_i\}_{i \in I}$ فصل مثاليات في R . إذن $\bigcap_{i \in I} A_i$ يكون مثالي في R . ليكن $r \in (\bigcap_{i \in I} A_i) : B$. إذن $r B \subseteq \bigcap_{i \in I} A_i$. إذن $r B \subseteq A_i$ ، لكل $i \in I$. إذن $r \in A_i : B$ ، لكل $i \in I$. إذن $r \in \bigcap_{i \in I} (A_i : B)$. إذن

$$(\bigcap_{i \in I} A_i) : B \subseteq \bigcap_{i \in I} (A_i : B)$$

ليكن $s \in \bigcap_{i \in I} (A_i : B)$. إذن $s \in A_i : B$ ، لكل $i \in I$. إذن $s B \subseteq A_i$ ، لكل $i \in I$. إذن $s B \subseteq \bigcap_{i \in I} A_i$. إذن $s \in (\bigcap_{i \in I} A_i) : B$. إذن

$$\bigcap_{i \in I} (A_i : B) \subseteq (\bigcap_{i \in I} A_i) : B$$

إذن

$$(\bigcap_{i \in I} A_i) : B = \bigcap_{i \in I} (A_i : B)$$

(ث) ليكن $\{B_i\}_{i \in I}$ فصل مثاليات في R . إذن $\Sigma_{i \in I} B_i$ يكون مثالي في R . ليكن $r \in A : \Sigma_{i \in I} B_i$. إذن $r (\Sigma_{i \in I} B_i) \subseteq A$. إذن $\Sigma_{i \in I} r B_i \subseteq A$. إذن $r B_i \subseteq A$ ، لكل $i \in I$. إذن $r \in A : B_i$ ، لكل $i \in I$. إذن $r \in \bigcap_{i \in I} (A : B_i)$. إذن

$$A : \Sigma_{i \in I} B_i \subseteq \bigcap_{i \in I} (A : B_i)$$

ليكن $s \in \bigcap_{i \in I} (A : B_i)$. إذن $s \in A : B_i$ ، لكل $i \in I$. إذن $s B_i \subseteq A$ ، لكل $i \in I$. إذن $\Sigma_{i \in I} s B_i \subseteq A$. إذن $s (\Sigma_{i \in I} B_i) \subseteq A$. إذن $s \in A : \Sigma_{i \in I} B_i$. إذن

$$\bigcap_{i \in I} (A : B_i) \subseteq A : \Sigma_{i \in I} B_i$$

إذن

$$A : \Sigma_{i \in I} B_i = \bigcap_{i \in I} (A : B_i)$$

(ج) ليكن $r \in A : C B$. إذن $r (C B) \subseteq A$. إذن $(r C) B \subseteq A$. إذن $(r c) B \subseteq A$ ، لكل $c \in C$. إذن $r c \in A : B$ ، لكل $c \in C$. إذن $r C \subseteq A : B$. إذن $r \in (A : B) : C$. إذن $A : C B \subseteq (A : B) : C$. ليكن $s \in (A : B) : C$. إذن $s C \subseteq A : B$. إذن $s c \in A : B$ ، لكل $c \in C$. إذن $s c B \subseteq A$ ، لكل $c \in C$. إذن $s (C B) \subseteq A$. إذن $s \in A : C B$. إذن $(A : B) : C \subseteq A : C B$. إذن $A : C B = (A : B) : C$.

٢٤٠. برهن أن $\mathbf{Z}[\sqrt{2}]$ يكون مثالي في الحلقة $\mathbf{R}$ مولد بالعنصرين $3+\sqrt{2}\ ,\ 2+3\sqrt{2}$.

الحل: ليكن $a+b\sqrt{2}\ ,\ c+d\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$. إذن

$$(a+b\sqrt{2}) - (c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbf{Z}[\sqrt{2}]\ ,$$

$$(a+b\sqrt{2})\,(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in \mathbf{Z}[\sqrt{2}]\ .$$

إذن $\mathbf{Z}[\sqrt{2}]$ تكون حلقة جزئية من الحلقة $\mathbf{R}$. نبين أن $\mathbf{R}\,(\mathbf{Z}[\sqrt{2}]) \subseteq \mathbf{Z}[\sqrt{2}]$. ليكن $r \in R$. إذن $r\,(a+b\sqrt{2}) = ra+rb\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$. لاحظ أن عملية ضرب الأعداد تكون ابدالية . إذن $\mathbf{Z}[\sqrt{2}]$ يكون مثالي في الحلقة $\mathbf{R}$. والآن نبين أن المثالي $\mathbf{Z}[\sqrt{2}]$ يتولد بالعنصرين $3+\sqrt{2}\ ,\ 2+3\sqrt{2}$ ، أي نبين أن $\mathbf{Z}[\sqrt{2}] = \langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle$. بما أن $\mathbf{R}$ حلقة ابدالية وتحتوي محايد ، فإن

$$\langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle = \{\, r\,(3+\sqrt{2}) + s\,(2+3\sqrt{2}) \mid r\,,s \in \mathbf{R} \,\}$$

ليكن $a+b\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$. نضع $a+b\sqrt{2} = x\,(3+\sqrt{2}) + y\,(2+3\sqrt{2})$. إذن

$$3x + 2y = a \quad , \quad x + 3y = b$$

بحل هاتين المعادلتين نحصل على $x = (3a-2b)/7\ ,\ y = (3b-a)/7$. إذن $x\,,y \in \mathbf{R}$. إذن $a+b\sqrt{2} \in \langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle$. إذن

$$\mathbf{Z}[\sqrt{2}] \subseteq \langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle$$

لكن

$$\langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle \subseteq \mathbf{Z}[\sqrt{2}]$$

إذن $\mathbf{Z}[\sqrt{2}] = \langle 3+\sqrt{2}\ ,\ 2+3\sqrt{2} \rangle$.

٢٤١. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I هي مجموعة كل العناصر المتلاشية القوى (nilpotent elements) في R . برهن أن

(أ) I يكون مثالي في R .

(ب) R / I لا يحتوي على عناصر متلاشية القوى غير العنصر الصفري .

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I هي مجموعة كل العناصر المتلاشية القوى في R .

(أ) من الواضح أن $0 \in I$. إذن $I \neq \emptyset$. ليكن $x,y \in I$. إذن يوجد $m,n \in \mathbf{N}$ ، بحيث $x^m = 0$, $y^n = 0$. إذن ينتج من مبرهنة ذات الحدين (Binomial theorem) أن $(x - y)^{m+n} = 0$. إذن $x - y$ يكون عنصر متلاشي القوى في R . إذن $x - y \in I$. إذن I تكون زمرة جزئية جمعية من الزمرة $(R , +)$. ليكن $r \in R$. بما أن R حلقة ابدالية ، فإن $(r\,x)^m = r^m x^m = 0$. إذن $r\,x$ يكون عنصر متلاشي القوى في R . إذن $r\,x \in I$. إذن $R\,I \subseteq I$. وبالتالي $I\,R \subseteq I$ (لأن R حلقة ابدالية) . إذن I يكون مثالي في R .

(ب) ليكن $x + I \in R / I$ عنصر متلاشي القوى . إذن يوجد $m \in \mathbf{N}$ ، بحيث $(x + I)^m = I$. إذن $x^m + I = I$. إذن $x^m \in I$. إذن x^m يكون عنصر متلاشي القوى في R . إذن يوجد $n \in \mathbf{N}$ ، بحيث $(x^m)^n = 0$. إذن $x^{mn} = 0$. إذن x يكون عنصر متلاشي القوى في R . إذن $x \in I$. إذن $x + I = I$. إذن R / I لا يحتوي على عناصر متلاشية القوى غير العنصر الصفري .

٢٤٢. ليكن R حلقة ، وليكن I , J مثاليين في R . برهن أن

$$R = I + J \iff x + I \cap y + J \neq \emptyset \;\; , \forall\, x,y \in R$$

الحل: ليكن R حلقة ، وليكن I , J مثاليين في R .

($\Leftarrow$) ليكن $x + I \cap y + J \neq \emptyset$ ، لكل $x,y \in R$. ليكن $x \in R , y \in J$. إذن $x + I \cap J \neq \emptyset$. إذن يوجد $a \in I , b \in J$ ، بحيث $x + a = b$. إذن $x = - a + b$. إذن $x \in I + J$. إذن $R \subseteq I + J$. $R = I + J$.

($\Rightarrow$) ليكن $R = I + J$. ليكن $x,y \in R$. إذن يوجد $a,u \in I , b,v \in J$ ، بحيث $x = a + b , y = u + v$. إذن $x + I = b + I$, $y + J = u + J$. إذن

$$b + u \in b + I \cap u + J = x + I \cap y + J$$

إذن $x + I \cap y + J \neq \emptyset$ ، لكل $x,y \in R$.

٢٤٣. ليكن R حلقة ابدالية ، بحيث $1 \in R$. وليكن I , J مثاليين غير صفريين في R ، بحيث $I \cap J = \{0\} , I + J = R$. برهن أن $R \cong I \times J$.

الحل: ليكن R حلقة ابدالية ، بحيث $1 \in R$. وليكن I , J مثاليين غير صفريين في R ، بحيث $I \cap J = \{0\} , I + J = R$. بما أن I , J مثاليين في R ، فإن كل من I , J يكون حلقة جزئية من R . إذن $I \times J$ يكون حلقة (بالنسبة لعمليتي جمع وضرب المركبات) . بما أن

$1 \in R$, $I + J = R$ ، فإنة يوجد $a \in I$, $b \in J$ بحيث $a + b = 1$. ليكن $u \in I$. إذن $a\,u + b\,u = u$. بما أن $I \cap J = \{0\}$, $b\,u \in I \cap J$ ، فإن $b\,u = 0$. إذن $u\,a = a\,u = u$ ، لكل $u \in I$ (لأن الحلقة R ابدالية) . إذن a يكون عنصر محايد (ضربي) في الحلقة (الجزئية) I . ليكن $v \in J$. إذن $a\,v + b\,v = v$. بما أن $I \cap J = \{0\}$, $a\,v \in I \cap J$ ، فإن $a\,v = 0$. إذن $v\,b = b\,v = v$ ، لكل $v \in J$ (لأن الحلقة R ابدالية) . إذن b يكون عنصر محايد (ضربي) في الحلقة (الجزئية) J . إذن (a , b) يكون عنصر محايد في الحلقة $I \times J$. ليكن $f : R \to I \times J$ ، بحيث $f(r) = (u , v)$ حيث $u + v = r$ لكل $r \in R$. نبرهن أن f يكون تماثل حلقي . بما أن $I + J = R$, $I \cap J = \{0\}$ ، فإن $R = I \oplus J$. وبالتالي كل عنصر $r \in R$ لة تمثيلاً وحيداً في الصورة $r = a + b$ ، حيث $a \in I$, $b \in J$. ليكن $r,r' \in R$. إذن يوجد $a,a' \in I$, $b,b' \in J$ ، بحيث $r = a + b$, $r' = a' + b'$. إذن

$$r = r' \iff r = a + b = a' + b' = r' \ , a,a' \in I , b,b' \in J$$
$$\iff a = a' , b = b' \ , a,a' \in I , b,b' \in J$$
$$\iff f(r) = (a , b) = (a' , b') = f(r') \ , a,a' \in I , b,b' \in J$$

إذن f يكون تطبيق معرف جيداً ومتباين . ومن الواضح أن f يكون شامل أيضاً . إذن f يكون تقابل . كذلك

$$f(r + r') = f(a + b + a' + b') = f((a + a') + (b + b')) = ((a + a') , (b + b'))$$
$$= (a , b) + (a' , b') = f(r) + f(r') \ ,$$
$$f(r\,r') = f((a + b)\,(a' + b')) = f(a\,a' + a\,b' + a'\,b + b\,b') = f(a\,a' + b\,b')$$
$$= (a\,a' , b\,b') = (a , b)\,(a' , b') = f(r)\,f(r')$$

إذن f يكون تشاكل حلقي . وبما أن f تقابل ، فإن f يكون تماثل حلقي .

٢٤٤. ليكن R حلقة ، وليكن $a \in R$ عنصر ثابت . ليكن $* : R \times R \to R$ بحيث $x * y = x\,a\,y$ لكل $x,y \in R$. برهن أن

(أ) $*$ تكون عملية ثنائية داخلية على R .

(ب) $R^{\wedge} = (R , + , *)$ يكون حلقة ، حيث + هي عملية الجمع على الحلقة R .

(ت) $I = \{x \in R \mid a\,x\,a = 0\}$ يكون مثالي في الحلقة $R^{\wedge}$.

(ث) ليكن $r \in R \setminus I$ ، بحيث $a\,r\,a = a$. إذن الحلقة $R^{\wedge}/ I$ تحتوي محايد .

الحل: ليكن R حلقة ، وليكن $a \in R$ عنصر ثابت ، وليكن $* : R \times R \to R$ بحيث $x * y = x\,a\,y$ لكل $x,y \in R$.

