مقدمة في

نظرية الحلقات والحقول

(نظري - عملي)

يحتوي على 503 مسألة محلولة وغير محلولة

الأستاذ الدكتور

صفوان محمد عادل عويرة

مكتبة المتنبي

AL MOTANABI BOOK SHOP

بسم الله الرحمن الرحيم

مقدمة :

الحمد لله الذي علَّمَ بالقلم ، ويُعلِّمُكُمُ الله والله بكلِّ شيءٍ عَلِيْمٌ ، والصلاة والسلام على خير وأجود المعلمين ، المبعوث رحمة للعالمين ، سيِّدنا مُحَمَّدْ وعلى آلهِ الطيبين الطاهرين ، وصحابته الغرِّ الميامين ، وبعد :

ظهر مفهوم الحلقة، عند دراسة الأعداد الصحيحة وكثيرات الحدود، وأول من أدخل هذا المفهوم، الرياضي الألماني هيلبرت David Hilbert (١٨٦٢-١٩٤٣ م) . لكن تعريف الحلقة المستخدم في هذا الكتاب وغيره من الكتب العلمية ، قُدِّمَ من قِبَل الرياضية الألمانية أيمي نيوثر Emmy Noither (١٨٨٢-١٩٣٥ م) .

ونشير أيضاً ، إلى أن الرياضي كرونيكر Kronecker (١٨٢٣-١٨٩١ م) قدَّم مفهوم الحلقة التامة ، كما عرَّف الرياضي الشهير آبل Abel (١٨٠٢-١٨٢٩ م) الحقل ، بأنه نظام رياضي ذو عمليتين جبريتين .

يُعَدُّ هذا الكتاب امتداداً طبيعياً لكتاب (مقدمة في نظرية الزمر) ، حيث أن الكثير من التعاريف والمبرهنات الواردة في نظرية الحلقات والحقول مرتبطة بشكل كبير بنظرية الزمر ، فمثلاً التماثل الحلقي هو تعميم لمثيلاتها في نظرية الزمر ، كما أن مفهوم الزمر الجزئية الناظمية يقوم بالدور الذي تقوم به المثاليات في الحلقات .

يهدف الكتاب المقدَّم إلى ما يلي :

(آ)- استكمال دراسة البنى الجبرية ، والتي درس الطالب قسماً منها من خلال مقرر نظرية الزمر ، وبكلامٍ آخر ، التعمُّق بعض الشيء في دراسة البنى الجبرية .

(ب)- تزويد الطالب بجملة من الأدوات الجبرية ، التي ستساعده في دراسته المستقبلية ، أو في عمله التدريسي .

(جـ)- ترجمة الأفكار الجبرية المجرَّدة إلى لغة جبرية تطبيقية ، وذلك ، من خلال دراسة وحل التمارين المحلولة وغير المحلولة ، والتي تمكِّن الطالب من استيعاب مقرر الحلقات والحقول بشكل جيد وتثبيت المعلومات في ذهن الطالب ،

وكسب الطالب الثقة بذاته في حل التمارين غير المحلولة .

حوى الكتاب على قسمين ، قسم نظري ، والآخر عملي .

شمل **القسم النظري** على سبعة فصول ، حيث غطَّت مفردات مقرر الحلقات والحقول، وحاولت في العرض أن أبرز الترابط بين كل فصل والفصول التي تليه، وأدَعِّمَ المواضيع النظرية بأمثلة متنوعة وعديدة . وهذه الفصول النظرية هي :

- **الفصل الأول :** عُرِضَ فيه مفهوم الحلقة وخواصها والحلقة التامة ومفهوم الحقل .
- **الفصل الثاني :** قُدِّمَ فيه مفهوم الحلقات والحقول الجزئية ، وتعريف المثالية وأنواعها والعمليات عليها .
- **الفصل الثالث :** دُرِسَ فيه نظرية التشاكلات الحلقية ، وبعض الحلقات الخاصة ، مثل حلقة المثاليات الرئيسة ، الحلقة الإقليدية ، وحلقة التحليل الوحيد ، وحقل القواسم ، كما قُدِّمَ فيه أساس جاكبسون .
- **الفصل الرابع :** والمُعنوّن بحلقة كثيرات الحدود ، قُدِّمَ فيه خوارزمية القسمة ومبرهنة الباقي والعامل ، وكثيرات الحدود غير القابلة للتحليل والاختبارات المناسبة لها ، كذلك عُرِضَ فيه حلقة القسمة لكثيرات الحدود على حقل .
- **الفصل الخامس :** وجاء بعنوان الفضاءات الحلقية ، ودُرِسَ فيه مفهوم الفضاء الحلقي ، والفضاء الحلقي الجزئي ، والفضاءات الحلقية منتهية التوليد ، والفضاء الحلقي لخارج القسمة ، والتشاكلات في الفضاءات الحلقية .
- **الفصل السادس** ، وكان بعنوان تمديد الحقول ، وفيه تمَّت دراسة حقول الانشطار والحقول المنتهية وحقل جالوا ، والامتداد القابل للفصل والامتداد الناظمي .
- تناولنا في **الفصل السابع** والأخير الحلقات الارتينية والنوثيرية وخواصهما الأساسية ، وعلاقة بعض المثاليات في الحلقة النوثيرية ، وعلاقة الحلقة الارتينية بالحلقة النوثيرية .

أما **القسم العملي** ، شمل على مجموعة جيدة متنوعة وعديدة ، من التمارين المحلولة وغير المحلولة ، مرتَّبة حسب ترتيب الفصول النظرية الواردة في هذا الكتاب ، وتهدف إلى تدعيم فهم الطالب للمقرر واستيعابه على أكمل وجه ، وكانت هذه التمارين شاملة لجميع الجوانب النظرية .

كما زُوِّدَ الكتاب بدليل للمصطلحات العلمية ، وقائمة بالمراجع العلمية المستخدمة وبعض الرموز المتداولة في متن الكتاب .

أخيراً :

إن هذا الكتاب لم يُؤلَّف ليسُدَّ نقصاً في المكتبة العربية ، ولا أدَّعي أنه يقدِّم كشفاً جديداً في نظرية الحلقات والحقول ، بل أقدِّمُهُ تلبيةً لحاجة الطالب العربي ، ليكون عوناً له في دراسته وفي حياته العملية ، وإنني لأرجو الله الكريم أن أكون قد وُفِّقْتُ في هدفي هذا لما فيه خير للمملكة العربية السعودية المعطاءة ، والـــوطن العربـــي الحبيب ، والله ولي التوفيق .

الأستاذ الدكتور

الدمام في / / ١٤٢٧ **صفوان محمد عادل عويرة**

المحتوى

(آ) القسم النظري

الموضوع	الصفحة

الفصل الأول : الحلقة والحلقة التامة

الفصل الثاني : الحلقات والحقول الجزئية والمثاليات

الموضوع	الصفحة

الفصل الثالث : التماثل الحلقي

الفصل الرابع : حلقة كثيرات الحدود

الموضوع | الصفحة

الفصل الخامس : الفضاءات الحلقية (الحلقيات)

الفصل السادس : تمديد الحقول

الفصل السابع : الحلقات الارتينية والنوثيرية

الموضوع	الصفحة

(ب) القسم العملي

(أ) القسم النظري

الفصل الأول

الحلقة والحلقة التامة

Ring & Integral domains

الفصل الأول

الحلقة والحلقة التامة

Ring & Integral domains

درسنا ، في نظرية الزمر ، مجموعات مزودة بعملية ثنائية واحدة ، ورمّزنا لهذه العملية بأحد الرموز ★ , ⊥ , o , + , •,... . سندرس الآن مجموعات مزودة بقانوني تشكيل داخليين . فمثلاً نرمز للأول بـ ★ والثاني o أو (+) للأول و(•) للثاني . أو أي رمزين آخرين .

نسمي هذه المجموعة المزودة بقانوني التشكيل الداخليين السابقين اسم حلقة Ring ، إذا حققت شروطاً معينة سنقدمها بعد قليل .

تعد الحلقة إحدى أهم البنى الجبرية ، لما لها من ارتباط ببنى جبرية جديدة ، ولأنها تدخل في كثير من التخصصات الرياضية المهمة والمتنوعة .

يعد الرياضي الألماني (David Hillert 1869-1943) أول من أدخل مفهوم الحلقة وكان ذلك عام 1879 .

لنذكّر القارئ الكريم بالمفاهيم التالية :

1- العملية الثنائية على مجموعة غير خالية ولتكن S هي تطبيق :

$\varphi: S\times S \longrightarrow S$ ، حيث تمثل $S\times S$ الجداء الديكارتي لـ S في نفسها ، أي أن $S\times S$ هي مجموعة كل الأزواج المرتبة (a,b) حيث $a,b\in S$. نكتب عادةً صورة الزوج المرتب (a,b) تحت تأثير φ بالشكل $a\star b$ حيث ★ الرمز المناسب للعملية الثنائية . لاحظ ، أن الترتيب مهم ، حيث أنه من المحتمل أن يكون $a\star b$ و $b\star a$ عنصرين مختلفين في S . وفي حالة كون $a\star b = b\star a$ لكل $a,b\in S$ فإن العملية ★ تسمى إبدالية Commutative .

2- شبه الزمرة (Semigroup) : هي مجموعة غير خالية ، ولتكن S مزودة

بعملية ثنائية ★ تحقق خاصة التجميع أو (الدامجة) أو التجميعية ، أي أن :
$(a\star b)\star c = a\star(b\star c)$ ، لكل $a,b,c\in S$.

3- الزمرة (Group) : هي مجموعة غير خالية ، ولتكن G مع عملية ثنائية ★ بحيث تتحقق الشروط التالية :

(1) تشكل $(G,\star)$ شبه زمرة .

(2) يوجد عنصر e من G يحقق $a\star e = e\star a = a$ لكل $a\in G$. يسمى العنصر e بالعنصر المحايد (Identity element) .

(3) لكل عنصر $a\in G$ معكوس (Inverse) وليكن $\bar{a}\in G$ بحيث يتحقق :

$$a\star\bar{a} = \bar{a}\star a = e$$

(1-1) مفهوم الحلقة :

لتكن R مجموعة ما غير خالية ، ولتكن (+) و(•) عمليتين جبريتين ثنائيتين معرفتين على R. نقول عن الثلاثية $(R,+,\cdot)$ إنها حلقة بالنسبة للعمليتين (+) و(•) إذا تحققت الشروط التالية :

1- $(R,+)$ زمرة إبدالية (Abelian group) .

2- $(R,\cdot)$ شبه زمرة (نصف زمرة) (Samigroup) .

3- العملية (•) توزيعية (Distributive) على العملية (+) من اليمين واليسار .
أو بكلام آخر ترتبط العمليتان (+) و(•) فيما بينهما بعملية توزيع الضرب على الجمع من الطرفين، وهذا يعني:

من أجل أي a,b,c من R ، فإن :

$$a\cdot(b+c) = a\cdot b + a\cdot c$$
$$(b+c)\cdot a = b\cdot a + c\cdot a$$

إذا كانت العملية (•) بالإضافة إلى الشروط السابقة ، عملية إبدالية على عناصر المجموعة R ، فإننا نقول إن الحلقة $(R,+,\cdot)$ هي **حلقة إبدالية Commutative ring** إذا وُجد في المجموعة R عنصر محايد بالنسبة لعملية

$(\bullet)$ (هذا العنصر وحيد) فإننا نقول عن هذا العنصر إنه عنصر وحدة في الحلقة $(R,+,\bullet)$ وسنرمز له بالرمز 1 أي أن : لكل $a\in R$ ، فإن $1\bullet a = a \bullet a = a$.

ونقول في هذه الحالة ، إن الحلقة $(R,+,\bullet)$ **حلقة واحدية** أو **حلقة ذات عنصر وحدة** أو **حلقة بمحايد (Ring with identity)** .

ملاحظة (1) :

نؤكد أن $(+)$ و$(\bullet)$ تمثلان عمليتين ثنائيتين مجردتين ، وليس عمليتي الجمع والضرب العاديتين .

ونرمز للمعكوس الضربي أي بالنسبة لعملية الضرب $(\bullet)$ للعنصر a في R بالرمز $\bar{a}$ ويسمى معكوس (مقلوب) العنصر a . أما المعكوس الجمعي للعنصر a في R نرمز له بـــ $-a$ ويسمى بالمعكوس (نظير) الجمعي للعنصر a في R .

سنرمز لصفر الحلقة $(R,+,\bullet)$ بـــ o .

نسمي العملية الجبرية الثنائية $(-)$ المعرفة على R بالشكل :

$$a - b = a + (-b) \quad , \quad \forall\, a,b\in R$$ **عملية الطرح**

وبالتالي يتحقق ما يلي :

$$a \bullet (b - c) = a \bullet b - a \bullet c$$

$$(b - c) \bullet a = b \bullet a - c \bullet a \quad , \forall\, a,b,c\in R$$

لأن من قانون التوزيع الضربي على الجمع نجد أن :

$$\begin{aligned} a \bullet (b - c) &= a \bullet (b + (-c)) = a \bullet b + a \bullet (-c) \\ &= a \bullet b + (-a \bullet c) = a \bullet b - a \bullet c \end{aligned}$$

وبنفس الطريقة ، نثبت أن :

$$(b - c) \bullet a = b \bullet a - c \bullet a$$

(2-1) أمثلة :

1- المجموعات العددية التالية : Z (مجموعة الأعداد الصحيحة) ، Q (مجموعة

الأعداد النسبية الكسرية) ، R (مجموعة الأعداد الحقيقية) تشكل حلقة إبدالية وبمحايد بالنسبة لعمليتي الجمع والضرب العاديتين .

أي أن $(Z,+,\cdot)$ و $(Q,+,\cdot)$ و $(R,+,\cdot)$ حلقات إبدالية بمحايد .

2- مجموعة الأعداد المركبة C بالنسبة لعمليتي $(+)$ و $(\cdot)$ المعرفتين بالشكل :

$$x = a + i\,b\ ,\ y = c + i\,d\ :\ \forall\, a,b,c \in R$$

حيث أن $a,b,c,d \in R$ و $i = \sqrt{-1}$.

$$x + y = a + i\,b + c + i\,d = (a + c) + i\,(b + d)$$
$$x \cdot y = (a + i\,b) \cdot (c + i\,d) = (a \cdot c - b \cdot d) + i\,(a \cdot d + b \cdot c)$$

تشكل حلقة إبدالية بمحايد .

تسمى حلقة الأعداد المركبة $(C,+,\cdot)$ حلقة جاوص الصحيحة (ring of Gaussian integers).

3- مجموعة الأعداد الفردية ، لا تشكل حلقة بالنسبة لعمليتي الجمع والضرب العاديتين لأنه على سبيل المثال ، حاصل جمع عددين فرديين هو عدد زوجي ، لذا فإن مجموعة الأعداد الفردية (ليست عملية ثنائية) ليست مغلقة بالنسبة لعملية الجمع العادي .

4- يمكن التحقق من أن المجموعة $Z[\sqrt{5}] = \{\, a + b\sqrt{5}\,;\, a,b \in Z \}$

تشكل حلقة إبدالية بمحايد ، بالنسبة للعمليتين الجمع والضرب العاديتين حيث أن : $0 + 0\sqrt{5}$ هو صفر الحلقة (المحايد الجمعي) و $1 + 0\sqrt{5}$ عنصر الوحدة (المحايد الضربي) .

5- إن $(M_2(R),+,\cdot)$ حلقة بالنسبة لعمليتي جمع وضرب المصفوفات حيث أن:

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a,b,c,d \in R \right\}$$

إن صفر هذه الحلقة هو المصفوفة الصفرية $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ وعنصر الوحدة فيها هو

المصفوفة الواحدية $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$. لكنها ليست إبدالية ، فعلى سبيل المثال :

$$\forall\begin{pmatrix}1 & -2\\3 & 4\end{pmatrix},\begin{pmatrix}1 & 2\\-1 & -3\end{pmatrix}\in M_2(R)$$

فإن :

$$\begin{pmatrix}1 & -2\\3 & 4\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\-1 & -3\end{pmatrix}=\begin{pmatrix}3 & 8\\-1 & -6\end{pmatrix}\neq\begin{pmatrix}7 & 6\\-10 & -10\end{pmatrix}$$
$$=\begin{pmatrix}1 & 2\\-1 & -3\end{pmatrix}\cdot\begin{pmatrix}1 & -2\\3 & 4\end{pmatrix}$$

ملاحظة (2) :

يمكن تعميم المثال السابق بالشكل :

لتكن $(R,+,\cdot)$ حلقة ، وإذا كانت $M_n(R)$ مجموعة المصفوفات المربعة من الدرجة n والتي عناصرها من R ، فإن $(M_n(R),+,\cdot)$ حلقة بالنسبة لعمليتي جمع وضرب المصفوفات . حيث أن المصفوفة الصفرية من الدرجة n هي صفر الحلقة ، المصفوفة الواحدية من المرتبة n هي عنصر الوحدة فيها .

6- إذا كانت M مجموعة جميع التطبيقات $f : R\longrightarrow R$. ولنعرف العمليتين الثنائيتين (+) و(•) بالشكل :

$$(f+g)(a)=f(a)+g(a)\qquad \forall a\in R$$
$$(f\cdot g)(a)=f(a)\cdot g(a)\qquad \forall a\in R$$

عندئذٍ تكون $(M,+,\cdot)$ حلقة إبدالية بمحايد .

إن التطبيق $I_0 : R\longrightarrow R$ المعرف بـ $i_0(x) = 0$ هو العنصر المحايد بالنسبة لعملية الجمع (المحايد الجمعي) $x\in R$ ، كما أن $I_1 : R\longrightarrow R$ المعرف بـ $I_1(x) = 1$ هو عنصر الوحدة بالنسبة لعملية الضرب (المحايد الضربي) .

7- لتكن $(R,+,\cdot)$ و$(S,T,\star)$ حلقتين إبداليتين واحديتين ولنرمز بـ o و o`

لصفريهما على الترتيب . وإذا كانت $D = \{(a,b)\ ;\ a\in R\ ,\ b\in S\}$ ، ولنعرف على المجموعة D العملية الثنائية Δ و $\perp$ بالشكل التالي :

$$(x,y)\ \Delta\ (x_1,y_1) = (x + x_1\ ,\ y\ T\ y_1)$$

$$(x,y) \perp (x_1,y_1) = (x \cdot x_1\ ,\ y \star y_1)$$

وذلك من أجل أي (x,y) و(x_1,y_1) من D ، عندئذٍ تكون $(D,\Delta,\perp)$ حلقة إبدالية واحدية .

الحل :

1) من تعريف المجموعة D ، نرى أن $D \neq \phi$.

2) العملية Δ دامجة (تجميعية) على عناصر D لأنه إذا كان : $(x_1,y_1)\ ,\ (x_2,y_2)\ ,\ (x_3,y_3) \in D$ فإن:

$$\begin{aligned}[(x_1,y_1)\ \Delta\ (x_2,y_2)]\ \Delta\ (x_3,y_3) &= (x_1 + x_2\ ,\ y_1\ T\ y_2)\ \Delta\ (x_3,y_3)\\ &= [(x_1 + x_2) + x_3\ ,\ (y_1\ T\ y_2)\ T\ y_3]\\ &= [x_1 + (x_2 + x_3)\ ,\ y_1\ T\ (y_2\ T\ y_3)]\\ &= (x_1,y_1)\ \Delta\ (x_2 + x_3\ ,\ y_2\ T\ y_3)\\ &= (x_1,y_1)\ \Delta\ [(x_2,y_2)\ \Delta\ (x_3,y_3)]\end{aligned}$$

3) العملية Δ إبدالية على عناصر D لأن إذا كان $(x_1,y_1),(x_2,y_2)$ عنصرين ما من D، فإن:

$$\begin{aligned}(x_1,y_1)\ \Delta\ (x_2,y_2) &= (x_1 + x_2\ ,\ y_1\ T\ y_2)\\ &= (x_2 + x_1\ ,\ y_2\ T\ y_1) = (x_2,y_2)\ \Delta\ (x_1,y_1)\end{aligned}$$

4) إن $(o,o`)$ عنصراً محايداً في المجموعة D بالنسبة للعملية $\Delta$ ، لأن من جهة أولى $(o,o`)$ عنصر من D ، ومن ناحية ثانية ، إن :

$$(x,y)\ \Delta\ (o,o`) = (x+o\ ,\ yTo`) = (x,y)\quad ;\ \forall\ (x,y)\in D$$

5) ليكن (x,y) عنصراً ما من D ، إن $(-x,-y)$ هو معكوس (نظير) العنصر (x,y) في D بالنسبة للعملية Δ ، حيث $-x$ هو معكوس x في R بالنسبة للعملية +

و y- هو معكوس العنصر y في S بالنسبة للعملية T ، لأن $(-x,-y)$ عنصراً من D أولاً ، ثم أن :

$$(x,y)\ \Delta\ (-x,-y) = \big(x + (-x)\ ,y\ T\ (-y)\big) = (o,o`)$$

مما سبق نستنتج أن (D,Δ) زمرة إبدالية .

لنثبت الآن أن $(D,\perp)$ شبه زمرة ، أي أن العملية $\perp$ تجميعية على عناصر المجموعة D .

6- لتكن (x,y) , (x_1,y_1) , (x_2,y_2) عناصر من المجموعة D ، فإن :

$$\begin{aligned}
\big[(x,y) \perp (x_1,y_1)\big] \perp (x_2,y_2) &= (x\cdot x_1, y\star y_1) \perp (x_2,y_2)\\
&= \big[(x\cdot x_1)\cdot x_2\ , (y\star y_1)\star y_2\big]\\
&= \big[x\cdot(x_1\cdot x_2)\ , y\star(y_1\star y_2)\big]\\
&= (x,y) \perp \big[(x_1\cdot x_2)\ , (y_1\star y_2)\big]\\
&= (x,y) \perp \big[(x_1,y_1) \perp (x_2,y_2)\big]
\end{aligned}$$

لنبرهن أن Δ و $\perp$ يحققان قانوني التوزيع .

7- ليكن (x,y) , (x_1,y_1) , (x_2,y_2) عناصر من D ، فإن :

$$\begin{aligned}
(x,y) \perp \big[(x_1,y_1)\ \Delta\ (x_2,y_2)\big] &= (x,y) \perp (x_1 + x_2\ , y_1\ T\ y_2)\\
&= \big[x\cdot(x_1+x_2)\ , y\star(y_1 T\ y_2)\big]\\
&= \big[(x\cdot x_1)\cdot x_2\ , y\star(y_1 T\ y_2)\big]\\
&= \big[(x\cdot x_1 + x\cdot x_2)\ , (y\star y_1)\ T\ (y\star y_2)\big]\\
&= (x\cdot x_1\ , y\star y_1)\ \Delta\ (x\cdot x_2\ , y\star y_2)\\
&= \big[(x,y) \perp (x_1,y_1)\big]\ \Delta\ \big[(x,y) \perp (x_2,y_2)\big]
\end{aligned}$$

$$\begin{aligned}
\big[(x_1,y_1)\ \Delta\ (x_2,y_2)\big] \perp (x,y) &= (x_1 + x_2\ , y_1\ T\ y_2) \perp (x,y)\\
&= \big[(x_1 + x_2)\cdot x\ , (y_1 T\ y_2)\star y\big]\\
&= (x_1\cdot x + x_2\cdot x\ , y_1\star y\ T\ y_2\star y)\\
&= (x_1\cdot x\ , y_1\star y)\ \Delta\ (x_2\cdot x\ , y_2\star y)\\
&= \big[(x_1,y_1) \perp (x,y)\big]\ \Delta\ \big[(x_2,y_2) \perp (x,y)\big]
\end{aligned}$$

نستنتج مما سبق أن $(D,\Delta,\perp)$ حلقة .

لنثبت الآن ، أن الحلقة $(D,\Delta,\perp)$ إبدالية . علماً أن كلاً من الحلقتين $(R,+,\cdot)$ و$(S,T,\star)$ إبداليتين . ليكن (x,y) , (x_1,y_1) عنصرين من D ، فإن :

$$\begin{aligned}(x,y) \perp (x_1,y_1) &= (x \cdot x_1 , y \star y_1)\\ &= (x_1 \cdot x , y_1 \star y)\\ &= (x_1,y_1) \perp (x,y)\end{aligned}$$

لنثبت أخيراً أن الحلقة $(D,\Delta,\perp)$ واحدية (ذات عنصر وحدة) .

لنرمز بـ 1 للعنصر الوحدة في الحلقة $(R,+,\cdot)$ وبـ e لعنصر الوحدة في الحلقة $(S,T,\star)$. عندئذٍ يكون $(1,e)$ هو عنصر وحدة في الحلقة $(D,\Delta,\perp)$ ، لأنه ، أولاً $(1,e)$ عنصر من D . وإذا كان (x,y) عنصراً ما من D ، فإن :

$$\begin{aligned}(x,y) \perp (1,e) &= (x \cdot 1, y \star e) = (x,y) = (1 \cdot x , e \star y)\\ &= (1,e) \perp (x,y)\end{aligned}$$

إذاً $(D,\Delta,\perp)$ حلقة إبدالية واحدية .

نتيجة (1) :

تماماً ، كما في نظرية الزمر ، إذا كانت $(R,+,\cdot)$ حلقة ما ، محايدها بالنسبة لعملية (+) هو o وإذا كان a عنصراً من R و n عدداً صحيحاً موجباً ، فإننا نصطلح ما يلي :

$$\underbrace{a.a.\cdots.a}_{\text{مرة}\, n} = a^n \quad , \quad o.a = o \qquad (1)$$

$$\underbrace{a+a+\cdots+a}_{\text{مرة}\, n} = n.a \quad \text{و} \quad n(-a) = (-n)a = -(na) \qquad (2)$$

$$m_1 (m_2.a) = (m_1 . m_2) . a \qquad (3)$$

$$m_1.a + m_2.a = (m_1 + m_2) . a \qquad (4)$$

$$(a^{n_1})^{n_2} = a^{n_1 \cdot n_2} \qquad (5)$$

$$a^{n_1}.a^{n_2} = a^{n_1 + n_2} \qquad (6)$$

من أجل أي عددين صحيحين m_1 وm_2 وn_1 وn_2 عددين صحيحين موجبين .

وإذا كانت $(R,+,\cdot)$ حلقة واحدية وe هو العنصر المحايد فيها) ، وإذا كان a عنصراً ما منها ، فإن : $(a^{-1})^n = a^{-n}$ حيث a^{-1} معكوس العنصر a في R بالنسبة للعملية $(\cdot)$ وn عدد صحيح موجب . ونصطلح على اعتبار $a^0 = e$. ويمكن التحقق من صحة ما يلي :

1- $(a^{-1})^{n_1} = (a^{n_1})^{-1}$

2- $(a^{n_1})^{n_2} = a^{n_1 \cdot n_2}$

3- $a^{n_1} . a^{n_2} = a^{n_1 + n_2}$

وذلك من أجل أي عددين صحيحين n_1 وn_2 .

(3-1) بعض خواص الحلقة $(R,+,\cdot)$:

نقدم بعض الخواص الأساسية للحلقة $(R,+,\cdot)$ من خلال المبرهنات والنتائج التالية :

مبرهنة (1) :

إذا كانت $(R,+,\cdot)$ حلقة ، ولنرمز لصفرها بـ o عندئذٍ يتحقق ما يلي :

(1) $a \cdot o = o \cdot a = 0$

(2) $(-c) \cdot a = -c \cdot a \ , \ a \cdot (-c) = -a \cdot c$

(3) $(-a) \cdot (-b) = a \cdot b$ وذلك من أجل أي b,a من R .

البرهان :

(1) بما أن العلاقتين :

$$(*) \quad \left.\begin{array}{l} a\cdot(b-c) = a\cdot b - a\cdot c \\ (b-c)\cdot a = b\cdot a - c\cdot a \end{array}\right\}$$

صحيحتان من أجل أي c,b,a من R ، فهما صحيحتان من أجل الحالة $b = c$ بوضع في العلاقتين السابقتين $b = c$ نجد :

$$\left.\begin{array}{l} a\cdot(b-b) = a\cdot b - a\cdot b \Rightarrow a\cdot o = o \ ; \forall a \in R \\ (b-b)\cdot a = b\cdot a - b\cdot a \Rightarrow o\cdot a = o \end{array}\right\}$$

(2) بما أن العلاقتين السابقتين (*) صحيحتان من أجل أي c,b,a من R ، فهما صحيحتان من أجل $b = 0$. بوضع $b = 0$ في العلاقتين (*) وبملاحظـــة (1) نجد :

$$a(o-c) = a\cdot o - a\cdot c \Rightarrow a\cdot(-c) = -a\cdot c$$

$$(o-c)\cdot a = -c\cdot a \quad ; \quad \forall\, a,c \in R$$

(3) بتبديل في (2) كل a بـــ -a نجد :

$$a\cdot(-c) = -a\cdot c$$

$$(-a)\cdot(-c) = -(-a)\cdot c$$

$$(-a)\cdot(-c) = -(-a\cdot c) = a\cdot c$$

ونسمي الحلقة التي تحوي الصفر فقط بالحلقة الصفرية (Zero ring) .

نتيجة (2) :

إذا كانت $(R,+,\cdot)$ حلقة واحدية ، (نرمز لعنصر الوحدة فيها بـــ 1) ولصفرها بـــ 0 فإذا كانت $R \neq \{0\}$ ، فإن $1 \neq 0$. و$(-1)\cdot a = -a$

البرهان :

بما أن $R \neq \{0\}$ ، عندئذٍ يوجد $a \in R$ بحيـــث $a \neq 0$. لنفـــرض جـــدلاً أن $1 = 0$، عندئذٍ ، يكون $a = a\cdot 1 = a\cdot 0 = 0$ أي أن $a = 0$ وهذا مخالف للفرض أن $a \neq 0$ ، وبذلك يكون الفرض الجدلي خاطئ ، إذن $1 \neq 0$.

لنبرهن ، أن $(-1)\cdot a = -a$.

حسب المبرهنة (1) السابقة في الفقرة (2) نجد :

$$(-1)\cdot a = -(1\cdot a) = -a \quad ; \quad \forall\, a \in R$$

سنفرض من الآن ، أن كل حلقة واحدية ، تحتوي على أكثر من عنصر واحد .

نتيجة (3) :

لتكن $(R,+,\cdot)$ حلقة ما ، إذا وُجد في R عنصر الوحدة ، فإنه سيكون وحيـــداً . وإذا وجد لعنصر ما من R معكوس ، فإنه يكون وحيداً أيضاً .

البرهان :

ليكن 1 و `1 عنصرين محايدين للحلقة الواحدية $(R,+,\cdot)$ ، فإن :

$$1 = 1\cdot 1` = 1`$$

وإذا كان a_1 و a_2 معكوسين للعنصر a في الحلقة الواحدية $(R,+,\cdot)$ ، فإن :

$$a_2 = a_2\cdot 1 = a_2\cdot(a\cdot a_1) = (a_2\cdot a)\cdot a_1 = 1\cdot a_1 = a_1$$

إذاً $a_1 = a_2$.

مبرهنة (2) :

لتكن $(R,+,\cdot)$ حلقة ذات عنصر الوحدة ، إذا كانت G_R مجموعة عناصر الوحدة في الحلقة $(R,+,\cdot)$ ، عندئذٍ ، $(G_R,\cdot)$ زمرة .

البرهان :

المجموعة $G_R \neq \phi$ ، لأنها تحوي على الأقل العنصر المحايد في الحلقة $(R,+,\cdot)$ والذي هو نفسه العنصر المحايد في المجموعة G_R .

إذا كان b,a عنصرين ما من G_R، فإنه يوجد عنصران b^{-1},a^{-1} من R بحيث يكون:

$$a\cdot a^{-1} = a^{-1}\cdot a = 1 \ , \ b\cdot b^{-1} = b^{-1}\cdot b = 1$$

وبالتالي فإن :

$$(a\cdot b)\,(b^{-1}\cdot a^{-1}) = a\cdot(b\cdot b^{-1})\cdot a^{-1} = a\cdot 1\cdot a^{-1} = a\cdot a^{-1} = 1$$

$$(b^{-1}\cdot a^{-1})\,(a\cdot b) = b^{-1}\cdot(a^{-1}\cdot a)\cdot b = b^{-1}\cdot 1\cdot b = b^{-1}\cdot b = 1$$

وهذا يعني أن $a\cdot b \in G_R$ (مغلقة) .

بما أن $(R,\cdot)$ تجميعية، فإن عملية الضرب تجميعية على عناصر المجموعة G_R لأنها $G_R \subseteq R$. إذن $(G_R,\cdot)$ زمرة .

نسمي عادةً الزمرة $(G_R,\cdot)$ بزمرة الوحدات (Group of units) للحلقة R .

(4-1) حلقة الأعداد الصحيحة قياس n :

(ring of integres modultion)

نذكّر القارئ الكريم أولاً، **بمفهوم التطابق قياس** n (Congruent modulo n) .

ليكن n عدداً صحيحاً موجباً ، نقول إن العددين الصحيحين b,a متطابقان قياس n إذا ، وفقط إذا، كان $a - b$ يقبل القسمة على n وهذا يكافئ $a - b = k.n$ حيث k عدد صحيح ، ونكتب بذلك : $a \equiv b \pmod{n}$.

إن علاقة التطابق قياس n هي علاقة تكافؤ على مجموعة الأعداد الصحيحة وأن فصول التكافؤ لهذه العلاقة هي : $[0],[1],\ldots,[n-1]$ حيث أن :

$$[x] = \{ x + t.n \ ; t \in Z \}$$

نسمي Z_n مجموعة الأعداد الصحيحة قياس n ، حيث Z_n مجموعة فصول التطابق قياس n .

وإذا عرّفنا على المجموعة Z_n العمليتين الثنائيتين $\oplus$ و$\otimes$ بالشكل :

$$[x] \oplus [y] = [x + y]$$

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

عندئذٍ $(Z_n,\oplus,\otimes)$ حلقة إبدالية بمحايد (ذات عنصر وحدة) .

نسمي عادةً هذه الحلقة بحلقة الأعداد الصحيحة قياس n .

البرهان :

لنبرهن أولاً أن العمليتين الثنائيتين $\oplus$ و$\otimes$ معرفتين جيداً (حسنة التعريف) ، من أجل ذلك ، ليكن $[x] = [x_1]$ و$[y] = [y_1]$ ، وبالتالي فإن :

$$x \equiv x_1 \bmod n \ , \ y \equiv y_1 \bmod n$$

أي أن $n / (x_1-x)$ و $n / (y_1-y)$ ، وهذا يؤدي إلى أن : $n / [(x_1+y_1) - (x+y)]$

وبالتالي فإن : $(x_1+y_1) \equiv (x+y) \bmod n$ ، أي أن : $[x+y] = [x_1+y_1]$.

إذن ، عملية الجمع $\oplus$ معرفة جيداً . لنبرهن أيضاً ، وبنفس الطريقة أن عملية

الضرب $\otimes$ معرفة جيداً :

ليكن $[x] = [x_1]$ ، $[y] = [y_1]$ وهذا يؤدي إلى أن :

$x_1 - x = k_1.n$ و $y_1 - y = k_2.n$ حيث k_1 و k_2 عددان صحيحان ، إذن :

$$x_1.y_1 = (x + k_1.n)(y + k_2.n) = x.y + xk_2n + yk_1.n + k_1k_2.n^2$$

وهذا يعطي : $x_1.y_1 \equiv x.y \bmod n$ ، ومنه $[x_1.y_1] = [x.y]$.

إذن عملية الضرب $\otimes$ معرفة جيداً أيضـــاً . أي أن العمليتـــين $\oplus,\otimes$ لا تتعلقـــان بالممثلين المختارين لفصلي التكافؤ .

لنبرهن الآن أن $(Z_n, \oplus)$ زمرة إبدالية .

ليكن $[x],[y],[z]$ من Z_n وبالتالي فإن :

$$\begin{aligned}([x] \oplus [y]) \oplus [z] &= [x + y] \oplus [z] = [x + y + z]\\ &= [x + (y + z)] = [x] \oplus [y + z]\\ &= [x] \oplus ([y] \oplus [z])\end{aligned}$$

كما أن :

$$[x] \oplus [y] = [x + y] = [y + x] = [y] \oplus [x]$$

لاحظ أننا استفدنا من كون عملية الجمع العادي + عملية تجميعية وإبدالية على Z .

إن $[o]$ هو العنصر المحايد بالنسبة لعملية الجمع $\oplus$ ، وكذلك $[n-x]$ هو معكوس للعنصر $[x]$ وهذا ينتج حسب تعريف عملية الجمع $\oplus$.

إذن $(Z_n, \oplus)$ زمرة إبدالية .

لنثبت الآن ، أن عملية الضرب $\otimes$ تجميعية على عناصر Z_n :

بما أن عملية الضرب العادي $(\bullet)$ عملية تجميعية على عناصر Z_n ، فيكون :

$$\begin{aligned}([x] \otimes [y]) \otimes [z] &= [x \bullet y] \otimes [z] = [(x \bullet y) \bullet z] = [x \bullet (y \bullet z)]\\ &= [x] \otimes [y \bullet z] = [x] \otimes ([y] \otimes [z])\end{aligned}$$

وهذا يبين لنا أن عملية $\otimes$ تجميعية على عناصر Z_n .

لنبرهن أن عملية الضرب $\otimes$ توزيعية على الجمع $\oplus$ من اليسار، وبالطريقة نفسها،

نبرهن أن عملية الضرب $\otimes$ توزيعية على الجمع $\oplus$ من اليمين .

$$[x] \otimes ([y] \oplus [z]) = [x] \otimes [y + z] = [x\cdot(y+z)] = [x\cdot y + x\cdot z]$$
$$= [x\cdot y] \oplus [x\cdot z] = ([x] \otimes [y]) \oplus ([x] \otimes [z])$$

نستنتج مما سبق ، أن $(Z_n,\oplus,\otimes)$ تشكل حلقة بمحايد وهو $[1]$. وبما أن عملية الضرب العادي في Z هي عملية إبدالية ، فإن :

$$[x] \otimes [y] = [x \cdot y] = [y\cdot x] = [y] \otimes [x]$$

إذن $(Z_n,\oplus,\otimes)$ حلقة إبدالية بمحايد .

(5-1) الحلقة التامة (المناطق التكاملية) Integral domains :

القاسم اليميني والقاسم اليساري للصفر في حلقة :

لتكن $(R,+,\cdot)$ حلقة ما ، ولنرمز لصفرها بـ o ، وليكن a عنصراً ما من A ، نقول عن a إنه قاسم يميني للصفر في الحلقة $(R,+,\cdot)$ ، إذا وجد في R عنصراً ، وليكن $b \neq o$ بحيث يكون $b \cdot a = o$.

ونقول عن a إنه قاسم يساري للصفر في الحلقة $(R,+,\cdot)$ ، إذا وجد في R عنصراً وليكن $c \neq o$ بحيث يكون : $a\cdot c = o$.

ينتج من التعريف السابق ما يلي :

(1) إذا كانت $(R,+,\cdot)$ حلقة ما ، و o صفرها ، وإذا كانت $R \neq \{o\}$ ، فإن o هو قاسم يميني ويساري للصفر في الحلقة $(R,+,\cdot)$ ، لأنه ، إذا كان $a \neq o$ عنصراً من R ، فإن :

$$a\cdot o = o\cdot a = o$$

(2) لتكن $(R,+,\cdot)$ حلقة واحدية ، وإذا كان a عنصراً منها ، وله معكوس فيها، فإن a لا يمكن أن يكون قاسماً يسارياً ولا يمينياً للصفر في هذه الحلقة .

البرهان :

لنرمز بـ 1 لعنصر الوحدة في الحلقة $(R,+,\cdot)$ ولصفرها بالرمز o . إن العنصر a من R لا يمكن أن يكون قاسماً يسارياً للصفر فيها،. لأنه إذا كان a

قاسماً يسارياً للصفر فيها ، فإنه بالإمكان إيجاد عنصر وليكن $b \neq o$ من R وبحيث يكون $a \bullet b = o$ ، لكن :

$$a \bullet b = o \Rightarrow a^{-1} \bullet (a \bullet b) = a^{-1} \bullet o \Rightarrow (a^{-1} \bullet a) \bullet b = o \Rightarrow$$
$$1 \bullet b = o \Rightarrow b = o$$

وهذا مخالف لكون $b \neq o$.

وبالطريقة نفسها ، نثبت أن العنصر a من R لا يمكن أن يكون قاسماً يمينياً للصفر في الحلقة $(R,+,\bullet)$.

ملاحظة (2) :

عندما نقول إن الحلقة $(R,+,\bullet)$ لا تحوي قواسم للصفر (Zero divisor) نقصد بذلك إن لم يكن بالإمكان إيجاد عنصرين b,a من R بحيث يكون :

$$a \neq o \;,\; b \neq o \;,\; a \bullet b = o$$

حيث o هو صفر الحلقة $(R,+,\bullet)$.

مثال (1) :

لتكن $(M_2(R),+,\bullet)$ حلقة المصفوفات المربعة الحقيقية من الدرجة الثانية . إن $\begin{pmatrix} o & o \\ c & d \end{pmatrix}$ ، حيث d,c من R ، قاسم للصفر من اليمين وأن $\begin{pmatrix} a & o \\ b & o \end{pmatrix}$ قاسم للصفر من اليسار ، في الحلقة $(M_2(R),+,\bullet)$.

الحل :

$$\begin{pmatrix} o & o \\ c & d \end{pmatrix} \neq \begin{pmatrix} o & o \\ o & o \end{pmatrix} , \begin{pmatrix} a & o \\ b & o \end{pmatrix} \neq \begin{pmatrix} o & o \\ o & o \end{pmatrix}$$

نلاحظ ، أولاً أن :

$$\begin{pmatrix} a & o \\ b & o \end{pmatrix} \bullet \begin{pmatrix} o & o \\ c & d \end{pmatrix} = \begin{pmatrix} o & o \\ o & o \end{pmatrix}$$

و

$$\begin{pmatrix} o & o \\ c & d \end{pmatrix} \bullet \begin{pmatrix} a & o \\ b & o \end{pmatrix} = \begin{pmatrix} o & o \\ o & o \end{pmatrix}$$

مثال (2) :

العدد 2 هو قاسم للصفر في الحلقة $(Z_4,\oplus,\otimes)$، وكذلك العـــددين 2 و3 فـــي الحلقة $(Z_6,\oplus,\otimes)$.

إن مجموعة الأزواج المرتبـــة $S = \{(a,b) : a,b \in Z\}$ مـــع عمليتـــي الجمـــع والضرب التاليتين :

$$(a,b) + (c,d) = (a+c\ ,\ b+d)$$

$$(a,b) \cdot (c,d) = (a \cdot c\ ,\ b \cdot d)$$

تشكل حلقة إبدالية وبمحايد ، حيث أن صفرها هو (o,o) ومحايدها هـــو $(1,1)$. كما أن $(1,o)$ قاسم للصفر لأن :

$$(1,o) \cdot (o,1) = (o,o)$$

علماً أن : $(o,1) \neq o\ ,\ (1,o) \neq o$.

الحلقة التامة (المنطقة التكاملية) (Integral domain) :

الحلقة التامة ، هي حلقة إبدالية بمحايد ، ولا تحوي قواسم للصفر .

مثال (3) :

إن حلقة الأعداد الصحيحة $(Z,+,\cdot)$ هي حلقة تامة ، لأنها حلقة إبدالية بمحايـــد وإذا كان $x,y \in Z$ بحيث يكون $x \cdot y = o$ ، فإنه إما $x = o$ أو $y = o$.

مثال (4) :

لتكن الحلقة $(Z_P,\oplus,\otimes)$ حيث P عدد أولي ، إن $(Z_P,\oplus,\otimes)$ حلقة تامة .

البرهان :

برهنّا سابقاً أن $(Z_P,\oplus,\otimes)$ حلقة إبدالية واحدية ، ولنثبت أنها لا تحـــوي قواســـم للصفر .

ليكن $[a],[b] \in Z_P$، حيث أن $[a]\otimes[b] = [o]$ أي أن $[a \cdot b] = [o]$ وهذا يعنـــي $P/(a \cdot b)$، لكن P عدد أولي، أي أن: P/a وP/b، ومنه $[a] = [o]$ أو $[b] = [o]$.

مثال (5) :

إن حلقة المصفوفات المربعة $(M_n(R),+,\cdot)$ لا تشكل حلقة تامة لأنها حلقة ليست إبدالية .

مثال (6) :

حل المعادلة : $x^2 - 4x + 3 = 0$ في الحلقة $(Z_{12},\oplus,\otimes)$.

الحل :

لدينا

$$x^2 - 4x + 3 = 0 \Rightarrow (x-3)(x-1) = 0$$

وبالتالي يكون $x = 3 , x = 1$.

لكن في الحلقة $(Z_{12},\oplus,\otimes)$ ليست فقط العلاقة التالية صحيحة

$$\bar{o}\otimes\bar{a} = \bar{a}\otimes\bar{o} = \bar{o} \quad , \forall \bar{a} \in Z_{12}$$

لأنه :

$$\bar{2}\otimes\bar{6} = \bar{3}\otimes\bar{4} = \bar{3}\otimes\bar{8} = \bar{4}\otimes\bar{6} = \bar{4}\otimes\bar{9} = \bar{6}\otimes\bar{6}$$
$$= \bar{6}\otimes\bar{8} = \bar{6}\otimes\overline{10} = \bar{9}\otimes\bar{8} = \bar{o}$$

إذن يوجد للمعادلة المذكورة في الحلقة $(Z_{12},\oplus,\otimes)$ بالإضافة إلى الحلين $\bar{1},\bar{3}$ حلان آخران وهما $\bar{9},\bar{7}$ لأن :

$$(\overline{9-3})(\overline{9-1}) = \bar{6}\otimes\bar{8} = \bar{o}$$
$$(\overline{7-3})(\overline{7-1}) = \bar{4}\otimes\bar{6} = \bar{o}$$

المبرهنة التالية ، تبين لنا أن قانون الاختصار يتحقق في الحلقات التامة .

مبرهنة (3) :

لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، عندئذٍ القضايا التالية متكافئة :

(1) الحلقة $(R,+,\cdot)$ تامة .

(2) من أجل c,b,a من R حيث $a \neq 0$ ، فإن :

$$a\cdot b = a\cdot c \Rightarrow b = c$$

البرهان :

: (1) ⇐ (2)

بما أن $a \bullet b = a \bullet c$ حيث $a \neq 0$ و $a,b,c \in R$، فإن $a\,(b-c) = 0$ وبما أن $a \neq 0$، فإن $b - c = 0$ ، أي أن $b = c$.

: (2) ⇐ (1)

نفرض جدلاً أنه يوجد قاسماً للصفر في الحلقة $(R,+,\bullet)$ وليكن a ، عندئذٍ يوجد عنصر b من R مغاير للصفر ويحقق $a \bullet b = 0$ ، ومنه $a \bullet b = a \bullet o$ ولكون $a \neq o$ وحسب الفرض يكون $b = o$ وهذا غير ممكن .

نستنتج مما سبق أن الحلقة $(R,+,\bullet)$ تامة لأنها لا تملك قواسم للصفر .

مثال (7) :

لتكن $(R,+,\bullet)$ حلقة تامة، وإذا كان y,x عنصرين ما من R بحيث $x^5 = y^5$ و $x^7 = y^7$. أثبت أن $x = y$.

الحل :

لنرمز لصفر الحلقة $(R,+,\bullet)$ بـ o (العنصر المحايد بالنسبة لعملية الجمع) إذا كان $x = o$ ، فإن $x^5 = 0$ وبالتالي فإن $y^5 = 0$ ومنه $y = 0$.

لنفرض الآن أن $x \neq 0$، بما أن $x^7 = y^7$، فإن : $x^5 \bullet x^2 = y^5 \bullet y^2$ ، وبالتالي فإن : $x^5 \bullet x^2 = x^5 \bullet y^2$ ومنه يكون $x^5 \bullet (x^2 - y^3) = 0$.

بما أن $(R,+,\bullet)$ حلقة تامة و $x \neq 0$ ، فإن $x^5 \neq 0$ ، وبالتالي نرى من المعادلة السابقة أن : $x^2 - y^2 = 0$ أي أن $x^2 = y^2$ ومنه (*) $x^6 = y^6$. وبما أن $x^7 = y^7$ فإن $x^6 \bullet x = y^6 \bullet y$ ، وبالتالي حسب (*) يكون $x^6 \bullet x = x^6 \bullet y$ أي أن $x^6 \bullet (x-y) = 0$. وبما أن $(R,+,\bullet)$ حلقة تامة و $x \neq 0$ فإن $x^6 \neq 0$ ، إذن $x - y = 0$ أي أن $x = y$.