(أ) لاحظ أولاً أن $x * y = x\,a\,y \in R$ لكل $x,y \in R$. ليكن $(x , y) , (x' , y') \in R \times R$. إذن

$$(x , y) = (x' , y') \Leftrightarrow x = x' \;,\; y = y' \Rightarrow x\,a\,y = x'\,a\,y'$$
$$\Leftrightarrow x * y = x' * y'$$

إذن $*$ يكون تطبيق معرف جيداً . إذن $*$ تكون عملية ثنائية داخلية على R .

(ب) ليكن $x,y,z \in R$. إذن $x * y = x\,a\,y \in R$. إذن R تكون مغلقة بالنسبة للعملية $*$. وبما أن عملية الضرب على الحلقة R دامجة ، فإن

$$x * (y * z) = x\,a\,(y\,a\,z) = (x\,a\,y)\,a\,z = (x * y)\,a\,z = (x * y) * z$$

إذن $*$ تكون عملية دامجة . وبما أن عملية الضرب على الحلقة R موزعة شمالياً ويمينياً بالنسبة لعملية الجمع ، فإن

$$x * (y + z) = x\,a\,(y + z) = x\,a\,y + x\,a\,z = (x * y) + (x * z) \;,$$
$$(y + z) * x = (y + z)\,a\,x = y\,a\,x + z\,a\,x = (y * x) + (z * x)$$

إذن العملية $*$ تكون موزعة شمالياً ويمينياً بالنسبة لعملية الجمع + . إذن $R^\wedge$ تكون حلقة .

(ت) ليكن $I = \{x \in R \mid a\,x\,a = 0\}$. ليكن $x,y \in I$. إذن

$$a\,(x - y)\,a = a\,x\,a - a\,y\,a = 0$$

إذن $x - y \in I$. إذن I يكون زمرة جزئية من الزمرة $(R , +)$. ليكن $r \in R$. إذن

$$a\,(r * x)\,a = a\,(r\,a\,x)\,a = a\,r\,(a\,x\,a) = a\,r\,0 = 0$$

إذن $r * x \in I$ ، لكل $x \in I , r \in R$. إذن $R * I \subseteq I$. كذلك

$$a\,(x * r)\,a = a\,(x\,a\,r)\,a = (a\,x\,a)\,r\,a = 0\,r\,a = 0$$

إذن $x * r \in I$ ، لكل $x \in I , r \in R$. إذن $I * R \subseteq I$. إذن I يكون مثالي في الحلقة $R^\wedge$.

(ث) ليكن $r \in R \setminus I$ ، بحيث $a\,r\,a = a$. ليكن $x + I \in R^\wedge / I$. إذن

$$a\,(r\,a\,x - x)\,a = (a\,r\,a)\,x\,a - a\,x\,a = a\,x\,a - a\,x\,a = 0$$

إذن $r\,a\,x - x \in I$. إذن $(r\,a\,x) + I = x + I$. كذلك

$$a\,(x\,a\,r - x)\,a = a\,x\,(a\,r\,a) - a\,x\,a = a\,x\,a - a\,x\,a = 0$$

إذن $x\,a\,r - x \in I$. إذن $(x\,a\,r) + I = x + I$.

إذن

$$(r + I) * (x + I) = (r * x) + I = (r\ a\ x) + I = x + I\ ,$$
$$(x + I) * (r + I) = (x * r) + I = (x\ a\ r) + I = x + I$$

إذن $r + I$ يكون عنصر محايد في الحلقة $R^{\wedge}/ I$.

٢٤٥. ليكن R حلقة وليكن $1 \in R$. وليكن I مثالي في حلقة المصفوفات $R^{n \times n}$. اثبت أنة يوجد مثالي J في R ، بحيث $I = J^{n \times n}$. أوجد كذلك كل المثاليات في الحلقة $(\mathbf{Z} /12\mathbf{Z})^{n \times n}$.

الحل: ليكن R حلقة وليكن $1 \in R$. وليكن I مثالي في حلقة المصفوفات $R^{n \times n}$. ليكن J هي مجموعة كل عناصر المصفوفات التي تنتمي إلى I . ليكن $x,y \in J$. إذن يوجد $A = [a_{ij}]\ , B = [b_{ij}]$ في I ، بحيث $x = a_{ij}\ , y = b_{st}$ حيث $i,j,s,t \in \{1,2,\ldots,n\}$. لاحظ أن تبديل أي صفين أو عمودين في مصفوفة ما في I يعطي مصفوفة في I ايضاً (لأن: ليكن $C \in I$. وليكن $I_{s,t}$ هي مصفوفة الوحدة في $R^{n \times n}$ بعد تبديل الصفين رقمي s , t . إذن $I_{s,t}\ C \in I$ ، لأن $I \subseteq I$ $R^{n \times n}$. لاحظ أن $I_{s,t}\ C$ هي المصفوفة C بعد تبديل الصفين رقمي s , t . ليكن $I^{s,t}$ هي مصفوفة الوحدة في $R^{n \times n}$ بعد تبديل العمودين رقمي s , t . إذن $C\ I^{s,t} \in I$ ، لأن $I\ R^{n \times n} \subseteq I$. لاحظ أن $C\ I^{s,t}$ هي المصفوفة C بعد تبديل العمودين رقمي s , t) . ليكن $D = (I_{i,s}\ B)\ I^{t,j}$. إذن $d_{ij} = b_{st}$. بما أن $A,D \in I$ ، فإن $A - D \in I$. بما أن $x - y = a_{ij} - b_{st} = a_{ij} - d_{ij}$ ، فإن $x - y$ هو العنصر رقم ij في المصفوفة $A - D \in I$. إذن $x - y \in J$. إذن J تكون زمرة جزئية من الزمرة $(R , +)$. ليكن $r \in R$. وليكن E هي مصفوفة الوحدة في الحلقة $R^{n \times n}$ بعد ضرب الصف رقم i في r . لاحظ أن $E\ A \in I$ وأن $E\ A$ هي المصفوفة A بعد ضرب الصف رقم i في r من الشمال . إذن $r\ x = r\ a_{ij}$ هو العنصر رقم ij في المصفوفة $E\ A$. إذن $r\ x \in J$. إذن $R\ J \subseteq J$. ليكن K هي مصفوفة الوحدة في الحلقة $R^{n \times n}$ بعد ضرب العمود رقم j في r . لاحظ أن $A\ K \in I$ وأن $A\ K$ هي المصفوفة A بعد ضرب العمود رقم j في r من اليمين . إذن $x\ r = a_{ij}\ r$ هو العنصر رقم ij في المصفوفة $A\ K$. إذن $x\ r \in J$. إذن $J\ R \subseteq J$. إذن J يكون مثالي في R . إذن $I = J^{n \times n}$. لاحظ أن

$$\mathbf{Z} / 12\mathbf{Z}\ ,\ 2\mathbf{Z} / 12\mathbf{Z}\ , 3\mathbf{Z} / 12\mathbf{Z}\ ,\ 4\mathbf{Z} / 12\mathbf{Z}\ ,\ 6\mathbf{Z} / 12\mathbf{Z}\ , \{0\}\ .$$

هي كل المثاليات في الحلقة $\mathbf{Z} / 12\mathbf{Z}$.

إذن كل المثاليات في الحلقة $(\mathbf{Z}/12\mathbf{Z})^{n \times n}$ هي

$(\mathbf{Z}/12\mathbf{Z})^{n \times n}$, $(2\mathbf{Z}/12\mathbf{Z})^{n \times n}$, $(3\mathbf{Z}/12\mathbf{Z})^{n \times n}$, $(4\mathbf{Z}/12\mathbf{Z})^{n \times n}$, $(6\mathbf{Z}/12\mathbf{Z})^{n \times n}$, $\{0\}$.

٢٤٦. ليكن R مجال متكامل (integral domain) ، وليكن $x,y \in R\backslash\{0\}$. برهن أن
y قاسم فعلي (proper divisor) لـ x $\Leftrightarrow$ $< x > \subset < y >$

الحل: ليكن R مجال متكامل (integral domain) ، وليكن $x,y \in R\backslash\{0\}$.

($\Leftarrow$) نفرض أن y قاسم فعلي لـ x . إذن $y \mid x$ و y ليس وحدة و x ليس شريك لـ y . إذن يوجد $a \in R \setminus R^*$ ، بحيث $x = a\,y$ (حيث R^* هي مجموعة الوحدات في R) . بما R مجال متكامل (بالتالي يكون ابدالي ويحتوي محايد) ، فإن $< y > = R\,y$, $< x > = R\,x$. بما أن $x = a\,y$ ، فإن $x \in < y >$. إذن $< x > \subseteq < y >$. نبين الآن أن $< x > \neq < y >$. نفرض أن $< x > = < y >$. إذن $y \in < x >$. إذن يوجد $b \in R$ ، بحيث $y = b\,x$. إذن $x = a\,y = a\,b\,x$. إذن $(1 - a\,b)\,x = 0$. لكن R خالي من قواسم الصفر (لأنة مجال متكامل) . إذن $1 - a\,b = 0$ (لأن $x \neq 0$) . إذن $a\,b = 1$. إذن a يكون وحدة ، أي أن $a \in R^*$. وهذا يتناقض مع الفرض $a \in R \setminus R^*$. إذن $< x > \neq < y >$. إذن $< x > \subset < y >$.

($\Rightarrow$) ليكن $< x > \subset < y >$. إذن $x \in < y > = R\,y$. إذن يوجد $r \in R$ ، بحيث $x = r\,y$. إذن $y \mid x$. نفرض أن $r \in R^*$ ، أي نفرض أن r يكون وحدة . إذن يوجد $s \in R$ ، بحيث $r\,s = 1$. إذن $y = r^{-1} x = s\,x$. إذن $y \in < x > = R\,x$. إذن $< y > \subseteq < x >$. إذن $< x > = < y >$. لكن هذا يتناقض مع الفرض بأن $< x > \neq < y >$. إذن $r \notin R^*$. إذن y يكون قاسم فعلي لـ x .

٢٤٧. ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$$\sqrt{I} = \{ x \in R \mid \exists\, n \in \mathbf{N} , \text{s. t. } x^n \in I\}$$

($\sqrt{I}$ يسمى جذر I (radical of I) ويسمى أيضاً جذر تلاشي I (nil radical of I))

برهن أن

(أ) $\sqrt{I}$ يكون مثالي في R ويحتوي I .

(ب) $\sqrt{(\sqrt{I})} = \sqrt{I}$.

الحل: ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$$\sqrt{I} = \{ x \in R \mid \exists\, n \in \mathbf{N} \text{, s. t. } x^n \in I\}$$

(أ) من الواضح أن $0 \in \sqrt{I}$. إذن $\sqrt{I} \neq \emptyset$. ليكن $x,y \in \sqrt{I}$. إذن يوجد $m,n \in \mathbf{N}$ ، بحيث $x^m , y^n \in I$. إذن $(x-y)^{m+n-1} \in I$. إذن $x - y \in \sqrt{I}$. إذن $\sqrt{I}$ يكون زمرة جزئية جمعية من الزمرة $(R , +)$. ليكن $r \in R$. إذن $(r\,x)^m = r^m x^m$ ، لأن R حلقة ابدالية . إذن $(r\,x)^m \in I$. إذن $r\,x \in \sqrt{I}$. إذن $R\sqrt{I} \subseteq \sqrt{I}$. إذن $\sqrt{I}$ يكون مثالي في R . ومن الواضح أن $I \subseteq \sqrt{I}$.

حل آخر: نعتبر المجموعة الجزئية K من R / I المعرفة كما يلي:

$x + I \in K$ إذا وفقط إذا كان $x + I$ عنصر متلاشي القوى (nilpotent)

أي أن K هي مجموعة كل العناصر المتلاشية القوى في الحلقة R / I . إذن ينتج من تمرين (٢٤١) (أ) أن K تكون مثالي في الحلقة R / I . ليكن $\pi : R \to R / I$ هو التشاكل القانوني (canonical homomorphism) . إذن $\pi(x) = x + I \;,\; \forall\, x \in R$. بما أن K مثالي في R ، فإن $\pi^{-1}(K)$ يكون مثالي في R . لاحظ أن

$$\begin{aligned} x \in \sqrt{I} &\Leftrightarrow \exists\, n \in \mathbf{N} \text{ s. t. } x^n \in I \\ &\Leftrightarrow \exists\, n \in \mathbf{N} \text{ s. t. } (x + I)^n = I \\ &\Leftrightarrow x + I \in K \end{aligned}$$

إذن

$$\begin{aligned} \pi^{-1}(K) &= \{x \in R \mid \pi(x) \in K\} \\ &= \{x \in R \mid x + I \in K\} \\ &= \{x \in R \mid x \in \sqrt{I}\} \\ &= \sqrt{I} \end{aligned}$$

إذن $\sqrt{I}$ يكون مثالي في R ويحتوي I .