نتيجة (4) :

لتكن $(R,+,\bullet)$ حلقة واحدية ، وليكن $u \in R$ عنصراً معكوساً (له معكوس) ،

عندئذٍ u ليس من قواسم الصفر .

لنتذكر أولاً مفهوم العنصر المعكوس : نقول عن العنصر $a \neq 0$ من الحلقة $(R,+,\bullet)$ إنه معكوس إذا وُجد عنصر $0 \neq c \in R$ ويحقق $a \bullet c = c \bullet a = 1$

نسمي عادةً العنصر c في هذه الحالة بمعكوس العنصر a في R .

لنبرهن الآن على صحة النتيجة :

لنثبت أنه إذا كان $r \in R$ بحيث $u \bullet r = 0$ أو $r \bullet u = 0$ ، فإن $r = 0$.

لذلك إذا كان $u \bullet r = 0$ فإن :

$$u^{-1} \bullet (u \bullet r) = u^{-1} \bullet (o) = o$$

$$u^{-1} \bullet (u \bullet r) = (u^{-1} \bullet u) \bullet r = o \Rightarrow 1 \bullet r = 0 \Rightarrow r = 0$$

كذلك إذا كان $r \bullet u = 0$ فإن :

$$(r \bullet u) \bullet u^{-1} = (o) \bullet u^{-1} = o$$

لكن

$$(r \bullet u) \bullet u^{-1} = r\,(u\,u^{-1}) = r \bullet 1 = r = 0$$

(6-1) مميز حلقة Charactaristic of ring :

لتكن $(R,+,\bullet)$ حلقة ما ، إذا وجد عدد صحيح موجب وليكن n بحيث $n.a = 0$ لكل $a \in R$ ، فإن أصغر عدد صحيح موجب يحقق هذه الخاصية يسمى مميز الحلقة . وإذا لم يوجد هذا العدد ، أي أن $n = 0$ هو العدد الصحيح الوحيد الذي يحقق $n.a = 0$ لكل $a \in R$ ، فإننا نقول إن الحلقة $(R,+,\bullet)$ مميزها الصفر .

نرمز عادةً لمميز الحلقة $(R,+,\bullet)$ بالرمز Char (R) .

مثال (8) :

مميز الحلقات $(Z,+,\bullet)$ و$(Q,+,\bullet)$ و$(R,+,\bullet)$ و$(C,+,\bullet)$ هو الصفر دوماً ، بينما مميز الحلقة $(Z_n,\oplus,\otimes)$ يساوي n . كما أن مميز الحلقة $(Z_4 \times Z_6, \oplus, \otimes)$ هو 12 أي أن : $Char(Z_4 \times Z_6) = 12$.

مثال (9) :

ليكن النظام $(P(X),+,\cdot)$ حيث X مجموعة غير خالية ، و $A \cdot B = A \cap B$ و $A+B = A \Delta B$ ، عندئذٍ $(P(X),+,\cdot)$ حلقة إبدالية بمحايد ، والمجموعة ϕ هو محايدها بالنسبة لعملية الجمع والمجموعة X هو محايدها بالنسبة لعملية الضرب (تأكد من ذلك) ، المطلوب حدّد مميز هذه الحلقة.

الحل : بما أن

$$2A = A \,\Delta\, A = (A - A) \cup (A - A) = \phi$$

لكل مجموعة $A \subseteq X$ ، فإن مميز الحلقة $(P(X),+,\cdot)$ يساوي 2 ونكتب $\text{Char}\,(P(X)) = 2$.

مبرهنة (4) :

لتكن $(R,+,\cdot)$ حلقة تامة ، عندئذٍ مميزها هو الصفر أو عدداً أولياً .

البرهان :

ليكن $\text{Char}\,(R) = n > 0$ ، ولنبرهن أولاً أن n هو أصغر عدد صحيح موجب يحقق $n \cdot 1 = 0$. بما أن $\text{Char}\,(R) = n$ ، فإن $n \cdot a = 0$ لكل $a \in R$ ، وبشكل خاص $n \cdot 1 = 0$ (أخذنا $a = 1$) .

لنفرض الآن أن $0 < m < n$ ، حيث $m \cdot 1 = 0$ ، عندئذٍ :

$m \cdot a = m \cdot (1 \cdot a) = (m \cdot 1) \cdot a = 0 \cdot a = 0$ لكل $a \in R$. أي أن :

$\text{Char}\,(R) = m = n$ ، وهذا تناقض .

لنفرض الآن أن n عدد غير أولي ، وبالتالي فإن $n = n_1 \cdot n_2$ حيث أن $n_2 < n$ و $1 < n_1$ ، عندئذٍ :

$$0 = n \cdot 1 = (n_1 \cdot n_2) \cdot 1 = (n_1 \cdot n_2) \cdot 1^2 = (n_1 \cdot 1)\,(n_2 \cdot 1)$$

وبما أن $(R,+,\cdot)$ لا تحوي قواسم للصفر ، فإن $n_1 \cdot 1 = 0$ أو $n_2 \cdot 1 = 0$ ، لكن $n_1 \cdot n_2 < n$ وهذا تناقض حيث أن n هو أصغر عدد صحيح موجب يحقق $n \cdot 1 = 0$ وبالتالي فإن $\text{Char}\,(R)$، يجب أن يكون عدداً أولياً .

(7-1) الحقل Field :

بدايةً نعرّف الحقل المتخالف (Skew field) .

نقول إن الحلقة بمحايد $(R,+,\cdot)$ حلقة قاسمية (Division ring) أو حقل متخالف ، إذا كان كل عنصر غير صفري من R هو عنصر وحدة .

مثال (10) :

وجدنا سابقاً أن $(Z_P,\oplus,\otimes)$ حلقة بمحايد حيث P عدد أولـــي . ولنبـــرهن أن $(Z_P,\oplus,\otimes)$ حلقة قاسمية (حقل متخالف) .

الحل :

ليكن $[o] \neq [a] \in Z_P$ فإن $\gcd(a,p) = 1$ ، وهذا يعني أنـــه يوجـــد عـــددان صحيحان $s,t \in Z$ بحيث يكون : $a\cdot s + p\cdot t = 1$ وبالتالي فإن :

$$[a]\otimes[s] \oplus [p]\otimes[t] = [1]$$

أي أن $[a]\otimes[s] = [1]$ وهذا يؤدي إلى أن $[s]$ هو معكـــوس $[a]$ الضـــربي، إذن $(Z_P,\oplus,\otimes)$ حلقة قاسمية .

لنعرف الآن الحقل field :

تعريف : كل حلقة $(R,+,\cdot)$ تسمى حقلاً إذا حققت الشروط التالية :

1- يوجد في R عنصران على الأقل .

2- يوجد في R عنصر محايد بالنسبة لعملية الضرب $(\cdot)$.

3- لكل عنصر مختلف عن الصفر من R معكوس في R بالنسبة للعملية $(\cdot)$.

بمعنى آخر :

كل حلقة $(R,+,\cdot)$ تسمى حقلاً إذا كانت $(R\backslash\{o\},\cdot)$ زمرة ، حيـــث أن o صـــفر الحلقة $(R,+,\cdot)$ (المحايد بالنسبة لعملية الجمع (+)) . ونقول عن الحقل $(F,+,\cdot)$ إنه إبدالي إذا كانت العملية $(\cdot)$ عملية إبدالية على عناصر F .

مثال (11) :

من الممكن التأكد أن $(R,+,\cdot)$ و $(Q,+,\cdot)$ و $(C,+,\cdot)$ هي حقول إبدالية ، لكن $(Z,+,\cdot)$ ليس حقلاً حيث أن $(+)$ و $(\cdot)$ عمليتي الجمع والضرب العاديتين .

مثال (12) :

لتكن $F=\{a+b\sqrt{5}\,;\,a,b\in Q\}$ أثبت أن $(F,+,\cdot)$ حقلاً حيث $(+)$ و $(\cdot)$ هما عمليتا الجمع والضرب العاديتين .

إن $(F,+,\cdot)$ حلقة إبدالية بمحايد صفرها هو o . (تأكد من ذلك) ولإثبات أن $(F,+,\cdot)$ حقل يجب أن نبرهن أن كل عنصر غير صفري هو عنصر وحدة . (حسب تعريف الحقل) .

لنفرض من أجل ذلك أن $a+b\sqrt{5}$ عنصر غير صفري في F ، وهذا يعني أن إما a أو b لا يساوي الصفر . كما أن :

$$\left(a+b\sqrt{5}\right)^{-1}=\frac{1}{a+b\sqrt{5}}=\frac{1}{a+b\sqrt{5}}\cdot\frac{a-b\sqrt{5}}{a-b\sqrt{5}}$$
$$=\frac{a}{a^2-5b^2}-\frac{b}{a^2-5b^2}\sqrt{5}$$

وبملاحظة أن $a^2-5b^2\neq 0$ ، وإلاّ كان $\sqrt{5}$ عدداً كسرياً ، وبالتالي فإن : $a/(a^2-5b^2)$ و $-b/(a^2-5b^2)$ عددان كسريان ، وهذا يؤدي إلى أن المعكوس عنصر في F .

نتيجة (5) :

في كل حلقة $(F,+,\cdot)$ ، ومهما يكن $a\in F\backslash\{o\}$ ومهما يكن $b\in F$ ، فإن هناك عنصر وحيد وليكن x يحقق العلاقة $a\cdot x+b=0$.

البرهان :

بما أن $(F,+)$ زمرة إبدالية ، فإن :

$$a\cdot x+b=0 \Leftrightarrow a\cdot x=-b \Leftrightarrow x=a^{-1}(-b)=-a^{-1}\cdot b$$

(لأن لـــ a معكوس) . إذن $x=-a^{-1}\cdot b$.

وإذا كان الحقل إبدالياً ، فنكتب الناتج السابق بالشكل $x = -b/a$ ونكون بذلك قد عرّفنا على $F \setminus \{o\}$ عملية نسميها عملية التقسيم وهي العملية المعاكسة للضرب .

ملاحظة (3) :

إذا كانت $(R,+,\bullet)$ حلقة قاسمية إبدالية ، فإننا نقول أن $(R,+,\bullet)$ حقل .

مثال (13) :

وجدنا سابقاً أن $(Z_P,\oplus,\otimes)$ حيث P عدد أولي ، حلقة قاسمية ، بما أن الضرب عملية إبدالية على عناصر Z_P ، فإن $(Z_P,\oplus,\otimes)$ حقل .

ملاحظة (4) :

إن أي حقل يجب أن يكون حلقة تامة لأن كل عنصر غير صفري منها هو عنصر وحدة (محايد) ولذا ليس قاسماً للصفر . لكن عكس هذه الحقيقة ليس صحيحاً ، فعلى سبيل المثال حلقة الأعداد الصحيحة $(Z,+,\bullet)$ هي حلقة تامة لكنها لا تشكل حقلاً . والمبرهنة التالية تقدم لنا في أي حالة يكون العكس صحيحاً.

مبرهنة (5) :

كل حلقة تامة منتهية ولتكن $(R,+,\bullet)$ هي حقل .

البرهان :

لتكن $a_1,a_2,\ldots,a_n$ عناصر الحلقة $(R,+,\bullet)$، وليكن a عنصراً غير صفري في R .

إذا كان $a\,a_i = a\,a_j$ حيث $i, j = 1,2,\ldots,n$ ، فإن $a\,(a_i - a_j) = 0$ ، وبما أن $(R,+,\bullet)$ حلقة تامة ، فإن $a_i = a_j$ حيث $i, j = 1,2,\ldots,n$. لذلك فإن العناصر $a\,a_1 , a\,a_2 , \ldots, a\,a_n$ هي جميع عناصر الحلقة $(R,+,\bullet)$، وبالتالي نستطيع أن نكتب كل عنصر في R بالشكل $a\,a_i$ حيث $1 \le i \le n$.

وبما أن $1 \in R$ ، لذلك فإن : $1 = a \bullet a_i$ حيث $1 \le i \le n$ وبما أن $(R,+,\bullet)$ حلقة إبدالية فإن $a \bullet a_i = a_i \bullet a = 1$ ، وهذا يؤدي إلى أن معكوس a هو a_i . أي أن كل عنصر غير صفري في R له معكوس . إذاً $(R,+,\bullet)$ حقل .

المبرهنة التالية تعطي الشرط اللازم والكافي لكي تكون حلقة الأعداد الصحيحة ،

قياس n، حقلاً .

مبرهنة (6) :

حلقة الأعداد الصحيحة قياس n $(Z_n,\oplus,\otimes)$ تكون حقلاً ، إذا وفقط إذا كان n عدداً أولياً .

البرهان :

لنفرض أولاً ، أن n أولي ، ولنبرهن أن $(Z_n,\oplus,\otimes)$ حقل .

ليكن $[o] \neq [a] \in Z_n$ أي أن $a \in Z$ بحيث $0 < a < n$. وبما أن $\gcd(a,n) = 1$، يوجد عددان صحيحان r,q بحيث يكون $1 = a\,q + r\,n$ ، وبملاحظة أن :

$$[a] \otimes [q] = [a.q] \oplus [0] = [a.q] \oplus [n.r] = [aq + n\,r] = [1]$$

وهذا يبين لنا أن العنصر [q] هو معكوس العنصر [a] من Z_n إذن $(Z_n,\oplus,\otimes)$ حقل .

لنبرهن العكس :

لنفرض أنه إذا كان n عدد غير أولي (عدد مؤلف) فإن $(Z_n,\oplus,\otimes)$ ليست حقلاً .
بما أننا فرضنا أن n غير أولي ، فإن $n = a.b$ حيث $o < a , b < n$ لذلك فإن :

$$[a] \otimes [b] = [a \cdot b] = [n] = [o]$$

وبما أن [a] و[b] عنصرين غير صفريين في Z_n ، إذن [a] و[b] قاسمين للصفر في Z_n ، وهذا يعني أن $(Z_n,\oplus,\otimes)$ ليست حلقة تامة . وبالتالي ليست حقلاً .

ملاحظة (5) :

كان بالإمكان برهان أن $(Z_n,\oplus,\otimes)$ حقل (في المبرهنة السابقة) ، علماً أن n عدد أولي . وذلك بالاستفادة من المثال (13) .

ملاحظة (6) :

من المبرهنة (4) إن مميز أي حقل هو إما الصفر أو عدداً أولياً .
ليكن $(F,+,\cdot)$ حقلاً ما ، ولنرمز لمحايده بالنسبة لعملية الجمع بـ o ، ولمحايده بالنسبة لعملية الضرب بـ e ، وإذا كان للحقل $(F,+,\cdot)$ مميز هو p ، فإن :

$p \cdot e = o$ (1)

$1 \cdot e = e \neq 0$ لأن $p > 1$ (2)

(3) p أولي لأنه إذا كان b,a عددين صحيحين موجبين بحيث يكون $p = a \cdot b$، فإن $o = (a \cdot e) \cdot (b \cdot e)$ ، وبالتالي فإنه إما أن يكون $a \cdot e = o$ أو أن يكون $b \cdot e = o$ ، أي أن إما أن يكون $a = p$ أو $b = p$.

تعريف العنصر معدوم (المتلاشي) القوى في حلقة (Nilpotent element) :

نقول إن العنصر $a \in R$ ، حيث $(R,+,\cdot)$ حلقة ما معدوم القوى (nilpotent) إذا وُجد عدد صحيح موجب وليكن n بحيث $a^n = o$.

مثال (14) :

لتكن $(R,+,\cdot)$ حلقة ، إن صفرها هو عنصر متلاشي ، ولأن $o^n = n$ حيث $n \in Z^n$.

كما أن العنصران 4,2 متلاشيان في الحلقة $(Z_8,+,\cdot)$، لأن $2^3 = o$، $4^2 = 16 = o$ حيث $2,3 \in Z^+$.

تعريف العنصر متساوي القوى في حلقة (Idenmpotent element) :

نقول إن العنصر $o \neq a \in R$ ، حيث $(R,+,\cdot)$ حلقة ما ، عنصر متساوي القوى idempotent ، إذا كان $a^2 = a$.

مثال (15) :

في الحلقة $(R,+,\cdot)$ العنصران $o,1$ متساويا القوى فيها ، لأن $o^2 = o$ و $1^2 = 1$

كما أن العنصران $(o,1)$, $(1,o)$ متساويا القوى في الحلقة $(R \times R,+,\cdot)$ ، لأن :

$$(1,o)^2 = (1,o) \ , \ (o,1)^2 = (o,1)$$

وفي الحلقة $(Z_6,+,\cdot)$ العنصران 4,3 متساويا القوى لأن $3^2 = 3$ و $4^2 = 4$.

نقول إن العنصر a في الحلقة بمحايد $(R,+,\cdot)$ أحادي القدرة unipotent إذا وفقط إذا كان $1 - a$ عنصر معدوم القوى .

لنعرّف الآن **حلقة بول** Boolean ring (جورج بول (1815-1864)) :

نسمي الحلقة $(R,+,\cdot)$ حلقة بول ، إذا كان كل عنصر فيها متساوي القوى ، أي لكل $a\in R$ ، فإن : $a^2 = a$.

مبرهنة (7) :

لتكن $(R,+,\cdot)$ حلقة بول ، عندئذٍ $(R,+,\cdot)$ حلقة إبدالية .

البرهان :

ليكن $a\in R$ ، فإن $a + a\in R$ ، وبالتـــالي ، $(a + a)^2 = a + a$ لأن $(R,+,\cdot)$ حلقة بول . لكن :

$$(a + a)^2 = a^2 + a^2 + a^2 + a^2$$

إذن :
$$a + a = a + a + a + a$$

ومنه $a + a = o$ ، إذن $a = -a$ ، لكل $a\in R$.

الآن من أجل $a,b\in R$ ، نجد أن :

$$(a + b) = (a + b)^2 = a^2 + ab + ba + b^2$$
$$= a + ab + ba + b$$

وبالتالي ، فإن : $ab + ba = o$ ، وعليه فإن $ab = -ba$ ولكن $-ba = ba$ كما تـــمّ إثباته في البداية، إذن $ab = ba$ ، فالحلقة $(R,+,\cdot)$ إبدالية .

الفصل الثاني

الحلقات والحقول الجزئية والمثاليات

Subring and subfields & Ideals

الفصل الثاني

الحلقات والحقول الجزئية والمثاليات

Subring and subfields & Ideals

(1-2) الحلقة الجزئية subring :

لتكن $(R,+,\bullet)$ حلقة ما ، ولتكن S مجموعة جزئية غير خالية من R . إذا كانت S حلقة بالنسبة للعمليتين $(+)$ و$(\bullet)$ على S ، فإننا نقول إن $(S,+,\bullet)$ حلقة جزئية من الحلقة $(R,+,\bullet)$ ، ونرمز لذلك بالشكل : $S \le R$

إذا كانت $S \le R$ و $S \ne R$ ، فإننا نقول أن $(S,+,\bullet)$ حلقة جزئية فعلية (Proper subring) من الحلقة $(R,+,\bullet)$ ونرمز لذلك بـ $S < R$.

نعلم من نظرية الزمر ، أن الشرط اللازم والكافي لكي تكون مجموعة جزئية غير خالية ولتكن H زمرة جزئية (Subgroup) من الزمرة $(G,\star)$ هو أن يكون $x \bullet y^{-1} \in H$ لكل y,x من H . سنستخدم هذا المفهوم في الحلقات الجزئية من خلال المبرهنة التالية :

مبرهنة (1) :

لتكن $(R,+,\bullet)$ حلقة ما ، وإذا كانت $\phi \ne S \subseteq R$ ، فإن الشرط اللازم والكافي لكي تكون $(S,+,\bullet)$ حلقة جزئية من الحلقة $(R,+,\bullet)$ هو أن يكون :

$$x \bullet y \in S \quad , \quad x - y \in S$$

وذلك من أجل أي y,x من S .

البرهان :

نفرض أولاً أن $(S,+,\bullet)$ حلقة جزئية من الحلقة $(R,+,\bullet)$ ، وبالتالي فإن $(S,+,\bullet)$ زمرة جزئية من R بالنسبة لعملية الجمع، وبالتالي يكون $x - y \in S$ لكل y,x من

S، وبما أن $(S,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ فإن $x\cdot y\in S$ لكل y,x من S
نفرض الآن العكس ، أي لنفرض أن $x-y\in S$ و$x\cdot y\in S$ لكل y,x من S ، وهذا يعني أن S زمرة جزئية بالنسبة لعملية الجمع في R ، وبما أن الخاصة الإبدالية صحيحة بالنسبة لعملية الجمع على R فهي صحيحة أيضاً على S ، إذن S زمرة جزئية إبدالية . وبما أن عمليتي التجميعية وعملية توزيع الضرب على الجمع صحيحتان على R فهما صحيحتان على S لكون S مجموعة جزئية من R ، إذن $S\le R$.

(2-2) أمثلة :

1- إن $\{o\}$ وR حلقتين جزئيتين بالنسبة لأي حلقة R ، تسمى عادةً الحلقة $(\{o\},+,\cdot)$ حلقة جزئية مبتذلة Trivial subring .

2- إن المجموعة $\{0,2,4\}$ تشكل حلقة جزئية بالنسبة للحقل $(Z_6,\oplus,\otimes)$.

3- إن حلقة الأعداد الصحيحة $(Z,+,\cdot)$ هي حلقة جزئية من حلقة الأعداد الحقيقية $(R,+,\cdot)$.

4- من أجل كل عدد صحيح موجب n ، المجموعة التالية :

$$n\cdot Z=\{0,\pm n\,,\pm 2n\,,\ldots.\}$$

هي حلقة جزئية من حلقة الأعداد الصحيحة $(Z,+,\cdot)$.

5- إن مجموعة الأعداد المركبة التالية : $Z[i]=\{a+i\,b\,;\,a,b\in Z\}$ تشكل حلقة جزئية من حلقة الأعداد المركبة $(C,+,\cdot)$.

الحل :

من الواضح أولاً أن $\phi\neq Z[i]\subseteq C$. ليكن $x,y\in Z[i]$ فإن : $x=a_1+i\,b_1$ و$y=a_2+i\,b_2$، حيث أن $a_1,a_2,b_1,b_2\in Z$

$$x-y=(a_1+i\,b_1)-(a_2+i\,b_2)=(a_1-a_2)+i\,(b_1-b_2) \qquad (1)$$

بما أن $b_1-b_2\,,\,a_1-a_2$ من Z ، فإن $x-y\in Z$

$$x \cdot y = (a_1 + i\, b_1) \cdot (a_2 + i\, b_2) = a_1 \cdot a_2 - b_1 \cdot b_2 + i\,(a_2\, b_1 + a_1\, b_2) \quad (2)$$

وبما أن $a_1a_2 - b_1b_2$ و $a_2b_1 + a_1b_2$ من Z ، فإن $x \cdot y \in Z$

6- لتكن المجموعة S التالية : $S = \{a + b\sqrt{5}\ ;\ a,b \in Z\}$

إن $(S,+,\cdot)$ حلقة جزئية من الحلقة $(Z,+,\cdot)$.

الحل :

من الواضح أن $\phi \neq S \subseteq Z$. ليكن y,x عنصرين ما من S ، وهذا يعني أن : $x = a + b\sqrt{5}$ ، $y = c + d\sqrt{5}$ ، حيث $a,b,c,d \in Z$. عندئذٍ يتحقق ما يلي :

$$x - y = (a + b\sqrt{5}) - (c + d\sqrt{5}) = (a - c) + (b - d)\sqrt{5} \quad (1)$$

وبما أن $a - c$ و $b - d$ من Z ، فإن $x - y \in S$.

$$x.y = (a + b\sqrt{5}) . (c + d\sqrt{5}) = (ac + 5bd) + (bc + ad)\sqrt{5} \quad (2)$$

وبما أن $a.c + 5bd$ و $bc + ad$ من Z ، فإن $x.y \in S$.

نستنتج مما سبق أن $\left(S = Z[\sqrt{5}],+,\cdot\right)$ حلقة جزئية من الحلقة $(Z,+,\cdot)$.

7- لتكن $(R,+,\cdot)$ حلقة ما، ولتكن $M = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ; a,b,c \in R\right\}$

إن $(M,+,\cdot)$ حلقة جزئية من الحلقة $(M_2(R),+,\cdot)$. (تسمى هذه بحلقة المصفوفات المثلثية العليا على R (Upper triangular matrices over R .

الحل :

من الواضح أن $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ من M ، إذن $M \neq \phi$.

لتكن $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, B = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}$ ، حيث $a,b,c,p,q,r \in R$ فإن :

$$A - B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} = \begin{pmatrix} a-p & b-q \\ 0 & c-r \end{pmatrix} \in M$$

$$A \bullet B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \bullet \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} = \begin{pmatrix} ap & aq+br \\ 0 & cr \end{pmatrix} \in M$$

ملاحظات :

(1) إذا كانت $(R,+,\bullet)$ حلقة بمحايد ، وليكن 1 العنصر المحايد (عنصر الوحدة) فيها ، وإذا كانت $(S,+,\bullet)$ حلقة جزئية من الحلقة $(R,+,\bullet)$ بحيث يكون $1 \in S$ ، فإن الحلقة الجزئية $(S,+,\bullet)$ بمحايد أيضاً والعنصر المحايد فيها هو 1 .

(2) إذا كانت $(S,+,\bullet)$ حلقة جزئية من حلقة ما ، ولتكن $(R,+,\bullet)$ فإنه من الممكن أن تكون :

- الحلقة $(R,+,\bullet)$ بمحايد، في حين أن الحلقة الجزئية $(S,+,\bullet)$ لا تكون بمحايد.
- الحلقة $(R,+,\bullet)$ بمحايد ، والحلقة الجزئية $(S,+,\bullet)$ بمحايد أيضاً ، إلاّ أن العنصر المحايد في R بالنسبة للعملية $(\bullet)$ لا ينتمي إلى S .
- الحلقة الجزئية $(S,+,\bullet)$ بمحايد، في حين أن الحلقة $(R,+,\bullet)$ لا تكون بمحايد.

مثال (7) :

من المعلوم أن حلقة الأعداد الصحيحة $(Z,+,\bullet)$ بمحايد وعنصر المحايد فيها هو العدد 1 ، علماً أن $(+)$ و$(\bullet)$ هما عمليتا الجمع والضرب العاديتان ، ولتكن $S = \{2a : a \in Z\}$ ، إن $(S,+,\bullet)$ هي حلقة جزئية من الحلقة $(Z,+,\bullet)$ ، ولا يوجد فيها عنصر محايد بالنسبة للعملية $(\bullet)$ لأن $1 \notin 2a$ لكل $a \in Z$.

مثال (8) :

هاتِ مثالاً يوضح فيه أن المحايد في حلقة جزئية يختلف عن المحايد في الحلقة الأصلية .

الحل :

لنأخذ الحلقة $(M_2(Z),+,\bullet)$ والحلقة الجزئية منها التالية :

$$(S,+,\bullet) = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \; ; \; a \in (Z,+,\bullet) \right\}$$

إن الحلقة $(M_2(Z),+,.)$ بمحايد ، حيث أن $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ هو المحايد فيها . إن الحلقة $(S,+,.)$ حلقة جزئية من الحلقة $(M_2(Z),+,.)$ ومحايــدها هــو $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ، وإن $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

تعريف مركز حلقة Center of ring

لتكن $(R,+,.)$ حلقة ما ، ولتكن $C(R) = \{ a\in R : a.x = x.a \ ; \ \forall x\in R \}$

إن $(C(R),+,.)$ حلقة ، تسمى بمركز الحلقة $(R,+,.)$.

المبرهنة التالية تبين لنا أن $(C(R),+,.)$ هي حلقة جزئية من الحلقة $(R,+,.)$.

مبرهنة (2) :

إذا كانت $(R,+,.)$ حلقة ، فإن $(C(R),+,.)$ حلقة جزئية من الحلقة $(R,+,.)$.

البرهان :

1- إن $\phi \neq C(R) \subseteq R$ ، لأن $C(R)$ من جهة أولى ، مجموعة جزئية من R من جهة ثانية، إذا رمزنا لصفر الحلقة $(R,+,.)$ بالرمز o ، فإن :

$o.x = x.o \ ; \ \forall x\in R$ ، ومنه $o\in C(R)$، إذن $C(R) \neq \phi$.

2- إذا كان a_2,a_1 عنصرين ما من $C(R)$ ، فإن :

$$a_1.x = x.a_1 \ \ \& \ \ a_2.x = x.a_2$$

وذلك من أجل أي x من R ، ومن ثم فإن :

$$(a_1 - a_2).x = a_1.x - a_2.x = x.a_1 - x.a_2 = x\,(a_1 - a_2)$$

$$(a_1.a_2).x = a_1.(a_2.x) = a_1.(x.a_2) = (a_1.x).a_2$$
$$= (x.a_1).a_2 = x.(a_1.a_2)$$

وذلك من أجل أي x من R ، ومنه يكون :

$$a_1.a_2 \in C(R) \ \ \& \ \ a_1 - a_2 \in C(R)$$

من (1) و(2) نستنتج أن $(C(R),+,\cdot)$ هي حلقة جزئية من الحلقة $(R,+,\cdot)$.

مثال (9) :

لتكن $(M_2(R),+,\cdot)$ حلقة ، أوجد $C(M_2(R))$.

الحل :

حسب تعريف مركز حلقة ، نرى أن :

$$C(M_2(R)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} ; a \in C(R) \right\}$$

حيث $(R,+,\cdot)$ حلقة ما .

(2-3) بعض العمليات على الحلقات الجزئية :

المبرهنتان التاليتان توضحان أن تقاطع حلقتين جزئيتان من حلقة ما هو حلقة جزئية ، بينما اتحاد حلقتين جزئيتين ليس من الضروري أن يكون حلقة جزئية .

مبرهنة (3) :

لتكن $(R,+,\cdot)$ حلقة ما، إذا كانت $\{(S_i,+,\cdot)\}_{i\in I}$ أسرة غير خالية من الحلقات الجزئية من الحلقة $(R,+,\cdot)$، عندئذٍ $\left(\bigcap_{i\in I} S_i,+,\cdot\right)$ حلقة جزئية من الحلقة $(R,+,\cdot)$.

البرهان :

لنرمز لمحايد الحلقة $(R,+,\cdot)$ بالرمز o ، بما أن $\{(S_i,+,\cdot)\}_{i\in I}$ أسرة حلقات جزئية من الحلقة $(R,+,\cdot)$ ، فإن : $o\in S_i$ لكل i من I ، ومن ثم فإن $o\in \bigcap_{i\in I} S_i$.

وهذا يبين لنا أن $\phi\neq \bigcap_{i\in I} S_i \subseteq R$.

ليكن y,x عنصرين ما من $\bigcap_{i\in I} S_i$، فإن : $x,y\in S_i$ لكل i من I، وبالتالي فإن :

$x-y\in S_i;\forall i\in I$ ومنه $x-y \in \bigcap_{i\in I} S_i$.

وبنفس الطريقة نرى أنه إذا كان $x,y\in S_i$ لكل i من I وبالتالي فإن $x\cdot y \in \bigcap_{i\in I} S_i$

لكل i من I .

نستنتج مما سبق أن $\left(\bigcap_{i\in I} S_i ,+,\cdot\right)$ حلقة جزئية من الحلقة $(R,+,\cdot)$.

ملاحظة (1) :

إن اتحاد حلقتين جزئيتين من حلقة ليس بالضرورة أن يكون حلقة جزئية من الحلقة المدروسة، والمثال التالي يوضح هذه الملاحظة .

مثال (10) :

لتكن حلقة الأعداد الصحيحة $(Z,+,\cdot)$ ، ولتكن الحلقتان الجزئيتان من الحلقة $(Z,+,\cdot)$: $S = (2Z,+,\cdot)$ و $T = (3Z,+,\cdot)$.

بيِّن أن $S \cup T$ ليس حلقة جزئية من الحلقة $(Z,+,\cdot)$.

الحل :

من الواضح أن : $2 \in S\cup T$ ، وكذلك $3 \in S\cup T$، بينما $2+3 = 5 \notin S\cup T$ ، أي أن $S\cup T$ ليست مغلقة بالنسبة لعملية الجمع فهي ليست حلقة جزئية من الحلقة $(Z,+,\cdot)$.

مُبَرهَنة (4) :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وكانت $(S,+,\cdot)$ و$(T,+,\cdot)$ حلقتين جزئيتين منها ، إن $(S\cup T,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ إذا وفقط إذا كانت $S \subseteq T$ أو $T \subseteq S$.

البرهان :

لنفرض أولاً أن $S \subseteq T$ أو $T \subseteq S$ ، ولنبرهن أن $(S\cup T,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$.

إذا كان $S \subseteq T$ أو $T \subseteq S$ ، فإن $S\cup T = T$ أو $S\cup T = S$ على التوالي ، إذن $(S\cup T,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$.

لنثبت الآن العكس : أي لنفرض أن $S\cup T$ حلقة جزئية من $(R,+,\cdot)$ ولنبرهن أن

$S \subseteq T$ أو $T \subseteq S$.

لنفرض أن $R \supseteq S \cup T$ ، وأن $S \not\subset T$ و $T \not\subset S$ ، عندئذٍ يوجد $a \in S$ و $a \notin T$ ، ويوجد $b \in T$ و $b \notin S$ ، وعليه فإن $a,b \in S \cup T$ ، لكن $(S \cup T,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ فرضاً إذن $a - b \in S \cup T$، لكن $a - b \notin S$ ، لأنه لو كان $a - b \in S$ فإن $b \in S$ ، وهذا يناقض كون $b \notin S$ ، كما أن $a - b \notin T$ ، لأنه لو كان $a - b \in T$ ، فإن $a \in T$ ، وهذا تناقض أيضاً .

إذن $a - b \notin S \cup T$ وهذا تناقض كون $(S \cup T,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ ، إذن $S \subseteq T$ أو $T \subseteq S$.

(4-2) الحقول الجزئية Subfield :

ليكن $(F,+,\cdot)$ حقلاً ما ، وإذا كانت K مجموعة جزئية غير خالية من F . نقول إن K حقل جزئي Subfield من الحقل $(F,+,\cdot)$ إذا كان $(K,+,\cdot)$ حقلاً ، حيث أن عمليتي الجمع $(+)$ والضرب $(\cdot)$ هما عمليتا الحقل $(F,+,\cdot)$.

ينتج من التعريف السابق أن لكل حقل يوجد له حقل جزئي مبتذل هو الحقل نفسه .

تعريف الحقل الأولي (Prime field) :

الحقل الذي لا يحوي حقولاً جزئية فعلية يدعى حقلاً أولياً .

المبرهنة التالية تقدم الشرط اللازم والكافي لكي يكون الحقل $(K,+,\cdot)$ حقلاً جزئياً من الحقل $(F,+,\cdot)$.

مبرهنة (4) :

ليكن $(F,+,\cdot)$ حقلاً ما ، ولتكن K مجموعة جزئية تحوي عنصرين على الأقل من F . إن الشرط اللازم والكافي لكي يكون $(K,+,\cdot)$ حقلاً جزئياً من الحقل $(F,+,\cdot)$ هو أن يتحقق الشرطان التاليان :

(1) إذا كان y,x عنصرين ما من K ، فإن $x - y \in K$.

(2) إذا كان y,x عنصرين ما من K ، وإذا كان $y \neq o$ فإن $x \cdot y^{-1} \in K$ حيث

o هو صفر الحقل $(F,+,\cdot)$.

مثال (11) :

أثبت أن حقل الأعداد النسبية $(Q,+,\cdot)$ يشكل حقلاً أولياً .

(5-2) أمثلة :

<u>1-</u> بيّنا في الفصل السابق أن كلاً من $(Q,+,\cdot)$ و$(R,+,\cdot)$ و$(C,+,\cdot)$ حقـول . فمن الواضح أن $(Q,+,\cdot)$ هو حقل جزئي من الحقل $(R,+,\cdot)$ ، كمـا أن $(R,+,\cdot)$ حقل جزئي من الحقل $(C,+,\cdot)$.

<u>2-</u> لتكن $S=\{a+b\sqrt{5}\ ;\ a,b\in Q\}$ ، ولنثبت أن S هي حقل جزئي مـن حقل الأعداد الحقيقية بالنسبة للعمليتين المألوفتين الجمع والضرب .

الحل :

1- من الواضح أن S تحوي عنصرين على الأقل مـن R وهمـا 0 و1 ، لأن $0=0+0\sqrt{5}$ و $1=1+0\sqrt{5}$.

2- ليكن $x=a+b\sqrt{5}$ و $y=c+d\sqrt{5}$ عنصرين ما مـن S ، حيـث أن $a,b,c,d\in Q$ ، فإن :

$$x-y=(a+b\sqrt{5})-(c+d\sqrt{5})=(a-c)+(b-d)\sqrt{5}\in S$$

3- ليكن $x=a+b\sqrt{5}$ و $y=c+d\sqrt{5}$ عنصرين مـا مـن S بحيـث أن $y\neq 0$ و$a,b,c,d\in Q$ ، بما أن $c+d\sqrt{5}\neq 0$،فإن: $c^2-5d^2\neq 0$ و $c-d\sqrt{5}\neq 0$ ومن ثم فإن :

$$x\cdot y^{-1}=\frac{x}{y}=\frac{a+b\sqrt{5}}{c+d\sqrt{5}}=\frac{(a+b\sqrt{5})(c-d\sqrt{5})}{c^2-5d^2}$$

$$=\frac{ac-5bd}{c^2-5d^2}+\frac{(cb-ad)\sqrt{5}}{c^2-5d^2}\in S$$

من (1) و(2) و(3) نستنتج أن $(S,+,\cdot)$ حقل جزئي من الحقل $(R,+,\cdot)$.

نقدم الآن بعض خواص الحقول الجزئية من خلال المبرهنات التالية :

مبرهنة (5) :

ليكن $(F,+,\cdot)$ حقلاً ما، إذا كانت $\{(K_i,+,\cdot)\}_{i\in I}$ أسرة غير خالية من الحقول الجزئية من الحقل $(F,+,\cdot)$،عندئذٍ $\left(\bigcap_{i\in I} K_i,+,\cdot\right)$ حقل جزئي من الحقل $(F,+,\cdot)$.

البرهان :

لنرمز لصفر الحقل $(F,+,\cdot)$ بـ o ولمحايده بـ 1 . وبما أن $\{(K_i,+,\cdot)\}_{i\in I}$ أسرة حقول جزئية من الحقل $(F,+,\cdot)$ ، فإن من أجل كل i من I يكون $0,1\in K_i$، وبالتالي فإن : $0,1\in\bigcap K_i$ إذن يوجد في $\bigcap_{i\in I} K_i$ عنصران على الأقل .

لنتحقق الآن من الشرطين الواردين في المبرهنة السابقة .

ليكن y,x عنصرين ما من $\bigcap_{i\in I} K_i$ ، فإن y,x من K_i لكل i من I ، وبالتالي فإن $x-y\in K_i$ لكل $i\in I$ ، أي أن $x-y\in\bigcap_{i\in I} K_i$.

إذا كان y,x عنصرين ما من $\bigcap_{i\in I} K_i$ وإذا كان $y\neq 0$ فإن : $y\neq 0$ و $x-y\in K_i$ لكل i من I. ومن ثم فإن : $x\,.y^{-1}\in K_i$ لكل i من I ومنه يكون $x\,.y^{-1}\in\bigcap_{i\in I} K_i$.

نستنتج مما سبق أن $\left(\bigcap_{i\in I} K_i,+,\cdot\right)$ حقل جزئي من الحقل $(F,+,\cdot)$.

مبرهنة (6) :

إذا كان $(F,+,\cdot)$ حقلاً إبدالياً ما ، ولنرمز لصفره بـ 0 ، ولتكن K مجموعة جزئية غير خالية من F ، إذا كانت $(K,+,\cdot)$ حلقة تامة . وإذا كانت $S=\{a\cdot b^{-1} : a,b\in K ,\ b\neq 0\}$ فإن $(S,+,\cdot)$ حقل جزئي من الحقل $(F,+,\cdot)$ يحوي K وهو أصغر حقل جزئي من الحقل $(F,+,\cdot)$ يحوي K .

البرهان :

لنرمز للعنصر المحايد في الحقل $(F,+,\cdot)$ بـ 1 .

إن S تحوي عنصرين على الأقل لأن : $0,1\in S$. لنتحقق الآن من شرطي الحقل الجزئي .

ليكن y,x عنصرين ما من S ، أي أن $x = a.b^{-1}$, $y = c.d^{-1}$ حيث أن :

$b \neq 0$, $d \neq 0$, $a,b,c,d\in K$ ، وبالتالي فإن :

$$\begin{aligned} x - y &= a.b^{-1} - c.d^{-1} \\ &= a.(d.d^{-1}).b^{-1} - c.(b.b^{-1}).d^{-1} \\ &= (a.d)\,(b.d)^{-1} - (c.b)\,(b.d)^{-1} \\ &= (a.d - c.b)\,(b.d)^{-1} \end{aligned}$$

وبمـــا أن $b \neq 0$, $d \neq 0$, $a,b,c,d\in K$ فـــإن : $b.d \neq 0$, $bd\in K$ و $a.d - cb$

ومنه يكون $(a.d - c.b)\,(b.d)^{-1} \in S$ ، أي أن $x - y\in S$.

لنبرهن الآن على صحة الشرط الآخر الوارد في المبرهنة قبل الأخيرة .

بالاستفادة مما سبق ، بما أن :

$$x = a.b^{-1}\,,\ y = c.d^{-1} \quad ; \quad a,b,c,d\in K\ ,\ b \neq 0\,,\ d \neq 0$$

وبالتالي فإن :

$$\begin{aligned} x.y^{-1} &= (a.b^{-1})\,(c.d^{-1})^{-1} = (a.b^{-1})\,(d.c^{-1}) \\ &= (a.d)\,(b^{-1}.c^{-1}) = (a.d)\,(c.b)^{-1} \end{aligned}$$

وبما أن :

$$c \neq 0\,,\ b \neq 0 \quad ; \quad a,b,c,d\in K\ ,\ d \neq 0$$

فإن :

$$a.d\,,\ c.b\in K\ ,\ c.b \neq 0$$

ومن ثم فإن $(a.d)\,(c.b)^{-1} \in S$ أي أن $x.y^{-1}\in S$.

مما سبق نستنتج أن $(S,+,\cdot)$ حقلاً جزئياً من الحقل $(F,+,\cdot)$.

إذا كان a عنصراً ما من K ، فإن :

$$a = a.1 = a.1^{-1} \in S$$

وهذا يبين لنا أن الحقل الجزئي $(S,+,\cdot)$ يحوي K .

لنبرهن أخيراً أن $(S,+,\cdot)$ هو أصغر حقل جزئي من الحقل $(F,+,\cdot)$.

ليكن $(S_1,+,\cdot)$ حقلاً جزئياً ما من الحقل $(F,+,\cdot)$ يحوي K . إن $S \subseteq S_1$ لأنه إذا كـــان x عنصـــراً مـــا من S ، فإنه بالإمكان كتابته بالشكل : $x = a.b^{-1}$ حيث أن $b \neq 0$ و $a,b \in K$ ، لكن :

$$a,b \in K \, , \, b \neq 0 \;\Rightarrow\; a,b \in S_1 \, , \, b \neq 0$$

أي أن : $a.b^{-1} \in S_1$ أي أن $x \in S_1$.

(6-2) المثاليات Ideals :

يعـــود ســـبب اكتشاف المثاليات إلى المحاولات العديدة التي قام بها العديد من الرياضـــيين لإثـــبات نظـــرية فيرما الأخيرة . ويعود الفضل أخيراً إلى الرياضي الألمانـــي كومر Kummer (1810-1893) في تقديم مفهوم المثالية Ideal وكان ذلـــك عام 1847 . ثم توسع هذا المفهوم من قبل الرياضي الألماني الآخر وديدكند Dedikind في عام 1871 وعرّفها تعريفاً دقيقاً .

تُعَدُّ المثاليات من أهم الحلقات الجزئية من حلقة ما ، وتلعب في الحلقات الدور الذي تلعبه الزمر الجزئية الناظمية في نظرية الزمر .

تعريف المثالية :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت I مجموعة جزئية غير خالية من R :

1- نقـــول عـــن المجموعـــة I إنها تشكل مثالية يسارية (Left ideal) في الحلقة $(R,+,\cdot)$ إذا تحقق ما يلي :

(1) $(I,+)$ زمرة جزئية من الزمرة $(R,+)$.

(2) لكل $r \in R$ فإن $r.I \subseteq I$.

2- نقـــول عـــن المجموعـــة I إنها تشكل مثالية يمينية (Right ideal) في الحلقة

$(R,+,\cdot)$ إذا حققت ما يلي :

(1) $(I,+)$ زمرة جزئية من الزمرة $(R,+)$.

(2) لكل $r \in R$ فإن $I.r \subseteq I$.

3- نقول عن المجموعة I إنها تشكل مثالية (Ideal) (ثنائية الجانب) في الحلقة $(R,+,\cdot)$ إذا كانت مثالية يسارية ويمينية في آنٍ واحد .

لنورد الآن شرط مكافئ للتعريف السابق من خلال التمهيدية التالية :

تمهيدية (1) :

لتكن $(R,+,\cdot)$ حلقة ما ، و I مجموعة جزئية وغير خالية من R فإن :

1- الشرط اللازم والكافي كي تكون المجموعة I مثالية يسارية في الحلقة $(R,+,\cdot)$ هو أن يتحقق ما يلي :

(a) لكل $a,b \in I$ ، فإن $a-b \in I$.

(b) لكل $a \in I$ و $r \in R$ ، فإن $r.a \in I$.

2- الشرط اللازم والكافي كي تكون المجموعة I مثالية يمينية في الحلقة $(R,+,\cdot)$ هو أن يتحقق ما يلي :

(a) لكل $a,b \in I$ فإن $a-b \in I$

(b) لكل $a \in I$ ، ولكل $r \in R$ ، فإن : $a.r \in I$.

3- الشرط اللازم والكافي كي تكون المجموعة I مثالية (ثنائية الجانب) في الحلقة $(R,+,\cdot)$ هو أن يتحقق ما يلي :

(a) لكل $a,b \in I$ فإن $a-b \in I$

(b) لكل $a \in I$ و $r_1,r_2 \in R$ فإن : $r_1.a.r_2 \in I$

البرهان :

لنبرهن على (1) وبالطريقة نفسها يمكن البرهان على (2) و(3) .

لزوم الشرط :

لنفرض أولاً أن I مثالية يسارية في الحلقة $(R,+,\cdot)$. بما أن $(I,+)$ زمرة جزئية من الزمرة $(R,+)$ ، فإنه من أجل أي $a,b\in I$ يكون $a-b\in I$، ومن ناحية ثانية، مهما يكن $r\in R$ و $a\in I$ فإن: $r.a\in r.I\subseteq I$

كفاية الشرط :

بما أنه لكل b,a من I يتحقق $a-b\in I$ ، وهذا يبين أن $(I,+)$ زمرة جزئية من الزمرة $(R,+)$. ليكن $r\in R$ ولكل $a\in I$ فإن : $r.a\in I$ ومنه يكون $r.I\subseteq I$

من التعريف والتمهيدية السابقتين ، نلاحظ ما يلي :

(1) إذا كانت I مثالية يسارية أو (يمينية) من الحلقة $(R,+,\cdot)$ ، فإن I حلقة جزئية من الحلقة $(R,+,\cdot)$. إلاّ أنه إذا كانت $(S,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ ، فليس ضرورياً أن تكون $(S,+,\cdot)$ مثالية يسارية أو (يمينية) في الحلقة $(R,+,\cdot)$.

فيما يلي ستستخدم كلمة مثالية للدلالة على المثالية ثنائية الجانب .

(2) إذا كانت $(R,+,\cdot)$ حلقة إبدالية ، فإن أي مثالية يسارية هي مثالية يمينية والعكس صحيح، لذلك ، فإنه في الحلقة الإبدالية أي مثالية يسارية أو يمينية هي مثالية في الحلقة $(R,+,\cdot)$.

(3) لتكن $(R,+,\cdot)$ حلقة ما ، ولنرمز لصفرها بـ o (محايدها بالنسبة للجمع) إذا كانت $R\neq\{o\}$ ، فإن الحلقة $(R,+,\cdot)$ تحوي مثاليتين على الأقل وهما R و $\{o\}$. كل مثالية في الحلقة $(R,+,\cdot)$ تختلف عن المثاليتين R و $\{o\}$ تسمى مثالية غير تافهة (مبتذلة) (trivial ideal) في الحلقة $(R,+,\cdot)$.

كل حلقة لا تحتوي على أية مثالية غير مبتذلة تسمى **بالحلقة البسيطة** .

(4) نقول إن المثالية I هي مثالية فعلية (Proper ideal) من حلقة ما $(R,+,\cdot)$ إذا كانت $I\neq R$.

نتيجة (1) :

ليكن $(F,+,\cdot)$ حقلاً ما ، عندئذٍ F لا يحوي سوى مثاليتين فقط وهما $F,\{o\}$.

البرهان :

لتكن I مثالية في الحقل $(F,+,\cdot)$. إذا كانت $I = o$ ، فإنه يتم المطلوب ، أما إذا لم يكن $I \neq o$ عندئذٍ يوجد في I عنصراً ما وليكن $a \neq o$. وبما أن للعنصر a معكوس (لأنه عنصر غير صفري من الحقل $(F,+,\cdot)$) فإنه $I = F$.

(7-2) أمثلة :

1- لتكن حلقة المصفوفات الحقيقية من الدرجة الثانية $(M_2(R),+,\cdot)$.

إن المجموعة $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ; a,b \in R \right\}$ هي مثالية يسارية ولكنها ليست مثالية يمينية في الحلقة $(M_2(R),+,\cdot)$.

الحل :

نلاحظ أولاً أن $\phi \neq I \subseteq M_2(R)$ لأن $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$.

لتكن $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$ عنصرين ما من I ، وإذا كانت $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(R)$ ، فإن :

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in I \qquad (1)$$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax+by & 0 \\ az+bw & 0 \end{pmatrix} \in I \qquad (2)$$

إذن ، من (1) و(2) ، نجد أن I مثالية يسارية . لنثبت الآن أن I ليست مثالية يمينية ، من أجل ذلك إن $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I$ و $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(R)$

لكـــن $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ ، إن $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin I$ وبالتالي فإن I ليست مثالية يمينية في الحلقة $(M_2(R), +, \cdot)$.

2- لتكن $(R,+,\cdot)$ حلقة جميع التطبيقات المتصلة على R، أثبت أن المجموعة : $I = \{g \in R : g(3) = 0\}$ مثالية .

الحل :

إن الحلقة $(R,+,\cdot)$ إبدالية (لأن عملية الجمع والضرب في التطبيقات إبدالية) .
بما أن التطبيق الصفري ينتمي إلى I ، فإن $I \neq \phi$ إذن $\phi \neq I \subseteq R$.
ليكن g,f من I وإذا كان h من R ، فإن :

$$(f - g)(3) = f(3) - g(3) = 0 - 0 = 0$$
$$(h \,.\, f)(3) = h(3) \,.\, f(3) = h(3) \,.\, 0 = 0$$

إذن $f - g \in I$ و $f \,.\, g \in I$ ، وبالتالـــي فـــإن I مثالية من حلقة التطبيقات المتصلة الإبدالية $(R,+,\cdot)$.

3- لتكن الحلقة $(Q,+,\cdot)$ ، بيّن فيما إذا كانت الحلقة الجزئية $(Z,+,\cdot)$ من الحلقة $(Q,+,\cdot)$ هي مثالية .

الحل :

إن $(Z,+,\cdot)$ ليست مثالية لأنه على سبيل المثال : إذا كان $\frac{1}{5} \in Q$ و $7 \in Z$ فإن $(7) \cdot \left(\frac{1}{5}\right) = \frac{7}{5} \notin Z$ ، أي أن الشـــرط الثانـــي الوارد في تعريف المثالية غير محقق . إذن $(Z,+,\cdot)$ ليست مثالية من الحلقة $(Q,+,\cdot)$.

قبل أن نقدم بعض العمليات على المثاليات ، نقدم المبرهنة الهامة التامة .

مبرهنة (7) :

إذا كانـــت $(R,+,\cdot)$ حلقـــة إبدالية بمحايد مثالياتها ، فقط المثاليان التافهان فإن

$(R,+,\cdot)$ حقل .

البرهان :

لنفرض أن الحلقة $(R,+,\cdot)$ لا تحتوي على مثاليات غير مبتذلة ، وليكن $a\in R\backslash\{0\}$، وهذا يعني أن $<a>\neq\{0\}$ ومن ثم فإن $<a>=R$ وبالتالي فإن:

$$1\in<a>=\{r.a \;:\; r\in R\}$$

إذن يوجد عنصر من R وليكن t بحيث يكون $1 = t.a$. وبسبب كون $(R,+,\cdot)$ إبدالية فإن $a.t = 1$ ، أي أن كل عنصر غير صفري a هو عنصر وحدة ، إذن $(R,+,\cdot)$ حقل .

(8-2) العمليات على المثاليات :

① جمع المثاليات :

لتكن J,I مثاليتين في حلقة ما $(R,+,\cdot)$. نسمي المجموعة :

$$\{x\in R : x=a+b \,;\, a\in I \,,\, b\in J\}$$

مجموع المثاليتين J,I ونرمز لها بالرمز $I+J$.

المبرهنة التالية تبين أن $I+J$ هي مثالية .

مبرهنة (8) :

لتكن J,I مثاليتين في حلقة ما $(R,+,\cdot)$. إن $I+J$ مثالية في الحلقة $(R,+,\cdot)$.

البرهان :

حسب التعريف السابق ، نلاحظ أن ، $\phi\neq I+J\subset R$.

إذا كان y,x عنصرين ما من $I+J$ ، فإنه يمكن كتابة ما يلي :

$$x=a+b \,;\, a\in I \,,\, b\in J$$

$$y=c+d \,;\, c\in I \,,\, d\in J$$

وبالتالي نجد :

$$x-y=(a+b)-(c+d)=(a-c)+(b-d)\in I+J$$

إذن الشرط الأول $x - y \in I + J$ محقق .

وإذا كان r من R و $x = a + b ; a \in I , b \in J$ من $I + J$ فإن :

$$r.x = r.(a + b) = r.a + r.b \in I + J$$

$$x.r = (a + b).r = a.r + b.r \in I + J$$

نستنتج مما سبق أن $I + J$ مثالية في الحلقة $(R,+,\cdot)$.

نستنتج من التعريف السابق ومن المبرهنة السابقة ما يلي :

(1) إذا كانت I,J,K ثلاث مثاليات في حلقة ما $(R,+,\cdot)$ ، فإن :

$$I + J = J + I$$

$$I + (J + K) = (I + J) + K$$

(2) إن مجموعة كل المثاليات في حلقة ما $(R,+,\cdot)$ مغلقة بالنسبة لعملية جمع المثاليات .

(3) إذا كانت $(R,+,\cdot)$ حلقة ما ، وكانت I و J مثاليتين يساريتين أو (يمينيتين) في الحلقة $(R,+,\cdot)$ فإن $I + J$ مثالية يسارية أو (يمينية) في نفس الحلقة $(R,+,\cdot)$.

② تقاطع مثاليات :

لتكن $(R,+,\cdot)$ حلقة ما ، إذا كانت I و J مثاليتين في الحلقة المذكورة . نسمي المجموعة :

$\{x \in R : x \in I , x \in J\}$ بتقاطع المثاليتين I و J ، ونرمز لها بالرمز $I \cap J$.

مبرهنة (9) :

إذا كانت J,I مثاليتين في حلقة ما $(R,+,\cdot)$، عندئذٍ $I \cap J$ مثالية في الحلقة $(R,+,\cdot)$.

البرهان :

نلاحظ أولاً أن $\phi \neq I \cap J \subseteq R$.

ليكن y,x عنصرين ما من $I \cap J$ ، فإن : $x,y \in J$ و $x,y \in I$ وبالتالي فإن $x - y \in I$ و $x - y \in J$ ومنه $x - y \in I \cap J$.

ليكن a,y عنصرين ما من $I\cap J$ و R على الترتيب، بما أن $y\in I\cap J$ ، فإن $y\in I$ و $y\in J$ ، وبالتالي فإن :

$$a.y\,,\,y.a\in I \;\;\&\;\; a.y\,,\,y.a\in J$$

إذن : $a.y\in I\cap J \;\;\&\;\; y.a\in I\cap J$

نستنتج مما سبق أن $I\cap J$ مثالية في الحلقة $(R,+,\cdot)$.

نستنتج من التعريف السابق والمبرهنة السابقة ما يلي :

1- إذا كانت I,J,K ثلاث مثاليات في حلقة ما $(R,+,\cdot)$ ، فإن :

$$I\cap J = J\cap I$$

$$I\cap(J\cap K) = (I\cap J)\cap K$$

2- إن مجموعة جميع المثاليات في الحلقة $(R,+,\cdot)$ مغلقة بالنسبة لعملية التقاطع المعرفة على المثاليات.

3- إذا كانت I,J مثاليتين يساريتين أو (يمينيتين) في حلقة ما $(R,+,\cdot)$ فإن $I\cap J$ مثالية يسارية أو (يمينية) في الحلقة $(R,+,\cdot)$.

4- ترتبط العمليتان السابقتان بالعلاقة التالية :

$$I\cap(J+K) = J+(I\cap K)$$

حيث I,J,K ثلاث مثاليات في الحلقة $(R,+,\cdot)$ ، حيث أن $J\subseteq I$.

③ ضرب (جداء) المثاليات :

إذا كانت I و J مثاليتين في حلقة ما $(R,+,\cdot)$ ، نسمي المجموعة :

$$\left\{ x\in R : x=\sum_{i=1}^{n} x_i\cdot y_i \;;\; x_i\in I\,,\,y_i\in J, n\in Z^+ \right\}$$

ضرب I بـــ J ونرمز لها بالرمز $I\cdot J$.

مبرهنة (10) :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت J,I مثاليتين فيها ، فإن $I\cdot J$ مثالية في الحلقـــة $(R,+,\cdot)$.

البرهان :

من الواضح (حسب تعريف جداء المثاليات) أن $\phi \neq I\cdot J \subseteq R$

إذا كان y,x عنصرين ما من $I\cdot J$ ، فإننا نستطيع كتابة ما يلي :

$$x = \sum_{i=1}^{n} x_i \cdot y_i \; ; \; x_i \in I \, , \, y_i \in J, n \in Z^+$$

$$y = \sum_{j=1}^{m} x'_j \cdot y'_j \; ; \; x'_j \in I \, , \, y'_j \in J \, , \, m \in Z^+$$

وبالتالي فإن :

$$x - y = \sum_{i=1}^{n} x_i \cdot y_i - \sum_{j=1}^{m} x'_j \cdot y'_j = \sum_{i=1}^{n} x_i \cdot y_i + \sum_{j=1}^{m} (-x'_j) \cdot y'_j \in I + J$$

ليكن الآن y عنصراً من $I\cdot J$ و a من R . بما أن $y \in I\cdot J$ فإن :

$$y = \sum_{i=1}^{n} x_i \cdot y_i \; ; \; x_i \in I \, , \, y_i \in J, n \in Z^+$$

وبالتالي يكون :

$$a \cdot y = a \cdot \left(\sum_{i=1}^{n} x_i \cdot y_i \right) = \sum_{i=1}^{n} (a \cdot x_i) \cdot y_i \in I \cdot J$$

$$y \cdot a = \left(\sum_{i=1}^{n} x_i \cdot y_i \right) \cdot a = \sum_{i=1}^{n} x_i \cdot (y_i \cdot a) \in I \cdot J$$

نستنتج مما سبق أن $I\cdot J$ مثالية في الحلقة $(R,+,\cdot)$.

نستنتج من التعريف السابق ومن المبرهنة السابقة ما يلي :

(1) إذا كانت I,J,K ثلاث مثاليات في الحلقة $(R,+,\cdot)$ ، فإن :

$$I \cdot (J \cdot K) = (I \cdot J) \cdot K$$

(2) إن مجموعة كل المثاليات في الحلقة $(R,+,\cdot)$ مغلقة بالنسبة لعملية ضرب المثاليات .

(3) ترتبط العمليات السابقة في المثاليات I,J,K في حلقة ما $(R,+,\cdot)$ بالعلاقات التالية :

$$I\bullet(J+K)=(I\bullet J)+I\bullet K$$

$$(J+K)\bullet I=J\bullet I+K\bullet I$$

أي أن عملية ضرب المثاليات توزيعي على عملية جمع المثاليات في $(R,+,\bullet)$ ، كما أن $I\bullet J\subseteq I\cap J$.

④ قسمة المثاليات :

بفرض أن $(R,+,\bullet)$ حلقة إبدالية ما ، وإذا كانت J,I مثاليتين في الحلقة $(R,+,\bullet)$ فإن المجموعة $\{x\in R : x.J\subseteq I\}$ تسمى حاصل قسمة I على J ، ونرمز لذلك بـ $I:J$ أو بـ (I/J) .

مبرهنة (11) :

إذا كانت J,I مثاليتين في حلقة إبدالية ما $(R,+,\bullet)$ ، عندئذٍ $I:J$ مثالية في الحلقة $(R,+,\bullet)$ تحوي I .

البرهان :

لنبرهن أولاً أن $\phi\neq I:J\subseteq R$. إن $I:J$ مجموعة جزئية من R . وإذا رمزنا لصفر الحلقة $(R,+,\bullet)$ بـ o ، فإن : $o\bullet J=\{o\}\subseteq I$ وهذا يعني أن $o\in I:J$ ، إذن $I:J\neq\phi$.

إذا كان y,x عنصرين ما من $I:J$ فإنه حسب التعريف السابق :

$$x\bullet J\subseteq I\ ,\ y\bullet J\subseteq I$$

وبالتالي يكون : $(x-y)\bullet J\subseteq I$ ومنه يكون : $x-y\in I:J$.

بفرض أن x عنصراً من $I:J$ و a من R ، وبالتالي بما أن $x\in I:J$ ، فهذا يعني أن $x\bullet J\subseteq I$ ، وبالتالي يكون لدينا :

$$a\bullet(x\bullet J)\subseteq I\ \Rightarrow\ (a\bullet x)\bullet J\subseteq I\ \Rightarrow\ a\bullet x\in I:J$$

نستنتج مما سبق أن $I:J$ مثالية في الحلقة $(R,+,\bullet)$.

لنبرهن أخيراً أن $I\subseteq I:J$ ، من أجل ذلك ، إذا كان a عنصراً من I ، فإن

$a \bullet J \subseteq I$ ، وهذا يعني أن $a \in I : J$.

⑤ **جذر المثاليات :**

لتكن $(R,+,\cdot)$ حلقة إبدالية ما ، المجموعة التالية :

$$\left\{ x \in R : \exists n \in Z^{+} ; x^{n} \in I \right\}$$

تسمى جذر المثالية I ، ونرمز لها بـ $\sqrt{I}$.

مبرهنة (12) :

إذا كانت $(R,+,\cdot)$ حلقة إبدالية ما ، فإن $\sqrt{I}$ هي مثالية في الحلقة $(R,+,\cdot)$ تحوي I .

البرهان :

نلاحظ أولاً أن $\phi \neq \sqrt{I} \subseteq R$.

إذا كان y,x عنصرين ما من $\sqrt{I}$ ، فحسب التعريف السابق ، يوجد عددان صحيحان موجبان m,n ، بحيث يكون $x^{n} \in I , y^{m} \in J$. وبالتالي فإن :

$$(x-y)^{n+m-1} \in I \Rightarrow x-y \in \sqrt{I}$$

وإذا كان x عنصراً ما من I و a من R ، فإنه يمكن إيجاد عدد صحيح موجب ، وليكن n ، بحيث يكون $x^{n} \in I$ ، وبالتالي فإن $(a.x)^{n} \in I$ ومنه يكون $a.x \in \sqrt{I}$.

نستنتج مما سبق أن $\sqrt{I}$ مثالية في الحلقة الإبدالية $(R,+,\cdot)$.

لنبرهن أخيراً أن $\sqrt{I}$ تحوي I في الحلقة $(R,+,\cdot)$.

ليكن y عنصراً ما من I ، وبالتالي فإن $y^{1} \in I$ ، وبالتالي فإن $y \in \sqrt{I}$ وهذا يعني أن $\sqrt{I}$ مثالية في الحلقة $(R,+,\cdot)$ تحوي I .

مثال (12) :

لتكن K,J,I مثاليات يسارية (يمينية) في حلقة ما ولتكن $(R,+,\cdot)$ ، وإذا كان $I \subseteq K$. أثبت أن :

$$I + (J \cap K) = (I + J) \cap K$$

الحل :

ليكن $x \in I + (J \cap K)$ وهذا يعني أن $x = a + b$ حيث $a \in I$ و $b \in J \cap K$ أي أن $b \in K$ و $b \in J$.

بما أن $b \in J$ فإن : $x = a + b \in I + J$.

من ناحية ثانية ، بما أن $b \in K$ ، وأن $a \in I \subseteq K$ نجد أن : $x = a + b \in K$

نستنتج مما سبق أن : $x = a + b \in (I + J) \cap K$. أي أن :

$$I + (J \cap K) \subseteq (I + J) \cap K$$

ليكن $y \in (I + J) \cap K$ ، عندئذٍ $y \in K$ و $y \in I + J$ ، وبالتالي ، فإن $y = a + b$ ، حيث أن $a \in I$, $b \in J$. وبما أن $I \subseteq K$ فإن $a \in K$ و $b = y - a \in K$ ، إذن $b \in J \cap K$ ، وهذا يبين لنا أن : $y = a + b \in I + (J \cap K)$ ، أي أن :

$$(I + J) \cap K \subseteq I + (J \cap K)$$

نستنتج مما سبق أن :

$$(I + J) \cap K = I + (J \cap K)$$

مثال (13) :

إذا كانت $(R,+,\cdot)$ حلقة إبدالية ما، ولتكن K,J,I مثاليات في هذه الحلقة ، أثبت صحة العلاقة:

$$I : (J \cdot K) = (I : J) : K$$

الحل :

ليكن x عنصراً ما من $I : (J \cdot K)$ ، وبالتالي فإن : $x \cdot (J \cdot K) \subseteq I$ ، ومنه يكون : $(x \cdot K) \cdot J \subseteq I$ إذن : $x \in (I : J) : K$.

لنبرهن العكس :

ليكن y عنصراً ما من $(I : J) : K$ ، وبالتالي فإن : $y \cdot K \subseteq I : J$ ، وبالتالي فإن:

$(y \cdot K) \cdot J \subseteq I$ ، أي أن $y \cdot (J \cdot K) \subseteq I$. إذن : $y \in I : (J \cdot K)$

نستنتج مما سبق أن : $I : (J \cdot K) = (I : J) : K$

ملاحظة (2) :

1- إذا كانـــت $(R,+,\cdot)$ حلقـــة ما ، وإذا كانت N,M مجموعتين جزئيتين غير خاليتين من R ، فإن مجموعة كل العناصر التي من الشكل $\sum_{i=1}^{n} x_i \cdot y_i$ حيث أن x_i مـــن M و y_i مـــن N و n عـــدد صحيح موجب، تسمى M لـــ N ويرمز لها بـــ $M \cdot N$.

وبصـــورة عامة : إذا كانت إحدى المجموعتين M,N ولتكن M تتألف من عنصر واحد فقط وليكن a مثلاً، فإننا سنرمز بـــ $M \cdot N$ في هذه الحالة بالشكل $a \cdot N$.

نتائج :

(1) إذا كانـــت $(R,+,\cdot)$ حلقة ما ، ولتكن I مثالية يسارية في الحلقة $(R,+,\cdot)$ ، وإذا كانت J مثالية يمينية في الحلقة $(R,+,\cdot)$، فإن $I \cdot J$ مثالية في الحلقة $(R,+,\cdot)$.

(2) إذا كانـــت I مثالـــية يسارية في حلقة ما ، ولتكن $(R,+,\cdot)$ ، وإذا كانت J مجموعة جزئية غير خالية من R ، فإن $I \cdot J$ مثالية يسارية في الحلقة $(R,+,\cdot)$.

(3) إذا كانـــت I مثالـــية يمينـــية فـــي حلقة ما ، ولتكن $(R,+,\cdot)$ وإذا كانت J مجموعة جزئية غير خالية من R ، فإن $I \cdot J$ مثالية يمينية في الحلقة $(R,+,\cdot)$.

(4) إذا كانـــت I مثالـــية في حلقة إبدالية ما $(R,+,\cdot)$ ، وإذا كانت J مجموعة جزئية غير خالية من R ، فإن $I \cdot J$ مثالية في الحلقة $(R,+,\cdot)$.

(9-2) حلقة القسمة Quotient group :

لتكـــن $(R,+,\cdot)$ حلقة ما، وإذا كانت I مثالية فيها . نعلم أن $(I,+)$ زمرة جزئية من الزمرة الإبدالية $(R,+)$. وبما أن كل زمرة جزئية من زمرة إبدالية هي زمرة جزئية ناظمية منها ، فإن الزمرة الجزئية $(I,+)$ ، هي إذاً زمرة جزئية ناظمية من الزمرة $(R,+)$ ، وبالتالي فإن $(R/I,+)$ زمرة إبدالية حيث أن :

$$R/I = \{x + I \ : \ x \in R\}$$

إن (+) عملية جبرية ثنائية معرفة على R/I بالشكل :

$$(x + I) + (y + I) = (x + y) + I \ ; \ \forall \ x,y \in I$$

ولنعرف على المجموعة R/I العملية (•) بالشكل :

$$(x + I) \bullet (y + I) = (x \bullet y + I) \ ; \forall \ x,y \in I$$

مجموعة العناصر من R/I ، تسمى عادةً بالمجموعات المشاركة Costes لـ I في R .

تبيّن المبرهنة التالية أن (R/I,+,•) حلقة ، وهذه الحلقة تسمى بحلقة القسمة .

مبرهنة (13) :

لتكن I مثالية في حلقة ما (R,+,•)، وإذا عرفنا على عناصر المجموعة $R/I = \{x + I \ ; x \in I\}$ العمليتين الجبريتين (+) و(•) بالشكل التالي :

$$(x + I) + (y + I) = (x + y) + I$$

$$(x + I) \bullet (y + I) = (x \bullet y) + I \ ; \ \forall x,y \in I$$

عندها تكون (R/I,+,•) حلقة . وإذا كانت الحلقة (R,+,•) إبدالية فإن (R/I,+,•) حلقة إبدالية . وإذا كانت الحلقة (R,+,•) بمحايد (ذات عنصر الوحدة) ، فإن الحلقة (R/I,+,•) ستكون بمحايد أيضاً .

البرهان :

لنبرهن أولاً أن عملية الضرب (•) حسنة التعريف (معرفة جيداً) .

لنفرض أن $x_1,x_2,y_1,y_2 \in R$ ، بحيث يكون :

$$x_1 + I = x_2 + I \ , \ y_1 + I = y_2 + I$$

فإن : $x_1 - x_2 \in I \ , \ y_1 - y_2 \in I$

وبالتالي فإن :

$$x_1.y_1 - x_2.y_2 = (x_1 - x_2).y_1 + x_2\,(y_2 - y_1) \in I$$

ومنه يكون :

$$x_1.y_1 + I = x_2.y_2 + I$$

لنثبت الآن أن $(R/I, .)$ شبه زمرة (تجميعية) .

لتكن z,y,x عناصر ما من الحلقة $(R,+,.)$ ، وبالتالي فإن :

$$(x + I).\left[(y + I)\ (z + I)\right] = (x + I)\ (y.z + I) = x\ (y.z) + I$$
$$= (x.y).z + I = (x.y + I).(z + I) = \left[(x + I).(y + I)\right].(z + I)$$

لنبرهن الآن أن عملية الضرب $(.)$ توزيعية على عملية الجمع $(+)$ في R/I .

$$(x + I)\ .\ \left[(y + I) + (z + I)\right] = (x + I).\left[(y + z) + I\right] = x.(y + z) + I$$
$$= (x.y + x.z) + I = (x.y+I) + (x.z + I)$$
$$= (x + I).(y + I) + (x + I).(z + I)$$

وبالطريقة ذاتها نبرهن أن :

$$\left[(y + I) + (z + I)\right].\ (x + I) = \left[(y + z) + I\right].(x + I) = (y + z).x + I$$
$$= (y.x + z.x) + I = (y.x+ I) + (z.x + I)$$
$$=(y + I).\ (x + I) + (z + I).\ (x + I)$$

بعد الأخذ بعين الاعتبار أن $(R/I,+,.)$ زمرة إبدالية .

نستنتج مما سبق أن $(R/I,+,.)$ حلقة ، ولنبرهن أنها إذا كانت $(R,+,.)$ إبدالية بمحايد فإن $(R/I,+,.)$ هي أيضاً إبدالية وبمحايد .

فإذا كان y,x عنصرين ما من الحلقة R ، فإن :

$$(x + I).(y + I) = x.y + I = y.x + I = (y + I).(x + I)$$

وإذا رمزنا لمحايد الحلقة $(R,+,.)$ بـ 1 فإن $1 + I$ ينتمي إلى R/I ، ومن جهة ثانية لدينا :

$$(x + I).(1 + I) = (1 + I).(x + I) = x + I\ ;\ x + I \in R/I$$

نود الإشارة إلى أن : $0 + I = I$ هو صفر حلقة القسمة R/I . كما أن العنصر $-x + I$ ، هو المعكوس التجميعي للعنصر $x + I$ ، حيث $x \in R$.

تعريف :

نسمي الحلقة الواردة في المبرهنة السابقة $(R/I,+,.)$ بحلقة القسمة Factor ring or Quotient ring.

مبرهنة (14) :

لتكن $(R,+,.)$ حلقة ما ، ولتكن I مثالية فيها . إن المثاليات اليسارية (اليمينية) في حلقة القسمة $\overline{R}=(R/I,+,.)$ هي من الشكل $\overline{K}=\frac{K}{I}$. حيث أن K مثالية يسارية (يمينية) في الحلقة $(R,+,.)$ وأن $I \subseteq K$.

البرهان :

لنفرض أن $\overline{K}$ مثالية يسارية في الحلقة $\overline{R}$ ، ولنبرهن أولاً أن $\overline{K}=\frac{K}{I}$ حيث K مثالية يسارية في الحلقة $(R,+,.)$ وتحوي I .

لنأخذ المجموعة $K = \{x : x\in R \,;\, x + I\in \overline{K}\}$، ولنثبت أن K هي مثالية يسارية في الحلقة $(R,+,.)$.

بما أن $\overline{K}$ مثالية يسارية في $\overline{R}$ فإن $\overline{o}=o+I\in\overline{K}$ ، ومنه $o\in K$ ، وهذا يعني أن $K\neq\phi$.

ليكن y,x عنصرين ما من K ، وبالتالي يكون :

$$\overline{x}=x+I \;,\; \overline{y}=y+I$$

ومنه :

$$(x-y)+I=(x+I)+(-y+I)=\overline{x}-\overline{y}\in\overline{K}$$

وهذا يبين لنا أن : $x-y\in K$.

كذلك ، أياً كان $a\in R$ فإن : $\overline{a}=a+I\in\overline{R}$ ، ومنه :

$$a.x+I=(a+I).(x+I)=\overline{a}.\overline{x}\in\overline{K}$$

نستنتج مما سبق أن المجموعة K تشكل مثالية يسارية في الحلقة $(R,+,.)$.

لنبرهن الآن أن $I\subseteq K$.

ليكن $a\in I$ ، فإن $a+I=\overline{a}\in\overline{K}$ ، أي أن $a\in K$ ، وبالتالي نجد : $I\subseteq K$.

لنبرهن أخيراً أن $\overline{K}=\frac{K}{I}$:

لـيكن $\overline{Z} = Z + I \in \frac{K}{I}$ ، وبالتـالي فـإن $z \in K$ ، ومنـه $z + I \in \overline{K}$ أي أن $\frac{K}{I} \subseteq \overline{K}$.

من ناحية أخرى ليكن $\overline{Z} \in \overline{K} \subseteq \frac{K}{I}$ ، عندئذٍ $\overline{Z} = Z + I$ حيث $Z \in R$. وبما أن $\overline{Z} = Z + I \in \overline{K}$ فإن $Z \in K$ ، وبالتـالي نجـد أن : $\overline{Z} = Z + I \in \frac{K}{I}$ ، أي أن $\overline{K} \subseteq \frac{K}{I}$.

مما سبق نجد أن $\overline{K} = \frac{K}{I}$.

(10-2) أمثلة :

1- من المعلوم أن $6.Z$ هي مثالية من الحلقة $(2Z,+,.)$ ، وبالتالي فإن :

$$\frac{2Z}{6Z} = \{0 + 2Z\,,\, 2 + 6Z\,,\, 4 + 6Z\}$$

حلقة إبدالية بمحايد (حسب المبرهنة السابقة) .

2- لتكن $(R,+,.)$ هي حلقة المصفوفات التي من الشكل :

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} ; a, b \in Z \right\}$$

بالنسبة للعمليتين جمع وضرب المصفوفات . ونعلم أن :

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} ; b \in Z \right\} \subseteq R$$

هي مثالية من الحلقة $(R,+,.)$ ، عندئذٍ $(R/I,+,.)$ هي حلقة إبدالية بمحايد .

الحل :

نلاحظ أولاً أن :

$$R/I = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I \,;\, a, b \in Z \right\}$$

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + I$$

يمكن التأكد بسهولة الآن أن $(R/I,+,\cdot)$ هي حلقة إبدالية بمحايد .

نتيجة (2) :

إذا كانت $(R,+,\cdot)$ حلقة تحتوي على قواسم للصفر ، وكانت I مثالية من الحلقة $(R,+,\cdot)$ ، فليس من الضروري أن تحتوي حلقة القسمة $(R/I,+,\cdot)$ ، على قواسم للصفر .

لإثبات ذلك ، نأخذ الحلقة $(Z\times Z,+,\cdot)$ التي تحتوي قواسم للصفر ، ولكن حلقة القسمة $\left(\frac{Z\times Z}{Z\times\{0\}},+,\cdot\right)$ لا تحتوي على قواسم للصفر .

الفصل الثالث

التماثل الحلقي

Isomorphism of ring

الفصل الثالث

التماثل الحلقي

Isomorphism of ring

لا يكتفي علم الجبر بدراسة البنى الجبرية وخواصها ، بل يتعداها إلى دراسة التطبيقات من بنية جبرية إلى أخرى . وتلعب التطبيقات التي تسمى تشاكلاً (Homomorphism) دوراً مهماً جداً في علم الجبر . والتماثل (Isomorphism) يمكّننا من معرفة ناتج عملية على عناصر إحدى البنيتين الجبريتين ، دون إجراء الحساب في هذه البنية ، وإنما إجراء الحسابات في البنية الأخرى، والتي قد تكون أيسر وأسرع . ويمكن تشبيه التماثل بقاموس (معجم) يمكننا من التحقق من أن جملة ما في إحدى اللغات ، تقابل جملة لها نفس المعنى في لغة أخرى .

(1-3) تعريف التشاكل Homomorphism :

لتكن $(R,+,\cdot)$ و$(S,T,\star)$ حلقتين ما ، وليكن φ تطبيقاً من R إلى S ، نسمي التطبيق φ تشاكلاً من الحلقة R إلى الحلقة S إذا تحقق الشرطان التاليان :

(a) لكل y,x من R ، يكون : $\varphi(x + y) = \varphi(x)\, T\, \varphi(y)$

(b) لكل y,x من R ، يكون : $\varphi(x\cdot y) = \varphi(x)\star\varphi(y)$

ونقول إن التطبيق $\varphi : R \longrightarrow S$ تشاكلاً للحلقة $(R,+,\cdot)$ على الحلقة $(S,T,\star)$ ، إذا كان التطبيق φ شاملاً ويحقق الشرطين (a) و(b) السابقين .

ونسمي التطبيق السابق φ تماثلاً للحلقة $(R,+,\cdot)$ في الحلقة $(S,T,\star)$ إذا كان التطبيق φ متبايناً (أحادياً) ، ويحقق الشرطين (a) و(b) أيضاً .

ويسمى التطبيق φ (السابق) تماثلاً للحلقة $(R,+,\cdot)$ على الحلقة $(S,T,\star)$ ، إذا كان التطبيق φ تقابلاً (متبايناً وشاملاً) ويحقق أيضاً الشرطين (a) و(b) .

ونرمز عادةً لهذا التماثل بـ $\cong$ ونكتب $(R,+,\cdot)\cong(S,T,\star)$ أو اختصاراً $R\cong S$.

ونقول إن الحلقتين $(R,+,\cdot)$ و $(S,T,\star)$ متماثلتان ، إذا وُجِدَ تماثل $\varphi: R \longrightarrow S$ أو $\varphi : S \longrightarrow R$.

ملاحظة (1) :

إذا كانت $(R,+,\cdot)$ و $(S,+,\cdot)$ حلقتين ما ، فإن التطبيق $\varphi:R \longrightarrow S$ يسمى تشاكلاً إذا حقق الشرطين التاليين :

$$\varphi(x + y) = \varphi(x) + \varphi(y) \qquad \text{(a)}$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \qquad \text{(b)}$$

لكل y,x من R .

الشرط الأول (a) يعني أن التطبيق φ يحافظ على عملية الجمع ، والشرط الثاني يعني أن φ يحافظ على عملية الضرب .

ونود الإشارة، إلى أن بعض المراجع الأجنبية تعرِّف التشاكل الحلقي $\varphi:R \longrightarrow S$ على أنه التطبيق الذي يحقق الشروط التالية :

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \text{(a)}$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \qquad \text{(b)}$$

$\varphi(1) = 1$ لكل b,a من R (c)

حيث أن 1 هو عنصر الوحدة في الحلقة $(R,+,\cdot)$.

(2-3) أمثلة :

<u>1-</u> لتكن $(R,+,\cdot)$ و $(S,T,\star)$ حلقتين ما ، ولنرمز لصفر الحلقة $(S,T,\star)$ بـ o' ، التطبيق: $\varphi : R \longrightarrow S$ والمعرف بالشكل $\varphi(x) = o' \; ; \forall x \in R$ هو تشاكل للحلقة R في الحلقة $(S,T,\star)$.

الحل :

من أجل أي عنصرين y,x من R ، فإن :

$$\varphi(x + y) = o' = o' \, T \, o' = \varphi(x) \, T \, \varphi(y)$$

$$\varphi(x \cdot y) = o' = o' \star o' = \varphi(x) \star \varphi(y)$$

يسمى عادةً التشاكل السابق بالتشاكل المبتذل (Trivial homomorphism) .

-2 لتكن $(R,+,\bullet)$ حلقة بمحايد ، ولنرمز لعنصر الوحدة (لمحايدها) بـ 1 ولتكن Δ_1 و Δ_2 عمليتين ثنائيتين معرفتين على R ، بالشكل :

$$x\,\Delta_1\,y = x + y + 1 \;\;,\;\; x\,\Delta_2\,y = x + y + x.y$$

لكل y,x من R .

من السهل التأكد من أن (R,Δ_1,Δ_2) حلقة .

المطلوب بيّن أن الحلقتين (R,Δ_1,Δ_2) و $(R,+,\bullet)$ متماثلتان .

الحل :

لنعرف التطبيق $\varphi : R \longrightarrow R$ بالشكل :

$$\varphi(x) = x + 1 \;\;;\;\; \forall x \in R$$

لنثبت أولاً أن φ تشاكل للحلقة (R,Δ_1,Δ_2) على الحلقة $(R,+,\bullet)$.

ليكن x,y عنصرين ما من R ، فإن :

$$\begin{aligned}\varphi(x\,\Delta_1\,y) &= \varphi(x + y + 1) = (x + y + 1) + 1\\ &= (x + 1) + (y + 1) = \varphi(x) + \varphi(y)\end{aligned}$$

الشرط الأول محقق .

$$\begin{aligned}\varphi(x\,\Delta_2\,y) &= \varphi(x + y + x\bullet y) = (x + y + x\bullet y) + 1\\ &= (x + 1)\bullet(y + 1) = \varphi(x)\bullet\varphi(y)\end{aligned}$$

الشرط الثاني محقق أيضاً ، إذن التطبيق φ تشاكل .

لنثبت الآن أن التطبيق φ متبايناً .

ليكن y,x عنصرين ما من $(R,+,\bullet)$، بحيث يكون $\varphi(x) = \varphi(y)$ ومنه يكون : $x + 1 = y + 1$ أي أن : $x = y$

لنبرهن أخيراً أن φ شامل :

ليكن y عنصراً ما من R ، إن $y - 1 \in R$ ، ومن ناحية ثانية إن $\varphi(y - 1) = y$.

نستنتج مما سبق أن φ تماثل للحلقة (R,Δ_1,Δ_2) على الحلقة $(R,+,\cdot)$ أي أن الحلقتين متماثلتان .

-3 ليكن التطبيق $Z_{10} \longrightarrow \varphi : Z_5$ والمعرف بالشكل :

$$\varphi(x) = 5x \;\; ; \;\; \forall x \in Z_5$$

بيّن فيما إذا كان التطبيق φ من الحلقة $(Z_5,+,\cdot)$ إلى الحلقة $(Z_{10},+,\cdot)$ تشاكلاً .

الحل :

نلاحظ أن الشرط الأول الوارد في تعريف التشاكل غير محقق لأنه على سبيل المثال :

$$\varphi(2+4) = \varphi(1) = 5 \cdot 1 = 5$$

كما أن :

$$\varphi(2) + \varphi(4) = 0 + 0 = 0$$

وبالتالي فإن :

$$\varphi(2+4) \neq \varphi(2) + \varphi(4)$$

-4 إن حلقة الأعداد الحقيقية $(R,+,\cdot)$ لا تماثل حلقة الأعداد المركبة $(C,+,\cdot)$ لأنه على سبيل المثال المعادلة $x^2 + 4 = 0$ لها حل $x = \pm\sqrt{-2}$ في الحلقة C ، ولكن لا يوجد لها حل في حلقة الأعداد الحقيقية .

-5 لتكن $(R,+,\cdot)$ حلقة بمحايد ، بيّن أن التطبيق φ المعرف بالشكل : $\varphi : Z \longrightarrow R$ ، $\varphi(n) = n.1$ حيث $n \in Z$ تشاكل :

الحل :

لكل m,n من الحلقة $(Z,+,\cdot)$ ، يكون لدينا :

$$\varphi(m+n) = (m+n)\cdot 1 = m\cdot 1 + n\cdot 1 = \varphi(m) + \varphi(n)$$

$$\begin{aligned}\varphi(m\cdot n) &= (m\cdot n)\cdot 1 = (m\cdot n)\,(1\cdot 1) = (m\cdot 1)\cdot(n\cdot 1)\\ &= \varphi(m)\cdot\varphi(n)\end{aligned}$$

نستنتج مما سبق أن التطبيق φ تشاكلاً .

(3-3) مفاهيم وملاحظات :

ليكن $(R,+,\cdot)$ و$(S,+,\cdot)$ حلقتين ما ، ولنفرض أن $\varphi : R \longrightarrow S$ تشاكلاً ، أي يحقق φ الشرطين الواردين في تعريف التشاكل :

(1) إذا كان φ تشاكلاً وتطبيقاً متبايناً ، فإننا نقول إن التطبيق φ تشاكل متباين (monomorphism) .

(2) إذا كان φ تشاكلاً ، وتطبيقاً شاملاً ، فإننا نقول إن التطبيق φ تشاكل شامل (epimorphism) .

(3) وإذا كان φ تشاكلاً تقابلاً ، فإننا نقول إن φ تماثل (isomorphism) .

(4) وإذا كان $\varphi : R \longrightarrow R$ تشاكلاً ، فإننا نقول إن φ تشاكل ذاتي (endomorphism) ، وإذا كان التطبيق φ تماثلاً . فإننا نقول إن φ تماثل ذاتي (automorphism) .

إذا كان $\varphi : R \longrightarrow S$ تماثلاً ، فإن $\varphi^{-1} : S \longrightarrow R$ تماثل أيضاً .

(5) لتكن $(R,+,\cdot)$ و$(S,T,\star)$ حلقتين ما ، ولنرمز لصفر الحلقة $(S,T,\star)$ بـ o' . ولنفرض أن التطبيق $\varphi : R \longrightarrow S$ تشاكل للحلقة $(R,+,\cdot)$ في الحلقة $(S,T,\star)$، فإن المجموعة التالية: $\{x \in R : \varphi(x) = o'\}$ تسمى بنواة التطبيق φ، ويرمز لها بالرمز $\mathrm{Ker}\,\varphi$. إذن :

$$\mathrm{Ker}\,\varphi = \{x \in R : \varphi(x) = o'\}$$

كما أن صورة التطبيق φ ونرمز لها عادةً بـ $\mathrm{Im}\,\varphi$ هي المجموعة :

$$\mathrm{Im}\,\varphi = \{\varphi(x) : x \in R\} = \varphi(R)$$

وكما درسنا في نظرية الزمر ، نقول إن التطبيق φ متباين إذا كان $\mathrm{Ker}\,\varphi = \{0\}$، حيث 0 صفر الحلقة $(R,+,\cdot)$. ونقول عنه إنه شامل إذا كانت $\mathrm{Im}\,\varphi = S$.

مثال (6) :

إذا كانت الحلقة الجزئية $(S,+,\cdot)$ من حلقة $(M_2(R),+,\cdot)$:

$$S=\left\{\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}; x,y\in R\right\}$$

وليكن التطبيق $\varphi : S \longrightarrow R$ المعرف بالشكل :

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

المطلوب ، بيّن أن التطبيق φ تشاكل ، ثم حدّد نواته .

الحل :

لكل $\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$ و $\begin{pmatrix} z & t \\ 0 & z \end{pmatrix}$ من S ، إن :

$$\varphi\left(\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}+\begin{pmatrix} z & t \\ 0 & z \end{pmatrix}\right)=\varphi\left(\begin{pmatrix} x+z & y+t \\ 0 & x+z \end{pmatrix}\right)=x+z$$

$$=\varphi\left(\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}\right)+\varphi\left(\begin{pmatrix} z & t \\ 0 & z \end{pmatrix}\right)$$

إذن الشرط الأول محقق .

$$\varphi\left(\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}\cdot\begin{pmatrix} z & t \\ 0 & z \end{pmatrix}\right)=\varphi\left(\begin{pmatrix} x\cdot z & x\cdot t+y\cdot z \\ 0 & x\cdot z \end{pmatrix}\right)=x\cdot z$$

$$=\varphi\left(\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}\right)\cdot\varphi\left(\begin{pmatrix} z & t \\ 0 & z \end{pmatrix}\right)$$

وبالتالي فإن φ تشاكل ، لنوجد الآن نواته .

حسب تعريف نواة التطبيق φ يكون لدينا :

$$\operatorname{Ker}\varphi=\left\{\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}: x=0\right\}=\left\{\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}; y\in R\right\}$$

مثال (7) :

لتكن $(Z_n,+,\cdot)$ حلقة الأعداد الصحيحة قياس n ، ولتكن حلقة المجموعات

المشاركة $(Z/nZ,+,\bullet)$. أثبت أن $Z/nZ \cong Z_n$.

الحل :

لنشكل التطبيق φ من Z/nZ إلى Z_n بالشكل التالي :

$$\varphi : Z/n.Z \longrightarrow Z_n$$
$$\varphi(x + n.Z) = [x]$$

لنثبت أولاً أن φ تشاكل .

لكل $x + n.Z$ و $y + n.Z$ من $Z/n.Z$ ، فإن :

$$\varphi[(x + n.Z) + (y + n.Z)] = \varphi(x + y + n.Z) = [x + y] =$$
$$= [x] + [y] = \varphi(x + n.Z) + \varphi(y + n.Z)$$

أي أن الشرط الأول محقق .

$$\varphi[(x + n\bullet Z)\bullet(y + n.Z)] = \varphi(x\bullet y + n\bullet Z) = [x\bullet y] =$$
$$= [x]\bullet[y] = \varphi(x + n\bullet Z)\bullet\varphi(y + n\bullet Z)$$

والشرط الثاني محقق أيضاً .

إذن التطبيق φ تشاكل .

لنبرهن الآن أن φ متباين . ليكن $x + n.Z \in Ker\ \varphi$ ، وهذا يعني : $\varphi(x + n.Z) = [0]$ ، ولكن $\varphi(x + n.Z) = [x]$ ، إذن $[x] = [0]$ وهذا يعني أن $x \in [0]$ ، أي أن $x + n.Z = n.Z$، وبما أن $n.Z$ هو صفر الحلقة $(Z/n.Z,+,\bullet)$ ، إذن φ متباين .

لنبرهن أخيراً أن φ شامل .

ليكن $[x]$ عنصراً ما من الحلقة $(Z_n,+,\bullet)$ ، أي أن $\varphi(x + n.Z) = [x]$ ، وهذا يعني أن φ شامل .

نستنتج مما سبق أن الحلقتين $(Z/n.Z,+,\bullet)$ و $(Z_n,+,\bullet)$ متماثلتان .

مبرهنة (1) :

ليكن $(F,+,\bullet)$ حقلاً منتهياً ما ، مميزه P ، عندها يكون التطبيق $\varphi : F \longrightarrow F$

المعرف بالشكل : $\varphi(x) = x^p$ ، لكل x من F ، تماثلاً ذاتياً على الحقل F ، ويكون $F_{\{\varphi\}} \cong Z_P$.

نسمي عادةً هذا التماثل بتماثل فرابينوس Frobenius Automorphism .

البرهان :

إذا كان y,x عنصرين من الحقل F ، عندئذٍ يكون :

$$(x+y)^P = x^P + (P-1)\, x^{P-1}.y + \frac{P(P-1)}{2} x^{P-2}.y^2 + \ldots + (P-1)\, x\, y^{P-1} + y^P$$

وبما أن P مميز الحقل F ، فيكون :

$$(x+y)^P = x^P + 0 + 0 + \ldots + 0 + y^P = x^P + y^P$$

وبالتالي يكون لدينا :

$$\varphi(x+y) = (x+y)^P = x^P + y^P = \varphi(x) + \varphi(y)$$

$$\varphi(x.y) = (x.y)^P = x^P.y^P = \varphi(x).\varphi(y)$$

إذن التطبيق φ يمثل تشاكلاً .

لنبرهن أن φ متباين (أحادي) .

بما أن $\varphi(x) = 0$ أي أن $x^P = 0$ ، وبالتالي يكون $x = 0$ ، وهذا يعني أن $\text{Ker}\,\varphi = 0$.

بما أن الحقل F منته ، وهذا يؤدي إلى أن التطبيق φ شامل .

إذن ، نستنتج مما سبق ، أن φ يمثل تماثلاً ذاتياً .

لنبرهن أخيراً أن $F_{\{\varphi\}} \cong Z_P$.

بما أن الحقل F منته ، ومميزه P ، فهو يحوي حقلاً جزئياً يماثل الحقل Z_P ، ويكون من أجل العنصر $a \in Z_P$:

$$\varphi(a) = a^P = a \;;\; \forall a \in Z_P$$

وذلك حسب مبرهنة فيرما .

وبالتالي فإن كثيرة الحدود $f(x) = a^P - a \in F[x]$ يكون لها P جذراً في الحقل F

وهي بالتحديد عناصر الحقل Z_P .

بما أن كثيرة الحدود $f(x)$ لها على الأكثر P جذراً في الحقل F ، إذن العناصر الثابتة من F تحت تأثير التماثل φ هي فقط عناصر الحقل Z_P .

إذن $F_{\{\varphi\}} \cong Z_P$.

لنقدم الآن بعض خواص التشاكل الحلقي ، من خلال المبرهنات التالية :

مبرهنة (2) :

لتكن $(R,+,\cdot)$ و $(S,T,\star)$ حلقتين ما ، ولنرمز لصفري الحلقتين السابقتين بالرمز o',o على الترتيب ، وإذا كان φ تشاكلاً للحلقة $(R,+,\cdot)$ في الحلقة $(S,T,\star)$ ، عندها يتحقق ما يلي :

1) $\varphi(o) = o'$.

2) $\varphi(-x) = -\varphi(x)$ ، لكل x من R .

3) أياً كان $n \in N^{\star}$ ، وأيّاً كان $x \in R$ ، فإن :

$$\varphi(x^n) = \left[\varphi(x)\right]^n \quad و \quad \varphi(n.x) = n.\varphi(x)$$

4) إن $(Ker\,\varphi,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$.

5) الصورة المباشرة وفق φ لأية حلقة جزئية من الحلقة $(R,+,\cdot)$ هي حلقة جزئية من الحلقة $(S,T,\star)$.