(ب)

$$\begin{aligned} x \in \sqrt{(\sqrt{I}\,)} &\Rightarrow \exists\, m \in \mathbf{N} \text{ s. t. } x^m \in \sqrt{I} \Rightarrow \exists\, n \in \mathbf{N} \text{, s. t. } (x^m)^n \in I \\ &\Rightarrow x^{mn} \in I \Rightarrow x \in \sqrt{I} \end{aligned}$$

إذن $\sqrt{(\sqrt{I}\,)} \subseteq \sqrt{I}$. لكن من (أ) يكون $\sqrt{I} \subseteq \sqrt{(\sqrt{I}\,)}$. إذن $\sqrt{(\sqrt{I}\,)} = \sqrt{I}$.

٢٤٨. ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي . ليكن I , J مثاليين في R , S على الترتيب . برهن أن

(أ) $f(\sqrt{I}) \subseteq \sqrt{f(I)}$ ، ويحدث التساوي إذا كان f شامل و $Ker(f) \subseteq I$.

(ب) $\sqrt{f^{-1}(J)} = f^{-1}(\sqrt{J})$.

الحل: ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي . ليكن I , J مثاليين في R , S على الترتيب . كما في التمرين السابق ، فإن $\sqrt{I}$ يكون مثالي في R ومعرف كما يلي

$$\sqrt{I} = \{ x \in R \mid \exists\, n \in \mathbf{N} , \text{s. t. } x^n \in I\}$$

(أ) ليكن $x \in f(\sqrt{I})$. إذن يوجد $y \in \sqrt{I}$ ، بحيث $x = f(y)$. بما أن $y \in \sqrt{I}$ ، فإنة يوجد $n \in \mathbf{N}$ بحيث $y^n \in I$. لكن f تشاكل حلقي . إذن $x^n = (f(y))^n = f(y^n) \in f(I)$. إذن $x \in \sqrt{f(I)}$. إذن $f(\sqrt{I}) \subseteq \sqrt{f(I)}$. ليكن f شامل و $Ker(f) \subseteq I$. نبرهن أن $\sqrt{f(I)} \subseteq f(\sqrt{I})$. ليكن $y \in \sqrt{f(I)}$. إذن يوجد $n \in \mathbf{N}$ بحيث $y^n \in f(I)$. إذن يوجد $x \in I$ ، بحيث $y^n = f(x)$. لكن f تشاكل حلقي شامل و $y \in S$. إذن يوجد $a \in R$ ، بحيث $f(a) = y$. إذن

$$f(x) = y^n = (f(a))^n = f(a^n)$$

إذن $f(x) - f(a^n) = f(x - a^n) = 0$. إذن $x - a^n \in Ker(f)$. لكن $Ker(f) \subseteq I$. إذن $x - a^n \in I$. لكن $x \in I$. إذن $a^n \in I$. إذن $a \in \sqrt{I}$. إذن $y \in f(\sqrt{I})$. إذن $\sqrt{f(I)} \subseteq f(\sqrt{I})$. إذن $f(\sqrt{I}) = \sqrt{f(I)}$.

(ب) ليكن $x \in \sqrt{f^{-1}(J)}$. يوجد $n \in \mathbf{N}$ بحيث $x^n \in f^{-1}(J)$. إذن $f(x^n) \in J$. إذن $(f(x))^n \in J$. إذن $f(x) \in \sqrt{J}$. إذن $x \in f^{-1}(\sqrt{J})$. إذن $\sqrt{f^{-1}(J)} \subseteq f^{-1}(\sqrt{J})$. ليكن $x \in f^{-1}(\sqrt{J})$. إذن $f(x) \in \sqrt{J}$. إذن يوجد $m \in \mathbf{N}$ ، بحيث $(f(x))^m \in J$. إذن $f(x^m) \in J$. إذن $x^m \in f^{-1}(J)$. إذن $x \in \sqrt{f^{-1}(J)}$. إذن $f^{-1}(\sqrt{J}) \subseteq \sqrt{f^{-1}(J)}$. إذن $\sqrt{f^{-1}(J)} = f^{-1}(\sqrt{J})$.

٢٤٩. ليكن R حلقة ابدالية تحتوي محايد . برهن أن $R[x] / \langle x \rangle \cong R$.

الحل: ليكن R حلقة ابدالية تحتوي محايد . إذن $R[x]$ تكون حلقة ابدالية تحتوي محايد . إذن $\langle x \rangle = x R[x]$. أي أن $\langle x \rangle = \{ x f(x) \mid f(x) \in R[x] \}$. ليكن

$\alpha : R[x] \to R$ ، بحيث $\alpha(\Sigma a_i x^i) = a_0$ لكل $\Sigma a_i x^i \in R[x]$ حيث a_0 هو الحد الثابت (المطلق) في كثيرة الحدود $\Sigma a_i x^i$. أي أن α ترسم كل كثيرة حدود في $R[x]$ إلى حدها الثابت . ليكن $f(x) , g(x) \in R[x]$ ، وليكن

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad , \quad g(x) = b_0 + b_1 x + \ldots + b_m x^m$$

إذا كان $f(x) = g(x)$ ، فإن $a_0 = b_0$ وبالتالي $\alpha(f(x)) = \alpha(g(x))$. إذن α يكون تطبيق معرف جيداً (well define mapping) . كذلك من الواضح أن

$$\alpha(f(x) + g(x)) = a_0 + b_0 = \alpha(f(x)) + \alpha(g(x)) \ ,$$
$$\alpha(f(x)\, g(x)) = a_0\, b_0 = \alpha(f(x))\, \alpha(g(x))$$

إذن α يكون تشاكل حلقي . ليكن $a \in R$. إذن

$$\alpha(a + a_1 x + \ldots + a_n x^n) = a \quad , \forall\, a_1,a_2,\ldots,a_n \in R$$

إذن α يكون شامل . إذن ينتج من مبرهنة التماثل الأولى في الحلقات أن

$$R[x] / Ker(\alpha) \ \cong R$$

لكن

$$Ker(\alpha) = \{ \Sigma a_i x^i \in R[x] \mid a_0 = 0 \}$$

إذن $x\, f(x) \in Ker(\alpha)$ ، لكل $f(x) \in R[x]$. إذن $x\, R[x] \subseteq Ker(\alpha)$. ليكن $g(x) \in Ker(\alpha)$. إذن

$$g(x) = b_1 x + b_2 x^2 + \ldots + b_m x^m$$
$$= x\, (b_1 + b_2 x + \ldots + b_m x^{m-1})$$

إذن $g(x) \in x\, R[x]$. إذن $Ker(\alpha) \subseteq x\, R[x]$. إذن $Ker(\alpha) = x\, R[x]$. إذن

$$R[x] / < x > \ \cong \ R$$

المثاليات العظيمة Maximal ideals

٢٥٠. اثبت أن أي مثالي غير بديهي في الحلقة $\mathbf{Z}_{15}$ يكون مثالي عظيم (maximal ideal) .

الحل: لاحظ أن $\mathbf{Z}_{15}$ تكون زمرة دائرية ، وبالتالي كل زمرة جزئية منها تكون دائرية . لاحظ كذلك أن كل زمرة جزئية من $\mathbf{Z}_{15}$ تكون مثالي في $\mathbf{Z}_{15}$. بما أن

$$\mathbf{Z}_{15} = < \overline{m} > \ \Leftrightarrow \ (m\, , 15) = 1$$

، فإن

$$\mathbf{Z}_{15} = <\ \overline{1} > = <\ \overline{2} > = <\ \overline{4} > = <\ \overline{7} > = <\ \overline{8} > = <\ \overline{11} > = <\ \overline{13} >$$
$$= <\ \overline{14} >$$

وبما أن

$$<\ \overline{a} > = <\ \overline{b} > \ \Leftrightarrow\ (a\,, b) \neq 1$$

، فإنة يكون في $\mathbf{Z}_{15}$

$$<\ \overline{3} > = <\ \overline{6} > = <\ \overline{9} > = <\ \overline{12} > \quad , \quad <\ \overline{5} > = <\ \overline{10} >$$

إذن يوجد في $\mathbf{Z}_{15}$ مثاليين غير بديهيين فقط هما $<\ \overline{3} > , <\ \overline{5} >$ ، وكل منهما يكون مثالي عظيم لأنة لا يوجد في $\mathbf{Z}_{15}$ مثالي I بحيث $<\ \overline{3} > \subset I \subset \mathbf{Z}_{15}$ أو $<\ \overline{5} > \subset I \subset \mathbf{Z}_{15}$.

حل آخر: لاحظ أن $\mathbf{Z}_{15} \cong \mathbf{Z}\,/15\mathbf{Z}$. إذن كل مثالي غير بديهي في $\mathbf{Z}_{15}$ يماثل مثالي غير بديهي في $\mathbf{Z}\,/15\mathbf{Z}$. المثاليات غير البديهية في $\mathbf{Z}\,/15\mathbf{Z}$ هي $5\mathbf{Z}\,/15\mathbf{Z}\ ,\ 3\mathbf{Z}\,/15\mathbf{Z}$. من مبرهنة التماثل الثالثة في الحلقات ينتج أن

$$(\mathbf{Z}\,/15\mathbf{Z})\,/\,(3\mathbf{Z}\,/15\mathbf{Z}) \ \cong\ \mathbf{Z}\,/3\mathbf{Z} \ \cong\ \mathbf{Z}_3\ ,$$

$$(\mathbf{Z}\,/15\mathbf{Z})\,/\,(5\mathbf{Z}\,/15\mathbf{Z}) \ \cong\ \mathbf{Z}\,/5\mathbf{Z} \ \cong\ \mathbf{Z}_5$$

لكن كل من $\mathbf{Z}_3\ , \mathbf{Z}_5$ يكون حقل (field) . إذن المثاليان $5\mathbf{Z}\,/15\mathbf{Z}\ ,\ 3\mathbf{Z}\,/15\mathbf{Z}$ يكونان عظيمين . وذلك ينتج من المبرهنة (ليكن I مثالي في حلقة R . إذن R/I يكون حقل إذا وفقط إذا كان I مثالي عظيم) . إذن يوجد في $\mathbf{Z}_{15}$ مثاليين عظيمين فقط أحدهما يماثل $\mathbf{Z}_5$ وهو $<\ \overline{3} >$ والآخر يماثل $\mathbf{Z}_3$ وهو $<\ \overline{5} >$.

٢٥١. إذا كان p عدد أولي قاسم للعدد $n \in \mathbf{N}$ ، فاثبت أن $<\ \overline{p} >$ يكون مثالي عظيم في الحلقة $\mathbf{Z}_n$.

الحل: ليكن p عدد أولي قاسم للعدد $n \in \mathbf{N}$. إذن يوجد $m \in \mathbf{N}$ ، بحيث $n = p\,m$. إذن $<\ \overline{p} >$ تكون زمرة جزئية (جمعية) من $\mathbf{Z}_n$ رتبتها m . من الواضح أن $<\ \overline{p} > \subseteq\ <\ \overline{p} >\ \mathbf{Z}_n$. إذن $<\ \overline{p} >$ يكون مثالي في $\mathbf{Z}_n$. ليكن I مثالي في $\mathbf{Z}_n$ ، بحيث $<\ \overline{p} >\ \subseteq\ I\ \subseteq \mathbf{Z}_n$. ليكن $|I| = r$. إذن $r \mid n\ ,\ m \mid r$. إذن يوجد $a,b \in \mathbf{N}$ ، بحيث

$n = r\,b$ ، $r = m\,a$. إذن $p\,m = n = m\,a\,b$. إذن $p = a\,b$. لكن p عدد أولي . إذن $a = 1\,,\,b = p$ أو $a = p\ ,\ b = 1$. إذا كان $a = 1$ ، فن $r = m$ ، وبالتالي $I = <\bar{p}>$. وإذا كان $b = 1$ ، فإن $r = n$ وبالتالي $I = \mathbf{Z}_n$. إذن $<\bar{p}>$ يكون مثالي عظيم في $\mathbf{Z}_n$.

٢٥٢. أوجد كل المثاليات العظيمة في $\mathbf{Z}_n$ ، ثم أوجد تقاطعها .

الحل: بما أن $\mathbf{Z}_n \cong \mathbf{Z}/n\mathbf{Z}$ ، فإن كل مثالي في $\mathbf{Z}_n$ يماثل مثالي في $\mathbf{Z}/n\mathbf{Z}$. كل مثالي في $\mathbf{Z}/n\mathbf{Z}$ يكون في الصورة $m\mathbf{Z}/n\mathbf{Z}$ ، حيث $m \mid n$. إذن $p\mathbf{Z}/n\mathbf{Z}$ يكون مثالي عظيم في الحلقة $\mathbf{Z}/n\mathbf{Z}$ إذا وفقط إذا كان p عدد أولي قاسم لـ n . لاحظ أن $p\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_{n/p}$. المثالي العظيم في $\mathbf{Z}_n$ الذي يماثل المثالي العظيم $p\mathbf{Z}/n\mathbf{Z}$ في $\mathbf{Z}/n\mathbf{Z}$ هو $<\bar{p}>$. ليكن $p_1\,,\,p_2\,,\,\ldots\,,\,p_s$ هي كل الأعداد الأولية المختلفة التي تقسم n . إذن كل المثاليات العظمى في $\mathbf{Z}/n\mathbf{Z}$ هى $p_1\mathbf{Z}/n\mathbf{Z}\ ,\ p_2\mathbf{Z}/n\mathbf{Z}\,,\,\ldots\,,\,p_s\mathbf{Z}/n\mathbf{Z}$. إذن كل المثاليات العظمى في $\mathbf{Z}_n$ هى $<\bar{p}_1>,<\bar{p}_2>,\ldots,<\bar{p}_s>$.