6) الصورة العكسية ، وفق φ ، لأية حلقة جزئية من الحلقة $(S,T,\star)$ هي حلقة جزئية من الحلقة $(R,+,\cdot)$.

البرهان :

1) بما أن التطبيق φ تشاكل للحلقة $(R,+,\cdot)$ في الحلقة $(S,T,\star)$ ، فإن :

$$\varphi(o + o) = \varphi(o)\ T\ \varphi(o)$$

أي أن :
$$\varphi(o) = \varphi(o)\ T\ \varphi(o)$$

وبالتالي فإن :
$$\varphi(o)\ T\ o' = \varphi(o)\ T\ \varphi(o)$$

ومنه نجد أن $\varphi(o) = o'$.

2) من أجل أي x من R يكون: $x + (-x) = o$ ، ومنه $\varphi(x + (-x)) = \varphi(o)$.
وبما أن φ تشاكل ، ومن (1) نجد أن : $\varphi(x)\ T\ \varphi(-x) = o'$ ، لكل x مـن R .
وبالتالي يكون : $-\varphi(x) = \varphi(-x)$ لكل x من R .

3) من أجل $n \in N^*$ و $x \in R$ يكون :

$$\varphi(n.x) = \varphi(x + x + \ldots + x)$$
$$= \varphi(x) + \varphi(x) + \ldots + \varphi(x) = n.\varphi(x)$$
$$\varphi(x^n) = \varphi(x.x.\ \ldots\ .x)$$
$$= \varphi(x).\varphi(x).\ \ldots\ .\varphi(x) = [\varphi(x)]^n$$

4) لنبرهن أولاً أن : $\phi \neq \operatorname{Ker}\varphi \subseteq R$.

حسب تعريف $\operatorname{Ker}\ \varphi$ ، أنها مجموعة جزئية من R ، من ناحية ثانيـة ، بمـا أن $\varphi(o) = o'$ حسب (1) ، فإن $o \in \operatorname{Ker}\varphi$ أي أن $\operatorname{Ker}\varphi \neq \phi$.

ليكن y,x عنصرين ما من $\operatorname{Ker}\varphi$ ، فإن : $\varphi(x) = \varphi(y) = o'$ وبالتالي فإن :

$$\varphi(x) \bigstar \varphi(y) = o' \bigstar o'$$
$$\varphi(x)\ T\ (-\varphi(y)) = o'\ T\ (-o')$$

وبالتالي فإن :

$$\varphi(x.y) = o' \Rightarrow x.y \in \operatorname{Ker}\varphi$$
$$\varphi(x)\ T\ (\varphi(-y)) = o'\ T\ o' \Rightarrow \varphi(x + (-y)) = o'$$

أي أن : $x + (-y) \in \operatorname{Ker}\varphi$

مما سبق ، نستنتج أن $(\operatorname{Ker}\varphi,+,.)$ حلقة جزئية من الحلقة $(R,+,.)$.

5) لتكن $(A,+,.)$ حلقة جزئيـة مـا ، مـن الحلقـة $(R,+,.)$. ولنبـرهن أن $(\varphi(A),+,.)$ هي حلقة جزئية من الحلقة $(S,T,\bigstar)$.

إن $\varphi(A)$ مجموعة جزئية من S ، كما أن $\phi \neq \varphi(A)$ ، لأنه : بمـا أن $(A,+,.)$

حلقة جزئية من الحلقة $(R,+,\cdot)$ ، فإن $o\in A$ ، وبالتالي ، فـــإن $\varphi(o)\in\varphi(A)$ ، إذن $\varphi(A)\neq\phi$.

ليكن الآن y_2 , y_1 عنصرين ما من $\varphi(A)$، وبالتالي يوجد عنصرين x_2 , x_1 من A بحيث يكون : $\varphi(x_1)=y_1 , \varphi(x_2)=y_2$ ، ومنه :

$$y_1 \, T \, (-y_2)=\varphi(x_1) \, T \, (-\varphi(x_2))=\varphi(x_1)+\varphi(-x_2)$$
$$=\varphi(x_1+(-x_2))\in\varphi(A)$$

و

$$y_1\star y_2=\varphi(x_1)\star\varphi(x_2)=\varphi(x_1.x_2)\in\varphi(A)$$

نستنتج مما سبق أن $(\varphi(A),T,\star)$ حلقة جزئية مـــن الحلقـــة $(S,T,\star)$. أي أن الصورة المباشرة وفق التطبيق φ ، لأية حلقة جزئية $(R,+,\cdot)$ هي حلقة جزئية من الحلقة $(S,T,\star)$.

6) لنبرهن أخيراً ، أن الصورة العكسية لأية حلقة جزئية ، ولتكن $(B,T,\star)$ من الحلقة $(S,T,\star)$ هي حلقة جزئية .

نلاحظ أولاً ، أن $\phi\neq\varphi^{-1}(B)\subseteq R$ ، لأن $\varphi^{-1}(B)$ مجموعة جزئية من R ، وبما أن $(B,T,\star)$ حلقة جزئية من الحلقة $(S,T,\star)$ فإن $o'\in B$ ومنه $\varphi(o)\in B$ ، أي أن $o\in\varphi^{-1}(B)$ إذن $\varphi^{-1}(B)\neq\phi$.

ليكن الآن x_2,x_1 عنصـــرين مـــا مـــن $\varphi^{-1}(B)$ ، وبالتـــالي ، فـــإن $\varphi(x_1)\in B$ و$\varphi(x_2)\in B$ أي أن :

$$\varphi(x_1) \, T \, (-\varphi(x_2))\in B \Rightarrow \varphi(x_1) \, T \, \varphi(-x_2)\in B$$
$$\varphi(x_1+(-x_2))\in B \Rightarrow x_1+(-x_2)\in\varphi^{-1}(B)$$
$$\varphi(x_1)\star\varphi(x_2)\in B \Rightarrow \varphi(x_1.x_2)\in B \Rightarrow x_1.x_2\in\varphi^{-1}(B)$$

نستنتج مما سبق أن $(\varphi^{-1}(B),+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$. إذن الصورة العكسية ، وفق φ ، لأية حلقة جزئية من الحلقة $(S,T,\star)$ هي حلقة جزئيـــة مـــن الحلقة $(R,+,\cdot)$.

المبرهنة التالية ، تقدم علاقة المثاليات بمفهوم التشاكل الحلقي .

مبرهنة (3) :

ليكن φ تشاكلاً لحلقة ما $(R,+,\cdot)$ في حلقة ما $(S,T,\star)$ ، عندئذٍ يتحقق ما يلي :

(1) $\text{Ker}\ \varphi$ مثالية في الحلقة $(R,+,\cdot)$.

(2) الصورة المباشرة ، وفق التطبيق φ ، لأية مثالية في الحلقة $(R,+,\cdot)$ ، هي مثالية في الحلقة $(S,T,\star)$.

(3) الصورة العكسية ، وفق التطبيق φ ، لأية مثالية في الحلقة $(S,T,\star)$ ، هي مثالية في الحلقة $(R,+,\cdot)$ ، تحوي نواة التطبيق φ .

(4) الحلقتان $(\varphi(R),+,\cdot)$ و $(R/\text{Ker}\ \varphi,+,\cdot)$ متماثلتان .

(الطلب الأخير من هذه المبرهنة يعرف باسم المبرهنة الأولى لتماثل الحلقات) First isomorphism theoem .

البرهان :

(1) بما أن $\varphi : R \longrightarrow S$ تشاكلاً ، فإن $(\text{Ker}(\varphi),+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$، أي أن $(\text{Ker}\ \varphi,+)$ زمرة جزئية من الزمرة $(R,+)$ ، بالإضافة لذلك ، إذا كان x,a عنصرين من $\text{Ker}\ \varphi$ و R على الترتيب ، فإن : $\varphi(x) = o'$ حيث أن o' هو صفر الحلقة $(S,T,\star)$ ، وبالتالي يكون لدينا :

$$\varphi(a.x) = \varphi(a)\star\varphi(x) = \varphi(a)\star o' = o'$$

$$\varphi(x.a) = \varphi(x)\star\varphi(a) = o'\star\varphi(a) = o'$$

ومنه يكون : $x.a \in \text{Ker}\ \varphi$ و $a.x$.

نستنتج مما سبق أن $\text{Ker}\ \varphi$ مثالية في الحلقة $(R,+,\cdot)$.

(2) لتكن J مثالية ما في الحلقة $(R,+,\cdot)$ ، وبما أن φ تشاكلاً من الحلقة $(R,+,\cdot)$ على الحلقة $(S,T,\star)$ ، فإن $(\varphi(J),T,\star)$ حلقة جزئية من الحلقة $(S,T,\star)$ ، وبالتالي ، فإن $(\varphi(J),T)$ زمرة جزئية من الزمرة (S,T) ، من ناحية ثانية ، ليكن y,s عنصرين من S و $\varphi(J)$ على الترتيب ، وبالتالي يمكن إيجاد

عنصرين a و x من R و J على الترتيب ، بحيث يكون : $\varphi(a) = s\ ,\ \varphi(x) = y$ ، وبالتالي فإن :

$$s\star y = \varphi(a)\star\varphi(x) = \varphi(a.x)\in\varphi(J)$$

$$y\star s = \varphi(x)\star\varphi(a) = \varphi(x.a)\in\varphi(J)$$

نستنتج من ذلك ، أن $\varphi(J)$ مثالية في الحلقة $(S,T,\star)$ ، وبالتالي فإن الصورة المباشرة وفق φ لأية مثالية في الحلقة $(R,+,\cdot)$ هي مثالية في الحلقة $(S,T,\star)$.

(3) ليكن I مثالية ما في الحلقة $(S,T,\star)$. بما أن φ تشاكلاً من الحلقة $(R,+,\cdot)$ في الحلقة $(S,T,\star)$، فإن $(\varphi^{-1}(I),+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ ، وبالتالي، فإن $(\varphi^{-1}(I),+,\cdot)$ زمرة جزئية من الزمرة $(R,+)$ ، وإذا كان a,y عنصرين ما من $\varphi^{-1}(I)$ و R على الترتيب ، فسيكون لدينا : $\varphi(a)\in S$ و $\varphi(y)\in I$.

وبما أن φ تشاكلاً ، فإن :

$$\varphi(a)\star\varphi(y) = \varphi(a.y)\in I \ \Rightarrow\ a.y\in\varphi^{-1}(I)$$

$$\varphi(y)\star\varphi(a) = \varphi(y.a)\in I \ \Rightarrow\ y.a\in\varphi^{-1}(I)$$

نستنتج أن $\varphi^{-1}(I)$ مثالية في الحلقة $(R,+,\cdot)$.

لنبرهن الآن أن هذه المثالية تحوي $\mathrm{Ker}\,\varphi$.

ليكن z عنصراً ما من $\mathrm{Ker}\,\varphi$، أي أن $\varphi(z) = o'\in I$ ، حيث أن o' هو صفر الحلقة $(S,T,\star)$. وبالتالي $z\in\varphi^{-1}(I)$.

نستنتج مما سبق ، أن الصورة العكسية وفق التطبيق φ ، لأية مثالية في الحلقة $(S,T,\star)$ ، هي مثالية في الحلقة $(R,+,\cdot)$ ، تحوي نواة التطبيق φ .

(4) لنعرف التطبيق : $\Psi : R/\mathrm{Ker}\,\varphi \longrightarrow \varphi(R)$ بالشكل :

$$\Psi(x + \mathrm{Ker}\,\varphi) = \varphi(x)\ ;\ \forall x\in R$$

وذلك أياً كان $x + \mathrm{Ker}\,\varphi \in R/\mathrm{Ker}\,\varphi$ ، ولنبين أولاً أن التطبيق Ψ حسن التعريف لكل $x + \mathrm{Ker}\,\varphi$ و $y + \mathrm{Ker}\,\varphi \in R/\mathrm{Ker}\,\varphi$ بحيث يكون :

$x + \mathrm{Ker}\,\varphi = y + \mathrm{Ker}\,\varphi$ وهذا يعني أن : $(x - y) + \mathrm{Ker}\,\varphi = \mathrm{Ker}\,\varphi$ ، أي

أن $(x-y)\in \text{Ker}\ \varphi$ وحسب تعريف نواة φ يكون $\varphi\ (x-y)$، أي أن $\varphi(x)=\varphi(y)$. أي أن :

$$\Psi\ (x+\text{Ker}\ \varphi)=\Psi\ (y+\text{Ker}\ \varphi)$$

إذن التطبيق Ψ حسن التعريف .

لنبرهن الآن أن Ψ تشاكل ، من أجل ذلك :

$$\begin{aligned}\Psi\ [(x+\text{Ker}\ \varphi)+(y+\text{Ker}\ \varphi)] &= \Psi\ [(x+y)+\text{Ker}\ \varphi]\\ &= \varphi(x+y)=\varphi(x)+\varphi(y)\\ &= \Psi\ (x+\text{Ker}\ \varphi)+\Psi\ (y+\text{Ker}\ \varphi)\end{aligned}$$

من ناحية ثانية لدينا :

$$\begin{aligned}\Psi\ [(x+\text{Ker}\ \varphi)\bullet(y+\text{Ker}\ \varphi)] &= \Psi\ [x\bullet y+\text{Ker}\ \varphi]\\ &= \varphi(x\bullet y)=\varphi(x)\bullet\varphi(y)\\ &= \Psi\ (x+\text{Ker}\ \varphi)\bullet\Psi\ (y+\text{Ker}\ \varphi)\end{aligned}$$

إن التطبيق Ψ شامل ، لأن إذا كان $Z\in \text{Im}\ \varphi$ ، فإنه يوجد عنصر r من R بحيث $Z=\varphi(r)$ ، وبالتالي ، فإن :

$$r+\text{Ker}\ \varphi\ \in R/\text{Ker}\ \varphi$$

وأن

$$\Psi\ (r+\text{Ker}\ \varphi)=\varphi(r)=Z$$

لنبرهن أخيراً أن Ψ متباين :

نفرض :

$$\Psi\ (x+\text{Ker}\ \varphi)=\Psi\ (y+\text{Ker}\ \varphi)\ \Rightarrow\ \varphi(x)=\varphi(y)$$

أي أن $\varphi(x-y)=0$ ، وهذا يعني أن $(x-y)\in \text{Ker}\ \varphi$. إذن :

$(x-y)+\text{Ker}\ \varphi=\text{Ker}\ \varphi$، أي أن $x+\text{Ker}\ \varphi=y+\text{Ker}\ \varphi$.

نستنتج مما سبق أن $R/\text{Ker}\ \varphi\cong \text{Im}\varphi=\varphi(R)$.

نتيجة (1) :

لتكن $(R,+,\cdot)$ و $(S,T,\star)$ حلقتين ما، وإذا كان $\varphi:R\longrightarrow S$ تشاكلاً ، إذا كان

φ شاملاً، فإن $R/\mathrm{Ker}\,\varphi \cong S$.

البرهان :

ينتج البرهان ، بوضع في المبرهنة السابقة $\mathrm{Im}\,\varphi = S$.

المبرهنة الثانية للتماثل الحلقي (2nd Isomorphism theerem) :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت $I \lhd R$ و $H \le R$ ، عندئذٍ :

$$(H+I)/I \cong H/(H \cap I)$$

البرهان :

لنثبت أولاً أنه إذا كان $a \in H$ و y,x من $H \cap I$ ، فإن $x-y$, $x.a$, $a.x$ من $H \cap I$.

واضح أن $I \lhd H+I$ ، لأن $I \lhd R$ و $I \le I+H$ ، وكذلك $H \cap I \lhd H$، لأنه إذا كان $x,y \in H \cap I$ و $a \in H$، فإن $x-y \in H$ و $x-y \in I$. وأيضـــاً $a.x\,,\,x.a \in I$، لأن $I \lhd R$ و $x.a \in H$ و $a.x \in H$ لأن $H \le R$ ، وبالتالي ، فإن $a.x\,,\,x.a$ و $x-y$ من $H \cap I$.

لنعرّف الآن التطبيق $\varphi : H \longrightarrow (H+I)/I$ بالشكل : $\varphi(a) = a+I$ لكل a من H .

بما أن $a = a + o \in H + I$ ، فإن $a + I \in (H+I)/I$.

لنبرهن الآن أن φ تشاكل حلقي .

لكل b,a من H ، فإن :

$$\varphi(a+b) = \left[(a+b)\right] + I = [a+I] + [b+I] = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = (a \cdot b) + I = (a+I)\cdot(b+I) = \varphi(a)\cdot\varphi(b)$$

لنبرهن الآن أن φ شامل، لكل $x + I \in (H+I)/I$ ، حيث $x \in H + I$ وبالتـــالي، فإن $x = a + i$ حيث $a \in H$ و $i \in I$ ، وبالتالي يكون لدينا :

$$x + I = (a+i) + I = a + I$$

وبالتالي $\varphi(x) = \varphi(a) = x + I$ ، وحسب المبرهنة الأولى للتماثل الحلقي يكون :

$$H/\mathrm{Ker}\,\varphi \cong (H+I)/I \qquad (*)$$

لنوجد أخيراً $\mathrm{Ker}\,\varphi$ ، لدينا :

$$\mathrm{Ker}\,\varphi = \{x\in H : \varphi(x) = I\} = \{x\in H : x + I = I\}$$
$$= \{x\in H : x\in H\} = \{x\in H : x\in H \cap I\} = H \cap I$$

بتعويض $\mathrm{Ker}\,\varphi$ في علاقة التماثل الأخيرة نجد أن :

$$(H+I)/I \cong H/(H\cap I)$$

مثال (8) :

لتكن $(S,+,\cdot)$ حلقة جزئية من الحلقة $(R,+,\cdot)$ ، وإذا كانت I مثالية في الحلقة $(R,+,\cdot)$ ، أثبت أن :

$$(S/(S\cap I),+,\cdot) \cong ((S+I)/I,+,\cdot)$$

الحل :

لنعرّف التطبيق : $\varphi : S \longrightarrow S + I$ بالشكل : $\varphi(x) = x + I \;;\; \forall x\in S$

ولنثبت أولاً ، أن التطبيق φ تشاكلاً من الحلقة $(S,+,\cdot)$ إلى الحلقة $((S+I)/I,+,\cdot)$ نواته $S\cap I$:

ليكن x_2,x_1 عنصرين ما من S ، فإن :

$$\varphi(x_1+x_2) = (x_1+x_2) + I = (x_1+I) + (x_2+I) = \varphi(x_1) + \varphi(x_2)$$
$$\varphi(x_1\cdot x_2) = (x_1\cdot x_2) + I = (x_1+I)\cdot(x_2+I) = \varphi(x_1)\cdot\varphi(x_2)$$

وإذا كان y عنصراً ما من $S + I$ ، وبالتالي يمكن كتابته بالشكل :

$$y = s + i \;;\; s\in S\,,\, i\in I$$

ومن ثم فإن :

$$\varphi(s) = s + I = (s + I) + I$$
$$= (s + I) + (i + I) = (s + i) + I$$
$$= y + I$$

لنبرهن الآن ، أن $\text{Ker}\,\varphi = S \cap I$.

ليكن $t \in \text{Ker}\,\varphi$ ، فإن :

$$\left.\begin{array}{l} t \in \text{Ker}\varphi\,;\, \text{Ker}\varphi \leq R \Rightarrow t \in S \\ t \in \text{Ker}\varphi \Rightarrow \varphi(t) = I \Rightarrow t + I = I \Rightarrow t \in I \end{array}\right\} \Rightarrow t \in S \cap I$$

بالعكس ، ليكن z عنصراً ما من $S \cap I$ ، فإن :

$$\left.\begin{array}{l} z \in S \;\;,\; z \in I \\ z \in S \;,\; \varphi(z) = I \end{array}\right\} \Rightarrow z \in \text{Ker}\,\varphi$$

مما سبق ، نستنتج أن φ تشاكل للحلقة $(S,+,\cdot)$ على الحلقة $(S+I/I,+,\cdot)$ نواتــه $S + I$. إذاً :

$$(S/(S \cap I),+,\cdot) \cong ((S+I)/I,+,\cdot)$$

المبرهنة التالية ، توضح ، أنه إذا كانت $(R,+,\cdot)$ حلقة بمحايد (ذات عنصر وحدة)، وإذا كان φ تشاكلاً للحلقة $(R,+,\cdot)$ على حلقة ما $(S,T,\star)$ ، فإن الحلقة $(S,T,\star)$ بمحايد أيضاً ومحايدها هو $\varphi(1)$ ، حيث 1 هو عنصر الوحدة في الحلقة $(R,+,\cdot)$.

مبرهنة (4) :

لتكن $(R,+,\cdot)$ حلقته بمحايد ، ولنرمز بـــ 1 لعنصر الوحدة فيها ، وإذا كـــان x عنصراً من R وله معكوس بالنسبة للعمليـــة $(\cdot)$ ، وإذا كـــان φ تشـــاكلاً للحلقـــة $(R,+,\cdot)$ في حلقة $(S,T,\star)$ ، فإن :

(1) $\varphi(1)$ محايد في الحلقة $(\varphi(R),+,\cdot)$.

(2) $\varphi(x^{-1})$ هو معكوس $\varphi(x)$ في $\varphi(R)$ بالنسبة للعملية $\star$.

البرهان :

(1) إذا كان y عنصراً ما من $\varphi(R)$ ، فإنه بالإمكان إيجاد عنصر x مـــن R، بحيث يكون : $\varphi(x) = y$

بما أن 1 هو المحايد في الحلقة $(R,+,\cdot)$ بالنسبة للعملية $(\cdot)$ ، فإن :

$$1 \cdot x = x \cdot 1 = x$$

وبالتالي ، يكون لدينا : $\varphi(1\cdot x) = \varphi(x\cdot 1) = \varphi(x)$

ومنه ، وبسبب φ تشاكل :

$$\varphi(1)\star\varphi(x) = \varphi(x)\star\varphi(1) = \varphi(x)$$

إذن :

$$\varphi(1)\star y = y\star\varphi(1) = y$$

وبملاحظة أن : $\varphi(1)\in\varphi(R)$ ، نجد أن $\varphi(1)$ هو المحايد في الحلقة $(\varphi(R),T,\star)$.

(2) بما أن $x\cdot x^{-1} = x^{-1}\cdot x = 1$ فإن :

$$\varphi(x\cdot x^{-1}) = \varphi(x^{-1}\cdot x) = \varphi(1)$$

وبالتالي ، فإن :

$$\varphi(x)\star\varphi(x^{-1}) = \varphi(x^{-1})\star\varphi(x) = \varphi(1)$$

وبملاحظة أن $\varphi(x^{-1})\in\varphi(R)$ نستنتج أن $\varphi(x^{-1})$ هو مقلوب $\varphi(x)$ في $\varphi(R)$ بالنسبة للعملية $\star$.

مبرهنة (5) (المبرهنة الثالثة لتماثل الحلقات) (3^{nd} Isomorphism theorem):

إذا كان I و J مثاليتين في الحلقة $(R,+,\cdot)$ وبحيث $J\subseteq I$ ، عندئذٍ يتحقق ما يلي :

(1) I/J مثالية في الحلقة $(R/J,+,\cdot)$.

(2) $\dfrac{R/J}{I/J}\cong R/I$.

البرهان :

(1) بما أن I مثالية في الحلقة $(R,+,\cdot)$ وتحوي المثالية J ، فإنه حسب المبرهنة (14) في الفصل الثاني نجد أن I/J مثالية في الحلقة $(R/J,+,\cdot)$.

(2) لنعرّف $\varphi: R/J \longrightarrow R/I$ بالشكل : $\varphi\,(r+J) = r+I$ ، لكل r من R و $r+J\in R/J$.

لنثبت أولاً أن φ حسن التعريف أيّاً كان $x + J , y + J \in R/J$ ، وبحيث يكون : $x + J = y + J$، فإن $(x - y) + J = J$ ، وبالتـــالي ، $(x - y) \in J \subseteq I$ ، أي أن $x + I = y + I$، أي أن :

$$\varphi(x + J) = \varphi(y + J)$$

لنثبت الآن أن φ تشاكلاً .

$$\varphi[(x + J) + (y + J)] = \varphi[(x + y) + J] = (x + y) + I$$
$$= (x + I) + (y + I) = \varphi(x + J) + \varphi(y + J)$$

كما أن :

$$\varphi[(x + J)\cdot(y + J)] = \varphi[(x \cdot y) + J] = (x \cdot y) + I$$
$$= (x + I)\cdot(y + I) = \varphi(x + J)\cdot\varphi(y + J)$$

لنبرهن الآن أن : $\text{Ker}\,\varphi = I/J$

ليكن $r + J \in \text{Ker}\,\varphi$ ، وبالتالي $\varphi(r + J) = I$ ، كما أن $\varphi(r + J) = r + I$ ، ومنه يكون : $r + I = I$ ، أي أن $r \in I$ ، وبالتالي $r + J \in I/J$ ، إذن $\text{Ker}\,\varphi \subseteq I/J$.

ليكن $z + J \in I/J$ ، عندئذٍ $z \in I$ ، كما أن : $\varphi(z + J) = z + I = I$، وبالتالي فإن: $z + J \in \text{Ker}\,\varphi$ ، إذن $I/J \subseteq \text{Ker}\,\varphi$ ، بهذا الشكل يكون : $I/J = \text{Ker}\,\varphi$.

من الواضح أن φ غامر ، إذن : $\dfrac{R/J}{I/J} \cong R/I$.

(4-3) بعض الحلقات الخاصة :

قبل البدء في تقديم بعض أنواع الحلقات ، نقدم بعض أنواع المثاليات الخاصـــة والتي تلعب دوراً أساسياً في الحلقات والحقول .

المثالية الأولية :

إذا كانت $(R,+,\cdot)$ حلقة إبدالية ما ، نسمي كل مثالية I في الحلقـــة المدروســـة مثالية أولية إذا تحقق الشرط التالي :

إذا كان b,a عنصرين ما من R بحيث $a.b\in I$ ، فإن أحد العنصرين b,a على الأقل ، ينتمي إلى I .

المثالية الأعظمية :

نقول عن المثالية I في الحلقة الإبدالية $(R,+,\cdot)$ إنها مثالية أعظمية إذا كان $I \neq R$ ، وإذا لم يكن بالإمكان إيجاد مثالية J في الحلقة $(R,+,\cdot)$ تحوي I ، وبحيث يكون $J \neq I , J \neq R$.

أولاً : حلقة المثاليات الرئيسة :

لتكن $(R,+,\cdot)$ حلقة إبدالية ما ، وإذا كان r عنصراً ما من R ، فإن $R.r$ مثالية في الحلقة $(R,+,\cdot)$ ، تسمى المثالية الرئيسية في الحلقة $(R,+,\cdot)$ مولدة بالعنصر r .
ينتج من المفهوم السابق ، أنه إذا كانت $(R,+,\cdot)$ حلقة إبدالية بمحايد ، وإذا كان r من R ، فإن $R.r = (r)$.

تعريف حلقة المثاليات الرئيسة :

لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، نقول عن الحلقة $(R,+,\cdot)$ إنها حلقة مثاليات رئيسة ، إذا، وفقط إذا، كانت كل مثالية في الحلقة $(R,+,\cdot)$ مثالية رئيسة فيها .

مثال (9) :

إذا كانت $(Z,+,\cdot)$ حلقة الأعداد الصحيحة ، أثبت أن هذه الحلقة هي حلقة مثالية رئيسة .

الحل :

لندرس الحالتين التاليتين :

أ- إذا كانت $A = \{0\}$ ، فإن $A = Z.0$ ، وبالتالي فإن A مثالية رئيسة في الحلقة $(Z,+,\cdot)$ مولدة بالعنصر 0 .

ب- إذا كانت $A \neq \{0\}$ ، وبالتالي يوجد في المجموعة A أعداد صحيحة موجبة وسالبة . ولنفرض أن n هو أصغر عدد صحيح موجب من A . إن $A = Z.n$ ، لأن $Z.n$ مجموعة جزئية من A .

ومن ناحية ثانية ، إذا كان a عنصراً ما من A ، فإنه يوجد عددان صحيحان r,q بحيث يكون :

$a = q.n + r \; ; 0 \le r < n$.

إن $r = 0$ ، وذلك لأنه ، إذا كان $r \neq 0$ ، عندها يكون $r = b - q.n \in A$ و $0 < r < n$ ، وهذا مناقض للفرض أن n هو أصغر عدد صحيح موجب من A .

بما أن $a = q.n + r$ و $r = 0$ فإن : $a = q.n \in Z.n$

بما أن $A = Z.n$ ، فإن المثالية A هي مثالية رئيسة في الحلقة $(Z,+,.)$ مولدة بالعدد n . وبما أن أية مثالية A في الحلقة $(Z,+,.)$ هي مثالية رئيسة فيها ، إذن الحلقة $(Z,+,.)$ هي حلقة مثاليات رئيسة .

مبرهنة (5) :

لتكن $(R,+,.)$ و $(S,T,\star)$ حلقتين أبداليتين ، وإذا كان φ تشاكلاً من R إلى S ، وإذا كانت I مثالية في الحلقة $(R,+,.)$ بحيث يكون $\mathrm{Ker}\,\varphi \subseteq I \neq R$. وإذا كانت J مثالية في الحلقة $(S,T,\star)$ وبحيث يكون $J \neq S$. عندها يتحقق ما يلي :

1- تكون المثالية I في الحلقة $(R,+,.)$ مثالية أولية ، إذا ، وفقط إذا ، كانت المثالية $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

2- تكون المثالية I في الحلقة $(R,+,.)$ مثالية أعظمية ، إذا ، وفقط إذا ، كانت المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$.

3- الشرط اللازم والكافي ، لكي تكون المثالية J مثالية أولية في الحلقة $(S,T,\star)$ ، هو أن تكون المثالية $\varphi^{-1}(I)$ مثالية أولية في الحلقة $(R,+,.)$.

4- الشرط اللازم والكافي لكي تكون المثالية J مثالية أعظمية في الحلقة $(S,T,\star)$ ، هو أن تكون المثالية $\varphi^{-1}(I)$ مثالية أعظمية في الحلقة $(R,+,.)$.

البرهان :

1- نفرض أولاً ، أن المثالية I مثالية أولية في الحلقة $(R,+,.)$ ، ولنبرهن أن $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

ليكن y,x عنصرين ما من S ، بحيث يكون $x\star y\in\varphi(I)$.

بما أن y,x من S ، فإنه يوجد عنصرين b,a من R ، بحيث يكون :

$$y=\varphi(b)\,,\,x=\varphi(a)$$

وبما أن $x\star y\in\varphi(I)$ فإن $\varphi(a)\star\varphi(b)\in\varphi(I)$. وبالتالي يكون $\varphi(a.b)\in\varphi(I)$، ومنه يكون: $a.b\in I$. وبما أن I مثالية أولية في الحلقة $(R,+,.)$ ، فإن أحد العنصرين b,a على الأقل ، ينتمي إلى I . وبالتالي ، فإن أحد العنصرين $y=\varphi(b)\,,\,x=\varphi(a)$ ، على الأقل ينتمي إلى $\varphi(I)$. وهذا يعني أن المثالية $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

لنبرهن الآن أن I مثالية أولية في الحلقة $(R,+,.)$ ، علماً أن $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

من أجل ذلك نفرض أن y,x عنصرين ما من R ، وبحيث يكون $x.y\in I$. بما أن $x.y\in I$ ، فإن $\varphi(x.y)\in\varphi(I)$ ، وهذا يؤدي بسبب أن φ تشاكلاً أن $\varphi(x)\star\varphi(y)\in\varphi(I)$.

بما أن المثالية $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$ ، فإن أحد العنصرين $\varphi(x)$ و$\varphi(y)$ على الأقل ينتمي إلى $\varphi(I)$ ، وبالتالي فإن أحد العنصرين y,x على الأقل ينتمي إلى I ، إذن I مثالية أولية في الحلقة $(R,+,.)$.

2- نفرض أولاً أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$ ولنبرهن أن المثالية I مثالية أعظمية في الحلقة $(R,+,.)$.

إن $I\neq R$ ، ومن جهة ثانية ، لا يمكن إيجاد مثالية في الحلقة $(R,+,.)$ تحوي I وتختلف عن I وعن R ، وذلك لأنه، إذا كان غير ذلك ، توجد مثالية I' في الحلقة $(R,+,.)$ تحوي I وبحيث يكون $I'\neq I$ و $I'\neq R$، عندها يكون $\varphi(I')$ مثالية في الحلقة $(S,T,\star)$ تحوي $\varphi(I)$ و $\varphi(I)\neq\varphi(I')$ و $\varphi(I')\neq R$ ، وهذا مخالف لفرضنا أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$.

لنبرهن العكس ، أي لنبرهن أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$ ،

ليكن y,x عنصرين ما من S ، بحيث يكون $x\star y\in\varphi(I)$.

بما أن y,x من S ، فإنه يوجد عنصرين b,a من R ، بحيث يكون :

$y=\varphi(b)\,,\,x=\varphi(a)$

وبما أن $x\star y\in\varphi(I)$ فإن $\varphi(a)\star\varphi(b)\in\varphi(I)$. وبالتالي يكون $\varphi(a.b)\in\varphi(I)$، ومنه يكون: $a.b\in I$. وبما أن I مثالية أولية في الحلقة $(R,+,.)$ ، فإن أحد العنصرين b,a على الأقل ، ينتمي إلى I . وبالتالي ، فإن أحد العنصرين $y=\varphi(b)\,,\,x=\varphi(a)$ ، على الأقل ينتمي إلى $\varphi(I)$. وهذا يعني أن المثالية $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

لنبرهن الآن أن I مثالية أولية في الحلقة $(R,+,.)$ ، علماً أن $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$.

من أجل ذلك نفرض أن y,x عنصرين ما من R ، وبحيث يكون $x.y\in I$. بما أن $x.y\in I$ ، فإن $\varphi(x.y)\in\varphi(I)$ ، وهذا يؤدي بسبب أن φ تشاكلاً أن $\varphi(x)\star\varphi(y)\in\varphi(I)$.

بما أن المثالية $\varphi(I)$ مثالية أولية في الحلقة $(S,T,\star)$ ، فإن أحد العنصرين $\varphi(x)$ و$\varphi(y)$ على الأقل ينتمي إلى $\varphi(I)$ ، وبالتالي فإن أحد العنصرين y,x على الأقل ينتمي إلى I ، إذن I مثالية أولية في الحلقة $(R,+,.)$.

2- نفرض أولاً أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$ ولنبرهن أن المثالية I مثالية أعظمية في الحلقة $(R,+,.)$.

إن $I\neq R$ ، ومن جهة ثانية ، لا يمكن إيجاد مثالية في الحلقة $(R,+,.)$ تحوي I وتختلف عن I وعن R ، وذلك لأنه، إذا كان غير ذلك ، توجد مثالية I' في الحلقة $(R,+,.)$ تحوي I وبحيث يكون $I'\neq I$ و $I'\neq R$، عندها يكون $\varphi(I')$ مثالية في الحلقة $(S,T,\star)$ تحوي $\varphi(I)$ و $\varphi(I')\neq\varphi(I)$ و $\varphi(I')\neq R$ ، وهذا مخالف لفرضنا أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$.

لنبرهن العكس ، أي لنبرهن أن المثالية $\varphi(I)$ مثالية أعظمية في الحلقة $(S,T,\star)$ ،

علماً أن I مثالية أعظمية في الحلقة $(R,+,.)$.

من أجل ذلك، نفرض العكس، أي نوجد مثالية I' في الحلقة $(S,T,\star)$ تحوي $\varphi(I)$ بحيث يكون $I' \neq \varphi(I)$ و $I' \neq S$. عندها تكون $\varphi^{-1}(I)$ مثالية في الحلقة $(R,+,.)$ تحوي I و $\varphi^{-1}(I) \neq I$ و $\varphi^{-1}(I) \neq R$، وهذا مخالف للفرض ، بأن المثالية I مثالية أعظمية في الحلقة $(R,+,.)$.

3- بما أن $\varphi^{-1}(J)$ مثالية في الحلقة $(R,+,.)$ تحوي نواة التطبيق φ، وبما أن $\varphi(\varphi^{-1}(J)) = J$، فمن (1) نجد أن الشرط اللازم والكافي لكي تكون المثالية J مثالية أولية في الحلقة $(S,T,\star)$ هو أن تكون المثالية $\varphi^{-1}(J)$ مثالية أولية في الحلقة $(R,+,.)$.

4- بما أن $\varphi^{-1}(J)$ مثالية في الحلقة $(R,+,.)$ تحوي نواة φ ، وبما أن $\varphi(\varphi^{-1}(J)) = J$ ، فمن (2) نجد أن الشرط اللازم والكافي لكي تكون المثالية J مثالية أعظمية في الحلقة $(S,T,\star)$ هو أن تكون المثالية $\varphi^{-1}(J)$ مثالية أعظمية في الحلقة $(R,+,.)$.

نتيجة (2) :

إذا كانت $(R,+,.)$ حلقة إبدالية بمحايد ، وبفرض أن I مثالية أعظمية في الحلقة $(R,+,.)$ ، عندئذٍ تكون I مثالية أولية في الحلقة $(R,+,.)$.

البرهان :

نفرض أن y,x عنصرين ما من R بحيث يكون : $x.y \in I$.

إذا كان $x \in I$ ، عندها تكون المثالية I مثالية أولية في الحلقة $(R,+,.)$ ، وبهذه الحالة يكون قد تمّ المطلوب. أما إذا كان $x \notin I$ ، عندئذٍ يكون : $I + R.x = R$ ، ولنرمز لمحايد الحلقة $(R,+,.)$ بالرمز 1 ، عندئذٍ يمكن كتابة العنصر x بالشكل : $1 = b + a.x$ ، لكل b من I و $a \in R$ ، وبالتالي يكون :

$$y = y.b + a.x.y \in I$$

وهذا يعني أن المثالية I أولية في الحلقة $(R,+,.)$.

نورد الآن بعض الشروط المكافئة لمفهوم المثاليات الأعظمية ، وذلك من خلال المبرهنات التالية :

مبرهنة (6) :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت $I \neq R$ مثالية يسارية (يمينية) في R ، عندها الشروط التالية متكافئة :

(1) المثالية اليسارية (اليمينية) I أعظمية في الحلقة $(R,+,\cdot)$.

(2) من أجل أي مثالية يسارية (يمينية) ، ولتكن J والتي تحقق $I \subseteq J \subset R$ ، يكون $I = J$.

(3) لا توجد مثالية يسارية (يمينية) J بحيث يكون $I \subset J \subset R$.

(4) أياً كانت المثالية اليسارية (اليمينية) K في الحلقة $(R,+,\cdot)$ والتي تحقق $I \subset J$ ، فيكون $J = R$.

البرهان :

(لنفرض أن M مجموعة المثاليات اليسارية في الحلقة $(R,+,\cdot)$ والتي كل منها لا تساوي R) .

$(1) \Leftarrow (2)$

نفرض أن المثالية اليسارية I مثالية أعظمية في الحلقة $(R,+,\cdot)$ ، وإذا كانت J مثالية يسارية في R بحيث يتحقق $I \subseteq J \subset R$ ، عندئذٍ يتحقق $I \in M$ ، وبما أن المثالية اليسارية I أعظمية في M فإن $I = J$ ، وذلك حسب تعريف المثالية الأعظمية .

$(2) \Leftarrow (3)$

نفرض العكس ، أي نفرض أنه توجد مثالية يسارية J في R بحيث يتحقق $I \subset J \subset R$ ، عندها ، حسب (2) يكون $I = J$ ، وهذا غير ممكن ، وبالتالي لا يوجد في الحلقة $(R,+,\cdot)$ مثالية يسارية J بحيث يتحقق $I \subset J \subset R$.

(3) ⇐ (4)

لتكن K مثالية يسارية في الحلقة $(R,+,\cdot)$ بحيث يكون $I \subset K$ ، وهنا نميز ما يلي : إما $K = R$ أو $K \neq R$، فإذا كان $K \neq R$ فهذا يناقض الفرض ، وبالتالي ، فإن $K = R$. وإذا كان $K = R$ يتم المطلوب .

(4) ⇐ (1)

لتكن I_1 مثالية يسارية في R بحيث $I_1 \neq R$ و $I \subseteq I_1$ وإذا كان $I \neq I_1$ فهذا يناقض الفرض، أي أن $I = I_1$.

المبرهنة التالية توضح متى تكون المثالية اليسارية $\{0\}$ مثالية أعظمية في أية حلقة .

مبرهنة (7) :

إذا كانت $(R,+,\cdot)$ حلقة ما حيث $R \neq \{0\}$ ، عندها تتكافئ الشروط التالية :

(1) المثالية اليمينية $\{0\}$ مثالية أعظمية في R .

(2) لا يوجد في الحلقة $(R,+,\cdot)$ مثاليات يمينية تختلف عن R و $\{0\}$.

(3) كل عنصر من R لا يساوي الصفر قابل للعكس من اليمين .

(4) كل عنصر لا يساوي الصفر قابل للعكس .

تقبل المبرهنة بدون برهان .

ملاحظة (4) :

المبرهنة السابقة تبقى صحيحة من أجل المثاليات اليسارية .

مبرهنة (8) :

إذا كانت $(R,+,\cdot)$ حلقة ما ، و I مثالية في R ، عندها الشرط اللازم والكافي كي تكون المثالية I أعظمية هو أن تكون حلقة القسمة R/I حقلاً .

البرهان :

نفرض أولاً أن المثالية I أعظمية في الحلقة $(R,+,\cdot)$ وحسب التمهيدية التالية :

إذا كانت $(R,+,.)$ حلقة و$I \neq R$ مثالية في R، فإن الشرط اللازم والكافي كي تكون المثالية I أعظمية في R هو أن يتحقق الشرط: لكل $m \notin I$ ، يوجد عنصر x من R حيث أن $1 - x.m \in I$. وبالتالي فإن المثالية I تكون أولية في الحلقة R (وبما أنه إذا كانت R حلقة وI مثالية في R ، فإن الشرط اللازم والكافي كي تكون المثالية I أولية في R هو أن تكون حلقة الخارج R/I حلقة تامة) فإن حلقة القسمة R/I هي حلقة تامة .

ليكن $I \neq a + I \in R/I$ ، ومنه $a \notin I$ ، وبالتالي ، فإن $I \subset I + a.R$ ، وحسب الفرض يكون لدينا : $I + a.R = R$ أي يوجد $m \in I$ و$r \in R$ حيث $1 = m + a.r$ ، وهذا يبين لنا أن :

$$1 + I = (m + a.r) + I = (m + I) + (a.r + I) = (a + I)\,(r + I)$$

أي أن كل عنصر لا يساوي الصفر في الحلقة R/I يملك معكوساً ، إذن الحلقة R/I حقل .

برهان العكس :

نفرض الآن أن R/I حقلاً ، عندها يكون $I \neq 1 + I$ وبالتالي ، فإن $1 \notin I$ أي أن $I \neq R$ ، ليكن $a \in R$ بحيث $a \notin I$ عندئذٍ : $I \neq a + I \in R/I$، وحسب الفرض يوجد $I \neq b + I \in R/I$ حيث أن:
$(a + I)\,(b + I) = 1 + I$ ، أي أن : $a.b + I = 1 + I$ ، وبالتالي فإن $1 - a.b \in I$ ، ومنه تكون المثالية I أعظمية في الحلقة R .

تعريف المثالية الأصغرية :

لتكن L مجموعة المثاليات اليسارية (اليمينية) في حلقة ما ، ولتكن $(R,+,.)$ حيث أن $R \neq 0$، والتي كل منها لا تساوي الصفر ، نقول عن المثالية اليسارية (اليمينية) $I \in L$ إنها مثالية أصغرية في R ، إذا كانت I عنصراً أصغرياً في L .

المبرهنة التالية : تقدم لنا بعض الشروط المكافئة لمفهوم المثاليات اليسارية (اليمينية) الأصغرية .

مبرهنة (9) :

لتكن $I \neq 0$ مثالية يسارية (يمينية) في الحلقة $(R,+,\cdot)$ حيث $R \neq 0$ ، عندئذٍ تتكافئ الشروط التالية :

(1) المثالية اليسارية (اليمينية) I أصغرية في الحلقة $(R,+,\cdot)$.

(2) إذا كانت J مثالية يسارية (يمينية) من الحلقة $(R,+,\cdot)$ حيث $0 \neq J \subseteq I$ ، عندها يكون $J = I$.

(3) لا يوجد في الحلقة $(R,+,\cdot)$ مثالية يسارية (يمينية) مثل K بحيث تحقق $0 \neq K \subset I$.

(4) إذا كانت المثالية اليسارية (اليمينية) F من الحلقة $(R,+,\cdot)$ ، حيث $F \subset I$ ، عندها يكون $F = 0$.

البرهان :

(1) ⇐ (2)

لتكن J مثالية يسارية في الحلقة $(R,+,\cdot)$ مغايرة للصفر ، ولتكن L مجموعة المثاليات اليسارية في الحلقة $(R,+,\cdot)$ المغايرة للصفر ، عندئذٍ $J \in L$ ، وبما أن I عنصر أصغري في L ، وإن $J \subseteq I$ نجد أن $I = J$.

(2) ⇐ (3)

نفرض أنه توجد مثالية يسارية في الحلقة $(R,+,\cdot)$ ولتكن K بحيث $0 \neq K \subset I$، عندئذٍ يكون $K \in L$ و $K \subset I$ وهذا غير ممكن حسب الفرض .

(3) ⇐ (4)

لتكن F مثالية يسارية في الحلقة $(R,+,\cdot)$ وبحيث يكون $F \subset I$، إذا كان $F = 0$ يتم المطلوب، أما إذا كان $F \neq 0$ فهذا يناقض الفرض .

(4) ⇐ (1)

لتكن $F \in L$ حيث $F \subseteq I$ ، وإذا كان $F = I$ ، فإنه يتم المطلوب ، لنفرض الآن أن $F \neq I$ ، وبالتالي حسب الفرض يكون $F = 0$ وهذا غير ممكن ، إذن المثالية

اليسارية I أصغرية في الحلقة $(R,+,\cdot)$.

مبرهنة (10) :

إذا كانت I مثالية يسارية أصغرية في الحلقة $(R,+,\cdot)$ ، عندئذٍ إمـــا $I^2 = 0$ أو $I = R.e$ ، حيث e عنصر جامد لا يساوي الصفر .

البرهان :

بما أن I مثالية يسارية في الحلقة $(R,+,\cdot)$ ، فإن I^2 مثالية يســـارية فـــي الحلقـــة $(R,+,\cdot)$ ، كما أن $I^2 \subseteq I$.

لنفرض أولاً أن $I^2 \neq 0$ (إذا كان $I^2 = 0$ فيتم المطلوب) ، وهذا يعني أنـــه يوجـــد عنصر وليكن a من I بحيث يكون $I.a \neq 0$ ، لأنه إذا كان $I.b = 0$ ، حيث $b \in I$، فإن $I^2 = 0$ ، وهذا غير ممكن . كما أن $I.a$ مثالية يسارية في الحلقـــة $(R,+,\cdot)$ ، وأن $0 \neq I.a \subseteq I$ ، وبما أن I مثالية يسارية أصغرية ، فإن $I.a = I$.

لتكن المجموعة :

$$M = \{r : r \in R : r.a = 0\}$$

إن $M \neq \phi$ لأن $0.a = 0$ ، كما أن M مثالية يسارية في الحلقة $(R,+,\cdot)$ ، لأنـــه ، إذا كان y,x عنصرين ما من M ، فإن :

$$(x-y).a = x.a - y.a = 0$$

أي أن $x - y \in M$. كما أن :

$$(r.x)\, a = r\,(x.a) = r.0 = 0$$

لكل r من R ، إذاً $r.x \in M$.

إن $I \cap M$ مثالية يسارية في الحلقة $(R,+,\cdot)$، وأن $I \cap M \neq I$ ، لأنـــه ، إذا كـــان $I \cap M = I$ ، فإن $I \subseteq M$، وبالتالي فإن $I.a = 0$ ، وهذا غير ممكـــن ، وبمـــا أن $I \cap M \subset I$ ، وأن المثالية اليسارية I أصغرية في الحلقة $(R,+,\cdot)$ ، ينتج من ذلك أن $I \cap M = 0$.

من ناحية ثانية ، بما أن $I.a = I$ ، وأن $a \in I = I.a$ فإنه يوجد عنصر وليكن $e \in I$

حيث $a = e.a$ ، ومنه $e.I = e^2.I$ ، وبالتالي فإن $(e - e^2).a = 0$ ، أي أن $e - e^2 \in I \cap M = 0$ ، إذن $e = e^2$ ، وهذا يعني أن e هو عنصر جامد ، كما أن $e \neq 0$ ، بما أن $e \in I$ ، فإن $0 \neq R.e \subseteq I$ ، وحيث أن I مثالية يسارية أصغرية ، ينتج من ذلك ، أن $I = R.e$.

ثانياً : الحلقات المنتظمة :

بدايةً نعرّف المجموع المباشر للمثاليات ، والحد المباشر للمثاليات .

إذا كانت $(R,+,\cdot)$ حلقة ما ، وكانت I_i حيث $1 \leq i \leq n$ مجموعة من المثاليات اليسارية (أو اليمينية) في الحلقة R ، نقول عن المجموع $I = \sum_{i=1}^{n} I_i$ إنه مجموع مباشر للمثاليات I_i ، إذا تحقق ما يلي :

لكل x من I ، يكتب العنصر x بصورة وحيدة بالشكل :

$$x = x_1 + x_2 + \ldots.. + x_n$$

من أجل $x_i \in I_i$ و $1 \leq i \leq n$.

نرمز عادةً للمجموع المباشر للمثاليات I_i ، حيث $1 \leq i \leq n$ ، بالشكل $\sum_{i=1}^{n} \oplus I_i$ ، أو اختصاراً، بالشكل $\bigoplus_{i=1}^{n} I_i$ ، نسمي كل حد I_i حدّاً مباشراً للمثالية $\sum_{i=1}^{n} I_i$.

ينتج من التعريف السابق ما يلي :

<u>(a)</u> إذا كانت $(R,+,\cdot)$ حلقة ما وI_i مجموعة من المثاليات اليسارية في الحلقة R، من أجل $1 \leq i \leq n$. عندئذٍ الشروط التالية متكافئة :

(1) المجموع $\sum_{i=1}^{n} I_i$ هو مجموع مباشر .

(2) إذا كانت $x_i \in I_i$ ، $1 \leq i \leq n$ والتي تحقق $\sum_{i=1}^{n} x_i = 0$ عندها يكون $x_i = 0$ حيث $1 \leq i \leq n$.

(3) $I_i \cap \left(\sum_{\substack{j=1 \\ j \neq i}}^{n} I_j \right) = 0$ حيث $1 \leq i \leq n$.

(b) إذا كانت $(R,+,\cdot)$ حلقة ما و I مثالية يسارية فيها ، تكون I حداً مباشراً للحلقة $(R,+,\cdot)$، إذا وُجِدَتْ مثالية يسارية J في الحلقة R ، بحيث يتحقق : $R = I \oplus J$.

لنعرّف الآن الحلقة المنتظمة :

إذا كانت $(R,+,\cdot)$ حلقة ما ، نقول عن الحلقة R إنها منتظمة (نظامية) إذا تحقق الشرط التالي :

لكل $x \in R$ ، يوجد عنصر a من R ، بحيث : $x = x.a.x$.

المبرهنة التالية تعطي الشروط المكافئة لمفهوم الحلقة المنتظمة .

مبرهنة (11) :

إذا كانت $(R,+,\cdot)$ حلقة ما ، الشروط التالية متكافئة :

(1) الحلقة $(R,+,\cdot)$ منتظمة .

(2) من أجل أي مثالية يسارية (أو يمينية) رئيسة هي حد مباشر في الحلقة R .

(3) من أجل أي مثالية يسارية (أو يمينية) منتهية التوليد هي حد مباشر في الحلقة R .

البرهان :

$(1) \Rightarrow (2)$

بفرض أن I مثالية يسارية رئيسة في الحلقة $(R,+,\cdot)$ ، وهذا يعني أن $I = R.x$، وحسب الفرض يوجد عنصر في R ، وليكن a بحيث يكون $x.a.x = x$ ، بوضع $e = a.x$ ، عندها يكون $e = e^2$ و $R.e$ حد مباشر للحلقة $(R,+,\cdot)$ ، ومنه يكون :

$$I = R.x = R.x.a.x \subseteq R.a.x = R.e$$

ليكن الآن $b \in R.e$ ، عندها يكون $b = r.e$ ، لكل r من R ، أي أن $b = r.e = r.a.x \in R.x$ ، وبالتالي $R.e \leq R.x$.

نستنتج مما سبق أن $R.e = R.x$ ، أي أن $R.x$ حد مباشر في الحلقة $(R,+,\cdot)$.

(3) $\Leftarrow$ (2)

لتكن J مثالية يسارية منتهية التوليد في الحلقــة $(R,+,.)$ ولـــتكن $\{b_i\}$ حيـــث $i = 1,2,\ldots,n$ المجموعة المولدة لها ، وبالتالي يكون : $J = \sum_{i=1}^{n} R.b_i$.

بطريقة الاستقراء الرياضي على n ، نجد أنه من أجل $n = 1$ ، يكون $J = R.b_i$ ، وحسب الفرض ، يكون $J = R.e$.

لنفرض الآن أن المبرهنة صحيحة من أجل $n - 1$ ، أي أن :

$$J = \sum_{i=1}^{n-1} R.b_i + R.b_n$$

وبوضع $I = \sum_{i=1}^{n-1} R.b_i$ ، نجد أن I مثالية يسارية منتهية التوليد ومولدة بـــ $n - 1$ عنصراً ، وحسب الفرض الاستقرائي ، فإن $I = R.e$ ، علماً أن $e = e^2$ ، ومنـــه يكون :

$$J = R.e + R.b_n$$

وبما أن $1 = e + (1 - e)$ ، فإن : $b_n = b_n e + b_n (1 - e)$ ، ومنه يكون ، لكل r من R :

$$r\, b_n = r\, b_n\, e + r\, b_n\, (1 - e)$$

أي أن :

$$r\,.b_n \in R.e + R.b_n\, (1 - e)$$

إذن :

$$R.b_n \subseteq R.e + R.b_n\, (1 - e)$$

من ناحية ثانية ، لدينا :

$$b_n\, (1 - e) = b_n - b_n\, e$$

ولكل r من R يكون :

$$r.b_n\, (1 - e) = r.\, b_n - r.b_n\, e \in R.b_n + R.e$$

أي أن :

$$R.b_n(1-e) \subseteq R.b_n + R.e$$

وبالتالي فإن :

$$R.b_n + R.e \subseteq R.e + R.e + R.b_n(1-e) = R.e + R.b_n(1-e)$$
$$\subseteq R.e + R.e + R.b_n = R.e + R.b_n$$

إذن :

$$R.e + R.b_n = R.e + R.b_n(1-e)$$

وحسب الفرض، يكون : $R.b_n(1\text{-}e) = R.\ell$ حيث $\ell = \ell^2$ ، وبالتالي :

$R.e + R.b_n = R.e + \ell$، وأن $\ell.e = 0$.

بوضع $h = (1-e)\ell$ نجد أن $h = h^2$ لأن :

$$h^2 = (1-e)\,\ell\,(1-e)\,\ell$$
$$= (\ell - e\ell)(\ell - e\ell) = \ell^2 - \ell e\ell - e\ell^2 + e\ell e\ell$$
$$= \ell - e\ell = (1-e)\,\ell = h$$

كما أن $e\,h = 0 = h\,e$، وأن $R.h = R.\ell$ ، لأنه $h = (1\text{-}e)\ell \in R.\ell$ ، أي أن $R.h \subseteq R.\ell$.

من ناحية ثانية :

$$\ell.h = \ell\,(1-e)\,\ell = \ell^2 - \ell e \ell = \ell \Rightarrow \ell \in R.h$$

أي أن $R.\ell \subseteq R.h$ ، نستنتج مما سبق أن $R.\ell = R.h$. وهكذا نجد :

$$R.e + R.b_n = R.e + R.\,\ell = R.e + R.h$$

لنبرهن أخيراً أن : $R(e+h) = R.e + R.h$

لـــدينا $R(e+h) \subseteq R.e + R.h$، لـــيكن $x \in R.e + R.h$ ، وهـــذا يعنـــي أن $x = x_1.e + x_2.h$ ، وبالتالي :

$$(x_1.e + x_2.h)(e+h) = x_1.e + x_1.e.h + x_2.h.e + x_2.h$$

$$= x_1.e + x_2.h = x$$

إذن $x \in R(e+h)$ ، أي أن :

$$R(e+h) = R.e + R.h$$

كما أن $(e+h)^2 = e+h$ ، وهذا يبين لنا أن :

$$R(e+h) = R.e + R.h$$

$$J = R.e + R.b_n = R.e + R.h = R(e+h)$$

(1) ⇐ (3)

ليكن r عنصراً ما من R، عندها يكون $R.e = R.r$ ، ومنه $e \in R.r$ وبالتالي ، فإن $e = x.r$ ، حيث أن x من R ، وبما أن : $R = R.e \oplus R(1-e)$ ، فإن : $R = R.r \oplus R(1-e)$، وبالتالي فإن : $1 = x.r + y(1-e)$ ، لكل y,x من R، أي أن $r = r.x.r + r.y(1-e)$ ، ومنه :

$$r - r.x.r = r.y(1-e) \in R(1-e)$$

$$r - r.x.r = (1-r.x)r \in R.r = R.e \;\Rightarrow\; r = r.x.r$$

ثالثاً : الحلقة الإقليدية Euclidean Ring :

من الحلقات المهمة، والتي تلعب دوراً رائداً وعملياً في نظرية الحلقات والحقول، هي الحلقات الإقليدية .

تعريف الحلقة الإقليدية :

نقول عن الحلقة التامة $(R,+,.)$ إنها حلقة إقليدية ، إذا وجدت دالة ، ولتكن $d : R^* \longrightarrow N$ بحيث تتحقق الشروط التالية :

(1) $d(x) \geq 0$ لكل x من R^*

(2) $d(x) \leq d(xy)$ لكل y,x من R^*

(3) إذا كان $a \in R$ و $b \in R^*$، فإنه يوجد عددان حقيقيان ، r,q بحيث : $a = b.q + r$ بحيث، إما $r = 0$ أو $d(r) < d(b)$.

الدالة d تسمى عادةً الدالة الإقليدية ، والشرط الأخير (3) يسمى بالقسمة الإقليدية .

مثال (10) :

إن الحلقة التامة $R = (Z[\sqrt{3}],+,.)$ تشكل حلقة تامة .

الحل :

لنعرّف أولاً الدالة الإقليدية ، بالشكل :

$$d : R^* \longrightarrow N \;;\; d(x+y\sqrt{3}) = \left|x^2 - 3y^2\right|$$

لكل $a = x+\sqrt{3}\,y$ من R^* .

ولنتحقق الآن من الشروط الثلاثة الواردة في التعريف السابق :

1- $d(a) \geq 0$ ، لكل a من R^*

2- لكل b,a من R^* ، لدينا :

$$d(a) = d(a).1 \leq d(a).d(b) = d(a.b)$$

3- ليكن b,a من R^* و $b \neq 0$ ، فإن $\frac{a}{b} \in z$ ، ويكون $\frac{a}{b} = z + t\sqrt{3}$ حيث $Z,d \in Q$ ، لنختر الأعداد بحيث يكون $|z-x| \leq \frac{1}{2}$ و $|t-y| \leq \frac{1}{2}$ ، عندها يكون لدينا :

$$\frac{a}{b} = z + t\sqrt{3} = x + y\sqrt{3} + \left[(z-x) + (t-y)\sqrt{3}\right]$$

أي أن :

$$\begin{aligned} a &= (z + t\sqrt{3})b \\ &= (x + y\sqrt{3})b + \left[(z-x) + (t-y)\sqrt{3}\right]b \\ &= q.b + r \end{aligned}$$

حيث أن :

$$q = x + y\sqrt{3} \;,\; r = \left[(z-x) + (t-y)\sqrt{3}\right]b$$

ويكون :

$$d(r) = d\left(\left[(z-x)+(t-y)\sqrt{3}\right]b\right)$$

$$= d\left[(z-x)+(t-y)\sqrt{3}\right].d(b)$$

$$= \left|(z-x)^2 - 3(t-y)^2\right|.d(b) \le \left|\frac{1}{4} - \frac{3}{4}\right|.d(b)$$

$$= \frac{1}{2}d(b) < d(b)$$

بما أن الشروط الثلاثة محققة ، فإن الحلقة التامة $(Z[\sqrt{3}],+,\cdot)$ حلقة إقليدية .

المبرهنة التالية ، تثبت أن كل حلقة إقليدية هي حلقة تامة رئيسة .

مبرهنة (12) :

إذا كانت $(R,+,\cdot)$ حلقة إقليدية ، فإن $(R,+,\cdot)$ هي حلقة تامة رئيسة .

البرهان :

لتكن I مثالية في الحلقة الإقليدية $(R,+,\cdot)$، ولتكن الدالة الإقليدية $d:R^* \longrightarrow N$ ، إذا كان $I = \{0\}$ ، فإن $I = <0>$ مثالية رئيسة في الحلقة R.

نفرض الآن أن $I \neq \{0\}$ ، وهذا يعني أنه يوجد عنصر $a \in I$ حيث $a \neq 0$ ، لنختر العنصر a بحيث تكون d(c) أصغر ما يمكن ، لنبرهن أن $I = <a>$.

نفرض أن $x \in I$ و $x \neq 0$. وبما أن $(R,+,\cdot)$ حلقة إقليدية ، فإنه يوجد عنصران q,r من R ، بحيث يكون $x = a.q + r$ بحيث يكون $r = 0$ أو $d(r) < d(a)$.

من العلاقة الأخيرة نجد أن : $r = x - a.q \in I$ لأن I مثالية $x,a \in I$, $q \in R$ ، إن $r = 0$ ، وهذا يؤدي إلى أن $x = a.q$ ، أي أن $I = <a>$.

ملاحظة (5) :

إن عكس المبرهنة السابقة ، بشكل عام ، ليس صحيحاً ، فمثلاً الحلقة التامة الرئيسة $(Z[\sqrt{-19}],+,\cdot)$ ليست حلقة إقليدية .

مفهوم القسمة Divisibility :

لتكن $(R,+,\cdot)$ حلقة تامة ، وليكن $b,a \neq 0$ عنصرين في R . نقول إن العنصر

a يقسم Divides العنصر b ، إذا وُجِدَ عنصر c في R يحقق العلاقة $b = a.c$ ، ونرمز لذلك بـ $a \mid b$. ونقول في هذه الحالة إن العنصر b يقبل القسمة Divisible على العنصر a في R. إذا كان a غير قاسم لـ b، فإننا سنرمز لذلك بالرمز $a \nmid b$.

نستنتج من التعريف السابق ما يلي :

لكل c,b,a من R فإن :

1- $a \mid a$ (كل عنصر يقسم نفسه) (الخاصة الانعكاسية) .

2- إذا كان $a \mid b$ و $b \mid c$ ، فإن $a \mid c$ (الخاصة المتعدية) .

3- إذا كان $a \mid b$ و $b \mid a$ ، فإن $a = u.b$ ، حيث u عنصر وحدة في R ، أي أنه قاسم للمحايد في R .

4- إذا كان $a \mid b$ و $a \mid c$ ، فإن لكل x,y من R ، $a \mid (xb \pm yc)$

5- إذا كان 1 هو عنصر الوحدة في $(R,+,\cdot)$ ، فإن العناصر القابلة للعكس في R ، هي فقط العناصر التي هي قواسم لـ 1 في R .

6- إذا كان 0 هو صفر الحلقة $(R,+,\cdot)$ ، وإذا كان $a \neq 0$ من R ، وإذا كان لـ a معكوس في R بالنسبة للعملية $(\cdot)$ ، فإن a يقسم أي عنصر من R في R .

مفهوم الترادف (التشارك) Associated :

لتكن $(R,+,\cdot)$ حلقة تامة ، نقول عن العنصرين b,a من R^* إنهما مترادفان أو متشاركان ، إذا تحقق الشرط : $a = u.b$ ، حيث أن u هو عنصر الوحدة في الحلقة التامة $(R,+,\cdot)$. نرمز عادةً للعنصرين المترادفين بـ $a \sim b$.

بكلامٍ آخر ، نقول إن العنصر a يترادف مع العنصر b في الحلقة التامة $(R,+,\cdot)$ إذا كان $a \mid b$ و $b \mid a$. (سنبرهن ذلك فيما بعد) .

ويمكن التحقق ، وبسهولة ، أن علاقة الترادف بين العناصر في الحلقة التامة $(R,+,\cdot)$ تمثل علاقة تكافؤ على R ، لأن :

(1) العلاقة $\sim$ انعكاسية (كل عنصر مترادف مع نفسه) ، أي $a \sim a$.

(2) العلاقة $\sim$ تناظرية ، إذا كان $a \sim b$ ، فإن $b \sim a$.

(3) العلاقة ~ متعدية ، أي إذا كان $a \sim b$ و $b \sim c$ ، فإن $a \sim c$.

لتكن $(R,+,\cdot)$ حلقة تامة ، ولنرمز لصفرها بالرمز 0 ، وليكن $a \neq 0$ و $b \neq 0$ عنصرين من R، إن الشرط اللازم والكافي لكي يكون b,a مترادفان في R هو أن يكون كل من العنصرين b,a قاسماً للآخر في R .

البرهان :

لنفرض أولاً ، أن a يقسم b و b يقسم a في R ، ولنبرهن أن b,a مترادفان في R . بما أن كلاً من العنصرين b,a قاسم للآخر في R ، فإنه يوجد عنصرين c_1 و c_2 من R بحيث يكون :

$$a = b.c_1 \ , \ b = a.c_2$$

ومنه يكون :

$$a = a\, c_2\, c_1 \qquad (*)$$

لنرمز للعنصر المحايد في R بالنسبة للعملية $(\cdot)$ بـ 1 ، فمن (*) نجد أن :

$$a\,(1 - c_2\, c_1) = 0$$

ومنه $1 - c_2\, c_1 = 0$ أي أن $1 = c_2\, c_1$ ، وهذا يعني أن c_2,c_1 قابلان للقلب في R، وبالتالي ، فإن كلاً من العلاقتين : $a = b.c_1$ و $b = a.c_2$ تبيّن لنا أن b,a مترادفان في R .

العكس ، واضح حسب التعريف .

تعريف :

لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، ولنرمز لصفرها بـ 0 . وإذا كان $a \neq 0$ عنصراً من R، إن العناصر القابلة للعكس في R ومرادفات العنصر a في R تسمى قواسم غير خاصة لـ a في R .

نتيجة (3) :

لكل عنصر غير صفري من حقلٍ ما وليكن $(F,+,\cdot)$ يوجد له عدد غير منته من العناصر المترادفة .

البرهان :

ليكن a عنصراً ما من الحقل F ، بحيث $a \neq 0$ ، يوجد عنصر b لا يساوي الصفر من F بحيث يتحقق $a = u.b$ ومنه يكون : $u = a.b^{-1}$

مثال (11) :

لتكن $(Z[\sqrt{3}],+,.)$ حلقة تامة ، أثبت أن العنصر $a = \sqrt{3}$ يترادف مع العنصر $3+2\sqrt{3}$ في الحلقة التامة المدروسة .

الحل :

بما أن $(2+\sqrt{3})\sqrt{3} = 3+2\sqrt{3}$ ، وبما أن $2+\sqrt{3}$ هو عنصر الوحدة في الحلقة التامة $(Z[\sqrt{3}],+,.)$ ، لأن :

$$(2+\sqrt{3}).(2-\sqrt{3}) = 1$$

إذن العنصران $\sqrt{3}$ و $3+2\sqrt{3}$ مترادفان .

مبرهنة (13) :

إذا كانت $(R,+,.)$ حلقة إقليدية دالتها الإقليدية d ، عندها يتحقق ما يلي :

(1) $d(1) < d(a)$ لكل a من R^* والعنصر 1 هو المحايد في R .

(2) إذا كان b,a من R^* مترادفين ، فإن : $d(a) = d(b)$.

(3) $d(u) = d(1)$ ، إذا وفقط إذا ، كان $u \in R^*$ عنصر وحدة في R .

البرهان :

1- بما أن $a = 1.a$ ، لكل a من R^* ، فيكون :

$$d(a) = d(a.1) \geq d(1)$$

2- بما أن b,a عنصرين مترادفين من R^* في R ، يوجد $u \in R^*$ بحيث يتحقق $a = u.b$ و u عنصر الوحدة ، وبالتالي :

$$d(a) = d(u.b) \geq d(b)$$

وبما أن $b = u^{-1}.a$ فيكون لدينا :

$d(b) = d(u^{-1}.a) \geq d(a)$

من المتباينتين السابقتين نجد أن : $d(a) = d(b)$

3- لنبرهن أولاً ، أنه إذا كان $u \in R$ عنصر وحدة ، فإن : $d(u) = d(1)$.

بما أن u عنصر الوحدة في R، يوجد عنصر $v \in R$ بحيث $u.v = 1$. ومنه يكون:

$d(u) \leq d(u.v) = d(1) \leq d(v)$

ومنه يكون :

$d(u) = d(1)$

لنبرهن الآن ، على العكس . بما أن $(R,+,\bullet)$ حلقة إقليدية يوجد عنصران q,r من R بحيث يكون $1 = u.q + r$ حيث u من R^* و $r = 0$ أو $d(r) < d(u)$. وبما أن $d(1)$ أصغر دالة لعناصر R، وبما أن $d(u) = d(1)$ فيكون $r = 0$ وهذا يؤدي إلى أن $u.q = 1$ ، أي أن u عنصر وحدة في الحلقة $(R,+,\bullet)$.

مبرهنة (14) :

لتكن $(R,+,\bullet)$ حلقة إقليدية ، ولنرمز لصفرها بـ 0 ، وإذا كان b,a من R^* ، وإذا كان a قاسماً لـ b في R ، وإذا كان $d(a) = d(b)$ فإن b,a مترادفان في R .

البرهان :

بما أن $(R,+,\bullet)$ حلقة إقليدية ، فإنه يوجد من أجل b,a عنصران q,r في R ، بحيث يكون : $a = b.q + r$ و $r = 0$ أو $d(r) < d(b)$.

إن r لا يختلف عن الصفر ، لأنه إذا كان $r \neq 0$ فإن :

$d(r) < d(b) = d(a)$

ومن ناحية ثانية بما أن a يقسم b في R ، فإنه بالإمكان إيجاد عنصر c من R ، بحيث يكون $b = a.c$ ، ومن ثم ، فإن :

$$\begin{aligned} a = b.q + r \Rightarrow r &= a - b.a = a - a.c.q \\ &= a\,(1 - c.q) \end{aligned}$$

حيث 1 هو عنصر الوحدة في الحلقة $(R,+,\bullet)$.

العلاقة الأخيرة ، تبين لنا أن a يقسم r في R ، ومن ثم ، فإن $d(a) \leq d(r)$ ، وهذا تناقض . إذن $r = 0$ وبالتالي من العلاقة : $a = b.q + r$ نجد أن $a = b.q$ ، وهـذا يبيّن لنا أن b يقسم a في R.

بما أن a يقسم b في R فرضاً ، وبما أن b يقسم a في R (برهاناً) فإن b,a مترادفان في R .

رابعاً : حلقة التحليل الوحيد (Unique factoriration domain) :

لدراسة حلقة التحليل الوحيد ، نحتاج إلى المفاهيم التالية : العناصر الأولية والعناصر غير القابلة للتحليل ، والقاسم المشترك الأعظم ، والمضاعف المشترك الأصغر .

1- القاسم المشترك الأعظم Greatest common divisior :

إذا كانت $(R,+,.)$ حلقة إبدالية ما ، ولنرمز لصفرها بالرمز o ، وإذا كان b,a عنصرين ما من R^* . نقول عن العنصر m المنتمي إلى R إنه قاسم مشترك أعظم لـ b,a في R ونرمز لذلك بـ (a,b) أو $gcd\,(a,b)$ إذا تحقق الشرطان التاليان :

(1) m قاسم مشترك لـ b,a في R ، أي : $m|a\ ,\ m|b$

(2) إذا وجد قاسم مشترك آخر m' لـ b,a في R ، فإن m' يقسم m في R .

ينتج من التعريف السابق ، أنه إذا كانت $(R,+,.)$ حلقة إبدالية بمحايد وصفرها هو o وكان $a,b \in R^*$ و u عنصراً قابل للعكس في R ، وإذا كان m هو قاسم مشترك أعظم لـ a و b في R، فإن العنصر $m.u$ هو، أيضاً قاسم مشترك أعظم لـ a و b في R .

مبرهنة (15) :

إذا كانت $(R,+,.)$ حلقة إقليدية، وإذا كان y,x عنصرين من R وغير معدومين، فإن لـ y,x قاسماً مشتركاً أعظم وليكن z في R من الشكل : $z = \alpha.x + \beta.y$ لكل β,α من R .

البرهان :

لنأخذ المجموعة $M = \{q.x + r.y\ :\ q,r \in R\}$

إن $M \neq \phi$ ، ويوجد فيها عناصر لا تساوي الصفر ، لأن :

$0 \neq x = 1.x + 0.b \in M$

$0 \neq y = 0.x + 1.b \in M$

حيث رمزنا لعنصر الوحدة في الحلقة بـــ 1 ولصفرها بـــ 0 . لنختر من عناصــر المجموعة M المختلفة عن الصفر ، العنصر z الذي من أجله يكون $\varphi(z)$ أصغرياً. حيث φ دالة إقليدية .

بما أن $z \in M$ ، فإن z يكتب بالشكل : $z = \alpha.x + \beta.y$ لكل β,α من R .

(1) لنبرهن أن z هو قاسم مشترك أعظم لـــ y,x في R . بما أن $(R,+,.)$ حلقة إقليدية ، فإنه من أجل العنصرين z,x يوجد عنصران t,s من R ، بحيث يكـــون : $x = z.s + t$ و t إما أن يساوي الصفر أو $\varphi(t) < \varphi(z)$.

إن t لا يمكن أن يساوي الصفر لأنه إذا كان $t \neq 0$ ، فـــإن $\varphi(t) < \varphi(z)$، ومـــن ناحية ثانية ، إن :

$$x = z.s + t \Rightarrow t = x - z.s$$

أي أن :

$$T = x - (\alpha.x + \beta.y) = (1 - \alpha.s) .x + (-\beta.s) .y \in M$$

وهذا مخالف لاختيارنا ، من مجموعة العناصر M المختلفة عن الصفر ، العنصر z الذي يكون من أجله $\varphi(z)$ أصغرياً . إذن $t = 0$ ، وبالتالي $x = d.s$ وهذا يبـــين لنا أن z يقسم x في R .

وبنفس الطريقة يمكن برهان أن z يقسم y في R .

(2) ليكن z' قاسم مشترك آخر لـــ y,x في R ، فإن z' يقسم $\alpha.x + \beta.y$ فـــي R ، أي أن z' يقسم z في R .

نستنتج من (1) و(2) أن z هو قاسم مشترك أعظم لـــ y,x في R .

2- المضاعف المشترك الأصغر Least common multiple :

إذا كانت $(R,+,.)$ حلقة إبدالية ، وإذا كان $a,b \in R^*$ ، نقول عن العنصر d إنه مضاعف مشترك أصغر للعنصرين b,a في R ، إذا تحقق الشرطان التاليان :

(1) $a|d$ و $b|d$

(2) إذا وُجِدَ $c \in R$ حيث $a|c$ و $b|c$ فإن $d|c$.

نرمز عادةً للمضاعف المشترك الأصغر للعـــددين b,a فـــي R بـــالرمز $[a,b]$ أو $\ell cm\ [a,b]$.

3- العناصر الأولية والعناصر غير القابلة للتحليل

Prime and irreducible elements

لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، وليكن P عنصراً ما من R ، نقـــول عـــن العنصر P إنه أولي Prime إذا تحقق الشرطان التاليان :

(1) $P \neq 0$ و P ليس عنصر وحدة في R .

(2) لكل b,a من R ، إذا كان $P|a.b$ ، فإن $P|a$ أو $P|b$.

لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، ولنرمز لصفرها بـــ o ، وإذا كان a عنصـــراً مغايراً للصفر في R ، نقول إن a غير قابل للتحليل (Irreducible) فـــي R ، إذا تحقق الشرطان التاليان :

(1) $a \neq 0$ و a ليس عنصر وحدة في R .

(2) كل قاسم لـــ a في R هو قاسم غير خاص له . أي ، إذا كان c,b عنصرين ما من R ، بحيث $a = b.c$ ، فإن أحد العنصرين c,b قابل للعكس في R .

بالاستفادة من المفهوم السابق ، نجد أنه :

(1) إذا كانت $(R,+,\cdot)$ حلقة إبدالية بمحايد ، وإذا كان u عنصراً قابلاً للعكس فـــي R، وإذا فرضنا أن $a \neq 0$ عنصراً من R وغير قابل للتحليل فيها ، فإن العنصـــر $a.u$ هو أيضاً غير قابل للتحليل في R حيث رمزنا لصفر الحلقة $(R,+,\cdot)$ بـــ 0 .

(2) العنصر الصفري في الحلقة $(R,+,\cdot)$ ، هـــو عنصـــر قابـــل للتحليـــل ، لأن $0 = 0.0$.

مثال (12) :

أي عدد أولي وليكن P في حلقة الأعداد الصحيحة $(Z,+,\cdot)$ هو عنصر أولـــي ، وغير قابل للتحليل .

مثال (13) :

بيِّن أن العدد 2 عنصر أولي ، لكنه قابل للتحليل في الحلقة $(Z_6,\oplus,\otimes)$.

الحل :

بما أن $2 \neq 0$ و 2 ليس عنصر وحدة في R . كما أن لكل b,a من Z_6 ، $2|a.b$ ، وبالتالي إما $2|a$ أو $2|b$ إذن 2 عنصراً أولي في Z_6 .

بما أن $2\otimes4 = 2$ في حين أن العددين 2 و 4 ليسا عنصري وحدة في الحلقة $(Z_6,\oplus,\otimes)$ ، وبالتالي ، فإن 2 عنصر قابل للتحليل في Z_6 .

مبرهنة (16) :

كل عنصر أولي في أية حلقة تامة هو عنصر غير قابل للتحليل .

البرهان :

لتكن $(R,+,\cdot)$ حلقة تامة ، وإذا كان P عنصر أولي من R ، ولنفرض أن b,a من R بحيث $P = a.b$.

إن $P|a.b$ ، وبالتالي إما $P|a$ أو $P|b$ ، لأن P عدد أولي .

إذا كان $P|a$ ، فإنه يوجد عنصر من R ، وليكن d بحيث يكون $a = d.P$ ومنه $P = d.P.b$ ، وبما أن $P \neq 0$ في R ، فإن $dP = 1$ ، أي أن b عنصر وحدة .

بنفس الطريقة تماماً نجد أنه إذا كان $P|b$ ، فإن a عنصر وحدة .

نستنتج مما سبق أن P عنصر غير قابل للتحليل في الحلقة $(R,+,\cdot)$.

نتيجة (4) :

يكون العنصر P أولياً في الحلقة التامة الرئيسة $(R,+,\cdot)$ ، إذا ، وفقط إذا ، كان P عنصراً غير قابل للتحليل فيها .

البرهان :

حسب المبرهنة السابقة، نجد بسهولة أن العنصر الأولي P غير قابل للتحليل في الحلقة $(R,+,\cdot)$.

لنبرهن الآن، أن P عنصر أولي في الحلقة $(R,+,\cdot)$ ، علماً أن P عنصراً غير قابل للتحليل في $(R,+,\cdot)$.

بما أن P غير قابل للتحليل في R فإن $P \neq 0$ وليس عنصر وحدة ، وليكن $P|a.b$ لكل b,a من R ، وبالتالي يكون $a.b = d.P$ حيث أن d من R ، وبما أن $(R,+,\cdot)$ حلقة تامة رئيسة ، فإن $< a,P > = < c >$ حيث أن $c \in R$.

إن $P \in < a,P >$ ، وبالتالي $P \in < c >$. إذن يوجد $t \in R$ بحيث يكون $P = c.t$ ، وبما أن العنصر P غير قابل للتحليل في R ، فإن c عنصر وحدة أو t عنصر وحدة . فإذا كان c عنصر وحدة في R، فإننا نجد $< a,P > = R$، وبالتالي يوجد عنصران y,x من R، حيث أن $x.a + y.P = 1$، ومنه يكون $x.a.b + y.P.b = b$

بما أن $a.b = d.P$ ، فيكون $x.d.P + y.P.b = b$ ، وبالتالي يكون $P|b$.

أما إذا كان t عنصر وحدة في R، فإن $c = P.t^{-1} \in < P >$، ويكون $< c > \subseteq < P >$، ومنه يكون $a \in < P >$، أي أن $P|a$ أي أن P عنصر أولي .

المبرهنة التالية تقدم الشرط اللازم والكافي لكي تكون المثالية في الحلقة التامة الرئيسة مثالية أعظمية .

مبرهنة (17) :

الشرط اللازم والكافي لكي تكون المثالية $< P >$ في الحلقة التامة الرئيسة $(R,+,\cdot)$ مثالية أعظمية هو أن يكون العنصر P غير قابل للتحليل في الحلقة R .

البرهان :

نفرض أولا أن P عنصر غير قابل للتحليل في R ، ولنبرهن أن $< P >$ مثالية أعظمية في R، إذا كان $< P > \subseteq < a >$ لكل a من R ، يكون $P = a.b$ ، لأجل b من R . إذا كان a عنصر وحدة ، فإن : $< a > = < 1 > = < R >$ ، أما إذا لم يكن a عنصر وحدة في R ، فيجب أن يكون b عنصر وحدة ، وبالتالي يوجد عنصر u من R ، بحيث يتحقق $b.u = 1$ ، وينتج في هذه الحالة أن :

$P.u = a.b.u = a$

وبالتالي يكون $<P> \subseteq <a>$ ، ويكون $<P> = <a>$.

إذن فرضنا أن $<P> \subseteq <a>$ يؤدي إما $<R> = <a>$ أو $<P> = <a>$.

لكن بما أن $<P> \neq R$ أو P عنصر وحدة ، إذن P مثالية أعظمية في R .

لنبرهن العكس ، أي لنبرهن أن P عنصر غير قابل للتحليل ، علماً أن $<P>$ مثالية أعظمية .

إذا كان $<P> = <a>$ ، فإن العنصرين a و P مترادفان في الحلقة $(R,+,\cdot)$ ، وبالتالي يكون b عنصر وحدة في R . أما إذا كان $<P> \neq <a>$ فإننا نجد $<R> = <1> = <a>$. وبما أن $<P>$ مثالية أعظمية في R ، فالعنصران a و 1 مترادفان ، وهذا يعني أن a عنصر وحدة ، وبالتالي فإن P عنصر غير قابل للتحليل في الحلقة $(R,+,\cdot)$.

لنأتي الآن لدراسة حلقة التحليل الوحيد .

تعريف حلقة التحليل الوحيد (حلقة تحليل) Unique factorization domain :

نقول عن الحلقة التامة $(R,+,\cdot)$ إنها حلقة تحليل وحيد ، إذا تحقق الشرطان التاليان :

1- من أجل أي عنصر a غير معدوم من R وغير قابل للعكس فيها ، يكتب على شكل جداء عدد منته لعناصر من R ، وكل منها غير قابل للتحليل في R .

2- إذا كان $a \neq 0$ عنصراً من R وغير قابل للعكس فيها ، وإذا تحقق :

$$a = P_1.P_2\dots P_m = q_1.q_2\dots q_n$$

حيث أن P_j , q_i من R و $i = 1,2,..,n$ و $j = 1,2,\dots,m$ ، وكل منها غير قابل للتحليل في R ، عندها $m = n$ ، وبتغيير مناسب لترتيب العناصر q_i حيث $i = 1,2,\dots,n$ في الجداء : $q_1.q_2\dots q_n$ نحصل على جداء كل عنصر من العناصر المكونة له مرادف العنصر المقابل له بالترتيب في الجداء $P_1.P_2\dots P_n$.

بكلامٍ آخر ، إذا كان $a \neq 0$ عنصراً من R وغير قابل للعكس في R ، فإن أي تحليلين للعنصر a إلى جداء منته من المضاريب كل منها غير قابل للتحليل في R ،

يختلفان احدهما عن الآخر ، فقط بترتيب تلك العناصر ، وبفارق عناصر قابلة للعكس في الحلقة $(R,+,\cdot)$.

المبرهنة التالية تقدم الشرط اللازم والكافي لكي تكون الحلقة التامة حلقة تحليل وحيد .

مبرهنة (18) :

إذا كانت $(R,+,\cdot)$ حلقة تامة ، الشرط اللازم والكافي لكي تكون $(R,+,\cdot)$ حلقة تحليل وحيد ، هو أن يتحقق الشرطان التاليان :

(1) كل عنصر غير معدوم وليكن a من R ، وغير قابل للعكس في R ، هو جداء منته لعناصر من R، كل منها غير قابل للتحليل في R .

(2) إذا كان $P \neq 0$ عنصراً من R وغير قابل للتحليل فيها ، وإذا كان $x \neq 0$ و$y \neq 0$ عنصران من R بحيث P يقسم x.y في R ، فإن P يقسم واحداً من العنصرين y,x ، على الأقل، في الحلقة التامة R .

البرهان :

نفرض أولاً ، أن $(R,+,\cdot)$ حلقة تحليل وحيد ، ولنبرهن أن الشرطين (1) و(2) محققان .

نلاحظ أولاً أن الشرط الأول محقق ، وذلك حسب تعريف حلقة التحليل الوحيد . لنبرهن على صحة الشرط الثاني .

بما أن $x \neq 0$ و $y \neq 0$ عنصران من R ، ولأن $(R,+,\cdot)$ حلقة تامة ، فإن $x.y \neq 0$ ، وبما أن P يقسم x.y في R ، فإنه بالإمكان إيجاد عنصر وليكن z من R على الأقل وبحيث يكون :

$$x.y = P.z \qquad (*)$$

إذا كان أحد العنصرين y,x قابلاً للعكس في R ، عندها من العلاقة (*) ينتج أن P يقسم العنصر الآخر في R . أما إذا كان y,x غير قابلين للعكس في R ، عندها يكون العنصر z غير قابل للعكس في R ، وبالتالي ستكون العناصر z,y,x هي

جداء منته لعناصر من R وكل منها غير قابل للتحليل فيها ، ولنفرض مثلاً ، أن :

$$x = x_1'.x_2'......x_m'$$

$$y = x_1''.x_2''......x_n''$$

$$z = y_1 . y_2 .... y_S$$

حيث أن x_i' و x_j'' وy_k عناصر من R ، وكل منها غير قابل للتحليل في R ، كما أن :

$$k = 1,2,..,s \;\; ; \;\; j = 1,2,...,n \;\; ; \;\; i = 1,2,...,m$$

وبملاحظة العلاقة (*) نجد أن :

$$x_1'.x_2'......x_m'.x_1''.x_2''...... .x_n'' = P.y_1.y_2.....y_S$$

وبسبب كون (R,+,.) منطقة تامة ، فإن المساواة الأخيرة ، توضح لنا أن P مرادف لأحد العناصر $x_1', x_2', ..., x_m', x_1'', x_2'', ..., x_n''$ ، وبالتالي فإن P يقسم أحد العنصرين y,x في R .

برهان العكس ، أي لنثبت أن (R,+,.) حلقة تحليل وحيد ، علماً أن الشرطان (1) و(2) محققان .

بما أن الشرط الأول في تعريف حلقة التحليل الوحيد محقق فرضاً ، فيكفي أن نبرهن على تحقق الشرط الثاني الوارد في تعريف حلقة التحليل الوحيد .

نلاحظ أولاً أن الشرط الثاني الوارد في تعريف حلقة التحليل الوحيد محقق من أجل أي عنصر من R مختلف عن الصفر وغير قابل للتحليل في R . ولنفرض الآن أن الشرط الثاني محقق من أجل أي عنصر لا يساوي الصفر في R وغير قابل للعكس فيها ، ويمكن تحليله إلى جداء t مضروباً في R وكل منها غير قابل للتحليل فيها ، ولنثبت أن الشرط الثاني الوارد في مفهوم حلقة التحليل الوحيد محقق ، وذلك من أجل كل عنصر من R لا يساوي الصفر ، وغير قابل للعكس في R ، ويمكن تحليله إلى جداء 1 + t مضروباً من R وكل منها غير قابل للتحليل في R . من أجل ذلك نفرض أن r عنصراً لا يساوي الصفر من R وغير قابل للعكس فيها ، ولنفرض أيضاً :

$$r = x_1.x_2...x_{t+1} = c_1.c_2....c_S$$

حيث أن c_i و P_j عناصر من R وكل منها غير قابل للتحليل فيها، حيث $1 \leq j \leq t+1, 1 \leq i \leq s$.

وبما أن :

$$x_1.x_2....x_{t+1} = c_1.c_2....c_S \qquad (*)'$$

فإن P_1 يقسم الجداء $c_1.c_2....c_S$ في R ، وبالتالي فإن P_1 يقسم واحداً من العناصر $c_1,c_2,....,c_S$ ، على الأقل ، في R ، ولنفرض على سبيل المثال أن P_1 يقسم c_1 في R . وبالتالي فإن P_1 و c_1 غير قابلين للتحليل في R ، كما أن P_1 و c_1 مترادفان في R (لأن P_1 يقسم c_1 في R) ، وبالتالي يمكن إيجاد عنصر قابل للعكس وليكن u بحيث يكون :

$$c_1 = P_1.u \qquad (*)''$$

من العلاقتين $(*)'$ و $(*)''$ نجد أن :

$$P_1.P_2....P_{t+1} = P_1.u.c_2....c_S$$

ومنه يكون :

$$P_2....P_{t+1} = u.c_2....c_S$$

وبما أن الشرط الثاني الوارد في تعريف حلقة التحليل الوارد محقق ، من أجل كل عنصر لا يساوي الصفر من R وغير قابل للعكس فيها، ويمكن تحليله إلى جداء t مضروباً من R وكل منها غير قابل للتحليل فيها، فإن $u\, c_2....\, c_S$, $P_2\, P_3....P_{t+1}$ يختلفان احدهما عن الآخر بترتيب تلك العناصر ، وبفارق عناصر قابلة للعكس في R . ويأخذ بعين الاعتبار العلاقة $(*)''$ نجد أن الجدائين $P_1.P_2....P_{t+1}$ و $c_1.c_2....c_S$ مختلفان عن بعضهما بترتيب تلك العناصر وبفارق عناصر قابلة للعكس في R .

نستنتج مما سبق ، تحقق الشرط الثاني الوارد في تعريف حلقة التحليل الوحيد .

مثال (14) :

إن حلقة الأعداد الصحيحة $(Z,+,\cdot)$ تشكل حلقة تحليل وحيد ، لأنه من أجل أي

عنصر فيها ، وليكن x حيث $x \notin \{0, \pm 1\}$ يمكن التعبير عنه كحاصل ضرب عدد منته من الأعداد الأولية .

مثال (15) :

كل حقل ، يمكن اعتباره حلقة تحليل وحيد ، لأن أي عنصر فيه لا يساوي الصفر هو عنصر وحدة في هذا الحقل .

نتيجة (5) :

كل حلقة تامة رئيسة هي حلقة تحليل وحيد .

مبرهنة (19) :

كل حلقة إقليدية هي حلقة تحليل وحيد .

البرهان :

لتكن $(R,+,\cdot)$ حلقة إقليدية ولنرمز لصفرها بـ 0 ولعنصر الوحدة فيها بـ 1 . ولنبرهن أن $(R,+,\cdot)$ حلقة تحليل وحيد ، أي لنتحقق من الشرطين :

(1) كل عنصر x لا يساوي الصفر من R وغير قابل للعكس فيها ، هو جداء منته لعناصر من R ، كل منها غير قابل للتحليل فيها .

(2) إذا كان $P \neq 0$ عنصراً من R وغير قابل للتحليل فيها ، إذا كان $x_1 \neq 0$ و$y_1 \neq 0$ عنصرين من R بحيث يكون P يقسم $x_1.y_1$ في R ، فإن P يقسم واحداً من العنصرين y_1,x_1 على الأقل في R . من أجل ذلك :

إن الشرط الأول محقق من أجل العنصر x من R ، إذا كان $\varphi(a) < \varphi(x)$ حيث φ دالة إقليدية (إن المساواة السابقة غير ممكنة إذا كان x عنصراً غير قابل للعكس في R). لنفرض الآن أن الشرط الأول محقق من أجل جميع العناصر a من R، التي من أجلها تحقق $\varphi(a) < \varphi(x)$، ولنبرهن أن الشرط الأول محقق من أجل العنصر x إذا كان x غير قابل للتحليل في R فيكون المطلوب . أما إذا لم يكن x كذلك ، فإنه بالإمكان كتابته بالشكل $x = b.c$ ، حيث أن c,b ليسا مترادفين في R ، وأيضاً x,c ليسا مترادفين في R ، وبالتالي :

$$\varphi(c) < \varphi(x) \quad , \quad \varphi(b) < \varphi(x)$$

إذاً كل من c,b هو جداء منته لعناصر من R كل منها غير قابل للتحليل فيها ، وبالتالي، فإن x هو أيضاً جداء منته لعناصر من R كل منها غير قابل للتحليل فيها.

لنبرهن الآن على تحقق الشرط الثاني :

إذا كان $P \neq 0$ عنصراً من R ، وغير قابل للتحليل في R ، وإذا كان $x_1 \neq 0$ و $y_1 \neq 0$ عنصرين من R بحيث أن P يقسم $x_1.y_1$ في R ، وإذا فرضنا أن P لا يقسم x_1 في R ، فإن $(P,a_1) = 1$ ، ومن ثم ، فإنه بالإمكان إيجاد عنصرين β,α من R بحيث يكون :

$$1 = \alpha.x_1 + \beta.P$$

وبالتالي يكون :

$$y_1 = y_1.\alpha.x_1 + y_1.\beta.P$$

بما أن P يقسم الجداء $x_1.y_1$ في R ، فإنه يمكن إيجاد عنصر وليكن z_1 من R بحيث يكون : $x_1.y_1 = P.z_1$ ، ومنه يكون :

$$y_1 = (\alpha.z_1 + \beta.y_1).P$$

وهذا يبين لنا أن P يقسم y_1 في R .

(5-3) حقل القواسم Field of Quotients :

لتكن $(R,+,\cdot)$ حلقة تامة ما ، لنبني حقل القواسم على الحلقة التامة السابقة ، لتكن :

$$X = \{(r,u) : r\in R\,,\, u\in R\,;\, u \neq 0\}$$

ولنعرّف على X العلاقة $\equiv$ بالشكل :

$$(r,u) \equiv (s,v) \iff r.v = s.u$$

ولنثبت أولاً أن العلاقة $\equiv$ تشكل (تمثل) علاقة تكافؤ على المجموعة X .

من الواضح ، أن $(r',u) \equiv (r',u)$ ، لكل (r',u) من X . أي أن العلاقة $\equiv$ انعكاسية (reflexive) .

إذا كان $(r,u) \equiv (s,v)$ ، فإن $r.v = s.u$ ، وبالتالي فإن : $v.r = u.s$ ، وبذلك يكون

$(r,u) \equiv (s,v)$، أي أن العلاقة $\equiv$ تناظرية (symmetric) ، وذلك من أجل $(r,u)\,,\,(s,v) \in X$.

لنبرهن أخيراً ، أن العلاقة $\equiv$ متعدية .

ليكن $(r,u)\,,\,(s,v)\,,\,(t,w)$ من X ، وبحيث يكون :

$$(r,u) \equiv (s,v) \iff r.v = s.u$$

$$(s,v) \equiv (t,w) \iff s.w = v.t$$

بما أن $(R,+,\bullet)$ إبدالية ، فيكون :

$$r.v.w = (s.u).w = u\,(s.w) = u.t.v$$

وبما أن $v \neq 0$ في الحلقة التامة $(R,+,\bullet)$ ، يكون لدينا $r.w = t.u$ ، وهذا يعني ، أن $(r,u) \equiv (t,w)$. إذن العلاقة $\equiv$ متعدية transitive .

نستنتج مما سبق أن العلاقة $\equiv$ هي علاقة تكافؤ على المجموعة X .

لنرمز لفصل التكافؤ للعلاقة $\equiv$ بالرمز $[(r,u)]$ لكل زوج (r,u) في X ، ونكتب أحياناً $[(r,u)] = r/u$.