بما أن $p\,\mathbf{Z} \cap q\,\mathbf{Z} = pq\,\mathbf{Z}$ ، لأي عددين أوليين $p\,,\,q$ ، فإن

$$
\begin{aligned}
p_1\mathbf{Z}/n\mathbf{Z} \cap p_2\mathbf{Z}/n\mathbf{Z} \cap \ldots \cap p_s\mathbf{Z}/n\mathbf{Z} \\
&= (p_1\mathbf{Z} \cap p_2\mathbf{Z} \cap \ldots \cap p_s\mathbf{Z})/n\mathbf{Z} \\
&= (p_1\,p_2\ldots p_s)\,\mathbf{Z}/n\mathbf{Z}
\end{aligned}
$$

إذن

$$<\bar{p}_1> \cap <\bar{p}_2> \cap \ldots \cap <\bar{p}_s> = <\bar{p}_1\,\bar{p}_2\,\ldots\,\bar{p}_s>$$

ملحوظة: إذا كان $n = p_1\,p_2\ldots p_s$ ، حيث $p_1\,,\,p_2\,,\,\ldots\,,\,p_s$ أعداد أولية مختلفة ، فإن تقاطع كل المثاليات العظمى في $\mathbf{Z}_n$ يساوي المثالي الصفري ، لأن كل المثاليات العظمى في $\mathbf{Z}_n$ هى $<\bar{p}_1>,<\bar{p}_2>,\ldots,<\bar{p}_s>$ ، وبالتالي

$$
\begin{aligned}
<\bar{p}_1> \cap <\bar{p}_2> \cap \ldots \cap <\bar{p}_s> &= <\bar{p}_1\,\bar{p}_2\,\ldots\,\bar{p}_s> \\
&= <\bar{n}> \\
&= <\bar{0}> \\
&= \{\bar{0}\}
\end{aligned}
$$

٢٥٣. ليكن R مجال متكامل غير منتهي يحتوي على عدد منتهي من الوحدات . برهن أن R يحتوي على عدد غير منتهي من المثاليات العظيمة .

الحل: ليكن R مجال متكامل غير منتهي يحتوي على عدد منتهي من الوحدات . بما أن R حلقة ابدالية وتحتوي محايد ، فإن R تحتوي على الأقل على مثالي عظيم (يحتوي المثالي الصفري) ، وذلك ينتج من المبرهنة التي تنص على أن (إذا كانت R حلقة ابدالية وتحتوي محايد ، فإنة لكل مثالي فعلي (أي لا يساوي R) في R يوجد مثالي عظيم يحتوية) .

ليكن $M_1 , M_2 , \dots , M_n$ مثاليات عظيمة مختلفة وغير صفرية في R . بما أن R مجال متكامل ، فإن

$$M_1 M_2 \dots M_n \subseteq M_1 \cap M_2 \cap \dots \cap M_n$$

ليكن $x \neq 0 \ , x \in M_1 M_2 \dots M_n$. بما أن R حلقة غير منتهية وتحتوي على عدد منتهي من الوحدات ، فإنة يوجد $r \in R$ ، بحيث العنصر $1 + r x \in R$ لا يكون وحدة . إذن $< 1 + r x > = R (1 + r x)$ ، لأن R حلقة ابدالية وتحتوي محايد . لاحظ أن $< 1 + r x >$ مثالي فعلي في R ، لأن $< 1 + r x > \neq R$. إذن يوجد مثالي عظيم M_{n+1} في R ، بحيث $R (1 + r x) \subseteq M_{n+1}$. إذن $M_{n+1} \neq M_i , \forall \ i = 1 , 2 , \dots , n$. وذلك لأننا إذا فرضنا العكس ، أي إذا فرضنا أن $M_{n+1} = M_i \ , i \in \{1 , 2 , \dots , n\}$ ، فإن $1 + r x \in M_i$ (لأن $1 \in R$) . لكن $x \in M_i$ ، وبالتالي $r x \in M_i$ ، وبالتالي $- r x \in M_i$. إذن $1 \in M_i$. إذن $M_i = R$. وهذا غير ممكن لأن M_i مثالي عظيم . إذن $M_1 , M_2 , \dots , M_n , M_{n+1}$ تكون مثاليات عظيمة مختلفة وغير صفرية في R . نكرر العمل السابق على المثاليات العظيمة $M_1 , M_2 , \dots , M_n , M_{n+1}$ ، فنحصل على مثالي عظيم M_{n+2} ، بحيث تكون $M_1 , M_2 , \dots , M_n , M_{n+1} , M_{n+2}$ مثاليات عظيمة مختلفة وغير صفرية في R . إذن بالتكرار المستمر للعمل السابق نحصل على عدد غير منتهي من المثاليات العظيمة في R .

٢٥٤. ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$$\sqrt{I} = \{ x \in R \mid \exists n \in \mathbf{N} , s.t. \ x^n \in I\}$$

($\sqrt{I}$ يسمى جذر I (radical of I) ويسمى أيضاً جذر تلاشي I (nil radical of I))

برهن أن

(أ) إذا كان I مثالي عظيم في R ، فإن $\sqrt{I} = I$.

(ب) ليكن $\sqrt{I}$ مثالي عظيم في R ، وليكن $x,y \in R$ بحيث $x y \in I , y \notin \sqrt{I}$. إذن $x \in I$.

الحل: ليكن R حلقة ابدالية تحتوي محايد ، وليكن I مثالي في R . ليكن

$\sqrt{I} = \{ x \in R \mid \exists n \in \mathbf{N}, \text{s. t. } x^n \in I\}$

إذن $\sqrt{I}$ يكون مثالي في R (انظر تمرين (٢٤٧) (أ)) .

(أ) ليكن I مثالي عظيم في R . من تمرين (٢٤٧) (أ) ينتج أن $I \subseteq \sqrt{I} \subseteq R$. لكن I مثالي عظيم في R . إذن $\sqrt{I} = R$ أو $\sqrt{I} = I$. نفرض أن $\sqrt{I} = R$. إذن $1 \in \sqrt{I}$. إذن $1 \in I$. إذن $I = R$. وهذا يتناقض مع الفرض بأن I مثالي عظيم . إذن $\sqrt{I} = I$.

(ب) ليكن $\sqrt{I}$ مثالي عظيم في R ، وليكن $x,y \in R$ بحيث $x\,y \in I , y \notin \sqrt{I}$. إذن $\sqrt{I} + R\,y = R$ (مبرهنة) . إذن يوجد $r \in R$, $z \in \sqrt{I}$ ، بحيث $z + r\,y = 1$. إذن $z = 1 - r\,y$. إذن يوجد $n \in \mathbf{N}$ ، بحيث $z^n \in I$. إذن $(1 - r\,y)^n \in I$. إذن ينتج من مبرهنة ذات الحدين (Binomial theorem) أن

$$(1 - r\,y)^n = 1 + s\,y$$

حيث $s \in R$. إذن $1 + s\,y \in I$. نضع $1 + s\,y = a$. إذن

$$x + x\,s\,y = x\,a$$

إذن

$$x = x\,a - x\,s\,y = x\,a - s\,(x\,y)$$

لكن $x\,a \in I , s\,(x\,y) \in I$ (لأن: من الفرض $xy \in I$ و I مثالي في R) . إذن $x \in I$.

٢٥٥. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I , J مثاليين عظيمين مختلفين في R . برهن أن

(أ) $I + J = R$

(ب) $I \cap J = I\,J$

(ت) $R / I\,J \cong R / I \times R / J$

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I , J مثاليين عظيمين مختلفين في R .

(أ) بما أن I , J مثاليين في R ، فإن $I + J$ يكون أيضاً مثالي في R . إذن $I \subseteq I + J \subseteq R$. لكن I مثالي عظيم . إذن $I + J = I$ أو $I + J = R$. نفرض أن $I + J = I$. إذن $J \subseteq I \subseteq R$. لكن J مثالي عظيم . إذن $I = J$ ، وهذا يتناقض مع الفرض بأن I , J مثاليين مختلفين أو $I = R$ ، وهذا يتناقض مع الفرض بأن I مثالي عظيم . إذن $I + J = R$.

(ب) نعلم أن $I\,J \subseteq I \cap J$. لذلك نبرهن أن $I \cap J \subseteq I\,J$. ليكن $x \in I \cap J$. من (أ) يكون $I + J = R$. وبما أن $1 \in R$ ، فإنة يوجد $u \in I , v \in J$ بحيث $u + v = 1$. إذن $x = x\,u + x\,v = u\,x + x\,v$. لكن $x\,v \in I\,J \;,\; u\,x \in I\,J$. إذن $x \in I\,J$. إذن $I \cap J \subseteq I\,J$. إذن $I \cap J = I\,J$.

(ت) من (ب) ينتج أن $I\,J = I \cap J$. إذن $R / I\,J = R / I \cap J$. ليكن $f : R / (I \cap J) \to R / I \times R / J$ ، بحيث $f(x + (I \cap J)) = (x + I , x + J)$ لكل $x + (I \cap J) \in R / (I \cap J)$. ليكن $x + (I \cap J) , y + (I \cap J) \in R / (I \cap J)$. إذن

$$
\begin{aligned}
x + (I \cap J) = y + (I \cap J) &\Leftrightarrow x - y \in I \cap J \\
&\Leftrightarrow x - y \in I \;,\; x - y \in J \\
&\Leftrightarrow x + I = y + I \;,\; x + J = y + J \\
&\Leftrightarrow (x + I , x + J) = (y + I , y + J) \\
&\Leftrightarrow f(x + (I \cap J)) = f(y + (I \cap J))
\end{aligned}
$$

إذن f يكون تطبيق معرف جيداً ومتباين . ليكن $(x + I , y + J) \in R / I \times R / J$. بما أن $R = I + J$ ، فإنة ينتج من تمرين (٢١٧) أن $x + I \cap y + J \neq \emptyset$. إذن يوجد $a \in I , b \in J$ بحيث $x + a = y + b$. إذن $y = x + a - b$. إذن $y + J = (x + a) + J$. إذن

$$
\begin{aligned}
x\,(x + I , y + J) &= ((x + a) + I , (x + a) + J) \\
&= f((x + a) + (I \cap J))
\end{aligned}
$$

إذن f يكون شامل . إذن f يكون تقابل . والآن نبين أن f يكون تشاكل حلقي .

$$
\begin{aligned}
f((x + (I \cap J)) + (y + (I \cap J))) &= f((x + y) + (I \cap J)) \\
&= ((x + y) + I , (x + y) + J) \\
&= (x + I , x + J) + (y + I , y + J) \\
&= f(x + (I \cap J)) + f(y + (I \cap J)) \quad ,
\end{aligned}
$$

$$
\begin{aligned}
f((x + (I \cap J))\,(y + (I \cap J))) &= f((x\,y) + (I \cap J)) \\
&= ((x\,y) + I , (x\,y) + J) \\
&= (x + I , x + J)\,(y + I , y + J) \\
&= f(x + (I \cap J))\,f(y + (I \cap J))
\end{aligned}
$$

إذن f يكون تشاكل حلقي . إذن f يكون تماثل حلقي .

المثاليات الأولية Prime ideals

٢٥٦. ليكن R مجال متكامل (integral domain) . وليكن لكل مثاليين I , J في R ، بحيث $I \subseteq J$ يوجد مثالي K في R ، بحيث $I = J K$. برهن أن كل مثالي أولي غير صفري في R يكون مثالي عظيم .

الحل: ليكن R مجال متكامل (integral domain) . وليكن لكل مثاليين I , J في R ، بحيث $I \subseteq J$ يوجد مثالي K في R ، بحيث $I = J K$. ليكن P مثالي أولي غير صفري في R . وليكن I مثالي في R ، بحيث $P \subset I$. نبرهن أن $I = R$. ينتج من الفرض أنة يوجد مثالي J في R ، بحيث $P = I J$. لكن P مثالي أولي . إذن $I \subseteq P$ أو $J \subseteq P$. من الفرض بأن $P \subset I$ ، ينتج أن الإحتمال $I \subseteq P$ يكون مرفوض . إذن $J \subseteq P$. لكن $P = I J \subseteq J$ (لأن $R J \subseteq J$) . إذن $J = P$. إذن $P = I P$. ليكن $x \in P , x \neq 0$. بما أن R مجال متكامل ، فإن R تكون ابدالية وتحتوي محايد ، وبالتالي $< x > = R x$. كذلك $R x \subseteq P$ لأن $x \in P , R P \subseteq P$. إذن $< x > \subseteq P$. إذن ينتج من الفرض أنة يوجد مثالي K في R ، بحيث $< x > = P K$. إذن

$$< x > = P K = I P K = I < x > = I (R x)$$

إذن يوجد $y \in I , r \in R$ ، بحيث $x = y r x$. إذن $y r x - x = 0$. إذن $(y r - 1) x = 0$.