قبل أن نعرّف عمليتي الجمع والضرب ، نذكر بأن :

$$[(r,u)] = [(s,v)] \iff (r,u) \equiv (s,v)$$

أو بالشكل التالي (القسمة) :

$$\frac{r}{u} = \frac{s}{v} \iff r.v = s.u \qquad (1)$$

ليكن Q مجموعة فصول التكافؤ $[(r,u)]$ حيث (r,u) من X . أي أن :

$$Q = \left\{ \frac{r}{u} : r,u \in R\,,\, u \neq 0 \right\}$$

لنعرف الآن عمليتي الجمع $(+)$ والضرب $(\bullet)$ على Q بالشكل :

$$\frac{r}{u} + \frac{s}{v} = \frac{r.v + s.u}{u.v} \quad , \quad \frac{r}{u} . \frac{s}{v} = \frac{r.s}{u.v}$$

ولمـــا كانـــت $(R,+,\bullet)$ حلقـــة تامـــة ، و $u \neq 0$ و $v \neq 0$ فـــإن $u.v \neq 0$. أي أن $\frac{r.v+s.u}{u.v} \in Q$ ، وكذلك $\frac{r.s}{u.v} \in Q$.

لنبرهن الآن أن الجمع (+) والضرب (•) عمليتان حسنتا التعريف (معرفتان جيداً) .

لنفرض أن $r/u = r'/u'$ و $s/v = s'/v'$ ، ولنثبت أن :

$$\frac{r'v'+s'u'}{u'.v'} = \frac{rv+su}{u.v}$$

لدينا $sv' = s'v\,,\, ru' = r'u$ (من العلاقة (1)) . ولنثبت أن :

$$u.v(r'v'+s'u') = u'v'(rv+su)$$

لدينا :

$$u.v\,(r'v' + s'u') = (r'u)\,v\,v' + (s'\,v)\,u\,u'$$
$$= r\,u'\,v\,v' + s\,v'\,u\,u' = u'\,v'\,(r\,v + s\,u)$$

بالطريقة نفسها ، يمكن إثبات أن عملية الضرب حسنة التعريف أيضاً .

المبرهنة التالية ، تبرهن أن المجموعة Q مع عمليتي الجمع والضـــرب الســـابقتان تشكل حقلاً ، نسمي عادةً هذا الحقل بحقل قواسم الحلقة التامة $(R,+,\bullet)$.

مبرهنة (20) :

المجموعة Q مع عمليتي الجمع والضرب المعرفة عليها تشكل حقلاً .

البرهان :

لنتحقق من أن عملية الجمع تجميعية على Q :

لتكن $r/u, s/v, t/w \in Q$ ، وبالتالي ، فإن :

$$\frac{r}{u}+\left(\frac{s}{v}+\frac{t}{w}\right)=\frac{r}{u}+\left(\frac{s.w+t.v}{v.w}\right)=\frac{r(v.w)+(s.w+t.v).u}{u(v.w)}$$

$$\frac{(r.v+s.u)w+t.u.v}{(u.v)w}=\left(\frac{r.v+s.u}{u.v}\right)+\frac{t}{w}=\left(\frac{r}{u}+\frac{s}{v}\right)+\frac{t}{w}$$

وبالطريقة نفسها ، نثبت أن عملية الضرب تجميعية على Q أيضاً . كما ، يمكن التأكد من أن عمليتي الجمع والضرب على Q عمليتان إبداليتان . ونلاحظ ، أن $\frac{0}{u}=$ [0,u] هو العنصر المحايد بالنسبة لعملية الجمع ، وأن $-r/u$ هو المعكوس الجمعي للعنصر r/u ، وبالتالي ، فإن (Q,+) تشكل زمرة إبدالية .

لكل s/v من Q ، فإن :

$$\frac{r}{r}.\frac{s}{v}=\frac{r.s}{r.v}=\frac{s}{v}$$

وبالتالي ، فإن r/r يشكل المحايد بالنسبة لعملية الضرب .

يمكن التحقق بسهولة أن عملية الضرب تتوزع على عملية الجمع .

ليكن r/u عنصراً غير صفري من Q، فيكون $r \neq 0$، ولذلك، فإن $r/u \in Q$ ، وبالتالي ، فإن :

$$\frac{r}{u}.\frac{u}{r}=\frac{r.u}{u.r}=\frac{r.u}{r.u}=1$$

وبما أن $r.u \neq 0$ ، فإن $\frac{r.u}{r.u}$ هو العنصر المحايد ، لذلك فإن $(r/u)^{-1}=u/r$.

وهكذا ، فإن (Q,+,•) حقل .

نستنتج مما سبق أن (Q,+,•) حلقة إبدالية بمحايد .

قبل أن نقدم مبرهنة الغمر ، نعرّف الحلقة المغمورة .

تعريف :

لتكن (R,+,•) و(R′,+,•) حلقتين ما ، نقول إن الحلقة (R′,+,•) مغمورة Imbedded في الحلقة (R,+,•) ، إذا وُجِدَتْ حلقة جزئية من R تشاكل الحلقة (R′,+,•) .

مبرهنة الغمر (21) Embedding theorem :

كل حلقة تامة يمكن غمرها بحقل قواسمها .

البرهان :

إذا كانت $(R,+,\cdot)$ حلقة تامة، وليكن $(F,+,\cdot)$ حقل قواسمها وإذا عرّفنا التطبيق : $\Psi:R \longrightarrow F$ بالشكل :

$$\Psi(r') = r/1 \;\; ; \;\; r' \in R \;\; [r,1] = r/1$$

لنثبت أن التطبيق Ψ تشاكل :

$$\Psi(r+s) = (r+s)/1 = r/1 + s/1 = \Psi(r) + \Psi(s)$$

$$\Psi(r \cdot s) = (r \cdot s)/1 = r/1 \cdot s/1 = \Psi(r) \cdot \Psi(s)$$

إذن التطبيق Ψ تشاكلاً .

ولنثبت أن Ψ متباين :

إذا كان $\Psi(r) = \Psi(s)$ أي أن $r/1 = s/1$ فإن $r = s$ ، وبالتالي فإن Ψ متباين .

كما أن Ψ شامل (ينتج ذلك من تعريف التطبيق Ψ) .

نستنتج مما سبق أن $R \cong \Psi(R) = F$.

مثال (16) :

إذا كانت الحلقة $(Z,+,\cdot)$ حلقة الأعداد الصحيحة ، فإن حقل الأعداد النسبية $(Q,+,\cdot)$ هو حقل القواسم للحلقة $(Z,+,\cdot)$.

ملاحظة (2) :

كما في نظرية الزمر ، يمكن برهان أن التطبيق Ψ متباين بالطريقة التالية :

ليكن $a \in \operatorname{Ker}\Psi$ ، فإن $\Psi(a) = 0$ ، وبالتالي ، فإن $\psi(a) = \frac{0}{1}$ ، ومن جهة ثانية $\psi(a) = \frac{a}{1}$ ، وبالتالي يكون $\frac{a}{1} = \frac{0}{1} \Rightarrow a = 0$ ، أي أن $\operatorname{Ker}\Psi = \{0\}$ ، أي أن Ψ متباين .

ملاحظة (3) :

يمكن كتابة كل عنصر r/u في Q بالصيغة التالية :

$$\frac{r}{u}=\frac{r}{1}.\frac{1}{u}=\frac{r}{1}.\left(\frac{1}{u}\right)^{-1}=r.u^{-1}\ ;\ r\in R\ ,\ u\in R^{*}$$

لأن كل حلقة تامة تغمر في حقل قواسمها ، وبالتالي ، فإنه يمكن مطابقة كل عنصر $a\in R$ مع صورته $a/1$ في Q ، لذلك نعتبر أن $(R,+,\bullet)$ حلقة جزئية من حقل قواسمها $(Q,+,\bullet)$.

نتيجة (6) :

لتكن $(R,+,\bullet)$ حلقة تامة ، إن أي حقل ، وليكن $(F,+,\bullet)$ يحوي R سيحوي حقل قواسمها .

البرهان :

ليكن $r.u^{-1}\in Q$ ، وبالتالي ، فإن $r,u\in R$ و $u\neq 0$ ، لذلك ، فإن $r,u\in F$ ، وبما أن u عنصر غير صفري ، إذن $u^{-1}\in F$ ، وهكذا ، فإن $r.u^{-1}\in F$ ، وبالتالي ، فإن $F\supset Q$.

مثال (17) :

إذا كان $(R,+,\bullet)$ و $(R',+,\bullet)$ حلقتين تامتين ، وكان $(F,+,\bullet)$ و $(F',+,\bullet)$ حقلي قواسمهما على الترتيب ، وإذا كان Ψ تشاكلاً من R إلى R' ، عندئذٍ يوجد تشاكل φ من F إلى F' بحيث يكون قيد (restriction) التطبيق φ على R يساوي Ψ .

الحل :

لنعرّف التطبيق $\varphi : F \longrightarrow F'$ بالشكل :

$$\varphi(a.b^{-1})=\Psi(a)\,.\,\Psi(b^{-1})\quad ;\quad a.b^{-1}\in F$$

بما أن $b\neq 0$ و Ψ تشاكل ، فإن $\Psi(b)\neq 0$.

لنثبت أولاً ، أن التطبيق φ حسن التعريف ، من أجل ذلك ، نفرض $a.b^{-1}=c.d^{-1}$، وبالتالي ، فإن $a.d=c.b$. كذلك ، فإن $\Psi(a.d)=\Psi(c.b)$ ، وهذا يعني أن :

$$\Psi(a)\,.\,\Psi(d)=\Psi(c)\,.\,\Psi(b)$$

أي أن :

$$\Psi(a).(\Psi(b))^{-1} = \Psi(c).(\Psi(d))^{-1}$$

أي أن :

$$\varphi(a.b^{-1}) = \varphi(c.d^{-1})$$

إذن φ حسن التعريف .

لنبرهن أن φ تشاكلاً .

1- إذا كان $a.b^{-1}, c.d^{-1} \in F$ ، عندئذٍ ، يكون :

$$\begin{aligned}\varphi(a.b^{-1} + c.d^{-1}) &= \varphi[(a.d + c.b)(b^{-1}.d^{-1})] = \varphi[(a.d + b.c)(d.b)^{-1}]\\ &= \Psi(a.d + b.c)(\Psi(d.b))^{-1}\\ &= (\Psi(a).\Psi(d) + \Psi(b).\Psi(c)) + (\Psi(d).\Psi(b))^{-1}\\ &= (\Psi(a).(\Psi(b))^{-1} + \Psi(c)(\Psi(d))^{-1}\\ &= \varphi(a.b^{-1}) + \varphi(c.d^{-1})\end{aligned}$$

-2
$$\begin{aligned}\varphi[(a.b^{-1})(c.d^{-1})] &= \varphi[(a.c(bd)^{-1}] = \Psi(ac)[\Psi(bd)]^{-1}\\ &= \Psi(a)\Psi(c)(\Psi(b)\Psi(d))^{-1}\\ &= \Psi(a)\Psi(c)(\Psi(d))^{-1}(\Psi(b))^{-1}\\ &= (\Psi(a).(\Psi(b))^{-1}.\Psi(c).(\Psi(d))^{-1}\\ &= \varphi(a.b^{-1}).\varphi(c.d^{-1})\end{aligned}$$

نستنتج مما سبق أن φ تشاكلاً .

لنبرهن الآن أن φ متباين (أحادي) .

ليكن $\varphi(a.b^{-1}) = 0$ ، وهذا يعني أن $\Psi(a).(\Psi(b))^{-1} = 0$ ، أي أن $\Psi(a) = 0$ ، لأن $b \neq 0$، وبما أن Ψ متباين ، إذن $a = 0$ أي أن $a.b^{-1} = 0$ ، ومنه ينتج أن φ متباين .

لنثبت أخيراً أن φ شامل .

ليكن $c\,d^{-1} \in F'$ حيث أن $c, d \in R'$ و $d \neq 0$ ، وهذا يعني أنه يوجد $a \in R$ و $b \in R^*$ بحيث يكون $\Psi(a) = c, \Psi(b) = d$. وبالتالي، فإن $c\,d^{-1} = \varphi(a\,b^{-1})$، أي أن φ شامل .

نستنتج مما سبق أن $F \cong F'$.

(6-3) أساس جاكبسون وجذر المثالية Jacobsom Basis & Ideal radical

لتكن $(R,+,.)$ حلقة ما ، نسمي تقاطع جميع المثاليات اليسارية (اليمينيــة) فــي الحلقة R بأساس جاكبسون للحلقة R ، ونرمز له عادةً بـــ $J(R)$.

بما أن تقاطع مثاليات هي مثالية ، فإن $J(R)$ مثالية يسارية في R ، كما أنــه ، إذا كان $R \neq 0$ ، فإن $J(R) \neq R$.

نسمي تقاطع جميع المثاليات الأولية في الحلقة $(R,+,.)$ ، بالأساس الأولي للحلقــة $(R,+,.)$، ونرمز له عادةً بـــ $\text{rad}\ (R)$ ، أو نسميه جذر الحلقة R . بما أن تقاطع أسرة من المثاليات في الحلقة R هي مثالية ، فإن $\text{rad}\ (R)$ هي مثالية أيضاً في R.

نقدم الآن، بعض خواص أساس جاكبسون وجذر مثالية، مــن خــلال المبرهنــات التالية :

مبرهنة (22) :

إذا كان x عنصراً ما من الحلقة $(R,+,.)$ ، عندئذٍ الشروط التالية متكافئة :

(1) $x \in J(R)$.

(2) لكل $y \in R$ ، إن $1 - y.x$ عنصر قابل للعكس من اليسار في الحلقة R .

البرهان :

$(1) \Leftarrow (2)$

بما أن $x \in J(R)$ ، فإن x ينتمي إلى جميع المثاليات اليسارية الأعظميــة فــي الحلقة R . ليكن I مثالية يسارية أعظمية في الحلقة R ، بما أن $x \in I$ ، فــإن أي عنصر وليكن y من R يكون $y.x \in I$ ، وبالتالي فإن $1 - y.x \notin I$ ، ومنه $1 - y.x$ قابل للعكس من اليسار في الحلقة R .

$(2) \Leftarrow (1)$

نفرض العكس ، أي نفرض وجود مثالية يسارية أعظمية ولتكن K في R حيث $x \notin K$ ، ومنه $K + R.x = R$، وبالتالي يوجد عنصر من R ولــيكن y_0 بحيــث

يكون $1-y_0.x\in K$، وهذا يبين لنا أن العنصر $1-y_0.x$ غير قابل للعكس من اليسار في R ، وهذا يناقض الفرض، وبالتالي، فإن $x\in K$ ، أي أن العنصر x ينتمي إلى جميع المثاليات اليسارية الأعظمية في R ، إذن $x\in J(R)$.

تهدف المبرهنة التالية إلى تقديم العلاقة بين العناصر عديمة القوى والأساس الأولي للحلقة $(R,+,\cdot)$.

مبرهنة (23) :

ليكن x عنصراً ما من الحلقة $(R,+,\cdot)$ ، عندئذٍ الشروط التالية متكافئة :

(1) $x\in rad\,(R)$.

(2) العنصر x عديم القوى .

البرهان :

$(1) \Leftarrow (2)$

لنفرض أن x ليس عديم القوى ، باستخدام النتيجة التالية [(سنبرهنها في القسم العملي) : إذا كانت $(R,+,\cdot)$ حلقة ما ، وإذا كان $x\in R$ عنصراً ليس عديم القوى ، عندئذٍ يوجد في الحلقة R مثالية أولية لا يحوي العنصر a] . توجد مثالية أولية P في الحلقة R ، حيث $x\notin P$ ، وبالتالي، فإن $x\in rad\ (R)$ ، وهذا ينــاقض كــون العنصر x ينتمي إلى جميع المثاليات الأولية في R .

نستنتج مما سبق أن العنصر x عديم القوى .

$(2) \Leftarrow (1)$

بما أن x عنصر من R معدوم القوى ، فيوجد n من N بحيث يكون $x^n = 0$ ، إذا كان P مثالية أولية في الحلقة $(R,+,\cdot)$ ، عندئذٍ يكون $x^n\in P$ ، وبما أن المثالية P أولية فإن $x\in P$. نستنتج مما سبق أن العنصر x ينتمي إلى جميـــع المثاليـــات الأولية في R ، إذن $x\in rad\ (R)$.

نتيجة (7) :

إذا كانت $(R,+,\cdot)$ حلقة ما، عندئذٍ من أجل كل عنصر $x\in rad\ \ (R)$ يكون كلاً من العنصرين $1-x$ و $1+x$ قابل للعكس في الحلقة R .

مبرهنة (24) :

إذا كانت $(R,+,.)$ حلقة ما ، عندئذٍ القضايا التالية محققة :

(1) $J(R)$ مثالية يمينية في الحلقة R .

(2) $J(R)$ مثالية في الحلقة R .

(3) لكل $a\in J(R)$ ، فإن $1-a$ قابل للعكس في الحلقة R .

(4) $J(R)$ أكبر مثالية في الحلقة R تحقق الشرط $a\in J(R)$ ، فإن $1\text{-}a$ ، قابل للعكس في R.

(5) $x\in J(R)$ إذا ، وفقط إذا كان ، لكل $y\in R$ ، فإن $1-y.x$ قابل للعكس في الحلقة R .

(6) $J(R)$ هي تقاطع جميع المثاليات اليمينية الأعظمية في الحلقة R .

البرهان :

حسب تعريف $J(R)$ ، إن $J(R)$ مثالية يسارية في R . ليكن $r\in J(R)$ ، حسب المبرهنة قبل الأخيرة ، لكل $t\in R$ فإن $1\text{-}t.r$ قابل للقلب من اليسار في الحلقة R، وبالتالي يوجد u من R بحيث $u.(1-t.r)=1$ ، وهذا يؤدي إلى أن : $u=1+u.t.r$.

أي أن :

$$(1+r.u.t)\,(1-r.t)=1-r.t+r.u.t-r.u.t.r.t$$
$$=1+r.u.t-r\,(1+u.t.r)\,.t$$
$$=1+r.u.t-r.u.t=1$$

وهذا يعني أن العنصر $1\text{-}r.t$ قابل للعكس من اليسار .

لنبرهن أن $r.t\in J(R)$.

لدينا أياً كان $a\in R$ ، فإن $a.r\in J(R)$ ، وبالتالي ، لكل $t\in R$ ، فإن $1\text{-}(a.r)t$ ، قابل للعكس من اليسار في R ، وبالتالي $1\text{-}a\ \ (r\ \ t)$ قابل للعكس من اليسار ، ومنه

يكون $r.t \in J(R)$.

نستنتج مما سبق أن $J(R)$ مثالية يمينية في الحلقة R .

(2) من التعريف ومن (1) نجد أن (2) محققة .

(3) ليكن $a \in J(R)$ ، فإن العنصر $1\text{-}a$ قابل للعكس من اليسار في الحلقة R وبالتالي يوجد عنصر u من R ، بحيث $u\,(1\text{-}a) = 1$ ، أي أن $u - u.a = 1$ ، وبما أن $J(R)$ مثالية في الحلقة R ، فإن $1\text{-}u = -u.a \in J(R)$ ، وبالتالي ، العنصر $u = 1\text{-}(1\text{-}u)$ ، قابل للعكس من اليسار ، وهذا يؤدي إلى وجود عنصر v من R ، بحيث $v.u = 1$ ، أي أن :

$$v = v.1 = v.u\,(1 - a) = 1 - a$$

وبالتالي ، فإن $(1\text{-}a).u = 1$ ، أي أن $1\text{-}a$ عنصر قابل للعكس من اليمين ، إذن العنصر $1\text{-}a$ قابل للعكس في الحلقة R .

(4) لتكن K مثالية في الحلقة R ، بحيث $1 - b$ قابل للعكس في R ، لكل b من R ، ولنثبت أن $K \subseteq J(R)$.

ليكن $a \in K$، عندها لكل $r \in R$ يكون $r.a \in K$ ، وبالتالي ، فإن $1\text{-}r.a$ قابل للعكس في الحلقة R، أي أن $1\text{-}r.a$ قابل للعكس من اليسار في الحلقة R ، إذن $a \in J(R)$ ، إذن $K \subseteq J(R)$.

(5) إذا كان $x \in J(R)$ ، فإنه لكل عنصر y من R يكون $y.x \in J(R)$ ، وحسب الشرط (3) يكون $1\text{-}y.x$ قابل للعكس في الحلقة R. إن برهان العكس ينتج مباشرةً من المبرهنة قبل الأخيرة.

(6) الشرط السادس ينتج مباشرةً من الشروط السابقة ومن المبرهنة قبل السابقة.

تعريف الصغير :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت I مثالية يسارية (يمينية) في الحلقة R . نقول عن I إنها صغير في الحلقة R ، إذا تحقق الشرط التالي : من أجل أية مثالية يسارية (يمينية) أخرى ولتكن J من R بحيث $J + I = R$ فإن $J = R$.

من التعريف السابق ، ينتج أنه في أية حلقة $(R,+,\cdot)$ المثالية الصفرية هي مثالية صغير في الحلقة R .

يمكن بسهولة برهان ما يلي :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وإذا كانت J,I مثاليتين يساريتين أو (يمينيتين) في الحلقة R ، فإن :

1- المثالية اليسارية (اليمينية) $I + J$ هي صغير في الحلقة R .

2- إذا كانت I صغير في R و K مثالية يسارية (يمينية) في الحلقة R حيث $K \subseteq I$ ، عندها K صغير في الحلقة R .

3- $J(R)$ مثالية يسارية (يمينية) صغير في الحلقة R .

4- الشرط اللازم والكافي لكي تكون المثالية اليسارية (اليمينية) F صغير في R هو أن يكون $F \subseteq J(R)$.

5- إن $J(R)$ أكبر مثالية يسارية (يمينية) صغير في الحلقة R .

مبرهنة (25) :

إذا كانت $\varphi : r \longrightarrow S$ تشاكلاً غامراً ، عندئذٍ يتحقق ما يلي :

(1) بفرض أن I مثالية يسارية (يمينية) صغيراً في الحلقة $(R,+,\cdot)$ ، فإن $\varphi(I)$ مثالية يسارية (يمينية) صغيراً في الحلقة $(S,+,\cdot)$.

(2) $\varphi\left(J(R)\right) \subseteq J(S)$

البرهان :

1- إذا كان J مثالية يسارية في الحلقة $(S,+,\cdot)$ بحيث $\varphi(I) + J = S$ ولنبرهن أن $I + \varphi^{-1}(J) = R$.

ليكن r عنصراً من الحلقة R ، وبالتالي ، فإن $\varphi(r) \in S = \varphi(I) + J$ ومنه $\varphi(r) = \varphi(y) + x$ حيث x من J و y من I ، وبالتالي ، فإن $\varphi(r - y) = x$ ومنه $r - y \in \varphi^{-1}(J)$ ، أي أن $r \in \varphi^{-1}(J) + I$ ، ومنه $R \subseteq \varphi^{-1}(J) + I$. وبما أن

$R \subseteq \varphi^{-1}(J) + I$ ، فإن $R = \varphi^{-1}(J) + I$.

بما أن المثالية I صغيراً في الحلقة $(R,+,\cdot)$ ، فإن $\varphi^{-1}(J) = R$ أي أن $J \subseteq \varphi(R) = S$ ، أي أن $J = S$ ، وبالتالي المثالية اليسارية $\varphi(I)$ صغيراً في الحلقة $(S,+,\cdot)$.

2- إن المثالية اليسارية $J(R)$ صغير في R ، وحسب الشرط الأول (السابق) يكون $\varphi\big(J(R)\big) \subseteq J(S)$.

الفصل الرابع

حلقة كثيرات الحدود

Ring of polynomials

الفصل الرابع

حلقة كثيرات الحدود

Ring of polynomials

درسنا في المرحلة الثانوية مفهوم كثيرة الحدود ، والعمليات الجبرية عليها ، وبعض طرق تحليلها ، كما تمّت دراسة الاتصال والاشتقاق والتكامل لكثيرات الحدود . وسنبين في هذا الفصل أن كثيرات الحدود هي عناصر من حلقة ، وسندرس بعض الخواص الجبرية لهذه الحلقة .

ترتبط حلقة كثيرات الحدود بحل معادلات حتى الدرجة الرابعة ارتباطاً وثيقاً .

(1-4) تعاريف ومفاهيم أساسية Difination's :

نذكّر أولاً القارئ الكريم ، بمفهوم كثيرة الحدود .

كثيرة الحدود ، هي دالة من الشكل : $P : R \longrightarrow R$ معرفة بـ :

$$P_n(x) = a_0 + a_1 x + a_2 x^2 + \ldots.. + a_n x^n + \ldots$$

أو بالشكل $P_n(x) = \sum_{i=0}^{\infty} a_i . x^i$. حيث أن المتحول x والمعاملات a_i ، $i = 0,1,2,\ldots,n$ تنتمي إلى R أو إلى C حيث C مجموعة الأعداد المركبة .

من المفهوم السابق ، نرى أن كثيرة الحدود ، يمكن التعبير عنها بالمتتابعة (والتي هي جملة من المعاملات) : $(a_0,a_1,\ldots,a_n,\ldots)$.

سنعمم مفهوم كثيرة الحدود ، وذلك بأن نستعيض عن مجموعة الأعداد الحقيقية R بحلقة ما .

لتكن $(R,+,\cdot)$ حلقة ما ، ولنرمز لصفرها بـ o ، نسمي كل متوالية من الشكل :

$$P = (a_n) = (a_0,a_1,a_2,\ldots..,a_n,\ldots)$$

حيث أن $a_i \in R$ من أجل $i = 0,1,2,\ldots,n$.

وحيث أن جميع حدود المتوالية بدءاً من حد معين ، معدومة ، بكثيرة حدود على الحلقة $(R,+,\cdot)$ (لا نقصد هنا أن R مجموعة الأعداد الحقيقية) .

إذا كانت جميع المعاملات a_i حيث أن $i = 0,1,\ldots,n$ أصفاراً ، فإن P تسمى بكثيرة حدود صفرية على الحلقة $(R,+,\cdot)$ ، ونكتب $P(x) = 0$.

نسمي كثيرة حدود واحدية (Monit polynomial) إذا كان معامل a_n يساوي الواحد . فمثلاً كثيرة الحدود $P_3(x) = 2x^3 - 4x + 5$ ليست واحدية، بينما كثيرة الحدود : $P_7(x) = x^7 - 6x^3 + x - 1$ كثيرة حدود واحدية .

إذا كانت $P = (a_n)$ و $Q = (b_n)$ كثيرتي حدود على الحلقة $(R,+,\cdot)$ ، فإننا نقول ، إن $P = Q$ ، إذا كان $a_n = b_n$ ، لكل $n = 0,1,2,\ldots$.

لتكن $(R,+,\cdot)$ حلقة ما ، ولنرمز لصفرها بـ 0 ، وليكن $P = (a_n) \neq 0$ كثيرة حدود على الحلقة R ، إذا كان n أكبر عدد صحيح من أجله يكون $a_n \neq 0$ ، فإننا نسمي n بدرجة كثيرة الحدود P، ونرمز لذلك بـ $\deg P_n(x) = n$. نسمي عادةً العناصر $a_0,a_1,\ldots,a_n$ بمعاملات كثيرة الحدود .

يصطلح ، عادةً ، على اعتبار أن درجة كثيرة الحدود الصفري تساوي $-\infty$.

لنعرّف الآن عمليتي الجمع والضرب على المجموعة P في الحلقة $(R,+,\cdot)$ التالية:

$$P = \{f = (a_0,a_1,\ldots,a_n,\ldots) \; ; a_i \in R\}$$

بالشكل التالي :

$$f + g = (a_n) + (b_n) = (a_n + b_n)$$
$$f \cdot g = (a_n) \cdot (b_n) = (r_n) \; ; \; r_n = \sum_{i+j=n} a_i . b_j$$

لكل : $f = (a_n)$, $g = (b_n)$, $n = 0,1,2,\ldots$

ملاحظة (1) :

لتكن $(R,+,\cdot)$ حلقة بمحايد (عنصرها المحايد هو 1) ولنرمز لصفرها بـ 0 ، ولنعتبر ، أنه لا فرق بين أي عنصر a من الحلقة R وكثيرة الحدود $(a,0,0,..,0,..)$ ، وإذا رمزنا لكثيرة الحدود $(0,1,0,..,0,..)$ بالرمز x ، عندئذٍ

يكون :

$$x^2 = (0,0,1,0,\ldots,0,\ldots)$$
$$x^3 = (0,0,0,1,0,\ldots,0,\ldots)$$

وبصورة عامة ، إذا كان t عدداً صحيحاً غير سالب، فإن:
$x^t = (c'_n)\ ;\ c'_t = 1, c'_n = 0$ لكل $n \neq t$.

مبرهنة (1) بناء حلقة كثيرات الحدود Construct the ring of polynomials

لتكن $(R,+,.)$ حلقة ما ، ولتكن S مجموعة كل كثيرات الحدود على الحلقة R ، وإذا كانت $\star , \Delta$ عمليتين جبريتين ثنائيتين معرفتين على المجموعة S بالشكل :

لكل $(a_n),(b_n)$ من S ،
$$(a_n)\star(b_n) = (a_n + b_n)$$
$$(a_n)\ \Delta\ (b_n) = (r_n)\ ;\ r_n = \sum_{i+j=n} a_i.b_j\ ,\ n = 0,1,2,\ldots$$

عندئذٍ يتحقق ما يلي :

1) $(S,\star,\Delta)$ حلقة ، وإذا كانت الحلقة $(R,+,.)$ بمحايد فإن الحلقة $(S,\star,\Delta)$ بمحايد أيضاً .

2) إذا كانت $(R,+,.)$ حلقة تامة ، فإن $(S,\star,\Delta)$ حلقة تامة أيضاً .

البرهان :

(1) من الواضح أن $(S,\star)$ زمرة إبدالية ، عنصرها المحايد هو كثير الحدود الصفري ، ومعكوس أي عنصر من S وليكن (a_n) هو $(-a_n)$ حيث أن $-a_n$ هو معكوس a_n في R بالنسبة لعملية الجمع (+) .

لنبرهن أن العملية Δ تجميعية على عناصر S .

إذا كان $(a_n),(b_n),(c_n)$ ثلاثة عناصر من S ، وإذا وضعنا :

$$(a_n)\ \Delta\ \left[(b_n)\ \Delta\ (c_n)\right] = \left[(a_n)\ \Delta\ (b_n)\right]\ \Delta\ (c_n)$$
$$(a_n)\ \Delta\ (c_n) = (w_n)\ \ \&\ \ (a_n)\ \Delta\ (w_n) = (u_n)$$

عندئذٍ ، من أجل كل عدد صحيح $n \geq 0$ ، يكون لدينا :

$$u_n = \sum_{i+q=n} a_i . w_q = \sum_{i+q=n} a_i . \left(\sum_{j+k=q} b_j . c_k \right)$$
$$= \sum_{i+q=n} \sum_{j+k=q} a_i . (b_j . c_k) = \sum_{i+q=n} \sum_{j+k=q} a_i . b_j . c_k$$
$$= \sum_{i+j+k=n} a_i . b_j . c_k \qquad (1)$$

وبوضع :

$$(r_n) \Delta (c_n) = (v_n) \ , \ (a_n) \Delta (b_n) = (r_n)$$

عندها ، من أجل كل عدد صحيح $n \geq 0$ ، يكون لدينا :

$$v_n = \sum_{h+k=n} r_h . c_k = \sum_{h+k=n} \left(\sum_{i+j=h} a_i . b_j \right) . c_k$$
$$= \sum_{h+k=n} \sum_{i+j=h} (a_i . b_j) . c_k = \sum_{h+k=n} \sum_{i+j=h} a_i . b_j . c_k$$
$$= \sum_{i+j+k=n} a_i . b_j . c_k \qquad (2)$$

من العلاقتين (1) و(2) نجد أن : $u_n = v_n$ ، لكل $n = 0,1,2,\ldots$ ، وبالتالي فإن : $(u_n) = (v_n)$، أي أن :

$$(a_n) \Delta (w_n) = (r_n) \Delta (c_n)$$

ومنه يكون :

$$(a_n) \Delta \left[(b_n) \Delta (c_n) \right] = \left[(a_n) \Delta (b_n) \right] \Delta (c_n)$$

لنبرهن الآن ، على تحقق قانوني التوزيع .

العمليتان $\Delta, \star$ ترتبطان فيما بينهما بقانوني التوزيع ، وذلك ، لأنـــه : إذا كانـــت $(c_n),(b_n),(a_n)$ ثلاثة عناصر من S ، وإذا وضعنا :

$$(a_n) \Delta \left[(b_n) \Delta (c_n) \right] = (a_n) \Delta (b_n + c_n) = (S_n)$$
$$(a_n) \Delta (b_n) = (r_n) \ , \ (a_n) \Delta (c_n) = (t_n)$$

عندها يكون من أجل كل عدد صحيح $n \geq 0$ ، يكون :

$$S_n = \sum_{i+j=n} a_i . (b_j + c_j) = \sum_{i+j=n} (a_i . b_j + a_i . c_j)$$

$$= \sum_{i+j=n} a_i . b_j + \sum_{i+j=n} a_i . c_j = r_n + t_n$$

وبالتالي يكون : $(S_n) = (r_n + t_n)$

أي أن : $(S_n) = (r_n) \star (t_n)$

ومنه يكون :

$$(a_n) \, \Delta \, [(b_n) \star (c_n)] = [(a_n) \, \Delta \, (b_n)] \star [(a_n) \, \Delta \, (c_n)]$$

وبالطريقة ذاتها ، يمكن البرهان على أن :

$$[(b_n) \star (c_n)] \, \Delta \, (a_n) = [(b_n) \, \Delta \, (a_n)] \star [(c_n) \, \Delta \, (a_n)]$$

نستنتج مما سبق أن : $(S, \star, \Delta)$ حلقة .

(2) نفرض أن $(R, +, .)$ حلقة بمحايد ، وإذا رمزنا لعنصر الوحدة فيها بـ 1 ، فإن المتوالية (I_n) حيث أن : $n \neq 0 \, , \, I_0 = 1 \, , \, I_n = 0$ هي عنصر الوحدة في الحلقة $(S, \star, \Delta)$.

(3) لنبرهن الآن ، أن $(S, \star, \Delta)$ حلقة تامة ، علماً أن $(R, +, .)$ حلقة تامة .

برهنّا سابقاً أن $(S, \star, \Delta)$ حلقة بمحايد ، ولنبرهن أنها إبدالية .

ليكن $(b_n), (a_n)$ عنصرين ما من الحلقة $(S, \star, \Delta)$ ، وبوضع :

$$(a_n) \, \Delta \, (b_n) = (r_n) \quad , \, (b_n) \, \Delta \, (a_n) = (r'_n)$$

عندها يكون ، لكل عدد صحيح $n \geq 0$:

$$r_n = \sum_{i+j=n} a_i . b_j = \sum_{i+j=n} b_j . a_i = r'_n$$

وبالتالي فإن $(r_n) = (r'_n)$ ، أي أن :

$$(a_n) \, \Delta \, (b_n) = (b_n) \, \Delta \, (a_n)$$

لنبرهن الآن أن الحلقة $(S, \star, \Delta)$ لا تحوي قواسم للصفر .

بفرض أن $P = (d_n) \neq 0 \, , \, q = (h_n) \neq 0$ عنصرين ما من الحلقة $(S, \star, \Delta)$، وإذا فرضنا أن :

$\deg P = m_2 \, , \, \deg q = m_1$، وإذا وضعنا $(h_n) \, \Delta \, (d_n) = (g_n)$، عندها يكـون

لدينا :

$$d_{m_2} \neq 0 \,,\, h_{m_1} \neq 0$$

وبالتالي يكون :

$$h_{m_1}.d_{m_2} \neq 0 \;\Rightarrow g_{m_1+m_2} \neq 0$$

إذن :

$$P \Delta q \neq 0$$

نستنتج مما سبق أن $(S,\star,\Delta)$ حلقة تامة .

مبرهنة (2) :

بالاستفادة من فرضيات المبرهنة السابقة، وإذا كان $g = (v_n) \neq 0, f = (u_n) \neq 0$ كثيرتي حدود على الحلقة R ، وإذا فرضنا أن $\deg u_n = n_1 \,,\, \deg v_n = n_2$ ، فإن :

1- $f \Delta g$ إما أن تكون كثيرة حدود صفرية ، أو أن تكون :

$$\deg(f \Delta g) \leq n_1 + n_2$$

2- الشرط اللازم والكافي لكي تكون : $\deg(f \Delta g) = n_1 + n_2$ ، هو أن يكون $u_{n_1}.v_{n_2} \neq 0$.

البرهان :

(1) بوضع $(u_n) \Delta (v_n) = (w_n)$ يكون لدينا :

$$w_{n_1+n_2} = u_{n_1}.v_{n_2} \qquad (1)$$

وإذا كان $n > n_1 + n_2$ ، فإن :

$$w_n = 0 \qquad (2)$$

فإذا كان $u_{n_1}.v_{n_2} \neq 0$ فمن العلاقتين السابقتين نجد أن :

$$\deg(f \Delta g) = n_1 + n_2$$

أما إذا كان $u_{n_1}.v_{n_2} = 0$ ، فمن العلاقتين (1) و(2) نجد ، أنه إما أن يكون :

$f \Delta g = 0$ أو $\deg(f \Delta g) \leq n_1 + n_2$

(2) بفـــرض أن $\deg(f \Delta g) = n_1 + n_2$ ، فإنـــه يكـــون : $w_{n_1+n_2} \neq 0$ ،
وبالتالي من العلاقة (1) نجد أن :

$$u_{n_1}.v_{n_2} \neq 0$$

لنبرهن على العكس، إذا كان $u_{n_1}.v_{n_2} \neq 0$ ، فإنه من العلاقتين (1) و(2) نجد أن:

$$\deg(f \Delta g) = n_1 + n_2$$

مبرهنة (3) :

بالاستفادة من فرضيات المبرهنة السابقة ، وإذا كان K مجموعة كل كثيـــرات الحدود التي هي من الشكل :

$$(a,0,0,\ldots,0,\ldots) \ ; \ a \in R$$

فإن : (1) $(K,\star,\Delta)$ حلقة جزئية من الحلقة $(S,\star,\Delta)$.

(2) $(R,+,.) \cong (K,\star,\Delta)$

البرهان :

(1) ليكن b,a عنصرين ما من الحلقة $(R,+,.)$ ، عندها :

$$(a,0,\ldots,0,\ldots)\ \Delta\ (b,0,\ldots,0,\ldots) = (a.b,0,0,\ldots,0,\ldots) \in K$$

$$\begin{aligned}(a,0,\ldots,0,\ldots)\star\left[-(b,0,\ldots,0,\ldots)\right] &= (a,0,\ldots,0,\ldots)\star(-b,0,\ldots,0,\ldots)\\ &= (a-b,0,0,\ldots,0,\ldots) \in K\end{aligned}$$

وبملاحظة أن $\phi \neq K \subseteq S$ ، يتبين لنا أن $(K,\star,\Delta)$ حلقة جزئيـــة مـــن الحلقـــة $(S,\star,\Delta)$.

(2) لنعرّف التطبيق : $\varphi : R \longrightarrow K$ بالشكل : $\varphi(x) = (x,0,..,0,..)$ ، لكل x من R ، وبالتالي يكون لدينا ، لكل y,x من R :

$$\begin{aligned}\varphi(x+y) &= (x+y,0,\ldots,0,\ldots) = (x,0,..,0,..)\star(y,0,..,0,..)\\ &= \varphi(x)\star\varphi(y)\end{aligned}$$

$$\begin{aligned}\varphi(x.y) &= (x.y,0,\ldots,0,\ldots) = (x,0,..,0,..)\ \Delta\ (y,0,..,0,..)\\ &= \varphi(x)\ \Delta\ \varphi(y)\end{aligned}$$

لنبرهن الآن أن التطبيق φ متبايناً :

إذا كان y,x عنصرين ما من R بحيث يكون : $\varphi(x) = \varphi(y)$ ، فإن :

$$(x,0,..,0,..) = (y,0,..,0,..)$$

ومنه يكون : $x = y$.

بالإضافة إلى ذلك ، إذا كان $(z,0,\dots,0,\dots)$ عنصراً ما من K فإن z ينتمي إلى R من جهة ، ومن جهة ثانية ، إن : $\varphi(z) = (z,0,\dots,0,\dots)$ أي أن التطبيق φ شامل .

نستنتج مما سبق أن $(R,+,\cdot) \cong (K,\star,\Delta)$.

نسمي الحلقة $(S,+,\cdot)$ الواردة سابقاً بحلقة كثيرات الحدود بمتحول واحد x على R وسنرمز لـ S بـ $R[x]$.

ملاحظة (2) :

العمليتان الجبريتان الثنائيتان $\Delta,\star$ المعرفتان على الحلقة $(S,\star,\Delta)$ ، بالشكل الوارد في المبرهنة السابقة ، سنرمز لهما بالرمزين $(\cdot)$ و$(+)$ على الترتيب . ويجب التمييز بين العمليتين $\star,+$ حتى لو رمزنا لهما بالرمز نفسه ، كذلك من الضروري التمييز بين العمليتين Δ و$(\cdot)$ حتى لو رمزنا لهما بالرمز نفسه .

تعريف (3) قيمة كثيرة حدود Evaluation of polynomial :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت : $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ كثيرة حدود في $R[x]$ ، وليكن a عنصراً ما من مركز الحلقة $Z(R)$ عندئذ : العنصر :

$$f(a) = a_0 + a_1a + a_2a^2 + \dots + a_na^n$$

من R والذي نحصل عليه بتبديل كل x بـ a في $f(x)$ ، يسمى بقيمة كثيرة الحدود $f(x)$ في النقطة a .

(2-4) أمثلة :

<u>1-</u> إذا كان $f(x) = a_0 + a_1x + a_2x^2$, $g(x) = b_0 + b_1x$ ، فإن :

$$f(x).g(x) = a_0b_0 + (a_0b_1 + a_1b_0)\,x + (a_1b_1 + a_2b_0)\,x^2 + a_2b_1\,x^3$$

حيث أن $a_0,a_1,a_2,b_0,b_1 \in R$.

-2 أوجد ناتج ما يلي في حلقة كثيرات الحدود $(Z[x],+,.)$.

$$(1 - 2x + x^3).(2 - x + x^2)$$

ثم اكتب $(x + 1)^3$ في الحلقة $(Z_3[x],+,.)$.

الحل :

في الحلقة $Z[x]$ يكون لدينا :

$$(1 - 2x + x^3).(2 - x + x^2) = 2 - 5x + 3x^2 - x^4 + x^5$$

أما في الحلقة $Z_3[x]$ فإن :

$$(x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x^3 + 1$$

لأن $3 = 0$ في Z_3 .

-3 إن كثيرة الحدود $f(x) = x - x^2 + 2x^3$ من الدرجة الثالثة ، بينما كثيرة الحدود $g(x) = x + 2$ فهي من الدرجة الأولى ، أما كثيرة الحدود $h(x) = -5$ فهي من الدرجة صفر .

-4 إذا كان $f(x) = 1 + 2x$، أوجد $f^2(x)$ في الحلقة $(Z_4[x],+,.)$ و $\deg[f(x).f(x)]$ و $\deg f(x) + \deg f(x)$.

الحل :

$$(f(x))^2 = (1 + 2x)\,(1 + 2x) = 1 + (2+2)\,x + 2^2.x = 1$$

لأن $4 = 0$ في Z_4 .

لدينا :

$$\deg\,[f(x).f(x)] = \deg 1 = 0$$

بينما :

$$\deg f(x) + \deg f(x) = 1 + 1 = 2$$

لاحظ أن :

$$\deg\left[f(x).f(x)\right] \neq \deg f(x) + \deg f(x)$$

والسبب هو أن $(Z_4[x],+,\cdot)$ ليست حلقة تامة .

5- لتكن $(R,+,\cdot)$ حلقة الأعداد الحقيقية، إذا كان a عنصراً من مركز الحلقة $Z(R)$، أثبت أن التطبيق: $\varphi_a:R[x] \longrightarrow R$ المعرف بالشكل: $\varphi_a[f(x)] = f(a)$ تشاكلاً حلقياً .

الحل :

ليكن : $f(x) = a_0 + a_1x + \ldots.\;,\; g(x) = b_0 + b_1x + \ldots.$

كثيرتي حدود من $R[x]$. عندئذٍ :

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)\,x + \ldots.$$

ومنه يكون :

$$\begin{aligned}
\varphi_a\left[f(x) + g(x)\right] &= (a_0 + b_0) + (a_1 + b_1)\,a + \ldots. \\
&= (a_0 + a_1a + \ldots) + (b_0 + b_1a + \ldots.) \\
&= \varphi_a\left[f(x)\right] + \varphi_a\left[g(x)\right]
\end{aligned}$$

كما أن :

$$f(x)\cdot g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots.$$

حيث أن لكل c_k و $k \geq 0$ المعامل c_k بالنسبة لـ x^k ، يعطى بالشكل :

$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots.. + a_kb_0$$

وبما أن العنصر a هو الحلقة R ، فيكون لدينا :

$$\begin{aligned}
\varphi_a\left[f(x)\right]\cdot\varphi_a\left[g(x)\right] &= (a_0 + a_1a + a_2a^2 + \ldots.)\cdot(b_0 + b_1a + b_2a^2 + \ldots.) \\
&= a_0b_0 + (a_0b_1a + a_1ab_0) + (a_0ba^2 + a_1aba + a_2a^2\,b_0) + \ldots.. \\
&= a_0b_0 + (a_0b_1 + a_1b_0)\,a + (a_0b_2 + a_1b_1 + a_2b_0)\,a^2 + \ldots.. \\
&= c_0 + c_1\,a + c_2\,a^2 + \ldots.. \\
&= \varphi_a\left[f(x)\cdot g(x)\right]
\end{aligned}$$

نستنتج مما سبق أن التطبيق φ_a تشاكل حلقي .

6- لتكن $f(x) = 5 + 4x - 2x^2 + x^3$, $g(x) = (x-1)(x^2 + x + 1)$

كثيرتي حدود في $(Z[x],+,\cdot)$ ، أوجد $f(3)$, $g(3)$.

الحل :

$$f(3) = 5 + 4.3 - 2(3)^2 + (3)^3 = 26$$

$$g(3) = (3-1)(3^2 + 3 + 1) = 26$$

7- لتكن $f(x) = x^3 - x$ في الحلقة $(Z_6[x],+,\cdot)$ ، أثبت أن $f(a) = 0$ لكل a من Z_6 .

الحل :

نلاحظ أولاً أن $a^3 = a$ لكل a من Z_6 ، وبالتالي يكون : $f(a) = a^3 - a = 0$.

تعريف (1) :

لتكن $(R,+,\cdot)$ حلقة إبدالية ، وإذا كان a عنصراً منها ، عندئذٍ نواة التطبيق φ_a.

حيث أن :

$\varphi_a : R[x] \longrightarrow R$ تعطى وفق المجموعة التالية :

$$\text{Ker}\, \varphi_a = \{f(x) \in R[x] : f(a) = 0\}$$

(3-4) خوارزمية القسمة (Division algorithm) :

إذا كانت $f(x) = \sum_{i=0}^{n} a_i . x^i$, $g(x) = \sum_{i=0}^{m} b_i . x^i$ كثيرتي حدود غير صفريتين

ولنفرض أن b_i قابل للعكس في R في الحلقة الإبدالية وبمحايد $(R[x],+,\cdot)$

ولنرمز لصفرها بـ 0 ، عندئذٍ توجد كثيرتا حدود وحيدتان $q(x), r(x)$ من $R[x]$،

بحيث يتحقق :

$$f(x) = g(x).q(x) + r(x)$$

و $r = 0$ أو $\deg r < \deg g$.

البرهان :

لنفرض، أولاً، أن $\deg f = n < \deg g = m$، وبأخـذ $q(x) = 0$ و $r(x) = f(x)$ نجد المطلوب .

نفرض الآن أن $n > m$ وباستخدام الاستقراء الرياضي على العدد n نبرهن ذلك .

فإذا كان $n = m = 0$، فـإن $r = 0 , f(x) = \alpha , g(x) = \beta \in R$ ومنـه يكـون: $f = (\alpha.\beta^{-1}).g + 0$ وبالتالي ، المبرهنة محققة .

لنفرض الآن ، أن المبرهنة صحيحة ، من أجل كثيرة الحدود $f(x)$ مـن $R[x]$ ، والتي تكون من أجلها $\deg f \leq n-1$ ، ولنبرهن على صحتها من أجل $\deg f = n$، علماً أن $b_m \neq 0 , a_n \neq 0$.