لكن الحلقة R خالية من قواسم الصفر (لأنها مجال متكامل) . إذن $y r - 1 = 0$ (لأن $x \neq 0$) .

إذن $y r = 1$. لكن $y r \in I$. إذن $1 \in I$. إذن $I = R$. إذن P يكون مثالي عظيم .

٢٥٧. ليكن R حلقة ابدالية وتحتوي محايد ، بحيث كل عنصر في أي حلقة قسمة لـ R يكون قاسم للصفر أو وحدة . برهن أن أي مثالي أولي في R يكون مثالي عظيم .

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، بحيث كل عنصر في أي حلقة قسمة لـ R يكون قاسم للصفر أو وحدة . ليكن P مثالي أولي في R . ليكن $x + P , y + P \in R / P$ ، بحيث $(x + P) (y + P) = P$. إذن $x y + P = P$. إذن $x y \in P$. لكن P مثالي أولي في R . إذن $x \in P$ أو $y \in P$. إذن $x + P = P$ أو $y + P = P$. إذن الحلقة R / P تكون خالية من قواسم الصفر . إذن ينتج من الفرض (كل عنصر في أي حلقة قسمة لـ R يكون قاسم للصفر أو وحدة) أن كل عنصر غير صفري في R / P يكون وحدة ، أي يوجد لة معكوس ضربي . وبما

أن R حلقة ابدالية وتحتوي محايد ، فإن R / P تكون أيضاً حلقة ابدالية وتحتوي محايد . إذن R / P يكون مجال متكامل (integral domain) يحتوي على معكوس ضربي لكل عنصر غير صفري فية . إذن R / P يكون حقل (field) . إذن P يكون مثالي عظيم (مبرهنة) .

٢٥٨. ليكن R حلقة ابدالية وتحتوي محايد . ليكن $x,y \in R\backslash\{0\}$ ، بحيث يكون x عنصر غير قاسم للصفر وبحيث $R\,x \subseteq R\,y \neq R$. إذا كان كل من $R\,x\,,\,R\,y$ مثالي أولي ، فاثبت أن $R\,x = R\,y$.

الحل: ليكن R حلقة ابدالية وتحتوي محايد . ليكن $x,y \in R\backslash\{0\}$ ، بحيث يكون x عنصر غير قاسم للصفر وبحيث $R\,x \subseteq R\,y \neq R$. إذن $x \in R\,x \subseteq R\,y \neq R$. إذن يوجد $a \in R$ ، بحيث $x = a\,y$. إذن $a\,y \in R\,x$. نفرض أن كل من $R\,x\,,\,R\,y$ يكون مثالي أولي ، ونبرهن أن $R\,x = R\,y$. بما أن $R\,x$ مثالي أولي في R و $a\,y \in R\,x$ ، فإن $a \in R\,x$ أو $y \in R\,x$. نفرض أن $a \in R\,x$. إذن يوجد $b \in R$ ، بحيث $a = b\,x$. إذن $x = a\,y = b\,x\,y$. لكن R حلقة ابدالية . إذن

$$(1 - b\,y)\,x = x - b\,y\,x = x - b\,x\,y = 0$$

لكن x عنصر غير صفري وغير قاسم للصفر في الحلقة R . إذن $1 - b\,y = 0$. إذن $b\,y = 1$. إذن $1 \in R\,y$. إذن $R\,y = R$. وهذا يتناقض مع الفرض بأن $R\,y \neq R$. إذن $y \in R\,x$. وبما أن $R\,x$ مثالي في R ، فإن $r\,y \in R\,x$ لكل $r \in R$. إذن $R\,y \subseteq R\,x$. إذن $R\,x = R\,y$.

٢٥٩. ليكن R حلقة ابدالية وتحتوي محايد . ليكن $n \in \mathbf{N}\,,\,n > 2$ ، بحيث $x^n = x$ لكل $x \in R$. برهن أن كل مثالي أولي في R يكون مثالي عظيم .

الحل: ليكن R حلقة ابدالية وتحتوي محايد . ليكن $n \in \mathbf{N}\,,\,n > 2$ ، بحيث $x^n = x$ لكل $x \in R$. ليكن P مثالي أولي في R . إذن الحلقة R / P تكون خالية من قواسم الصفر (لأنة كما جاء في حل تمرين (٢٢٩) يكون: ليكن $x + P\,,\,y + P \in R / P$ ، بحيث $(x + P)\,(y + P) = P$. إذن $x\,y + P = P$. إذن $x\,y \in P$. لكن P مثالي أولي في R . إذن $x \in P$ أو $y \in P$. إذن $x + P = P$ أو $y + P = P$. إذن الحلقة R / P تكون خالية من قواسم الصفر) . وبما أن R حلقة ابدالية وتحتوي محايد ، فإن R / P تكون أيضاً حلقة ابدالية وتحتوي محايد . إذن R / P يكون مجال متكامل (integral domain) . لاحظ أن العنصر

المحايد الضربي في R / P هو $1 + P$. ليكن $x + P \neq P$, $x + P \in R / P$. إذن $x \notin P$.
من الفرض بأن $x^n = x$ لكل $x \in R$ حيث $n > 2$ يكون $x (x^{n-1} - 1) = 0$. إذن

$$(x + P) ((x^{n-1} - 1) + P) = x (x^{n-1} - 1) + P = 0 + P = P$$

لكن R / P حلقة خالية من قواسم الصفر و$x + P \neq P$. إذن $(x^{n-1} - 1) + P = P$. إذن $x^{n-1} - 1 \in P$. إذن $(x + P) (x^{n-2} + P) = x^{n-1} + P = 1 + P$. إذن العنصر غير الصفري $x + P$ في الحلقة R / P لة معكوس ضربي (هو $x^{n-2} + P$) . هذا يعني أن كل عنصر غير صفري في الحلقة R / P لة معكوس ضربي . إذن R / P يكون حقل . إذن P يكون مثالي عظيم في R (مبرهنة) .

٢٦٠. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I مثالي في R . إذا كان

$$J_x = \{ r \in R \mid r x = 0 \} \ , x \in I$$

فبرهن أن

(أ) J_x يكون مثالي في R ، لكل $x \in I$.

(ب) كل عنصر عظيم (maximal element) (بالنسبة لعلاقة الإحتواء $\subseteq$) في المجموعة $S = \{ J_x \mid x \in I \setminus \{0\} \}$ يكون مثالي أولي في R .

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن I مثالي في R . ليكن

$$J_x = \{ r \in R \mid r x = 0 \} \ , x \in I$$

(أ) ليكن $x \in I$. بما أن $0 \in J_x$ ، فإن $J_x \neq \emptyset$. ليكن $r,s \in J_x$. إذن $r x = s x = 0$. إذن $(r - s) x = 0$. إذن $r - s \in J_x$. إذن J_x تكون زمرة جزئية من الزمرة $(R , +)$. ليكن $r' \in R$. إذن $(r' r) x = r' (r x) = 0$. إذن $r' r \in J_x$ ، لكل $r' \in R$. إذن $R J_x \subseteq J_x$. وبما أن R حلقة ابدالية ، فإن $J_x R \subseteq J_x$. إذن J_x تكون مثالي في R ، لكل $x \in I$.

(ب) ليكن $S = \{ J_x \mid x \in I \setminus \{0\} \}$. وليكن P عنصرعظيم في S بالنسبة لعلاقة الإحتواء $\subseteq$. نبرهن أن P يكون مثالي أولي في R . ليكن $a,b \in P$ ، بحيث $a b \in P$. نبرهن أن $a \in P$ أو $b \in P$. بما أن $P \in S$ ، فإنة يوجد $x \in I \setminus \{0\}$ بحيث $P = J_x$. إذن $a b \in J_x$. إذن $(a b) x = 0$. نفرض أن $b \notin P = J_x$. إذن $b x \neq 0$. إذن $b x \neq 0$, $a (b x) = 0$. إذن $a \in J_{bx}$. لاحظ أن $P = J_x \subseteq J_{bx} \in S$ ،لأن $b x \neq 0$. لكن J_x عنصر عظيم في S . إذن $P = J_x = J_{bx}$. إذن $a \in J_{bx} = P$. إذن P يكون مثالي أولي في R .

٢٦١. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S هي مجموعة كل المثاليات غير منتهية التوليد في R . برهن أن كل عنصر عظيم (maximal element) (بالنسبة لعلاقة الإحتواء $\subseteq$) في S يكون مثالي أولي في R .

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S هي مجموعة كل المثاليات غير منتهية التوليد في R . ليكن $P \in S$ عنصر عظيم بالنسبة لعلاقة الإحتواء $\subseteq$. نبرهن أن P يكون مثالي أولي في R . ليكن $x,y \in R$ ، بحيث $x\,y \in P$. نبرهن أن $x \in P$ أو $y \in P$. نفرض أن $x , y \notin P$. بما أن R حلقة ابدالية وتحتوي محايد ، فإن $< x > = R\,x$ يكون مثالي في R . إذن $P + < x >$ يكون مثالي في R . ليكن $P + < x > = R$. إذن يوجد $z \in P , r \in R$ ، بحيث $z + r\,x = 1$. إذن $y = z\,y + r\,x\,y$. إذن $y \in P$ (لأن $z , x\,y \in P$) . لكن هذا يتناقض مع الفرض بأن $y \notin P$. إذن $P + < x > \neq R$. كذلك $P + < x > \neq P$ ، لأن $x \notin P$, $x \in P + < x >$. بما أن $P \subset P + < x >$ و P عنصر عظيم بالنسبة لعلاقة الإحتواء $\subseteq$ في S ، فإن $P + < x > \notin S$. إذن $P + < x >$ يكون مثالي منتهي التوليد في R .
إذن يوجد $a_1 , a_2 ,\dots, a_n \in R$, $p_1 , p_2 ,\dots, p_n \in P$ ، بحيث

$$P + < x > = < p_1 + a_1 x , p_2 + a_2 x , \dots , p_n + a_n x >$$

ليكن $p \in P$. إذن $p \in P + < x >$. إذن يوجد $r_1 , r_2 ,\dots, r_n \in R$ ، بحيث

$$p = r_1(p_1 + a_1 x) + r_2 (p_2 + a_2 x) + \dots + r_n (p_n + a_n x)$$

$$= (r_1 p_1 + r_2 p_2 + \dots + r_n p_n) + (r_1 a_1 + r_2 a_2 + \dots + r_n a_n)\, x$$

إذن

$$(r_1 a_1 + r_2 a_2 + \dots + r_n a_n)\, x = p - (r_1 p_1 + r_2 p_2 + \dots + r_n p_n) \in P$$

ليكن $I = \{r \in R \mid r\,x \in P\}$. من السهل اثبات أن I يكون مثالي في R . لاحظ أن $I \neq P$ ، لأن $y \in I , y \notin P$. لاحظ كذلك أن $I \neq R$ ، لأن $1 \notin I$ (لأن $x \notin P$) . إذن $P \subset I$. لكن $P \in S$ عنصر عظيم بالنسبة لعلاقة الإحتواء $\subseteq$. إذن $I \notin S$. إذن I يكون مثالي منتهي التوليد في R . إذن يوجد $b_1 , b_2 ,\dots, b_m \in R$ ، بحيث

$$I = < b_1 , b_2 ,\dots, b_m >$$

بما أن $(r_1 a_1 + r_2 a_2 + \dots + r_n a_n)\, x \in P$ ، فإن $r_1 a_1 + r_2 a_2 + \dots + r_n a_n \in I$.
إذن

$P = < p_1 , p_2 ,\ldots, p_n , b_1 x , b_2 x ,\ldots, b_m x >$

إذن P يكون مثالي منتهي التوليد ، وهذا يتناقض مع الفرض بأن $P \in S$. إذن على الأقل يكون $x \in P$ أو $y \in P$. إذن P يكون مثالي أولي .

٢٦٢. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S مجموعة جزئية غير خالية من R ، بحيث تكون مغلقة بالنسبة لعملية الضرب على R . ليكن I مثالي في R بحيث $I \cap S = \emptyset$. برهن أنة يوجد مثالي أولي P في R بحيث $P \cap S = \emptyset$, $I \subseteq P$.