من أجل ذلك نعرّف كثيرة الحدود :

$$f_1(x) = f(x) - \left(\frac{a_n}{b_m}\right) x^{n-m}.g(x) \qquad (1)$$

فـي الحلقـة $(R[x],+,\cdot)$، وبالتـالي، فـإن معامـل x^n فـي $f_1(x)$ هـو $a_n - (a_n b_m - 1).b_m = 0$ ، وبالتالي ، فإن $\deg f_1 < n$. وحسـب الاسـتقراء الرياضي توجد كثيرتا حدود $g(x),r(x) \in R[x]$ بحيث يكون :

$f_1(x) = g(x)\, q(x) + r(x)$ و $\deg r < \deg g$ أو $r = 0$.

بتعويض قيمة $f_1(x)$ من (2) في (1) نجد :

$$f(x) - \left(\frac{a_n}{b_m}\right) x^{n-m}.g(x) = g(x).q(x) + r(x)$$

ومنه يكون :

$$f(x) = \left(\frac{a_n}{b_m} x^{n-m} + q(x)\right).g(x) + r(x)$$

وبوضع $p(x) = \frac{a_n}{b_m} x^{n-m} + q(x)$ نجد أن :

$f(x) = p(x) . g(x) + r(x) \quad ; \quad p(x) , r(x) \in R[x]$

و $r = 0$ أو $\deg r < \deg g$ ، وبالتالي المبرهنة صحيحة لكل $n \in Z^+$.

لنبرهن أخيراً على وحدانية كثيرتي الحدود $r(x),q(x)$ في $R[x]$.

لتكن :

$$f(x) = q_2(x)\, g(x) + r_2(x) \;,\; f(x) = q_1(x) . g(x) + r_1(x)$$

و $\deg r_1 , \deg r_2 < \deg g \,,\; r_1 = r_2 = 0$

بطرح العلاقتين السابقتين نجد :

$$[q_1(x) - q_2(x)]\, g(x) = r_2(x) - r_1(x)$$

ومنه يكون :

$$\deg(r_2 - r_1) = \deg(q_1 - q_2) + \deg g$$

أي أن: $\deg(r_2 - r_1) \geq \deg g$ ، وهذا يناقض كون $\deg r_2 < \deg g$ و $\deg r_1$،
وبالتالي سيكون $r_1 = r_2$ و $q_1 = q_2$.

مثال (8) :

لتكن: $f(x) = x^4 + 3x^3 + x + 1$ و $g(x) = x^2 + 1$ كثيرتي حدود في الحلقة $(R[x],+,.)$. طبّق خوارزمية القسمة لإيجاد كثيرتي الحدود $r(x) , q(x)$.

الحل :

باستخدام عملية التقسيم المألوفة نجد :

$$f(x) = (x^2 + 1)\,(x^2 + 3x - 1) + (-2x + 2)$$

أي أن :

$$\deg r < \deg g = 2 \,,\; q(x) = x^2 + 3x - 1 \;,\; r(x) = -2x + 2$$

(4-4) مبرهنة (4) : مبرهنة العامل Factor theorem

لتكن $(R,+,.)$ حلقة إبدالية ذات عنصر الوحدة ، ولتكن $f(x)$ كثيرة حدود في $R[x]$ ، وإذا كان a عنصراً من R ، ولنرمز لصفرها بـ 0 ولعنصرها المحايد بـ 1 ، عندئذٍ : $f(a) = 0$ ، إذا ، وفقط إذا ، كان $f(x) = (x - a).q(x)$ ، من

أجل $q(x)\in R[x]$ (أي إذا كان $(x-a)$ قاسم لـــ $f(x)$ في $R[x]$) .

البرهان :

لنفرض أولاً أن : $f(a)=0$ ، ولنبرهن أن $x-a$ قاسم لـــ $f(x)$ في $R[x]$.
بما أن : $\deg(x-a)=1$ ، فإنه حسب مبرهنة التقسيم الخوارزمي ، يمكن إيجاد كثيرة حدود $q(x)$ من $R[x]$ وعنصر b من R بحيث يكون : $f(x)=q(x)\,(x-a)+b$ ، وبالتالي يكون : $f(a)=b$.
وبما أن $f(a)=0$ ، فإن $b=0$ ، وبالتالي فإن $f(x)=q(x)\,(x-a)$ ، وهذا يعني أن $x-a$ يقسم $f(x)$ في $R[x]$.
لنبرهن العكس : أي لنبرهن أن $f(a)=0$، علماً أن $(x-a)$ يقسم $f(x)$ في $R[x]$، بما أن $x-a$ يقسم $f(x)$ في $R[x]$ ، فإنه يمكن إيجاد كثيرة حدود $q_1(x)$ من $R[x]$ بحيث يكون : $f(x)=q_1(x)\,(x-a)$ ومنه $f(a)=0$.

(5-4) مبرهنة الباقي Remainder theorem :

لتكن$(R,+,\cdot)$ حلقة إبدالية، وإذا كان $f(x)\in R[x]$ يقسم $x-a$ ، عندئذٍ يكون الباقي هو $f(a)$.

تطبيق لمبرهنة الباقي :

لتكن $f(x)=2x^3+x+1$ كثيرة حدود في $Z_6[x]$ ، وإذا كان $a=2$ ، عندئذٍ يكون لدينا : $x-2=x+4$ في $Z_6[x]$.
تعطى خوارزمية القسمة بالشكل : $f(x)=(x-2)\,(2x^2+4x+3)+1$
لأن :

$$
\begin{array}{r|l}
 & 2x^2+4x+3 \\
\hline
x+4 & 2x^3+x+1 \\
 & 2x^3+2x^2 \\
\cline{2-2}
 & \quad 4x^2+x+1 \\
 & \quad 4x^2+4x \\
\cline{2-2}
 & \qquad 3x+1 \\
 & \qquad 3x \\
\cline{2-2}
 & \qquad\quad 1
\end{array}
$$

لاحظ أن الباقي هو 1 ويساوي $f(2)$.

تعريف (4) تعريف جذر كثيرة الحدود Root of polynomial :

ليكن $f(x) \in R[x]$، حيث $(R[x],+,\cdot)$ حلقة إبدالية ، العنصر a من R يسمى جذر لـ $f(x)$، إذا كان $f(a) = 0$.

الجذر a يسمى جذر مضاعف ، ودرجة تضاعفه هو العدد $m \geq 1$ ، إذا كان $f(x) = (x-a)^m . g(x)$ ، حيث أن $g(a) \neq 0$.

مثال (9) :

بيّن أن العدد 2 هو جذر مضاعف لـ : $f(x) = x^4 + 5x^3 + 3x^2 + 4$ في $Z_8[x]$.

الحل :

بما أن $f(2) = 0$ ، إذن العدد 2 هو جذر لـ $f(x)$ في $Z_8[x]$.

كما أن $f(x) = (x-2)\, g_1(x)$ ، حيث أن $g_1(x) = x^3 - x^2 + x + 2$

باستخدام خوارزمية القسمة . ليكن $g_1(2) = 0$ أيضاً ، لذلك نكتب :

$g_1(x) = (x-2) . g_2(x)$ ، حيث أن $g_2(x) = x^2 + x + 3$، وبما أن $g_2(x) \neq 0$، إذن :

$$f(x) = (x-2)^2\,(x^2 + x + 3)$$

إذن $a = 2$ جذر مضاعف لـ $f(x)$ ودرجة تضاعفه هي 2 .

مثال (10) :

كثيرة الحدود $x^2 + 9$ لا تملك جذوراً في حلقة الأعداد الحقيقية $(R,+,\cdot)$ ، لكنها تملك جذرين مختلفين في حلقة الأعداد المركبة $(C,+,\cdot)$ وهما $x_1 = +3i\, , x_2 = -3i$.

مثال (11) :

إن لكثيرة الحدود $x^2 - 1$ جذرين هما $+1$ و -1 في أية حلقة إبدالية لكن لها أربعة جذور وهي 7,5,3,1 في $(Z_8,+,\cdot)$.

المبرهنة الأساسية في الجبر Fundamental theorem of Algebra :

إذا كانت $f(x)$ كثيرة حدود غير ثابتة من حلقة كثيرات الحدود $(C[x],+,\cdot)$ على الحقل $(C,+,\cdot)$ ، عندها يوجد لـ $f(x)$ جذر في C حيث C حقل الأعداد المركبة .

مبرهنة (6) : مبرهنة الجذور n – Root theorem

لتكن $(R,+,\cdot)$ حلقة تامة ، وإذا كان $f(x)$ كثيرة حدود غير صفرية من الدرجة n في $R[x]$ عندئذٍ $f(x)$ تملك n جذراً في R (ليس من الضروري أن تكون جميعها مختلفة) .

البرهان :

باستخدام الاستقراء الرياضي على n حيث $n = \deg f(x)$.

إذا كان $n = 0$ ، فإن $f(x)$ كثيرة حدود ثابتة (غير معدومة) ، وفي هذه الحالة لا تملك $f(x)$ جذوراً .

إذا كان $n = 1$ ، فإن $f(x) = a_0 + a_1.x$ حيث أن $a_1 \neq 0$ ، وليكن b,a جذران لـ $f(x)$ ، عندها يكون $a_0 + a_1.a = 0 = a_0 + a_1.b$ ، وبالتالي $a_1 (b - a) = 0$ ، ومنه يكون $b - a = 0$ لأن R حلقة تامة .

لنفرض الآن $n > 1$.

إذا كانت $f(x)$ لا تملك جذوراً في r ، فإنه يكون قد اكتمل البرهان .

إذا كان $f(a) = 0$ حيث أن : a من R ، عندئذٍ نستطيع كتابة حسب مبرهنة العامل $f(x) = (x - a).g(a)$ ، حيث أن $\deg g(x) = n - 1$. لنفرض أن b هو جذر لـ $f(x)$ ومختلف عن a ، عندها يكون :

$$0 = f(b) = (b - a)\, g(b)$$

لذا $g(b) = 0$ ، لأن R حلقة تامة . لكن كثيرة الحدود $g(x)$ تملك $(n-1)$ جذراً في R (حسب الاستقراء الرياضي) لذلك يكون لـ $f(x)$ على الأكثر $(n-1)$ جذراً مختلفاً عن الجذر a وبالتالي، فإن كثيرة الحدود $f(x)$ تملك n جذراً في R .

مثال (12) :

حدّد عدد وجذور كثيرة الحدود التالي :

$$f(x) = (x^2 - 4)^2 (x^2 - 5x + 6)$$

الحل :

بما أن درجة $f(x)$ هي 6 ، فسيكون لـــ $f(x)$ ستة جذور على الأكثر(قد يكون بعضاً منها مكرراً).

$$\begin{aligned} f(x) &= (x^2 - 4)^2 (x^2 - 5x + 6) \\ &= (x - 2)^2 (x + 2)^2 (x - 2) (x + 3) \\ &= (x - 2)^3 (x + 2)^2 (x + 3) \end{aligned}$$

إن جذور $f(x)$ هي : $\{2,2,2,-2,-2,-3\}$.

مبرهنة الجذور النسبية (الكسرية) Rational roots theorem

لتكن $f(x) = a_0 + a_1x + \ldots + a_nx^n$ كثيرة حدود في حلقة الأعداد الصحيحة $(Z[x],+,.)$ ، حيث أن $a_0 \neq 0$ و $a_n \neq 0$ ، وبفرض أن $c/d \in Q$ جذراً لـــ $f(x)$ حيث Q مجموعة الأعداد النسبية، وبحيث $\gcd(c,d) = 1$ ، عندئذٍ c/a_0 و d/a_n.

البرهان :

لدينا : $0 = f(c/d) = a_0 + a_1c/d + \ldots + a_nc^n/d^n$

نضرب طرفي العلاقة السابقة بـــ d^n نحصل على :

$$0 = a_0 d^n + a_1cd^{n-1} + \ldots + a_{n-1}c^{n-1}.d + a_n.c^n$$

بما أن c يدخل في كل تركيب من التراكيب السابقة ما عدا الأول منها لذا يكـــون c/a_0d^n . وبما أن $\gcd(c,d^n) = 1$ ، ومنه يكون c/a_0 وبشكل مشابه يكون d/a_n.

ملاحظة (3) :

استخدمنا في البرهان السابق الحقيقة الرياضية التالية :

إذا كان n,m عددان أوليان نسبياً ، أي $(m,n) = 1$ ، فإن :

1- إذا كان m/k , n/k ، لكل k عدد صحيح ، فإن : $m.n/k$

2- إذا كان $m/k.n$ ، لكل k عدد صحيح ، فإن : m/k .

المثال التالي يوضح المبرهنة السابقة :

مثال (13) :

ليكن $f(x) = 3x^3 - x^2 - x - 4$ في $Q[x]$ ، طبّق نظرية العامل لـ $f(x)$ في $Q[x]$.

الحل :

إذا كان c/d (عدداً نسبياً) جذراً لـ $f(x)$ ، فإن $c/(-4)$ و $d/3$ حسب المبرهنة السابقة .

بما أن $c = \pm1,\pm2,\pm4$ و $d = \pm1,\pm3$ وبالتالي فإن الإمكانات المتاحة لـ c/d هي:

$$c = \pm1 , \pm2 , \pm4 , \pm1/3 , \pm2/3 , \pm4/3$$

إن $4/3$ هو جذر لـ $f(x)$ ، وبالتالي ، فإن $x-\frac{4}{3}$ العامل لـ $f(x)$ في $Q[x]$.

وبما أن $(3x - 4)$ هو عامل في $Q[x]$ وباستخدام مبرهنة التقسيم الخوارزمي ، نجد أن :

$$f(x) = (3x - 4)(x^2 + x + 1)$$

ومن الواضح أنه ليس لـ $(x^2 + x + 1)$ جذوراً في $Q[x]$.

ملاحظة (4) :

سنرمز لحلقة كثيرات الحدود على الحقل $(F,+,\cdot)$ بالرمز $F[x]$.

(6-4) القاسم المشترك الأعظم لكثيرات الحدود

Greatest common divisor of polynomails

تعريف القاسم المشترك الأعظم لكثيرات الحدود :

إذا كانت $(F[x],+,\cdot)$ حلقة كثيرات الحدود على الحقل $(F,+,\cdot)$ ، وبفرض أن $f(x)$ و $g(x)$ كثيرتي حدود غير صفريتين على $F[x]$. نقول عن كثيرة حدود

$d(x)$ من $F(x)$ إنها قاسم مشترك أعظم لكثيرتي الحدود $f(x)$ و$g(x)$ إذا تحقق ما يلي :

1- $d(x)/g(x)$, $d(x)/f(x)$

2- إذا وُجِدَتْ كثيرة حدود، ولتكن $h(x) \in F(x)$، بحيث $h(x)/f(x)$ و$h(x)/g(x)$، فإن $h(x)/d(x)$

نرمز عادةً للقاسم المشترك الأعظم لكثيرتي الحدود $f(x)$ و$g(x)$ في $F[x]$ بالرمز $(f(x),g(x))$.

المبرهنة التالية ، تبيّن لنا على وجود ووحدانية القاسم المشترك الأعظم $d(x)$.

مبرهنة (7) :

لتكن $(F[x],+,.)$ حلقة كثيرات الحدود على الحقل $(F,+,.)$ ، وإذا كانت $f(x)$ و$g(x)$ كثيرتي حدود غير صفريتين في $F[x]$، عندئذٍ يوجد لهما قاسم مشترك أعظم وحيد $d(x)$ يعطى بالعلاقة :

$$d(x) = \alpha(x).f(x) + \beta(x).g(x) \ ; \ \forall \ \alpha(x),\beta(x) \in F[x]$$

البرهان :

باستخدام مبرهنة التقسيم الخوارزمي نجد :

$$f(x) = q_1(x).g(x) + r_1(x) \ ; \ \deg r_1(x) < \deg g(x)$$

$$g(x) = q_2(x).r_1(x) + r_2(x) \ ; \ \deg r_2(x) < \deg r_1(x)$$

....

$$r_{k-2}(x) = q_k(x).r_{k-1}(x) + r_k(x) \ ; \ \deg r_k(x) < \deg r_{k-1}(x)$$

$$r_{k-1}(x) = q_k(x).r_k(x) + 0$$

نستنتج مما سبق أن $r_k(x)$ قاسم لكثيرتي الحدود $f(x)$ و$g(x)$ ، وإذا استخدمنا المعادلات الأخيرة من الأسفل نحو الأعلى نستطيع إيجاد كثيرتي الحدود $\alpha(x),\beta(x)$ من $F[x]$ بحيث يكون :

$$d(x) = \alpha(x).f(x) + \beta(x).g(x)$$

لنثبت الآن على الوحدانية . من أجل ذلك ، نفرض وجود قاسم مشترك آخر لكثيرتي الحدود $f(x)$ و$g(x)$ وهو $L(x)$ ، وبالتالي يكون : $L(x)/f(x)$ و$L(x)/f(x)$، ومنه يكون : $d(x)/L(x)$ و $L(x)/d(x)$ ، إذن $L(x) = d(x).n(x)$ و $d(x) = L(x).m(x)$ ، إذن : $d(x) = d(x).m(x).n(x)$. وبما أن $F(x)$ حلقة تامة، إذن $m(x).n(x) = 1$، وبالتالي، فإن كل من كثيرتي الحدود $m(x)$ و$n(x)$ عدد ثابت، إذن: $d(x) = L(x)$.

مبرهنة (8) :

إذا كانت $(F[x],+,\cdot)$ حلقة كثيرات الحدود على الحقل F ، فإن هذه الحلقة تشكل حلقة إقليدية .

البرهان :

نشكّل الدالة الإقليدية : $d:F^*[x] \longrightarrow N$ بالشكل التالي : $d(f) = \deg f$

وبسهولة ، نتحقق من الشروط :

(1) $d(f) \geq 0$ لكل f من $F^*[x]$.

(2) من أجل أي $f(x)$ و$g(x)$ من $F^*[x]$ يكون : $\deg f \leq \deg(f.g)$

(3) لكل كثيرتي حدود $f(x),g(x) \in F^*[x]$ ، توجد كثيرتا حدود $q(x),r(x) \in F^*[x]$ بحيث يكون :

$$f(x) = g(x).q(x) + r(x) \ , \ r = 0 \ , \ \deg r < \deg g$$

وذلك حسب مبرهنة التقسيم الخوارزمي ، إذن $(F[x],+,\cdot)$ تشكل حلقة إقليدية .

مثال (14) :

أوجد القاسم المشترك الأعظم لكثيرتي الحدود :

$$f(x) = x^3 + 2x^2 + 3x + 6 \ , \ g(x) = x^2 + 5x + 6$$

على حلقة كثيرات الحدود $(Q[x],+,\cdot)$.

الحل :

حسب تعريف القاسم المشترك الأعظم ، لدينا :

$$f(x) = (x^2 + 3)(x + 2) \ , \ g(x) = (x + 3)(x + 2)$$

وبالتالي فإن :

$$d(x) = \big(f(x),g(x)\big) = x + 2$$

مثال (15) :

مستفيداً من المبرهنة قبل الأخيرة ، أوجد القاسم المشترك الأعظم $d(x)$ في الحلقة $(Z_3[x],+,.)$ لكثيرتي الحدود : $f(x) = x^5 + 2 \, , \, g(x) = 2(x^4 + 1)$

الحل :

حسب المبرهنة قبل الأخيرة ، لنوجد كثيرتي الحدود $\alpha(x) \, , \, \beta(x)$ بحيث يكون :

$d(x) = \alpha(x).f(x) + \beta(x).g(x)$ لكل $\alpha(x) \, , \, \beta(x)$ من $Z_3[x]$

باستخدام مبرهنة التقسيم الخوارزمي ، نكتب :

$$x^5 + 2 = 2x\,(2x^4 + 2) + (2x + 2)$$
$$2x^4 + 2 = (x^3 + 2x^2 + x + 2)\,(2x + 2) + 1$$
$$2x + 2 = (2x + 2).1 + 0$$

إذن : $d(x) = \big(f(x),g(x)\big) = 1$

باستخدام المعادلات السابقة نجد :

$$\begin{aligned} 1 &= 2x^4 + 2 - (x^3 + 2x^2 + x + 2)\,(2x + 2) \\ &= 2x^4 + 2 - (x^3 + 2x^2 + x + 2)\,\big[(x^5 + 2 - 2x)\,(2x^4 + 2)\big] \\ &= (2x^4 + x^3 + 2x^2 + 1)\,(2x^4 + 2) + (2x^3 + x^2 + 2x + 1)\,(x^5 + 2) \end{aligned}$$

إذن نجد :

$$\alpha(x) = 2x^4 + x^3 + 2x^2 + 1 \quad , \quad \beta(x) = 2x^3 + x^2 + 2x + 1$$

(7-4) المضاعف المشترك الأصغر Least common multiple :

ليكن $(F,+,.)$ حقلاً إبدالياً ما ، وإذا كانت $f(x) \neq 0 \neq g(x) \in K[x]$ ، نعرّف المضاعف المشترك الأصغر لكثيرتي الحدود $f(x)$ و$g(x)$ بأنها كثيـرة الحـدود الواحدية ولتكن $c(x)$ من حلقة كثيرات الحدود $(K[x],+,.)$ بحيث يتحقق ما يلي :

(1) $f(x)/c(x)$ و $g(x)/c(x)$

(2) إذا كان $c_1(x)\in K[x]$ وكان $f(x)/c_1(x)$ و $g(x)/c_1(x)$ عندئذٍ يكـــون $c(x)/c_1(x)$

نرمـــز عـــادةً للمضـــاعف المشـــترك الأصـــغر لـــــ $f(x)$ و $g(x)$ بـــالرمز : $c(x) = \ell cm\,(f,g)$.

يمكن البرهان بسهولة على ما يلي :

المضاعف المشترك الأصغر لكثيرتي الحدود المغايرتين للصفر تتعين بشكل وحيد.

مبرهنة (9) :

لتكن $f(x) \neq 0 \neq g(x)\in K[x]$ ، ولنأخذ المثالية الرئيسة $c(x).K[x]$ الـــذي يساوي التقاطع :

$f(x).K[x]\cap g(x).K[x]$ للمثاليتين الرئيسيتين المولدتين بـــ $f(x)$ و $g(x)$ ، حيث $c(x)$ كثيرة حدود واحدية ، عندها تكون $c(x)$ المضاعف المشترك الأصغر لــــ $f(x)$ و $g(x)$.

البرهان :

لدينا فرضاً : $c(x).K[x] = f(x).K[x]\cap g(x).K[x]$

حيث أن $c(x)$ كثيرة حدود واحدية ، وبالتالي فإن $c(x)\in f(x)K[x]$ أي انه توجد كثيرة حدود $q(x)$ من $K[x]$ بحيث يكون : $c(x) = f(x).g(x)$ ، وهذا يعنـــي أن $f(x)/c(x)$. وكذلك $c(x)\in g(x)K[x]$ ، ومنـــه، وبصـــورة مشـــابهة نجـــد أن $g(x)/c(x)$.

من ناحيـــة ثانيـــة ، إذا كانـــت $c_1(x)\in K[x]$ ، بحيـــث يكـــون : $f(x)/c_1(x)$ و $g(x)\in c_1(x)$ ، عندها توجد كثيرتي حدوديتين مثـــل $\varphi(x)$ و $\Psi(x)$ ، بحيـــث يتحقق :

$$c_1(x) = f(x).\varphi(x)\in f(x).K[x]$$
$$c_1(x) = g(x).\Psi(x)\in gx).K[x]$$

وهذا يعني أن $c_1(x)\in c(x).K[x]$ ، إذن توجد كثيرة حدود $\Psi(x)$ بحيث يكون :

$c_1(x) = c(x).\Psi(x)$ ، وهذا يعني أن $c(x)/c_1(x)$.

نستنتج مما سبق أن $c(x)$ هي المضاعف المشترك الأصغر لكثيرتي الحدودتين $f(x)$ و $g(x)$.

مبرهنة (10) :

إن حلقة كثيرات الحدود $(F[x],+,\cdot)$ على الحقل $(F,+,\cdot)$ هي حلقة تامة رئيسة .

البرهان :

إذا كانت I مثالية في الحلقة $(F[x],+,\cdot)$ ، وإذا كان $I = \{o\}$، فيكون $I = < o >$ وهي مثالية رئيسة في الحلقة $(F[x],+,\cdot)$.

ولنفرض الآن أن $I \neq \{o\}$ ، وإذا كانت $f(x)$ كثيرة حدود غير صفرية في I درجتها اصغر ما يمكن، وإذا كان $\deg f = 0$ ، فإن $f(x) = a \in F$ ، فإن a عنصر وحدة ، ويكون في هذه الحالة :

$$f(x) = < a > \in F[x]$$

إذن I مثالية رئيسة .

لنفرض الآن أن $\deg f \geq 1$ ، وإذا كان $g(x) \in I$ فحسب مبرهنة التقسيم الخوارزمي يكون :

$$f(x) = g(x).q(x) + r(x)$$

و $r = 0$ و $\deg r < \deg g$ ، وبالتالي يكون لدينا :

$$r(x) = g(x) - f(x).q(x)$$

لأن I مثالية في $F[x]$ ، ولأن $g(x) \neq 0$ ، درجته اصغر ما يمكن ضمن عناصر المثالية I إذن $r = 0$ ، وبالتالي ، فإن $g(x) = f(x).q(x0$ ، أي أن $I = < f >$.

نستنتج مما سبق أن حلقة كثيرات الحدود $(F[x],+,\cdot)$ هي حلقة تامة رئيسة .

(8-4) كثيرات الحدود غير القابلة للتحليل Irreducible polynomials :

تعريف (5) :

ليكن $(F,+,\cdot)$ حقل ما ، نقول عن كثيرة الحدود غير الصفرية $P(x)$ في $F[x]$ إنها غير قابلة للتحليل على F أو في $F[x]$ إذا تحقق ما يلي :

$\deg P(x) \geq 1$ (1)

(2) إذا كان $P(x) = f(x).g(x)$ في $F[x]$، عندها ، إمـا $\deg f(x) = 0$ أو $\deg g(x) = 0$.

ونقول إن كثيرة الحدود $P(x)$ من $F[x]$ إنها قابلة للتحليل (Reducible) ، إذا لم يتحقق أحد الشرطين السابقين ، بكلامٍ آخر ، نقول عن $P(x)$ إنها قابلة للتحليل إذا كانت $P(x) = f(x).g(x)$ حيث :

$$0 < \deg g(x) < \deg P(x)$$
$$0 < \deg f(x) < \deg P(x)$$

لكل $f(x)$ و$g(x)$ من $F[x]$.

مثال (16) :

ليكن $(F,+,\cdot)$ حقلاً ما ، أثبت أن كل كثيرة حدود خطية تكون غير قابلة للتحليل على F .

الحل :

لـتكن كثيـرة الحـدود $P(x) = ax + b$ ، مـن أجـل $a \neq 0$ ، وبفـرض أن $P(x) = f(x).g(x)$ في $F[x]$ ، بما أن F حلقة تامة ، فإن :

$$\deg f(x) + \deg g(x) = \deg P(x) = 1$$

ولدينا $\deg f(x) \geq 0$ و$\deg g(x) \geq 0$ ، وهما عبارة عـن أعـداد صـحيحة ، وبالتالي فإن درجة أحدهما تساوي الصفر .

نلاحظ مما سبق أن قابلية تحليل كثيرة حدود تعتمد على الحقل المدروس ، فمـثلاً في المثال السابق إن كثيرة الحدود $x^2 + 1$ غير قابلة للتحليل على الحقل $(R,+,\cdot)$ لكنها قابلة للتحليل على حقل الأعداد المركبة $(C,+,\cdot)$. ويكون :

$$x^2 + 1 = (x + i)(x - i)$$

نتيجة (1) :

ليكن $(F,+,\cdot)$ حقلاً ما ، وإذا كانت c كثيرة الحدود $P(x)$ من $F[x]$ غير قابلة للتحليل على الحقل F ، فإن $a.P(x)$ كثيرة حدود غير قابلة للتحليل أيضاً على F ،

حيث أن $a \neq 0$ من F .

البرهان :

إذا كان $a.P(x) = f(x).g(x)$ في F[x] ، عندئذٍ يكون $P(x) = [a^{-1} f(x)].g(x)$.

وبسبب كون كثيرة الحدود P(x) غير قابلة للتحليل في F[x] ، يؤدي إلى أن إما :

$\deg(a^{-1} f(x)) = \deg f(x) = 0$ أو $\deg g(x) = 0$

وهذا يبين لنا أن a.P(x) كثيرة حدود غير قابلة للتحليل في F[x] .

مبرهنة (11) :

إذا كان E حقلاً جزئياً من الحقل (F,+,.) ، ولتكن $f(x) \in E[x]$ كثيرة حدود غير قابلة للتحليل على E ، وإذا كان $a \in F$ جذراً لكثيرة الحدود f(x) ، فإن الشرط اللازم والكافي لكي يكون $a \in F$ جذراً مضاعفاً لـ f(x) هو أن يكون a جذراً لكثيرة الحدود $f'(x)$ (مشتقة كثيرة الحدود f(x)) .

البرهان :

إذا كان $a \in F$ جذراً مضاعفاً لكثيرة الحدود f(x) ، فإنه يوجد عدد صحيح موجب، ليكن $n > 1$ يكون من أجله $f(x) = (x-a)^n . g(x)$ حيث أن $g(x) \in E[x]$ ، وبالتالي يكون لدينا :

$$f'(x) = n\,(x-a)^{n-1} . g(x) + (x-a)^n . g'(x)$$

وبما أن $(n-1) > 0$ ، فإن $(x-a)/f'(x)$ ، أي أن a جذر لكثيرة الحدود $f'(x)$.

لنبرهن الآن أن a جذر مضاعف لكثيرة الحدود f(x) .

بما أن a جذر لكثيرة الحدود $f'(x)$ ، فإن $f'(a) = 0$ ، وبما أن a جذر لكثيرة الحدود f(x) ، فيكون :

$$f(x) = (x-a)\, g(x) \;;\; g(x) \in E[x] \qquad (1)$$

باشتقاق العلاقة الأخيرة نجد أن :

$$f'(x) = g(x) + (x-a)\, g'(x)$$

وبالتالي يكون :

$$0 = f'(a) = g(a) + (a-a)\, g'(a)$$

إذن : $g(a) = 0$ ، وبالتالي ، يكون $(x-a)/g(x)$ ، أي أن :

$$g(x) = (x-a).\, h(x) \;;\; h(x) \in E(x)$$

بتعويض $g(x)$ في العلاقة (1) نجد :

$$f(x) = (x-a)^2.\, h(x)$$

إذن a جذر مضاعف لكثيرة الحدود $f(x)$.

مبرهنة (12) :

ليكن $(F,+,.)$ حقلاً ما ، ولتكن كثيرة الحدود $P(x)$ من $F[x]$ بحيث يكون $\deg P(x) \geq 2$ ، عندئذٍ يتحقق ما يلي :

(1) إذا كانت $P(x)$ غير قابلة للتحليل على F، فإن $P(x)$ لا تملك جذراً في F.

(2) إذا كانت درجة $P(x)$ تساوي 2 أو 3 ، عندئذٍ تكون $P(x)$ غير قابلة للتحليل على F ، إذا، وفقط إذا ، لم يكن لها جذر في F .

البرهان :

(1) إذا كان لكثيرة الحدود $P(x)$ جذراً وليكن $a \in F$ ، فإن $P(a) = 0$ ، لذلك $P(x) = (x-a)\, q(x)$ (حسب نظرية العامل) ، وبما أن $\deg P(x) \geq 2$ فهذا يعني أن كثيرة الحدود قابلة للتحليل ، وهذا يناقض الفرض ، إذن $P(x)$ ليس لها جذر في R .

(2) لنفرض أن $P(x) = f(x).g(x)$ وليس لـ $P(x)$ جذراً في F ، عندئذٍ $f(x)$ و$g(x)$ لا تملكان أي جذر في F ، لذا : $\deg f(x) \neq 1$ و $\deg g(x) \neq 1$. لكن ، بما أن :

$$\deg f(x) + \deg g(x) = \deg P(x)$$

وأن درجة $P(x)$ هي 2 أو 3، فهذا يبين لنا أن إما $\deg f(x) = 0$ أو

. $\deg g(x) = 0$

إذن $P(x)$ غير قابلة للتحليل .

برهان العكس ينتج مباشرةً من (1) .

مثال (17) :

بيّن فيما إذا كانت كثيرة الحدود $P(x) = x^3 + 3x^2 + x + 2$ غير قابلة للتحليل على Z_5 .

الحل :

بما أن $Z_5 = \{0,1,2,3,4\}$ ، وبالتالي نستطيع تحديد أي من العناصر السابقة تمثل جذراً لـ $P(x)$:

إن $P(0) = 2 , P(1) = 2 , P(2) = 4 , P(3) = 4 , P(4) = 3$

بما أن $P(x)$ ليس لها أي جذر في Z_5 ، حسب المبرهنة السابقة تكون $P(x)$ غير قابلة للتحليل في Z_5 .

مثال (18) :

كثيرة الحدود $P(x) = x^2 + 9$ غير قابلة للتحليل في $R[x]$ ، لأنه (حسب المبرهنة السابقة) لا تملك جذراً في R .

ملاحظة (5) :

يبيّن الجزء الثاني من المبرهنة السابقة ، أن اختبار قابلية التحليل أو غير قابلية التحليل لكثيرة الحدود $P(x)$ تصح فقط في حالة $\deg P(x)$ هي 2 أو 3 لكنها تفشل في حالة $\deg P(x)$ تساوي أربعة أو أكثر . فعلى سبيل المثال ، إذا كانت :

$$P(x) = x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$$

من الواضح أنها قابلة للتحليل في $R[x]$ ، لكن ليس لها جذور في R .

مبرهنة (13) :

لتكن $f(x) \in C[x]$ حيث أن $\deg f(x) = n \geq 1$ ، عندئذٍ يتحقق ما يلي :

$$f(x) = u\,(x - u_1)(x - u_2) \ldots\ldots (x - u_n) \qquad (1)$$

حيث أن u_i ، $i = 1,2,\ldots,n$ (جذور لـ $f(x)$ في C) ، (ليس من الضروري أن تكون مختلفة فيما بينها) . و u عامل لـ $f(x)$.

(2) كثيرة الحدود الوحيدة غير القابلة للتحليل في $C[x]$ هي كثيرة الحدود الخطية في $C[x]$.

البرهان :

(1) باستخدام مبدأ الاستنتاج الرياضي على n نجد :

إذا كان $n = \deg f(x) = 1$ ، فهذا يعني أن $f(x) = ux + b$ ، حيث $u \neq 0$.

إن $f(x) = ux + b = u(x + u^{-1}.b)$ ، لذلك $u_1 = -u^{-1}.b$.

إذا كان $n > 1$ ، فيكون لـ $f(x)$ جذر وليكن u_1 حسب النظرية الأساسية في الجبر لذا يكون : $f(x) = (x - u_1).q(x)$ حيث أن $\deg q(x) = n - 1$.

وباستخدام الاستقراء الرياضي :

$$q(x) = u(x - u_2)(x - u_3)\ldots\ldots(x - u_n)$$

وبالتالي يكون :

$$f(x) = u(x - u_1)(x - u_2)\ldots\ldots(x - u_n)$$

حيث أن $u_1,u_2,\ldots,u_n$ جذور لـ $f(x)$ في $c[x]$.

(2) ينتج من (1) مباشرةً .

مأخوذة غوص Gauss's Lemma :

إذا كانت $f(x) = g(x).h(x)$ في $Z[x]$ ، وإذا كان P عدداً أولياً يقسم كل معاملات لـ $f(x)$، عندئذٍ P يقسم كل معاملات لـ $g(x)$ أو P يقسم كل معاملات لـ $h(x)$.

(9-4) كثيرة الحدود البدائية (الأولية) Prmitive polynomail

لنعرّف أولاً سعة كثيرة الحدود .

تعريف (6) سعة كثيرة حدود Content :

ليكن $(F,+,\cdot)$ حقلاً ما ، ولتكن $f(x)\in(F[x]$ كثيرة حدود غير صفرية على

الحقل F ، نسمي القاسم المشترك الأعظم لمعاملات كثيرة الحدود f(x) بسعة كثيرة الحدود ، ونرمز لها عادةً بـــ c(f) .

وفي حالة خاصة ، إذا كانت $c(f) = 1$ ، فإننا نسمي كثيرة الحـــدود f(x) بكثيــرة الحدود البدائية Primitive polynomaila .

مثال (19) :

بيّن أي من كثيرات الحدود التالية بدائية :

$$f(x) = 22x^3 + 10x^2 - 21x \in Q[x]$$

$$g(x) = 3x^4 + 18x^2 - 81x + 27 \in Q[x]$$

الحل :

بما أن $c(f) = 1$ ، إذن كثيرة الحدود f(x) بدائية ، لأن القاسم المشترك الأعظـــم للمعاملات 21,10,22- هو الواحد . أما $c(g) = 3$ لأن القاسم المشترك الأعظـــم للمعاملات 3,18,-8,27 هو 3 ، إذن كثيرة الحدود g(x) ليست بدائية .

تبيّن ، المبرهنة التالية ، أن حاصل ضرب كثيرتي حدود بدائيتين هي كثيرة حدود بدائية .

مبرهنة (14) :

إذا كانت $f(x),g(x) \in Z[x]$ كثيرتي حدود بدائيتين على الحلقة $(Z,+,\cdot)$ ، فإن حاصل ضربهما f(x).g(x) كثيرة حدود بدائية على الحلقة Z .

البرهان :

لتكن $$f(x) = \sum_{i=0}^{n} a_i . x^i \in Z[x] \,,\; g(x) = \sum_{i=0}^{m} b_i . x^i \in Z[x]$$

ولتكن $$h(x) = f(x).g(x) = \sum_{k=0}^{n+m} c_k . x^k$$

إذا كانت $c(h) \neq 0$ ، فهذا يعني أن معاملات كثيرة الحدود h(x) تقبل القسمة على العدد الأولي P . بما أن f(x) كثيرة حدود ، فإن P لا تقسم بعض المعـــاملات a_i لـــ f(x) ، وليكن a_t هو المعامل الأول في f(x) الذي لا يقبل القســمة علـــى P ،

وكذلك بالنسبة لكثيرة الحدود $g(x)$ ، وليكن b_s العامل الأول في $g(x)$ الذي لا يقبل القسمة على العدد الأولي P ، بما أن :

$$c_{t+s} = a_0 . b_{t+s} + a_1 . b_{t+s-1} + \dots + a_{t-1} .b_{s+1} + a_t . b_s + \dots + a_{t+s} . b_0$$

وبما أن P لا يقسم a_i، لكل $i < t$، نجد أن P لا يقسم المجموع التالي : $.a_0.b_{t+s} + \dots +a_{t-1}.b_{s+1}$

وبما أن P لا يقسم b_j لكل $j < s$ ، وبالتالي ، فإن P لا يقسم المجموع التالي :

$$a_{t+1}.b_{s-1} + \dots + a_{t+s} . b_0$$

وبالتالي فإن P لا يقسم c_{t+s} ، أي P لا يقسم $a_t b_s$ ، لأن P لا يقسم a_t و P لا يقسم b_s ، إذن P لا يقسم c_{t+s} ، أي أن $h(x)$ كثيرة حدود بدائية .

نتيجة (2) :

إذا كانت $f(x)$ كثيرة حدود غير قابلة للتحليل على الحقل F من $F[x]$ ، وإذا كان $\deg f > 1$، عندئذٍ $f(x)$ كثيرة حدود بدائية .

البرهان :

لتكن $f(x) = c(f).g(x)$ ، وبالتالي ، فإما $c(f)$ أو $g(x)$ عنصر وحدة في الحلقة $(F[x],+,.)$ ، لأن $f(x)$ غير قابلة للتحليل على الحقل F، ولكن $g(x)$ ليس عنصر وحدة ، لأن $\deg g(x) > 1$، إذن $c(f)$ عنصر وحدة ، وهذا يعني أن $c(f) = 1$.

مبرهنة وحدانية التحليل Unique Factorisation in F[x] :

لتكن $(F[x],+,.)$ حلقة كثيرات الحدود على الحقل $(F,+,.)$ ، ولتكن $f(x)$ كثيرة حدود من $F[x]$ حيث $n = \deg f(x) \geq 1$ ، عندئذٍ يتحقق ما يلي :

$$f(x) = \alpha\, P_1(x).P_2(x).\dots.P_n(x) \qquad (*)$$

حيث α من F و$P_i(x)$ كثيرات حدود واحدية غير قابلة للتحليل على الحقل F و$1 \leq i \leq m$ ، كما أن هذا التحليل (*) وحيد (عدا إمكانية إعادة ترتيب العوامل) .

البرهان :

تبرهن المبرهنة المذكورة بطريقة الاستنتاج (الاستقراء) الرياضي على n .

إذا كان $n = 1$ ، فمن الواضح أن كثيرة الحدود $f(x)$ غير قابلة للتحليل على الحقل

F . لنفرض الآن $n > 1$ ، يكون $f(x) = g(x).h(x)$ حيث أن :

$$0 < \deg h < n \ , \ 0 < \deg g < n$$

ومن الاستنتاج الرياضي ، فإن كثيرتي الحدود $h(x)$ و$g(x)$ تكتبان على شكل حاصل ضرب غير قابل للتحليل . وإذا كانت $f(x) = q_1(x).q_2(x)....q_m(x)$ ، حيث $q_i(x)$ كثيرات حدود غير قابلة للتحليل على F ، من أجل $1 \leq i \leq m$ ، وإذا كان α_i المعامل الرئيسي لكثيرة الحدود $q_i(x)$, $1 \leq i \leq m$.

لنضع الآن $P_i(x) = \alpha_i^{-1}.q_i(x)$ و $\alpha = \alpha_1.\alpha_2 ..... \alpha_m$ فنجد أن $f(x)$ تكتب على شكل حاصل ضرب كثيرة حدود غير قابلة للتحليل على F ، أي أن :

$$f(x) = \alpha\, P_1(x).P_2(x) .... P_m(x)$$

لنبرهن الآن على وحدانية التحليل (*) :

نفرض أن :

$$f(x) = \alpha\, P_1(x).P_2(x) .... P_m(x)$$
$$= \beta\, q_1(x).q_2(x) .... q_t(x)$$

فإن $\alpha = \beta$ ، لأن كلاً منهما معامل رئيسي لكثيرة الحدود $f(x)$ ، وبالتالي ، فإن $P_1(x)$ تقسم إحدى كثيرات الحدود $q_j(x)$ ، ولتكن $q_1(x)$ ، وبما أن $q_1(x)$ كثيرة حدود غير قابلة للتحليل على F ، يكون :

$q_1(x) = \gamma_1 P_1(x)$ ، حيث $\gamma_1 \in F$ ، وبما أن كل من $P_1(x)$ و$q_1(x)$ كثيرة حدود واحدية (فرضاً) فإن $\gamma_1 = 1$ ، أي أن $P_1(x) = q_1(x)$ وبالتالي فإن :

$$P_1(x).P_2(x)... P_m(x) = P_1(x).q_2(x) .... q_t(x)$$

باختصار طرفي العلاقة السابقة على $P_1(x)$ نحصل على :

$$P_2(x)... P_m(x) = q_2(x) .... q_t(x)$$

وباتباع نفس الطريقة السابقة نجد : $q_2(x) = P_2(x)$ ، وهكذا نجد أن :

$m = t$ و$P_i(x) = q_j(x)$ لكل $1 \leq i \leq m$ و$1 \leq j \leq t$ مع إمكانية الترتيب للعوامل.

مثال (20) :

لتكن حلقة كثيرات الحدود $(Z_5[x],+,.)$ على الحقل $(Z_5,+,.)$ ، أثبت أن كثيرة

الحدود :

$f(x) = x^4 - 2x^3 + 2x - 1 \in Z_5[x]$ ، تتحلل بشكل وحيد إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل على الحقل Z_5 .

الحل :

إن
$$f(x) = x^4 - 2x^3 + 2x - 1 = (x + 1)(x - 1)^3$$
وهي العوامل غير القابلة للتحليل على الحقل Z_5 (عدا الضرب بعدد ثابت في Z_5)، فمثلاً يكون :
$$(x + 1)(x - 1)^3 = (x - 1)^2 (4x - 4)(5x + 5)$$
المثال التالي ، يقدم ، طريقة أخرى لإثبات أن كثيرة حدود على حقل ما غير قابلة للتحليل .

مثال (21) :

أثبت أن كثيرة الحدود $f(x) = x^5 + 2x^2 + 1$ في $Q[x]$ غير قابلة للتحليل .

الحل :

لدينا أولاً :
$$f(x) = x^5 + 2x^2 + 1 = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$$
بإجراء عملية الضرب في الطرف الأيمن ثم إجراء المطابقة مع الطرف الأيسر نحصل على المعادلات التالية :
$$a + c = 0 \,,\, d + ac + b = 0 \,,\, e + ad + bc = 0 \,,\, a.e + b.d = 0 \,,\, b.e = 1$$
المعادلة الأخيرة تعطي $b = e = \pm 1$، وبالتالي فإن آخر معادلتين تعطيان $a + d = 0$.

وبسبب $a + c = 0$ أيضاً ، فالمعادلة الثانية تأخذ الشكل $-a - a^2 + b = 0$. وهكذا a جذر صحيح لـ $x^2 + x - b$ ، حيث أن $b = \pm 1$. وباستخدام مبرهنة الجذور النسبية (الكسرية) نجد أن $f(x)$ غير قابلة للتحليل .

معيار جاوس (مأخوذة جاوس) (Gauss's Lemma)

إذا كانت $f(x) \in Z[x]$ كثيرة حدود بدائية على الحلقة $(Z,+,.)$ ، فإن ، الشرط اللازم ، والكافي لكي تكون $f(x)$ قابلة للتحليل على Z ، هو أن تكون $f(x)$ قابلة

للتحليل على الحلقة $(Q,+,\cdot)$.

البرهان :

من الواضح ، أنه إذا كانت $f(x)$ كثيرة حدود قابلة للتحليل في $Z[x]$ ، فإنها قابلة للتحليل على $Q[x]$. لنبرهن الآن على العكس :

نفرض أن $f(x) = g(x).h(x)$ ، حيث أن :

$$g(x).h(x) \in Q[x] \quad , \quad \deg h(x) < \deg f(x) \quad , \quad 1 \le \deg g(x)$$

لنوجد المضاعف المشترك لمقامات معاملات الحدود وبإخراجها خارج قوسين نجد أن :

$f(x) = \frac{a}{b}\left(q(x).r(x)\right)$ حيث أن b,a من Z ، و $q(x),r(x)$ من $Z[x]$

كثيرتي حدود بدائيتين ، وبالتالي فإن $q(x).r(x)$ كثيرة حدود بدائية أيضاً ، وبالتالي يكون لدينا :

$$b.f(x) = a\left(q(x).r(x)\right)$$

ومنه يكون $a = b$ ، إذن $f(x) = q(x).h(x)$ قابلة للتحليل على Z .

نلاحظ من معيار جاوس السابق ، أنه من الصعب تطبيق هذا الاختبار ، لذا وجدت اختبارات أسهل ، من هذه الاختبارات ، منها اختبار اينشتاين .

المعيار التالي ، والمسمى بمعيار اينشتاين (فرديناند اينشتاين (1823-1852) وكان تلميذاً لغاوس) يبيّن لنا وبدلالة عدد أولي معطى فيما إذا كانت كثيرة حدود ما على حقل ما غير قابلة للتحليل .

معيار إنيشتاين (Eisenstein,s Criterion) :

لتكن كثيرة الحدود $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ في $Z[x]$ ، حيث $n \ge 1$ ، وبفرض أن P عدد أولي معطى ، بحيث يتحقق ما يلي :

(1) P يقسم الأعداد $a_{n-1} , \dots, a_1,a_0$

(2) P لا يقسم العدد a_n

(3) P^2 لا يقسم a_0

عندئذ كثيرة الحدود $f(x)$ غير قابلة للتحليل في $Q[x]$.

قبل أن نقدم برهان هذا المعيار نقدم المثال التوضيحي لهذا المعيار .

مثال (22) :

مستخدماً معيار اينشتاين ، بيّن فيما إذا كانت كثيرة الحدود :

$$f(x) = 2x^5 + 27x^3 - 18x + 12 \in Z[x]$$

حيث $P = 3$ غير قابلة للتحليل في $Q[x]$.