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S مجموعة جزئية غير خالية من R ، بحيث تكون مغلقة بالنسبة لعملية الضرب على R . ليكن I مثالي في R بحيث $I \cap S = \emptyset$. نضع

$E(S) = \{ J \mid J \cap S = \emptyset$ بحيث R مثالي في $J \}$

إذن $I \in E(S)$. إذن $E(S) \neq \emptyset$. لاحظ أن تمهيدية زورن (Zorn's lemma) تنص على أن : إذا وُجد لكل سلسلة (chain) في المجموعة المرتبة جزئياً (poset) حد أعلى (upper bound) ، فإن هذة المجموعة تحتوي على عنصر عظيم (maximal element) .
إذن ينتج من تمهيدية زورن (Zorn's lemma) أن $E(S)$ تحتوي على عنصر عظيم وليكن P .
إذن P يكون مثالي في R بحيث $P \cap S = \emptyset$. بما أن $I \in E(S)$ وبما أن P عنصر عظيم في $E(S)$ ، فإن $I \subseteq P$. نبرهن أن P يكون مثالي أولي في R . ليكن $x,y \in R$ ، بحيث $x\, y \in P$. نبرهن أن $x \in P$ أو $y \in P$. نفرض أن $x , y \notin P$. بما أن R حلقة ابدالية وتحتوي محايد ، فإن $< x > = R\, x$ يكون مثالي في R . إذن $P + < x >$ يكون مثالي في R . ليكن $P + < x > = R$. إذن يوجد $z \in P , r \in R$ ، بحيث $z + r\, x = 1$. إذن $y = z\, y + r\, x\, y$. إذن $y \in P$ (لأن $z , x\, y \in P$) . لكن هذا يتناقض مع الفرض بأن $y \notin P$. إذن $P + < x > \neq R$. كذلك $P + < x > \neq P$ ، لأن $x \notin P$, $x \in P + < x >$.
بما أن $P \subset P + < x >$ و P عنصر عظيم بالنسبة لعلاقة الإحتواء $\subseteq$ في S ، فإن $P + < x > \notin S$. إذن $P + < x >$ يكون مثالي منتهي التوليد في R . بما أن $P \subset P + < x >$ و P عنصر عظيم في $E(S)$ ، فإن $P + < x > \notin E(S)$. إذن $(P + < x >) \cap S \neq \emptyset$. بالمثل يمكن اثبات أن $(P + < y >) \cap S \neq \emptyset$. إذن يوجد $p_1 , p_2 \in P , r_1 , r_2 \in R , s_1 , s_2 \in S$ بحيث

$$p_1 + r_1\, x = s_1 \ , \quad p_2 + r_2\, y = s_2$$

إذن ينتج من الفرض بأن S مجموعة جزئية غير خالية من R ، بحيث تكون مغلقة بالنسبة لعملية الضرب على R ، أن

$$(p_1 + r_1 x)(p_2 + r_2 y) = s_1 s_2 \in S$$

وبما أن $x\,y \in P$ و $p_1 , p_2 \in P$ ، فإن

$$p_1 p_2 + p_1 r_2 y + p_2 r_1 x + r_1 r_2 x y \in P \cap S$$

لكن هذا يتناقض مع الفرض بأن $P \cap S = \emptyset$ (لأن $P \in E(S)$) . إذن $x \in P$ أو $y \in P$.

إذن P يكون مثالي أولي في R ، ويحقق $P \cap S = \emptyset$, $I \subseteq P$.

٢٦٣. ليكن R حلقة ابدالية وتحتوي محايد . برهن أن

كل مثالي في R يكون مثالي رئيس (principal ideal) $\Leftrightarrow$ كل مثالي أولي في R يكون مثالي رئيس

الحل: ليكن R حلقة ابدالية وتحتوي محايد .

($\Leftarrow$) واضح

($\Rightarrow$) نفرض أن كل مثالي أولي في R يكون مثالي رئيس . نبرهن أن كل مثالي في R يكون مثالي رئيس . نفرض عكس المطلوب . أي نفرض أن R يحتوي على مثالي غير رئيس وليكن A . ليكن S هي مجموعة كل المثاليات غير الرئيسة في R . إذن $A \in S$. إذن $S \neq \emptyset$. بما أن R حلقة ابدالية وتحتوي محايد ، فإن $R = <1>$. إذن $R \notin S$. لاحظ أن S مع علاقة الإحتواء $\subseteq$ تكون مجموعة مرتبة جزئياً (poset) . ليكن $\{J_i\}_{i \in I}$ مجموعة جزئية من S مرتبة كلياً (totally ordered) ، أي تكون سلسلة . ليكن $U = \bigcup_{i \in I} J_i$. إذا كانت المجموعة $\{J_i\}_{i \in I}$ منتهية ، أي إذا وُجد $n \in \mathbf{N}$ بحيث $I = \{1,2,\ldots,n\}$ ، فإن $U = J_n \in S$ يكون حد أعلى (upper bound) للمجموعة $\{J_i\}_{i \in I}$. نفرض أن المجموعة $\{J_i\}_{i \in I}$ غير منتهية . نبرهن أن $U \in S$. ليكن $x,y \in U$. إذن يوجد $i , j \in I$ ، بحيث $x \in J_i , y \in J_j$. بما أن المجموعة $\{J_i\}_{i \in I}$ مرتبة كلياً (totally ordered) ، فإن $J_i \subseteq J_j$ أو $J_j \subseteq J_i$. نفرض أن $J_i \subseteq J_j$. إذن $x,y \in J_j \subseteq U$. إذن $x - y \in J_j \subseteq U$. إذن U تكون زمرة جزئية من الزمرة $(R , +)$. كذلك $r\,x \in J_j \subseteq U$ ، لكل $r \in R$. إذن U يكون مثالي في R . إذا كان U مثالي رئيس في R ، فإنة يوجد $x \in R$ بحيث $U = <x>$. لكن R حلقة ابدالية وتحتوي محايد . إذن $U = R\,x$. إذن يوجد $i \in I$ ، بحيث $x \in J_i$. إذن $U = J_i$. إذن J_i يكون مثالي رئيس في R . لكن هذا يتناقض مع الفرض . إذن U يكون مثالي غير رئيس في R . إذن

$U \in S$. إذن U يكون حد أعلى (upper bound) للمجموعة $\{J_i\}_{i \in I}$ الجزئية من S . لاحظ أن تمهيدية زورن (Zorn's lemma) تنص على أن : إذا وُجد لكل سلسلة (chain) في المجموعة المرتبة جزئياً (poset) حد أعلى (upper bound) ، فإن هذة المجموعة تحتوي على عنصر عظيم (maximal element) . إذن ينتج من تمهيدية زورن (Zorn's lemma) أن S تحتوي على عنصر عظيم ، وليكن P . نبرهن أن P يكون مثالي أولي في R . ليكن $x,y \in R$ ، بحيث $x\,y \in P$. نبرهن أن $x \in P$ أو $y \in P$. نفرض أن $x , y \notin P$. بما أن R حلقة ابدالية وتحتوي محايد ، فإن $< x > = R\,x$ يكون مثالي في R . إذن $P + R\,x$ يكون مثالي في R . ليكن $P + R\,x = R$. إذن يوجد $z \in P , r \in R$ ، بحيث $z + r\,x = 1$. إذن $y = z\,y + r\,x\,y$. إذن $y \in P$ (لأن $z , x\,y \in P$) . لكن هذا يتناقض مع الفرض بأن $y \notin P$. إذن $P + R\,x \neq R$. كذلك $P + R\,x \neq P$ ، لأن $x \in P + R\,x ,\ x \notin P$. بما أن $P \subset P + R\,x$ و P عنصر عظيم بالنسبة لعلاقة الإحتواء $\subseteq$ في S ، فإن $P + R\,x \notin S$. إذن $P + R\,x$ يكون مثالي رئيس في R . إذن يوجد $z \in R$ ، بحيث $P + R\,x = R\,z$. إذن يوجد $p \in P , a \in R$ ، بحيث $p + a\,x = z$. ليكن $K = \{r \in R \mid r\,z \in P\}$. من الواضح أن K يكون مثالي في R . ليكن $p' + r\,y \in P + R\,y$. إذن

$$(p' + r\,y)\,z = p'\,z + r\,y\,(p + a\,x) = p'\,z + r\,y\,p + r\,a\,x\,y \in P$$

إذن $p' + r\,y \in K$. إذن $P \subset P + R\,y \subseteq K$. لكن P عنصر عظيم في S . إذن $K \notin S$. إذن K يكون مثالي رئيس في R . إذن يوجد $u \in R$ ، بحيث $K = < u > = R\,u$. بما أن $p \in P \subset P + R\,x = R\,z$ ، فإنة يوجد $s \in R$ بحيث $p = s\,z$. إذن $s \in K$. لكن $K = R\,u$. إذن يوجد $b \in R$ بحيث $s = b\,u$. إذن $p = b\,u\,z$. إذن $p \in R\,u\,z$. إذن $P \subseteq R\,u\,z$. وبما أن $u \in K$ ، فإن $u\,z \in P$. إذن $r\,(u\,z) \in P$ ، لكل $r \in R$. إذن $R\,u\,z \subseteq P$. إذن $P = R\,u\,z$. لكن P مثالي غير رئيس في R و $R\,u\,z$ مثالي رئيس في R . بالتالي نحصل على تناقض . إذن P يكون مثالي أولي في R . لاحظ أن P يكون أيضاً مثالي غير رئيس في R . لكن هذا يتناقض مع الفرض بأن كل مثالي أولي في R يكون مثالي رئيس . إذن $S = \emptyset$. إذن كل مثالي في R يكون مثالي رئيس .

٢٦٤. في الحلقة $\mathbf{Z}[x]$ اثبت أن المثالي الرئيس $< x >$ يكون أولي ولا يكون عظيم .

الحل: ليكن $a(x) , b(x) \in \mathbf{Z}[x]$ ، بحيث $a(x)\,b(x) \in < x >$. ليكن

$$a(x) = a_0 + a_1\,x + \ldots + a_m\,x^m \quad , \quad b(x) = b_0 + b_1\,x + \ldots + b_n\,x^n$$

إذن

$$a(x)\, b(x) = a_0\, b_0 + (a_0\, b_1 + a_1\, b_0)\, x + \ldots + a_m\, b_n\, x^{m+n}$$

بما أن $a(x)\, b(x) \in <x>$ ، فإنة يوجد $c(x) \in \mathbf{Z}[x]$ بحيث $a(x)\, b(x) = c(x)\, x$. لكن الحد الثابت في $c(x)\, x$ يساوي 0 . إذن الحد الثابت في $a(x)\, b(x)$ يساوي 0 . إذن $a_0\, b_0 = 0$. بالتالي توجد الإحتمالات التالية :

(أ) $a_0 = b_0 = 0$

في هذة الحالة يكون

$$a(x) = (a_1 + a_2\, x + \ldots + a_m\, x^{m-1})\, x \;\; ,$$
$$b(x) = (b_1 + b_2\, x + \ldots + b_n\, x^{n-1})\, x$$

إذن $a(x)\, ,\, b(x) \in <x>$.

(ب) $a_0 = 0 \;\; , \;\; b_0 \neq 0$

في هذة الحالة ينتج كما في (أ) أن $a(x) \in <x>$.

(ت) $a_0 \neq 0 \;\; , \;\; b_0 = 0$

في هذة الحالة ينتج كما في (أ) أن $b(x) \in <x>$.

إذن في كل الحالات يكون $a(x) \in <x>$ أو $b(x) \in <x>$. إذن $<x>$ يكون مثالي أولي .
بما أن $\mathbf{Z}[x] \supset <x\, , 3> \supset <x>$ ، فإن المثالي $<x>$ لا يكون مثالي عظيم .

٢٦٥. ليكن R حلقة ابدالية تحتوي على محايد ، وليكن P مثالي أولي في R . برهن أن $\sqrt{P} = P$.

الحل: ليكن R حلقة ابدالية تحتوي على محايد ، وليكن P مثالي أولي في R . من تمرين (٢٤٣) (أ) ينتج أن $P \subseteq \sqrt{P}$. إذن نبرهن أن $\sqrt{P} \subseteq P$. ليكن $x \in \sqrt{P}$. إذن يوجد $n \in \mathbf{N}$ ، بحيث $x^n \in P$. لكن P مثالي أولي في الحلقة الإبدالية R المحتوية على محايد . إذن $x \in P$. إذن $\sqrt{P} \subseteq P$. إذن $\sqrt{P} = P$.

المثاليات الإبتدائية Primary ideals

٢٦٦. ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي .

(أ) ليكن Q مثالي ابتدائي في R وليكن f شامل و $\mathrm{Ker}(f) \subseteq Q$. برهن أن $f(Q)$ يكون مثالي ابتدائي في S .

(ب) ليكن 'Q مثالي ابتدائي في S . برهن أن $f^{-1}(Q')$ يكون مثالي ابتدائي في R .

الحل: ليكن R , S حلقتين ابداليتين ، وليكن $f : R \to S$ تشاكل حلقي .

(أ) ليكن Q مثالي ابتدائي في R وليكن f شامل و $Ker(f) \subseteq Q$. نبرهن أن $f(Q)$ يكون مثالي ابتدائي في S . بما أن f شامل ، فإن $f(Q)$ يكون مثالي في S (مبرهنة) . ليكن $a,b \in S$ ، بحيث $a\,b \in f(Q)\ ,\ a \notin f(Q)$. بما أن f شامل ، فإنة يوجد $x,y \in R$ ، بحيث $f(x) = a\ ,\ f(y) = b$. إذن $f(x\,y) = f(x)\,f(y) = a\,b \in f(Q)$. إذن $x\,y \in Q\ ,\ x \notin Q$. لكن Q مثالي ابتدائي في R . إذن يوجد $n \in \mathbf{N}$ ، بحيث $y^n \in Q$. إذن

$$b^n = (f(y))^n = f(y^n) \in f(Q)$$

إذن $f(Q)$ يكون مثالي ابتدائي في S .

(ب) ليكن 'Q مثالي ابتدائي في S . نبرهن أن $f^{-1}(Q')$ يكون مثالي ابتدائي في R . لاحظ أن $f^{-1}(Q')$ يكون مثالي في R (مبرهنة) . ليكن $a,b \in R$ ، بحيث $a\,b \in f^{-1}(Q')\ ,\ a \notin f^{-1}(Q')$. إذن $f(a\,b) = f(a)\,f(b) \in Q'$. بما أن $a \notin f^{-1}(Q')$ ، فإن $f(a) \notin Q'$. لكن 'Q مثالي ابتدائي في S . إذن يوجد $n \in \mathbf{N}$ ، بحيث $(f(b))^n \in Q'$. إذن $f(b^n) \in Q'$. إذن $b^n \in f^{-1}(Q')$. إذن $f^{-1}(Q')$ يكون مثالي ابتدائي في R .

٢٦٧. في الحلقة $\mathbf{Z}[x]$ برهن أن $< x^2 >$ يكون مثالي ابتدائي وأن $< x >$ هو المثالي الأولي المناظر لة (associated prime ideal) .

الحل: ليكن $a(x)\ ,\ b(x) \in \mathbf{Z}[x]$ ، بحيث $a(x) \notin < x^2 >\ ,\ a(x)\,b(x) \in < x^2 >$. لاحظ أن $\mathbf{Z}[x]$ حلقة ابدالية وتحتوي على محايد . إذن $< x^2 > = (\mathbf{Z}[x])\,x^2$. إذن يوجد $c(x) \in \mathbf{Z}[x]$ ، بحيث $a(x)\,b(x) = c(x)\,x^2$. ليكن

$$a(x) = a_0 + a_1\,x + \ldots + a_m\,x^m \quad , \quad b(x) = b_0 + b_1\,x + \ldots + b_n\,x^n$$

إذن

$$a(x)\,b(x) = a_0\,b_0 + (a_0\,b_1 + a_1\,b_0)\,x + \ldots + a_m\,b_n\,x^{m+n}$$

إذن ينتج من $a(x)\,b(x) = c(x)\,x^2$ ، أن $a_0\,b_1 + a_1\,b_0 = 0\ ,\ a_0\,b_0 = 0$.

إذن توجد الإحتمالات التالية:

(١) $a_0 = 0\ ,\ b_0 = 0$

في هذة الحالة يكون $b(x) = d(x)\,x$ ، حيث $d(x) = b_1 + b_2\,x + \ldots + b_n\,x^{n-1}$. إذن $(b(x))^2 = (d(x))^2\,x^2$. إذن $(b(x))^2 \in < x^2 >$.

(٢) $a_0 = 0 \ , \ b_0 \neq 0$

في هذه الحالة يكون $a_1 = 0$. إذن $a(x) = e(x)\,x^2$ ، حيث

$e(x) = a_2 + a_3 x + \ldots + a_m x^{m-1}$

إذن $a(x) \in \langle x^2 \rangle$. لكن هذا يتناقض مع الفرض بأن $a(x) \notin \langle x^2 \rangle$. إذن هذا الإحتمال مرفوض .

(٣) $a_0 \neq 0 \ , \ b_0 = 0$

في هذه الحالة يكون $b_1 = 0$. إذن $b(x) = f(x)\,x^2$ ، حيث

$f(x) = b_2 + b_3 x + \ldots + b_n x^{n-2}$

إذن $b(x) \in \langle x^2 \rangle$.

إذن ينتج من هذة الإحتمالات أن $b(x) \in \langle x^2 \rangle$ أو $(b(x))^2 \in \langle x^2 \rangle$. إذن $\langle x^2 \rangle$ يكون مثالي ابتدائي في الحلقة $\mathbf{Z}[x]$.

المثالي الأولي المناظر (associated prime ideal) للمثالي $\langle x^2 \rangle$ هو $\sqrt{\langle x^2 \rangle}$. لذلك نبرهن أن $\sqrt{\langle x^2 \rangle} = \langle x \rangle$. ليكن $f(x) \in \langle x \rangle$. إذن يوجد $g(x) \in \mathbf{Z}[x]$ ، بحيث $f(x) = g(x)\,x$. إذن $(f(x))^2 = (g(x))^2 x^2$. إذن $(f(x))^2 \in \langle x^2 \rangle$. إذن $f(x) \in \sqrt{\langle x^2 \rangle}$. إذن $\langle x \rangle \subseteq \sqrt{\langle x^2 \rangle}$. بما أن $\mathbf{Z}[x]$ حلقة ابدالية وتحتوي محايد ، فإن $(\langle x \rangle)^2 = \langle x \rangle \langle x \rangle = \langle x^2 \rangle$. وبما أن $\langle x^2 \rangle \subseteq \langle x \rangle$ ، فإن $\sqrt{\langle x^2 \rangle} \subseteq \sqrt{\langle x \rangle}$ (مبرهنة) . لكن $\sqrt{\langle x \rangle} = \langle x \rangle$ ، لأن $\langle x \rangle$ مثالي أولي في الحلقة $\mathbf{Z}[x]$ (انظر تمرين (٢٥٩) وتمرين (٢٦٠)) . إذن $\sqrt{\langle x^2 \rangle} = \langle x \rangle$.

٢٦٨. ليكن R حلقة ابدالية وتحتوي محايد ، وليكن Q , J , I مثاليات في R بحيث Q يكون مثالي ابتدائي . برهن أن

(أ) إذا كان $I \not\subset \sqrt{Q} \ , \ I\,J \subseteq Q$ ، فإن $J \subseteq Q$.

(ب) إذا كان J منتهي التوليد و $I\,J \subseteq Q$ ، فإن $I \subseteq Q$ أو يوجد $n \in \mathbf{N}$ بحيث $J^n \subseteq Q$.

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن Q , J , I مثاليات في R بحيث Q يكون مثالي ابتدائي .

(أ) ليكن $I \not\subset \sqrt{Q} \ , \ I\,J \subseteq Q$. نبرهن أن $J \subseteq Q$. بما أن $I \not\subset \sqrt{Q}$ ، فإنة يوجد $y \in I \setminus \sqrt{Q}$. إذن $y^n \notin Q$ ، لكل $n \in \mathbf{N}$. نفرض عكس المطلوب . أي نفرض أن $J \not\subset Q$.

إذن يوجد $x \in J$ ، بحيث $x \notin Q$. بما أن Q مثالي ابتدائي في R وبما أن $y\,x \in I\,J \subseteq Q$ ،

فإنة يوجد $m \in \mathbf{N}$ بحيث $y^m \in Q$. لكن هذا يتناقض مع $y^n \in Q$ ، لكل $n \in \mathbf{N}$. إذن $J \subseteq Q$.

(ب) ليكن J منتهي التوليد و $I\,J \subseteq Q$. إذن يوجد $a_1 , a_2 , \ldots , a_m \in R$ ، بحيث $J = < a_1 , a_2 ,\ldots, a_m >$. إذا كان $I \subseteq Q$ ، فإن المطلوب يتحقق . لذلك نفرض أن $I \not\subset Q$. إذن يوجد $x \in I \setminus Q$. بما أن $I\,J \subseteq Q$ ، فإن $x\,a_1 , x\,a_2 ,\ldots, x\,a_m \in Q$. لكن Q مثالي ابتدائي في R و $x \notin Q$. إذن يوجد $n_1 , n_2 ,\ldots, n_m \in \mathbf{N}$ ، بحيث $(a_1)^{n_1} , \ldots , (a_m)^{n_m} \in Q$. ليكن $s = Max\{n_1 , n_2 , \ldots , n_m\}$. ليكن $n = m\,s$. إذن $(a_1)^s , \ldots , (a_m)^s \in Q$. ليكن $t_1 , t_2 , \ldots , t_m \in \mathbf{N}$ ، بحيث $t_1 + t_2 + \ldots + t_m = n$. إذن يوجد $k \in \{1,2,\ldots,m\}$ ، بحيث $t_k \geq n_k$ (لأن: نفرض أن $t_i < n_i$ ، لكل $i \in\{1,2,\ldots,m\}$. إذن

$$n = m\,s = t_1 + t_2 + \ldots + t_m < n_1 + n_2 + \ldots + n_m \leq m\,s = n$$

وهذا غير ممكن) . إذن $(a_k)^{t_k} \in Q$. إذن $(a_1)^{t_1} \ldots (a_m)^{t_m} \in Q$.

بما أن R حلقة ابدالية وتحتوي محايد ، فإن

$< a , b > = < a > + < b >$, $< a > < b > = < a\,b >$ لكل $a,b \in R$ (مبرهنة) . إذن $J = < a_1 > + < a_2 > + \ldots + < a_m >$. إذن J^n يساوي مجموع مثاليات رئيسة ، كل منها مولد بعنصر في الصورة $(a_1)^{t_1} \ldots (a_m)^{t_m}$. إذن $J^n \subseteq Q$.

الحلقات النوثيرية والحلقات الأرتينية

Noetherian rings and Artinian rings

٢٦٩. ليكن R حلقة ابدالية وتحتوي محايد . برهن أن

R تكون حلقة نوثيرية (Noetherian ring) $\Leftrightarrow$ كل مثالي أولي في R يكون منتهي التوليد

الحل: ليكن R حلقة ابدالية وتحتوي محايد ، وليكن S هي مجموعة كل المثاليات غير منتهية التوليد في R .

($\Leftarrow$) ليكن R حلقة نوثيرية (Noetherian ring) . إذن كل مثالي أولي في R يكون منتهي التوليد (مبرهنة) .

($\Longrightarrow$) نفرض أن كل مثالي أولي في R يكون منتهي التوليد . نفرض أن R تحتوي على مثالي غير منتهي التوليد وليكن I . إذن $I \in S$. إذن $S \neq \emptyset$. إذن ينتج من مبرهنة زورن أن S تحتوي على عنصر عظيم ، وليكن M . إذن $I \subseteq M$. إذن ينتج من تمرين (٢٣٣) أن M يكون مثالي أولي في R . إذن من الفرض بأن كل مثالي أولي في R يكون منتهي التوليد ينتج أن M يكون منتهي التوليد . لكن هذا يتناقض مع كون $M \in S$. إذن R لا تحتوي على مثاليات غير منتهية التوليد . إذن أي سلسلة تصاعدية من المثاليات في R تكون منتهية . إذن R تكون حلقة نوثيرية (Noetherian ring) .

٢٧٠. ليكن R حلقة نوثيرية (Noetherian ring) ، وليكن $f : R \to R$ تشاكل حلقي شامل . برهن أن f يكون متباين .

الحل: ليكن R حلقة نوثيرية (Noetherian ring) ، وليكن $f : R \to R$ تشاكل حلقي شامل . ليكن (m مرة) $f^m = f\,f \ldots f$. إذن $f^m : R \to R$ يكون تشاكل حلقي شامل أيضاً . $\mathrm{Ker}(f^m)$ يكون مثالي في R ، لكل قيم m . إذن

$$\mathrm{Ker}(f\,) \subseteq \mathrm{Ker}(f^2) \subseteq \mathrm{Ker}(f^3) \subseteq \ldots$$

تكون سلسلة تصاعدية من مثاليات في R . وبما أن R حلقة نوثيرية ، فإنة يوجد $n \in \mathbf{N}$ بحيث $\mathrm{Ker}(f^n) = \mathrm{Ker}(f^{n+1}) = \ldots$. لكن

$$x \in \mathrm{Ker}(f^{n+1}) \Leftrightarrow f^{n+1}(x) = 0 \Leftrightarrow f(f^n(x)) = 0 \Leftrightarrow f^n(x) \in \mathrm{Ker}(f\,)$$
$$\Leftrightarrow x \in (f^n)^{-1}(\mathrm{Ker}(f\,))$$

إذن $\mathrm{Ker}(f^n) = \mathrm{Ker}(f^{n+1}) = (f^n)^{-1}(\mathrm{Ker}(f\,))$. إذن

بما أن f^n شامل ، فإن $f^n\left((f^n)^{-1}(\mathrm{Ker}(f\,)\right) = \mathrm{Ker}(f\,)$. إذن $\mathrm{Ker}(f\,)$. إذن f يكون متباين .

٢٧١. ليكن R حلقة نوثيرية (Noetherian ring) ابدالية . برهن أن مجموع كل المثاليات المتلاشية القوى (nilpotent ideals) في R يكون مثالي متلاشي القوى أيضاً في R .

الحل: ليكن R حلقة نوثيرية (Noetherian ring) ابدالية . نفرض أن $C = \{N_i\}_{i \in I}$ هى مجموعة كل المثاليات المتلاشية القوى (nilpotent ideals) في R . نضع $N = \Sigma_{i \in I} N_i$. إذا كانت الحلقة R متلاشية القوى ، فإن كل حلقة جزئية منها تكون أيضاً متلاشية القوى . بالتالي كل مثالي في R يكون متلاشي القوى . إذن N يكون مثالي متلاشي القوى في R . نفرض أن الحلقة R ليست متلاشية القوى . بما أن R حلقة نوثيرية ، فإن المجموعة C تحتوي على عنصر عظيم

(maximal element) (مبرهنة) ، وليكن M . بما أن $M \in C$ ، فإن M يكون مثالي متلاشي القوى في R . لكن مجموع أي مثاليين متلاشيي القوى في R يكون مثالي متلاشي القوى أيضاً في R (مبرهنة) . إذن $M + N_i$ يكون مثالي متلاشي القوى في R ، لكل $i \in I$. إذن $M + N_i \in C$ ، لكل $i \in I$. لكن $M \subseteq M + N_i$ ، لكل $i \in I$. لكن M عنصر عظيم في C . إذن $M = M + N_i$ ، لكل $i \in I$. إذن $N_i \subseteq M$ ، لكل $i \in I$. إذن $N \subseteq M$. بما أن $M \in C$ ، فإنة يوجد $j \in I$ بحيث $M = N_j$. إذن $N = \Sigma_{i \in I} N_i \subseteq N_j$. إذن $N = N_j$.

إذن N يكون مثالي متلاشي القوى في R .

٢٧٢. اثبت أن الحلقة الجزئية من حلقة نوثيرية (Noetherian ring) لا تكون بصفة عامة حلقة نوثيرية .

الحل: لاثبات أن الحلقة الجزئية من حلقة نوثيرية (Noetherian ring) لا تكون بصفة عامة حلقة نوثيرية نعطي مثالاً لحلقة نوثيرية وحلقة جزئية منها غير نوثيرية . نعتبر حلقة كثيرات الحدود $\mathbf{Q}[x]$. لاحظ أن الحلقة $\mathbf{Q}[x]$ تكون ابدالية وتحتوي محايد وهو العدد الصحيح 1. بما أن $\mathbf{Q}$ حقل (field) ، فإن $\mathbf{Q}$ تكون حلقة نوثيرية (لأن أي حقل لا يحتوي على مثاليات غير بديهية) . من مبرهنة هلبرت الأساسية (Hilbert Basis Theorem) ينتج أن $\mathbf{Q}[x]$ تكون حلقة نوثيرية . ليكن R هي مجموعة كل كثيرات الحدود في $\mathbf{Q}[x]$ التي حدودها الثابتة (المطلقة) أعداد صحيحة . من الواضح أن $R \neq \emptyset$. من السهل اثبات أن R تكون حلقة جزئية ابدالية من $\mathbf{Q}[x]$ وتحتوي 1 . نبرهن أن R تكون حلقة غير نوثيرية . نعتبر سلسلة المثاليات التالية

$$< x > \subset < 1/2\, x > \subset < 1/4\, x > \subset < 1/8\, x > \subset \ldots \qquad (*)$$

من الواضح أن (*) سلسلة مثاليات تصاعدية وغير منتهية في R . إذن R لا تحقق الشرط ACC (Ascending chain condition) . إذن R تكون حلقة غير نوثيرية .

٢٧٣. ليكن R حلقة نوثيرية . إذا كان I مثالي في R ، فاثبت أن الحلقة R / I تكون حلقة نوثيرية .

الحل: ليكن R حلقة نوثيرية ، وليكن I مثالي في R . ليكن

$$\bar{J}_1 \subseteq \bar{J}_2 \subseteq \ldots$$

سلسلة مثاليات تصاعدية في الحلقة R / I . من مبرهنة التناظر في الحلقات (Correspondence theorem) ينتج أنة لكل مثالي $\overline{J}_i$ في الحلقة R / I يوجد مثالي J_i في الحلقة R ، بحيث $\overline{J}_i = J_i / I$, $I \subseteq J_i$ حيث $i = 1 , 2 , \ldots$. إذن

$$J_1 \subseteq J_2 \subseteq \ldots$$

تكون سلسلة مثاليات تصاعدية في الحلقة R . لكن R حلقة نوثيرية . إذن يوجد $n \in \mathbf{N}$ ، بحيث

$$J_n = J_{n+1} = \ldots$$

إذن

$$\overline{J}_n = \overline{J}_{n+1} = \ldots$$

إذن الحلقة R / I تكون حلقة نوثيرية .

٢٧٤. ليكن R حلقة ابدالية تحتوي محايد . إذا كانت حلقة كثيرات الحدود $R[x]$ حلقة نوثيرية ، فبرهن أن R تكون حلقة نوثيرية .

الحل: ليكن R حلقة ابدالية تحتوي محايد ، بحيث حلقة كثيرات الحدود $R[x]$ تكون حلقة نوثيرية . بما أن R حلقة ابدالية تحتوي محايد ، فإنة ينتج من تمرين (٢٤٥) أن $R \cong R[x] / < x >$. لكن ينتج من تمرين (٢٦٩) أن الحلقة $R[x] / < x >$ تكون حلقة نوثيرية لأن $R[x]$ حلقة نوثيرية . إذن R تكون حلقة نوثيرية .

٢٧٥. اذكر مثالاً لحلقة نوثيرية وغير أرتينية .

الحل: حلقة الأعداد الصحيحة $\mathbf{Z}$ تكون حلقة نوثيرية وغير أرتينية .

٢٧٦. اذكر مثالاً لحلقة أرتينية وغير نوثيرية

الحل:

$$\mathbf{Z}(p^\infty) = \{ m / p^m \mid 0 \le m \le p^n , m \in \mathbf{Z} , n = 0,1,2,\ldots \}$$

تكون حلقة (ابدالية وبدون عنصر محايد) أرتينية وغير نوثيرية .

٢٧٧. اذكر مثالاً لحلقة أرتينية تحتوي على حلقة جزئية غير أرتينية .

الحل: كل حقل يكون حلقة أرتينية . بالتالي $\mathbf{Q}$ تكون حلقة أرتينية . $\mathbf{Z}$ تكون حلقة جزئية غير أرتينية من $\mathbf{Q}$.

٢٧٨. اذكر مثالاً لحلقة غير أرتينية تحتوي على حلقة جزئية أرتينية .

الحل: ليكن F حقل . إذن F تكون حلقة أرتينية . حلقة كثيرات الحدود $F[x]$ تكون حلقة غير أرتينية ، لأن

$$< x > \supset < x^2 > \supset < x^3 > \supset \ldots$$

تكون سلسلة غير منتهية من المثاليات في $F[x]$. إذن $F[x]$ تكون حلقة غير أرتينية وتحتوي على حلقة جزئية أرتينية هي F .

٢٧٩. اذكر مثالاً لحلقة غير نوثيرية وغير أرتينية .

الحل: ليكن $Map(\mathbf{R}, \mathbf{R})$ هي مجموعة كل التطبيقات من **R** إلى **R** . من السهل اثبات أن $Map(\mathbf{R}, \mathbf{R})$ تكون حلقة ابدالية بالنسبة لعمليتي الجمع والضرب التاليتين

$$(f + g)(x) = f(x) + g(x) \ , \ (f\,g)(x) = f(x)\,g(x) \ , \forall\, x \in \mathbf{R} .$$

التطبيق $o : \mathbf{R} \to \mathbf{R}$ ، حيث $o(x) = 0$ لكل $x \in \mathbf{R}$ هو العنصر المحايد الجمعي في $Map(\mathbf{R}, \mathbf{R})$. الحلقة $Map(\mathbf{R}, \mathbf{R})$ تحتوي على عنصر محايد ضربي هو تطبيق الوحدة $1 : \mathbf{R} \to \mathbf{R}$ ، حيث $1(x) = x$ لكل $x \in \mathbf{R}$. الحلقة $Map(\mathbf{R}, \mathbf{R})$ تكون حلقة غير نوثيرية وغير أرتينية ، لأن:

ليكن

$$I_r = \{ f \in Map(\mathbf{R}, \mathbf{R}) \mid f(x) = 0 \ , \ \forall \ -r \le x \le r \} \ , r \in \mathbf{R}$$

من السهل اثبات أن I_r تكون مثالي في الحلقة $Map(\mathbf{R}, \mathbf{R})$. لاحظ أن $I_r \subset I_s$ لكل $r,s \in \mathbf{R}$ ، بحيث $s < r$.

$$I_1 \subset I_{1/2} \subset I_{1/3} \subset \ldots$$

تكون سلسلة تزايدية غير منتهية من مثاليات في الحلقة $Map(\mathbf{R}, \mathbf{R})$. إذن الحلقة $Map(\mathbf{R}, \mathbf{R})$ لا تحقق الشرط ACC (Ascending chain condition) . إذن الحلقة $Map(\mathbf{R}, \mathbf{R})$ تكون حلقة غير نوثيرية .

كذلك

$$I_1 \supset I_2 \supset I_3 \supset \ldots$$

تكون سلسلة تناقصية غير منتهية من مثاليات في الحلقة $Map(\mathbf{R}, \mathbf{R})$. إذن الحلقة $Map(\mathbf{R}, \mathbf{R})$ لا تحقق الشرط DCC (Descending chain condition) . إذن الحلقة $Map(\mathbf{R}, \mathbf{R})$ تكون حلقة غير أرتينية .

٢٨٠. اذكر مع الاثبات حلقة نوثيرية يمينية وغير نوثيرية شمالية .

الحل: نعتبر المجموعة التالية

$$R = \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \middle| \ x \in \mathbf{Z} , y,z \in \mathbf{Q} \right\}$$

من السهل اثبات أن R تكون حلقة ابدالية بالنسبة لعمليتي جمع وضرب المصفوفات وتحتوي محايد هو مصفوفة الوحدة $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

نثبت الآن أن R تكون حلقة نوثيرية يمينية . نفرض I مثالي يميني في R . ليكن m هو أصغر عدد صحيح موجب بحيث يوجد $\begin{bmatrix} m & y \\ 0 & z \end{bmatrix} \in I$. بما أن I مثالي يميني ، فإن

$$\begin{bmatrix} m & y \\ 0 & z \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} , \begin{bmatrix} m & y \\ 0 & z \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I$$

إذن

$$\begin{bmatrix} m & 0 \\ 0 & 0 \end{bmatrix} , \begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix} \in I$$

إذن

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1/m \end{bmatrix} \in I$$

إذن

$$\begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & y \end{bmatrix} \in I$$

كذلك

$$\begin{bmatrix} 0 & 0 \\ 0 & z \end{bmatrix} = \begin{bmatrix} m & y \\ 0 & z \end{bmatrix} - \begin{bmatrix} m & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix} \in I$$

إذا كان $z \neq 0$ ، فإن $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I$. إذن

$$I = \left\langle \begin{bmatrix} m & 0 \\ 0 & 0 \end{bmatrix} , \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} , \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle$$

إذن I يكون مثالي منتهي التوليد في الحلقة R .

وإذا كان كل عنصر في I في الصورة $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$ ، حيث $y \in \mathbf{Q}$, $x \in \mathbf{Z} \setminus \{0\}$ ، فإنة ينتج مما سبق أن

$$I = \left\langle \begin{bmatrix} m & 0 \\ 0 & 0 \end{bmatrix} , \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right\rangle$$

إذن أي مثالي يميني في R يكون منتهي التوليد . بالتالي R تحقق الشرط ACC (Ascending chain condition) للمثاليات اليمينية . إذن R تكون حلقة نوثيرية يمينية . فيما يلي نثبت أن R لا تكون حلقة نوثيرية شمالية .

ليكن n عدد صحيح موجب . ليكن

$$I_n = \left\{ \begin{bmatrix} 0 & a/2^n \\ 0 & 0 \end{bmatrix} \middle| \, a \in \mathbf{Z} \right\}$$

من السهل اثبات أن I_n يكون مثالي شمالي في الحلقة R . لاحظ أن $I_n \subset I_{n+1}$ ، لأن

$$\begin{bmatrix} 0 & a/2^n \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & a/2^{n+1} \\ 0 & 0 \end{bmatrix} \quad , \forall\, a \in \mathbf{Z}$$

إذن

$$I_1 \subset I_2 \subset I_3 \subset \ldots \qquad (*)$$

بما أن

$$\begin{bmatrix} 0 & a/2^{n+1} \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \begin{bmatrix} 0 & a/2^n \\ 0 & 0 \end{bmatrix} \quad , \forall\, x,a \in \mathbf{Z} \;,\; y,z \in \mathbf{Q}$$

فإن $I_{n+1} \not\subset I_n$. إذن المتسلسلة (*) تكون غير منتهية . إذن الحلقة R لا تحقق الشرط ACC للمثاليات الشمالية . إذن R لا تكون حلقة نوثيرية شمالية .