الحل :

لدينا : $a_0 = 12$, $a_1 = -18$, $a_2 = 27$, $a_3 = a_n = 2$, $P = 3$

لنطبق الشروط الواردة في التعريف السابق :

(1) $P = 3$ يقسم 12 و18- و27

(2) 3 لا يقسم $a_n = 2$

(3) $P^2 = 9$ لا يقسم 12

بما أن الشروط محققة ، إذن $f(x)$ غير قابلة للتحليل في $Q[x]$.

لنبرهن الآن مبرهنة اينشتاين السابقة .

إذا كانت كثيرة الحدود قابلة للتحليل في الحلقة $(Z,+,\cdot)$ ، وهذا يعني أنه يمكن كتابة $f(x) = g(x).h(x)$ في $Z[x]$ ، حيث أن :

$$g(x) = b_0 + b_1 x + b_2 x^2 + \dots\dots + b_m x^m$$

$$h(x) = c_0 + c_1 x + c_2 x^2 + \dots\dots + c_t x^t$$

لكل c_j , b_i من Z و $1 \le i \le m$, $1 \le j \le t$.

وبما أن $t,m > 0$ ، فإن $n = t + m$ ، ومن تعريف حاصل ضرب كثيرتي حدود ، نجد أن $a_0 = b_0 c_0$ ، وبما أن P/a_0 وP^2 لا يقسم a_0 ، فإن P يقسم إما b_0 أو c_0 . ولنفرض مثلاً أن P/b_0 و P لا يقسم c_0 ومن كون P لا يقسم a_n، حيث

$a_n = b_m.c_t$ ، فإن P لا يمكن أن يقسم كلاً من الأعداد الصحيحة $b_0,b_1,\ldots,b_m$.
ولنفرض أن s أصغر عدد صحيح حيث P لا يقسم b_s وبما أن :

$$a_s = b_0 c_s + b_1 c_{s-1} + \ldots + b_{s-1} c_1 + b_s c_0$$

ولدينا : P/a_s , P/b_0 , P/b_1 , … , P/b_{s-1} ، إذن P/b_sc_0 ، ومن كون P لا يقسم c_0 ، نجد أن P يقسم b_s ، وهذا تناقض ، وبالتالي فإن f(x) غير قابلة للتحليل في Q[x] .

ملاحظة (6) :

يمكن صياغة اختبار اينشتاين بالشكل التالي :

ليكن $P \in Z$ عدداً أولياً ، وبفرض أن كثيرة الحدود $f(x) = a_n x^n + \ldots + a_0$ في Z[x] .

وإذا كـان $a_n \not\equiv o \pmod P$ ، لكـن $a_i \equiv o \pmod P$ ، مـن أجـل $i < n$ و $a_0 \not\equiv o \pmod{P^2}$ ، عندئذٍ f(x) كثيرة حدود غير قابلة للتحليل على Q .

مثال (23) :

إن كثيرة الحدود : $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$

وبأخذ P = 3 ، نجد ما يلي :

$25 \not\equiv o \pmod 3$

$-9,3,-12 \equiv o \pmod 3$

$-12 \not\equiv o \pmod 9$

إذن f(x) كثيرة حدود غير قابلة للتحليل .

مثال (24) :

إذا كان P عدداً أولياً ، وإذا كانت كثيرة الحدود :

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in Z[x]$$

فإن $\Phi_p(x)$ غير قابلة للتحليل في Q[x] .

الحل :

لنبرهن أولاً أن كثيرة الحدود $\Phi_p(x+1)$ غير قابلة للتحليل في $Q[x]$ بدلاً من $\Phi_p(x)$، لأنه إذا كانت $\Phi_p(x) = g(x).h(x)$ فإن :

$$\Phi_p(x+1) = g(x+1).h(x+1)$$

الآن :

$$(x-1)\,\Phi_p(x) = (x-1)\,(x^{p-1} + x^{p-2} + \dots + x + 1) = x^p - 1$$

لنبدل كل x بـ $x + 1$ في العلاقة السابقة فنحصل على :

$$x\,\Phi_p(x+1) = (x+1)^p - 1$$

أي أن :

$$\Phi_p(x) = \frac{(x+1)^p - 1}{x}$$

باستخدام نظرية ذي الحدين نجد أن :

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}.x^{p-2} + \dots + \binom{p}{p-1}.x + p$$

وباستخدام معيار إينشتاين السابق، نجد أن : p يقسم $\binom{p}{p-i}$ لكل $1 \le i \le p-1$.

كما يمكن التحقق من بقية الشروط الواردة في معيار اينشتاين ، إذن كثيرة الحدود $\Phi_p(x+1)$ غير قابلة للتحليل على $Q[x]$.

ملاحظة (7) :

كثيرة الحدود السابقة $\Phi_p(x)$ تسمى بكثيرة حدود سايكلوموتك Cyclotomic polynomial .

سندرس الآن اختباراً آخر ، لا يقل شأناً عن سابقيه لكثيرات الحدود غير القابلة للتحليل على الحلقة $Z[x]$ وذلك بدلالة عدد أولي معطى .

اختبار لكثيرات الحدود القياسية غير القابلة للتحليل :

Modular Irreducibility test

لتكن كثيرة الحدود $f(x)$ من $Z[x]$، وبفرض أن P عدد أولي معطى ، وبحيث يتحقق ما يلي :

(1) P لا يقسم المعامل الرئيسي لـ $f(x)$.

(2) إن $\overline{f(x)}$ غير قابل للتحليل في الحلقة $Z_p[x]$ ، حيث أن :

$$f(x) \equiv \overline{f(x)} . \bmod P$$

عندئذٍ تكون كثيرة الحدود $f(x)$ غير قابلة للتحليل في $Q[x]$.

البرهان :

لتكن $f(x) = a_0 + a_1 x + \dots + a_n x^n \in Z[x]$

فإن :

$$\overline{f(x)} = \overline{a_0} + \overline{a_1} x + \dots + \overline{a_n} x^n \in Z_p[x]$$

وبالتالي ، يكون : $\deg f(x) = \deg \overline{f(x)}$ (من (1)) .

إذا كانت $f(x)$ قابلة للتحليل في الحلقة $Q[x]$ ، فهذا يعني أنه بالإمكان كتابة $f(x)$ بالشكل :

$f(x) = g(x).h(x)$ في $Z[x]$. وبالتالي يكون لدينا : $\overline{f(x)} = \overline{g(x)}.\overline{h(x)}$ ، وهذا يناقض كون $\overline{f(x)}$ غير قابلة للتحليل في $ZP[x]$ ، وبسبب كون :

$$\deg \overline{g(x)} \le \deg g(x) < \deg f(x) = \deg \overline{f(x)}$$

وبشكل مشابه يكون أيضاً :

$$\deg \overline{h(x)} < \deg \overline{f(x)}$$

مثال (25) :

أثبت أن كثيرة الحدود $f(x) = x^3 + 4x^2 + 6x + 2$ غير قابلة للتحليل في الحلقة $(Q[x],+,\cdot)$.

الحل :

بأخذ $P = 3$ ، يكون $\overline{f(x)} = x^3 + x^2 + 2$ ونلاحظ أن $\overline{f(x)}$ لا تملك أي جذر في $Z_3[x]$ ، وبتطبيق الاختيار السابق تكون $f(x)$ غير قابلة للتحليل في $Q[x]$.

(10-4) حلقة القسمة لكثيرات الحدود فوق حقل :

Factor rings of polynomials over afield

نعلم أن كل مثالية لـ Z لها الشكل $n.Z$ ، حيث أن $n \geq 0$ ، وإذا كان $n > 0$ فإن حلقة القسمة تكون $Z/n.Z = Z_n$ ، سندرس الآن حلقة القسمة لكثيرات الحدود على حقل ، آخذين بعين الاعتبار الفكرة السابقة .

مبرهنة (15) :

ليكن $(F,+,.)$ حقلاً ما ، وإذا كانت $I \neq 0$ مثالية لـ $F[x]$ ، عندئذٍ توجد كثيرة حدود واحدية $h(x)$ في $f(x)$ بحيث يكون :

$$A = \langle h(x) \rangle = h(x) . F[x]$$

نتيجة (3) :

$$R = R[x]/I = \left\{ \overline{a_0} + \overline{a_1}\, t + \ldots + \overline{a_{m-1}}\, t^{m-1} ;\ a_i \in F \right\}$$

البرهان :

ليكن $\overline{f(x)} \in R = R[x]/I$ ، حيث أن $f(x) \in F[x]$ ، باستخدام خوارزمية القسمة، توجد $q(x)$ في $F[x]$ ، بحيث يكون :

$$f(x) = q(x).h(x) + (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}) \ ; \ a_i \in R$$

وبسبب كون $h(x) \in I$ ، يكون لدينا $\overline{h(x)} = \overline{o}$ في R ، لذلك :

$$\overline{f(x)} = \overline{a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}} = \overline{a_0} + \overline{a_1}\, t + \ldots + \overline{a_{m-1}}\, t^{m-1}$$

ملاحظة (8) :

إذا كان :

$$a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1}$$

في $R[x]/I$ ، حيث أن المثالية $I \neq 0$ ، عندئذٍ $a_i = b_i$ من أجل جميع قيم i .

نتيجة (4) :

في حلقة القسمة $R[x]/I$ ، حيث $I \neq 0$ ، إذا كان :

$$h(x) = c_0 + c_1 x + \ldots + c_{m-1} x^{m-1} + x^m$$

فإن $h(t) = 0$ ، حيث أن $t = x + I$.

البرهان :

بما أن : $h(x) = c_0 + c_1 x + \ldots + c_{m-1} x^{m-1} + x^m$

و $t = x + I$ ، ولنكتب $a = \overline{a} = a + I$ حيث $a \in F$ (F حقل) ، وبالتالي يكـــون لدينا :

$$\begin{aligned} h(t) &= c_0 + c_1 t + \ldots + c_{m-1} t^{m-1} + t^m \\ &= \overline{c_0} + \overline{c_1}\,.\,\overline{x} + \ldots\ldots + \overline{c_{m-1}}\,.\,\overline{x}^{\,m-1} + \overline{x}^{\,m} \\ &= \overline{c_0 + c_1 x + \ldots. + c_{m-1} x^{m-1} + x^m} \\ &= \overline{h(x)} = \overline{o} \end{aligned}$$

ومنه يكون $h(t) = 0$ في $R[x]/I$.

مبرهنة (16) :

ليكن $(F,+,.)$ حقلاً ما ، ولتكن $h(x)$ كثيرة حدود واحدية في $F[x]$ من الدرجة $m \geq 1$ ، عندئذٍ حلقة القسمة $F[x]/<h(x)>$ تعطى بالشكل :

$$F[x]/<h(x)> = \left\{a_0 + a_1 t + \ldots. + a_{m-1} t^{m-1} \;:\; a_i \in F \,;\, h(t) = 0 \right\}$$

بالإضافة إلى ذلك ، العناصر من $F[x]/<h(x)>$ تكتب بشكل وحيــد ، وهــذا يعني :

$$a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} = b_0 + b_1 t + \ldots + b_{m-1} t^{m-1} \Leftrightarrow a_i = b_i$$

من أجل جميع قيم i .

الأمثلة التالية ، توضح المبرهنة السابقة :

مثال (26) :

ليكن $(F,+,.)$ حقلاً ما ، وإذا كانت $h(x) = x^2 + 1$ ، عندئذٍ يكون :

$$F[x]/<x^2+1> = \{a + b\,t \;:\; a,b \in F \,,\, t^2 + 1 = 0\}$$

إن عمليتي الجمع والضرب تكونا :

$$(a + b\,t) + (c + d\,t) = (a + c) + (b + d)\,t \quad ; \quad t^2 = -1$$

$$(a + b\,t)\cdot(c + d\,t) = a\,c + (ad + bc)\,t + bd\,t^2$$

$$= (ac - bd) + (ad + bc)\,t$$

وإذا كان $F = R$ ، وبوضع i مكان t نحصل على حلقة الأعداد المركبة C .

مثال (27) :

صف حلقة القسمة $F[x] / < x^2 >$ ، حيث أن F حقلاً ما .

الحل :

بتطبيق المبرهنة السابقة ، حيث أن $h(x) = x^2$ و $m = 2$ يكون :

$$F[x]/<x^2>= \{a + b\,t \ : a,b \in F\,,\, t^2 = 0\}$$

كما أن في R يكون :

$$(a + b\,t) + (c + d\,t) = (a + c) + (b + d)\,t$$

بالإضافة إلى ذلك ، وبسبب $t^2 = 0$ تكون عملية الضرب من الشكل :

$$(a + b\,t)\cdot(c + d\,t) = a\,c + (ad + bc)\,t$$

وبأخذ الحالة الخاصة : $F = Z_2 = \{0,1\}$ ، نجد :

$$F[x]/<x^2>= \{0\,,\,1\,,\,t\,,\,t+1\}$$

هي حلقة بأربعة عناصر . بسبب أن $1 + 1 = 0$ في Z_2 و $t^2 = 0$ ، فإن جـدولي الجمع والضرب يكونا بالشكل :

$+$	0	1	t	$1+t$
0	0	1	t	$1+t$
1	1	0	$1+t$	t
t	t	$1+t$	0	1
$1+t$	$1+t$	t	1	0

$\times$	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	0	t
$1+t$	0	$1+t$	t	1

مبرهنة (17) :

لتكن $h(x)$ كثيرة حدود واحدية من الدرجة $m \geq 1$ في $F[x]$ حيث أن $(F,+,\cdot)$

حقلاً ما ، عندئذٍ تتكافأ الشروط التالية :

(1) $F[x] / < h(x) >$ حقل

(2) $F[x] / < h(x) >$ حلقة تامة

(3) $h(x)$ غير قابلة للتحليل على الحقل F

البرهان :

(1) $\Leftarrow$ (2)

واضح لأن كل حقل هو حلقة تامة .

(2) $\Leftarrow$ (3)

لسهولة الكتابة ، سنكتب $f(x) = f$ و $I = < h >$. إذا كان $h = f \bullet g$ في $F[x]$ و:

$$(f + I)(g + I) = f \bullet g + I = h + I = o + I$$

في $F[x]/I$ ، ومن (2) يكون $f + I = o + A$ أو $g + I = o + I$ ، وبالتالي يكون $f \in I$ أو $g \in I$.

إذا كان $f \in I$ ، عندئذٍ $f = q.h$ ، من أجل $q \in F[x]$. وهكذا $h = f.g = q.h.g$ ، لذا (بسبب $F[x]$ حلقة تامة) $1 = q.g$ ، وهذا يعني أن $\deg g = 0$ ، وبشكل مشابه إذا كان $g \in I$ فإن $\deg f = 0$. وهذا يؤدي إلى (3) .

(3) $\Leftarrow$ (1)

لتكن $f + I \neq o$ ، حيث أن $f \in F[x]$ ، عندئذٍ $f \notin I$ ، لذا فإن h لا تقسم f .

لتكن $d = \gcd(h,f)$، عندها يكون d/h ، لذا وبسبب h غير قابل للتحليل وh,d أوليتان ، يكون، إما $h = 1$ أو $h = d$. لكن $h = d$ ، وهذا يؤدي إلى أن h/f .

وهكذا $d = 1$ ، وبالتالي يوجد v,u في $F[x]$ بحيث يكون $1 = uh + vf$. عندئذٍ يكون :

$(v + I)(f + I) = 1 + I$ ، وهذا يعني أن $f + I$ واحدية في $F[x]/I$ ، وهذا يعطي (1) .

مثال (28) :

أنشئ حقلاً مؤلف من أربعة عناصر فقط .

الحل :

إن كثيرة الحدود $x^2 + x + 1$ لا تملك جذور في الحلقة Z_2 ، كما أنها غير قابلة للتحليل في الحلقة Z_2 . وبالتالي ، يمكن أخذ الحقل F بالشكل :

$$F = \frac{Z_2[x]}{< x^2 + x + 1 >} = \{a + b\,t \ : a,b \in Z_2 \,,\, t^2 + t + 1 = 0\}$$

وهكذا يكون لـ F :

$$F = \{0 \,,\, 1 \,,\, t \,,\, 1 + t\}$$

وبما أن : $1 + 1 = 0$ في الحلقة Z_2 و $t^2 = t + 1$. فإن جدولي العمليتين الجمع والضرب يكونان :

×	0	1	t	1+t
0	0	0	0	0
1	0	1	t	1+t
t	0	t	1+t	1
1+t	0	1+t	1	t

+	0	1	t	1+t
0	0	1	t	1+t
1	1	0	1+t	t
t	t	1+t	0	1
1+t	1+t	t	1	0

مبرهنة (18) :

إذا كانت $I = < f >$ مثالية في الحلقة $(F[x],+,\cdot)$ على الحقل $(F,+,\cdot)$ ، الشرط اللازم والكافي ، لكي تكون I مثالية أعظمية في $F[x]$ هو أن تكون كثيرة الحدود $f(x)$ غير قابلة للتحليل على الحقل $(F,+,\cdot)$.

البرهان :

لنبرهن أولاً ، أن $f(x)$ كثيرة حدود غير قابلة للتحليل على الحقل F ، علماً أن I مثالية أعظمية .

ليكن $I = < f > \neq \{0\}$ مثالية أعظمية في $F[x]$ ، فإن $< f > \neq F[x]$ ، وهذا يعني أن $f(x) \notin F$ ، لتكن $f(x) = g(x).h(x)$ حيث أن $g(x),h(x) \notin F[x]$ ،

وبما أن $< f >$ مثالية أعظمية فهي أولية ، ومن العلاقة : $g(x).h(x) \in < f >$ ، نجد أنه إما $g(x) \in < f >$ أو $h(x) \in < f >$ ، وتكون $f(x)$ إحدى العوامل لكثيرتي الحدود $g(x)$ أو $h(x)$ أي أن $\deg f < \deg g$ أو $\deg f < \deg h$ ، وهذا تناقض مع مفهوم قابلية التحليل لكثيرات الحدود ، إذن $f(x)$ كثيرة حدود غير قابلة للتحليل على الحقل F .

لنبرهن الآن أن $I = < f >$ مثالية أعظمية ، علماً أن كثيرة الحدود $f(x)$ غير قابلة للتحليل .

لتكن J مثالية في الحلقة $(F[x],+,.)$ ، حيث $< f > \subseteq J \subseteq F[x]$.

بما أن J مثالية رئيسة فيكون $I = < g >$ حيث أن $g(x) \in I$ و $f(x) = g(x).h(x)$ حيث $h(x) \in F[x]$.

بما أن $f(x)$ غير قابلة للتحليل على الحقل F، إذن إما $\deg g = 0$ أو $\deg h = 0$، فإذا كان $\deg g = 0$ فإن $g(x) = c \in F$ حيث c ثابت، وبالتالي فإن $g(x)$ عنصر وحدة في الحلقة $F[x]$، وبالتالي :

$< g > = J = F\ [x]$. أما إذا كان $\deg h = 0$ ، أي أن $h(x) = d \in F$ حيث d ثابت ، فيكون : $g(x) = \left(\frac{1}{d}\right).f(x) \in < f >$ ، أي أن $J = < f >$ ، وبالتالي يكون $< f > \subset J \subset F[x]$ ، وهذا غير ممكن ، إذن $< f >$ مثالية أعظمية في الحلقة $(F[x],+,.)$.

ينتج من المبرهنة السابقة النتيجة الهامة التالية :

نتيجة (5) :

إذا كان $(F,+,.)$ حقلاً ما و$f(x)$ كثيرة حدود غير قابلة للتحليل على F ، عندئذٍ $F[x]/< f >$ يكون حقلاً .

إن برهان هذه النتيجة ينتج من المبرهنة السابقة ، ومن المبرهنة : تكون الحلقة التامة R/I حقلاً ، إذا كانت المثالية I أعظمية .

ننهي هذا الفصل بتعريف حلقة كثيرات الحدود بمتغيرين y,x .

لتكن $(R,+,\cdot)$ حلقة ما ، ولتكن $R[x]$ حلقة كثيرات الحدود على الحلقــة R فــي المتغير x ، لنشكل الحلقة $\left((R[x])[y],+,\cdot \right)$ على الحلقة $R[x]$ في المتغير y، والتي نرمز لها عادةً بــ $(R[x,y],+,\cdot)$. ويطلق عليها اسم حلقة كثيرات الحدود بمتغيرين y,x .

كثيرة حدود بمتحولين من $R[x,y]$ تكتب بالشكل :

$$f(x,y) = \sum_{i\geq 0}\sum_{j\geq 0} a_{ij}\, x^i\, y^j$$

$$= a_{00} + a_{10}\, x + a_{10}\, y + a_{20}\, x^2 + a_{11}\, x\, y + a_{02}\, y^2 + \ldots.$$

كما أن الشرط اللازم والكافي، لكي يكون $\sum a_{ij}\, x^i\, y^j = \sum b_{ij}\, x^i\, y^j$ هــو أن يكون $a_{ij} = b_{ij}$ ، لكل i,j.

مثال (29) :

إن

$$f(x,y) = 2x - 3y + 3x^2\, y - 4x\, y^4 + 1 \in R[x,y]$$

كثيرة حدود بمتحولين حقيقيين هما x و y .

الفصل الخامس

الفضاءات الحلقية (الحلقيات)

Modules

الفصل الخامس

الفضاءات الحلقية (الحلقيات)

Modules

يعد الفضاء الحلقي على حلقة ما ، من المفاهيم الحديثة نسبياً في البنى الجبرية ، إذ يرجع ظهوره إلى منتصف القرن التاسع عشر الميلادي ، وقد ظهر عند دراسة الفضاءات المتجهة على حقل ما .

سنعرض في بداية هذا الفصل بعض المفاهيم والتعاريف للفضاءات الحلقية ثم ندرس الفضاء الحلقي الجزئي ، والمجموع المباشر للفضاءات الحلقية ، وفضاء القسمة الحلقي والتشاكلات والفضاء الحلقي الحر ....

يمكن الاستفادة من الفضاءات الحلقية على حلقة في مواضيع جبرية عديدة كالزمر الإبدالية ، وجبر – لي وفي المصفوفات وغيرها من العلوم الرياضية والفيزيائية .

(1-5) تعاريف ومفاهيم أساسية :

1- الفضاء الحلقي اليساري (من اليسار) على حلقة Left module over a ring

لتكن $(R,+,\cdot)$ حلقة ما، إذا كانت M مجموعة غير خالية ، وإذا كانت $\star$ عملية جبرية ثنائية معرفة على M ، وإذا كان φ تطبيقاً بالشكل : $\varphi : R\times M \longrightarrow M$ (يسمى عادةً عملية خارجية معرفة على المجموعة M) معرفاً بالشكل : $\varphi(r,m) = r.m$ ، لكل $r\in R$ و $m\in M$ ، فإننا نقول عن M إنه فضاء حلقي يساري بالنسبة للحلقة $(R,+,\cdot)$ ، إذا تحققت الشروط التالية :

(1) $(M,\star)$ زمرة إبدالية

(2) $\varphi(r, x\star y) = \varphi(r,x)\star\varphi(r,y)$

(3) $\varphi(r+s , x) = \varphi(r,x)\star\varphi(s,x)$

(4) $\varphi(r.s , x) = \varphi\big(r,\varphi(s,x)\big)$

وذلك من أجل أي s,r من R و y,x من M .

لاحظ ، أنه كان بالإمكان كتابة الشروط السابقة بالشكل :

`(1) $(M,\star)$ زمرة إبدالية

`(2) $r.(x+y) = r.x + r.y$

`(3) $(r+s).x = r.x + s.x$

`(4) $(r.s)\,x = r.(s.x)$

لكل s,r من R و y,x من M .

<u>-2</u> إذا كانت الحلقة $(R,+,\cdot)$ ذات عنصر وحدة 1 ، وإذا تحقق ، بالإضافة إلى الشروط الأربعة السابقة ، الشرط التالي : $\varphi(1,x) = x$ لكل $x \in M$ ، أي تحقق الشرط : $1.x = x$ ، فإننا نقول عن M إنه فضاء حلقي يساري واحدي (بمحايد على الحلقة $(R,+,\cdot)$.

<u>-3</u> الفضاء الحلقي اليميني على حلقة Right module over aring

لتكن $(R,+,\cdot)$ حلقة ما ، إذا كانت M مجموعة غير خالية ، وإذا كانت $\star$ عملية جبرية ثنائية معرفة على M ، وإذا كان التطبيق φ معرفاً بالشكل : $\varphi : M\times R \longrightarrow M$ ، $\varphi(x,r) = x.r$ لكل x من M و r من R ، فإننا نقول عن M إنه فضاء حلقي يميني بالنسبة للحلقة $(R,+,\cdot)$ إذا تحققت الشروط التالية :

1) $(M,\star)$ زمرة إبدالية

2) $\varphi(x\star y\,,\,r) = \varphi(x,r)\star\varphi(y,r)$ ، أي أن : $(x\star y)\,.\,r = x.r\star y.r$

3) $\varphi(x\,,\,r+s) = \varphi(x,r)\star\varphi(x,s)$ ، أي أن : $x\,.(r+s) = x.r\star x.s$

4) $\varphi(x\,,\,r.s) = \varphi\big(\varphi(x,r)\,,\,s\big)$ ، أي أن : $x.(a.b) = (x.a).b$

وذلك لكل s,r من R و y,x من M .

<u>-4</u> إذا كانت الحلقة $(R,+,\cdot)$ بمحايد (ذات عنصر وحدة 1) ، وإذا تحقق بالإضافة إلى الشروط الأربعة السابقة ، الشرط التالي : $\varphi(x,1) = x$ لكل x من M أي أن $x.1 = x$ ، فإننا نقول عن M إنه فضاء حلقي يميني بمحايد (واحدي)

على الحلقة $(R,+,\cdot)$.

5- إذا كانت الحلقة $(R,+,\cdot)$ إبدالية ، وكان M فضاءً حلقياً يسارياً على الحلقة $(R,+,\cdot)$ ، فإنه يتحول إلى فضاء حلقي من اليمين على R. وهذا يعني أن $x.r = r.x$ ، لكل x من M و r من R.

نسمي عادةً عناصر الحلقة في التعريف السابق بعناصر قياسية ، كما نسمي عناصر الفضاء الحلقي M بمتجهات .

6- إن شروط الفضاء الحلقي هي شروط الفضاء المتجهي نفسها ، والفارق الوحيد بينهما هو أن الفضاء الحلقي M معرفاً على حلقة ما $(R,+,\cdot)$ ، بينما فضاء المتجهات يكون معرفاً على حقل ما وليكن $(F,+,\cdot)$.

7- من الضروري التمييز بين العملية الجبرية الثنائية ★ المعرفة على M وبين العملية الجبرية الثنائية (+) المعرفة على الحلقة $(R,+,\cdot)$ ، علماً أننا من الآن فصاعداً سنرمز لها بالرمز نفسه .

8- الشرط الأول الوارد في تعريف الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ يبيّن لنا أن $(M,+)$ زمرة إبدالية ، وبالتالي ، فإن كما في أية زمرة إبدالية ، مجموع عدد من الأشعة لا يتعلق بترتيب الحدود في هذا المجموع ، كما أنه لا يتعلق بوضع الأقواس فيه ، بالإضافة إلى ذلك يوجد في M متجه وحيد وليكن x_1 يكون من أجله $x = x + x_1$ لكل x من M ، سنرمز للمتجه x_1 بـ 0 ونسميه بالمتجه الصفري في الفضاء الحلقي M أو نسميه صفر الفضاء الحلقي M .

كما أنه من أجل أي متجه x من M ، يوجد متجه وحيد وليكن x_2 يكون من أجله $x + x_2 = 0$ ، نرمز للمتجه x_2 بـ -x ونسميه معكوس (نظير) x .

9- بالاستفادة من الملاحظة السابقة ، إذا كان y,x متجهين ما من M ، فإن :

$$0 + 0 = 0\,,\ \ x + (-x) = 0\ \ ,\ \ (x + y) + (1 - x) + (-y) = 0$$

وبالتالي ، فإن :

$$0 = -0 \quad ,\ x = -(-x) \quad ,\ -(x + y) = (-x) + (-y)$$

10- ليكن M فضاء حلقي ما على الحلقة $(R,+,\cdot)$ ، نعرف العملية الثنائية (-) على M بالشكل :

لكل y,x من M ، $x - y = x + (-y)$

وتسمى هذه العملية بعملية طرح (فرق) المتجهات .

(2-5) أمثلة :

(1) كل حلقة بمحايد ، ولتكن $(R,+,\cdot)$ تشكل فضاءً حلقياً على نفسها .

الحل :

لنعرف التطبيق $\varphi : R\times R \longrightarrow R$ بالشكل $\varphi(x,r) = x.r$ لكل r,x من R وفي هذه الحالة تتطابق المجموعتان R,M وبسهولة يمكن التأكد من الشروط الواردة في مفهوم الفضاء الحلقي اليساري أو اليميني .

(2) إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، وإذا كانت A مجموعة جزئية من R وغير خالية ، ولنفرض أن M مجموعة كل التطبيقات التالية :

$\varphi : A \longrightarrow R$

ولنعرف على M عملية ثنائية داخلية (+) بالشكل :

$(\varphi + \Psi)(x) = \varphi(x) + \Psi(x)$

لكل x من A و g,f من M ، وعملية خارجية بالشكل : $(r\,\varphi)(x) = r\,\varphi(x)$ لكل r من R و φ,x من M . المطلوب أثبت أن M فضاء حلقي بمحايد على الحلقة $(R,+,\cdot)$.

الحل :

1- يمكن البرهان بسهولة أن : $(M,+)$ زمرة إبدالية .

2- ليكن Ψ,φ عنصرين ما من M ، وإذا كان s,r عنصرين ما من R ، فإن :

$$\begin{aligned}(r(\varphi + \Psi))(x) &= r.\big((\varphi + \Psi)(x)\big) = r.\big(\varphi(x) + \Psi(x)\big)\\ &= r.\varphi(x) + r.\Psi(x) = (r.\varphi)(x) + (r.\Psi)(x)\\ &= (r.\varphi + r.\Psi)(x)\end{aligned}$$

لكل x من A . أي أن :

$$r(\varphi + \Psi) = r.\varphi + r.\Psi$$

-3 $\big((r+s)\varphi\big)(x) = (r+s).\varphi(x) = r.\varphi(x)+s.\varphi(x) = (r.\varphi)(x)+(s.\varphi)(x)$

$$= (r.\varphi) + s.\Psi)(x)$$

لكل x من A ، إذن : $(r+s)\varphi = r.\varphi + s.\varphi$

-4 $\big((r.s)\varphi\big)(x) = (r.s).\varphi(x) = r.\big(s.\varphi(x)\big) = r.\big((s.\varphi)(x)\big)$

$$= \big(r.(s.\varphi)\big)(x)$$

لكل x من A ، إذن $(r.s)\varphi = r.(s.\varphi)$

نستنتج مما سبق أن M فضاء حلقي على الحلقة $(R,+,\cdot)$، لنثبت أخيراً أنه بمحايد.

لنرمز لعنصر الوحدة في الحلقة $(R,+,\cdot)$ بالرمز 1 ، وبالتالي يكون لدينا :

$$(1.\varphi)(x) = 1.\varphi(x) = \varphi(x)$$

لكل $x\in A$ و $\varphi\in M$ ، أي أن $1.\varphi = \varphi$.

<u>(3)</u> لتكن $(Z,+,\cdot)$ حلقة الأعداد الصحيحة Z ، ولنعرف التطبيق φ على المجموعة غير الخالية M بالشكل :

$$\varphi : Z\times M \longrightarrow M$$

$\varphi(r,x) = r.x$ ، لكل x من M و r من Z .

إن M فضاء حلقي بمحايد على Z .

الحل :

بسهولة ، نرى أن ، $(M,+)$ زمرة إبدالية . كما يمكن التحقق من الشروط التالية :

$$r(x+y) = rx + ry$$

$$(r+s)x = r.x + s.y$$

$$(r.s)(x) = r.(s.x)$$

إذا كانت $(Z,+,\cdot)$ حلقة بمحايد (1)، فإن $1.x = x$. لكل y,x من M و r,s من Z.

مبرهنة (1) :

لتكن $(R,+,.)$ حلقة ما ، إذا كان M فضاءً حلقياً على R ، ولنرمز بـــ O و $O`$ لصفر الحلقة $(R,+,.)$ ولصفر الفضاء الحلقي M على الترتيب ، عندها يكون :

1) $O.x = O`$ لكل x من M

2) $r.O` = O`$ لكل r من R

3) إذا كان $x\in M$ و $r\in R$ ، فإن : $(-r).x = r(-x) = -r.x$

4) $\left(\sum_{i=1}^{s} r_i\right).x = \sum_{i=1}^{s} r_i.x$ ، لكل x من M و $r_1,r_2,\dots,r_s\in R$، حيث أن، $s \geq 2$

5) $r.\left(\sum_{i=1}^{s} x_i\right) = \sum_{i=1}^{s} r.x_i$ ، لكل r من R و $x_1,x_2,\dots,x_s\in M$ و $s \geq 2$

البرهان :

1) ليكن x متجهاً ما من M ، فإن :

$$O.x + O.x = (O + O).x = O.x = O.x + O`$$

ومنه يكون $O.x = O`$

2) ليكن r عنصراً ما من R ، فإن :

$$a.O` = a\,(O` + O`) = a\,O` = a\,O` + O`$$

وبالتالي يكون : $a\,O` = O`$

3) ليكن x متجهاً ما من M ، وإذا كان r عنصراً ما من R ، وبما أن :

$$r.x + (-r).x = (r + (-r)).x = O.x = O`$$

فإن :

$$(-r).x = -(r.x) \qquad (1)$$

وبما أن :

$$r.x + r\,(-x) = r\,(x + (-x)) = r.O` = O`$$

فإن :

$r\,(-x) = -(r.x)$ (2)

بمقارنة العلاقتين (1) و (2) نجد أن :

$(-r).x = r\,(-x) = -\,(r.x)$

4) ليكن x عنصراً ما من M ، وإذا كان $r_1,r_2,\ldots,r_s$ عناصر من R ، فإن :

$$\left(\sum_{i=1}^{s} r_i\right).x = \left(r_1 + \sum_{i=2}^{s} r_i\right).x = r_1.x + \left(\sum_{i=2}^{s} r_i\right).x$$

$$= \ldots = r_1.x + \ldots + r_s.x = \sum_{i=1}^{s} r_i.x$$

5) إذا كان r عنصراً ما من R، وإذا فرضنا أن $x_1,x_2,\ldots,x_s$ عناصر من M،
فإن :

$$r.\left(\sum_{i=1}^{s} x_i\right) = r.\left(x_1 + \sum_{i=2}^{s} x_i\right) = r.x_1 + r.\sum_{i=2}^{s} x_i$$

$$= \ldots = r\,x_1 + \ldots + r\,x_s = \sum_{i=1}^{s} r.x_i$$

نتيجة (1) :

إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، وليكن M فضاءً حلقياً بمحايد على R ، ولنفرض أن r من R ، وإذا كان العنصر r قابلاً للعكس في R ، وإذا كان y,x عنصرين من M ، عندئذٍ ، إذا كان: $r.x = r.y$ ، فإن : $x = y$

البرهان :

لنرمز لعنصر الوحدة في الحلقة $(R,+,\cdot)$ بالرمز 1 .

بما أن $r.x = r.y$ ، فإن :

$r^{-1}.\,(r.x) = r^{-1}.\,(r.y)$

$(r^{-1}.\,r)\,.\,x = (r^{-1}.\,r)\,.\,y$

$1.x = 1.y$

وبالتالي يكون : $x = y$.

نتيجة (2) :

إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وإذا رمزنا لعنصر الوحدة في R بالرمز 1 ، فإن : $(-1)\,x = -x$ ، لكل x من M .

البرهان :

بما أن : $(-r)\,x = -(r.x)$ لكل x من M و r من R

فإن : $(-1)\,x = -(1.x)$ لكل x من M

وبالتالي يكون $(-1)\,x = -x$

(3-5) الفضاءات الحلقية الجزئية Submodules :

تعريف (11) الفضاء الحلقي الجزئي على حلقة :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً ما على R ، الفضاء الحلقي الجزئي N من M ، هو مجموعة جزئية غير خالية من M تحقق الشرطين :

1) لكل y,x من N ، فإن : $x - y \in N$

2) إذا كان r عنصراً ما من R ، وكان x عنصراً ما من N ، فإن : $r.x \in N$

يتضح من التعريف السابق ، أن الفضاء الحلقي M على حلقة $(R,+,\cdot)$ ، يحـوي على الأقل ، فضاءين جزئيين هما $\{O`\}$ والفضاء الحلقي M نفسه ، علماً أن O\` هو صفر الفضاء الحلقي M .

ملاحظة (1) :

يمكن دمج الشرطين (1) و(2) الواردين في التعريف السابق ، بالشرط التالي : يكون N فضاءً حلقياً جزئياً من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$، إذا وفقط، إذا تحقق الشرط :

$$\forall\, x,y \in N ,\ \forall\, r,s \in R \ :\ r.x + s.y \in N$$

مثال (4) :

إذا كانت $(H,+)$ زمرة جزئية من الزمرة $(G,+)$ ، فإن $(A,+)$ تشكل فضاءً حلقياً

جزئياً من الفضاء الحلقي G على الحلقة $(Z,+,.)$ ، لأن إذا كان $n\in Z$ و $r\in A$ ، فإن :

$$n.r = \pm (a + a + \ldots + a)$$

مثال (5) :

لتكن $(R,+,.)$ حلقة ما ، وبفرض أن M_2 فضاء حلقي عناصره هي مصفوفات حقيقية على R، وإذا كانت $N = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} ; x, y \in R \right\}$ ، إن N فضاء حلقي جزئي من M_2 .

الحل :

من الواضح ، أن $\phi \neq N \subseteq M_2$.

وإذا كان $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \begin{pmatrix} z & t \\ -t & z \end{pmatrix}$ عنصرين ما من N ، فإن :

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} - \begin{pmatrix} z & t \\ -t & z \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} + \begin{pmatrix} -z & -t \\ t & -z \end{pmatrix}$$
$$= \begin{pmatrix} x-z & y-t \\ -y+t & x-z \end{pmatrix} \in N$$

وإذا كان r من R وكان $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ من N ، فإن :

$$r.\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} r.x & r.y \\ r.(-y) & r.x \end{pmatrix} = \begin{pmatrix} r.x & r.y \\ -(r.y) & r.x \end{pmatrix} \in N$$

نستنتج مما سبق تحقق الشرطين (1) و(2) الواردين في تعريف الفضاء الحلقي الجزئي إذن N فضاء حلقي جزئي من M_2 .

نقدم الآن بعض العمليات على الفضاءات الحلقية الجزئية .

أولاً : عملية الجمع :

لتكن $(R,+,.)$ حلقة ما ، وإذا كان M فضاءً حلقياً ما على R ، وليكن N_1 وN_2 فضاءين حلقيين جزئيين من M ، نسمي المجموعة :

$$\{x \in M : x = x_1 + x_2 \;;\; x_1 \in N_1 , x_2 \in N_2\}$$

بمجموع N_1 وN_2 ، ونرمز لذلك بالرمز $N_1 + N_2$.

يمكن التأكد بسهولة ، أنه إذا كانت N_3,N_2,N_1 فضاءات حلقية جزئية من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ ، فإن :

$$N_1+N_2 = N_2+N_1$$

$$N_1+(N_2+N_3) = (N_1+N_2) +N_3$$

توضح المبرهنة التالية ، أن حاصل مجموع فضاءين حلقيين جزئيين هو فضاء حلقي جزئي من فضاء حلقي .

مبرهنة (2) :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وبفرض أن N_1 وN_2 فضاءين حلقيين جزئيين من M ، عندئذٍ يكون N_1+N_2 فضاء حلقي جزئي من M .

البرهان :

حسب تعريف المجموعة N_1+N_2 ، نجد أن $\phi \neq N_1+N_2 \subseteq M$.

ليكن y,x عنصرين ما من N_1+N_2 ، وبالتالي يمكن كتابتهما بالشكل :

$$x = x_1 + x_2 \;;\; \forall\, x_1 \in N_1 ,\; x_2 \in N_2$$

$$y = y_1 + y_2 \;;\; \forall\, y_1 \in N_1 ,\; y_2 \in N_2$$

وبالتالي ، فإن :

$$x - y = (x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) \in N_1+N_2$$

ليكن الآن r عنصراً ما من R وx عنصراً ما من N_1+N_2 ، إن العنصر x يكتب بالشكل :

$$x = x_1 + x_2 \;;\; x_1 \in N_1 ,\; x_2 \in N_2$$

وبالتالي فإن :

$$r.x = r\,(x_1 + x_2) = r\,x_1 + r\,x_2 \in N_1+N_2$$

نستنتج مما سبق أن N_1+N_2 فضاء حلقي جزئي من M على الحلقة $(R,+,\cdot)$.

يمكن تعميم المبرهنة السابقة بالشكل التالي :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وإذا كانت $\{N_i\}_{i=1}^{n}$ أسرة من الفضاءات الحلقية الجزئية من M ، عندئذٍ يكون : $\sum_{i=1}^{n} N_i$ فضاء حلقي جزئي من M .

العملية الثانية عملية التقاطع :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وليكن M فضاءً حلقياً على R ، وبفرض أن N_1 و N_2 فضاءين حلقيين جزئيين من M ، المجموعة :

$\{x\in N : x\in N_1 \ , \ x\in N_2\}$ تسمى تقاطع N_1 و N_2 ويرمز لها بالرمز $N_1 \cap N_2$.

كما في عملية الجمع السابق ، يتضح من التعريف السابق أنه إذا كانت N_3,N_2,N_1 ثلاثة فضاءات حلقية جزئية من M ، فإن :

$$N_1 \cap N_2 = N_2 \cap N_1$$

$$N_1 \cap (N_2 \cap N_3) = (N_1 \cap N_2) \cap N_3$$

المبرهنة التالية ، تثبت أن تقاطع فضاءين حلقيين جزئيين من M هو فضاء حلقي جزئي أيضاً .

مبرهنة (3) :

بفرض أن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وليكن N_2,N_1 فضاءين حلقيين جزئيين من M ، عندئذٍ $N_1 \cap N_2$ فضاء حلقي جزئي من M .

البرهان :

من تعريف تقاطع فضاءين حلقيين جزئيين نجد أن $\phi \neq N_1 \cap N_2 \subseteq M$.

بفرض أن y,x عنصرين ما من $N_1 \cap N_2$ ، فإن : $x.y\in N_1 \ , \ x.y\in N_2$ ،

وبالتالي فإن :

$x-y\in N_2$, $x-y\in N_1$ ، وبالتالي فإن : $x-y\in N_1\cap N_2$.

ليكن الآن r عنصراً ما من R و x عنصراً ما من $N_1\cap N_2$ ، وهذا يؤدي إلى أن $x\in N_1$ و $x\in N_2$ ، وبالتالي ، فإن : $r.x\in N_2$, $r.x\in N_1$ ، ومنه يكون $r.x\in N_1\cap N_2$.

نستنتج مما سبق ، أن $N_1\cap N_2$ فضاء حلقي جزئي .

يمكن تعميم المبرهنة السابقة بالشكل :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وليكن M فضاء حلقي ما من R ، وإذا كانت $\{N_i\}_{i=1}^{n}$ أسرة غير خالية من الفضاءات الجزئية من M ، عندئذٍ $\bigcap_{i=1}^{n} N_i$ فضاء حلقي جزئي من M ، علماً أنه يرمز بـ $\bigcap_{i=1}^{n} N_i$ للمجموعة :

$$\{x\in M : x\in N_i \; ; i=1,2,..,n\}$$

نتيجة (3) :

يمكن البرهان بسهولة على ما يلي :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاء حلقي على R ، وإذا كانت N_1,N_2,N_3 ثلاثة فضاءات حلقية جزئية من M ، بحيث أن $N_2\subseteq N_1$ ، فإن :

$$N_1\cap (N_2+N_1) = N_2 + (N_1\cap N_3)$$

المساواة السابقة تبيّن لنا ارتباط عمليتي الجمع والتقاطع السابقتين ببعضهما .

مثال (6) :

لتكن B,A مجموعتين جزئيتين غير خاليتين من M,R على الترتيب، حيث $(R,+,\cdot)$ حلقة ما، M فضاء حلقي . وإذا كان :

$$AB=\left\{ \sum_{i=1}^{n} a_i.x_i \; ; a_i\in A \, , \, x_i\in B \, , \, n\in Z^+ \right\}$$

وإذا كانت A مثالية يسارية في الحلقة $(R,+,\cdot)$، فإن AB فضاء حلقي جزئي من

. M

الحل :

حسب تعريف المجموعة AB نجد أن $\phi \neq AB \subseteq M$. ليكن y,x عنصرين ما من AB ، فإنه يمكن كتابتهما بالشكل : $x=\sum_{i=1}^{n} a_i.x_i \ , \ y=\sum_{j=1}^{m} b_j.y_j$ ، حيث أن a_i و b_j من A و x_i و y_j من B و m,n عددان صحيحان موجبان ، وبالتالي فإن :

$$x-y=\sum_{i=1}^{n} a_i.x_i - \sum_{j=1}^{m} b_j.y_j$$

$$=\sum_{i=1}^{n} a_i.x_i + \sum_{j=1}^{m} (-b_j).y_j \in AB$$

بفرض أن r عنصر ما من R و x عنصر ما من AB ، لأن العنصر x يكتب بالشكل : $x=\sum_{k=1}^{S} c_k.x_k$ حيث أن c_k من A و x_k من B و s عدد صحيح موجب ، وبالتالي ، فإن :

$$a.x=a.\left(\sum_{k=1}^{S} c_k.x_k\right)=\sum_{k=1}^{S} a.(c_k.x_k)=\sum_{k=1}^{S} (a.c_k).x_k \in AB$$

نستنتج مما سبق أن AB فضاء حلقي جزئي من M .

(4-5) الفضاءات الحلقية منتهية التوليد Finite generated modules :

ليكن M فضاءً حلقياً ما على حلقة ما $(R,+,\cdot)$ ، ولتكن S مجموعة جزئية غير خالية من M، نعلم أن تقاطع كل الفضاءات الحلقية الجزئية من M التي يحوي كل منها S هو فضاء حلقي جزئي من M يحوي S . نسمي هذا الفضاء الحلقي الجزئي من M بالفضاء الحلقي الجزئي المولد بالمجموعة S ، ونرمز له عادةً بـ $< S >$.

بحالة خاصة ، إذا كانت المجموعة S منتهية ، أي أن $S = \{x_1,\ldots,x_n\}$ فإن $< S >$ تكتب بالشكل :

$$< S > = < x_1,\ldots,x_n >$$

نستنتج من التعريف السابق ، أنه إذا كان M فضاءً حلقياً على حلقة ما ، ولــتكن (R,+,•) ، وإذا كانت S مجموعة جزئية غير خالية من M ، فإن الفضاء الحلقــي الجزئي من M ، المولد بالمجموعة S ، هو أصغر فضاء حلقي جزئـــي مــن M يحوي S .

مبرهنة (4) :

لتكن S مجموعة جزئية غير خالية من الفضاء الحلقي M على الحلقة (R,+,•) ولنرمز بــ F لمجموعة كل التراكيب الخطية من الشكل : $\sum_{i=1}^{n} a_i . x_i + \sum_{j=1}^{m} b_j . y_j$ ، لكل a_i من R و x_i , y_i من S و b_j من Z و m,n عددان صحيحان موجبان ، عندئذ F فضاء حلقي جزئي من M يحوي S ، وهو أصغر فضاء حلقي جزئي مــن M يحوي S .

ملاحظة (2) :

ليكن M فضاءً حلقياً ما علـــى حلقـــة مـــا ، ولــتكن (R,+,•) ، وإذا كانــت $M \supseteq S \neq \phi$ ، إن الفضاء الحلقي الجزئي من M ، المولد بالمجموعة S يتــألف من جميع التراكيب الخطية التي من الشكل : $\sum_{i=1}^{n} a_i . x_i + \sum_{j=1}^{m} b_j . y_j$ ، حيــث أن y_i,x_i من S و a_i من R و b_j من Z و m,n عددان صحيحان موجبان .

وإذا كانت المجموعة S تتألف من عنصر واحد فقط ، وليكن x مثلاً ، فإن الفضاء الحلقي الجزئي من M، المولد بالعنصر x يتألف من جميع العناصر التي هي من الشكل $ax + bx$ حيث a من R و n من Z .

تعريف (12) :

الفضاء الحلقي M على الحلقة بمحايد (R,+,•) يسمى فضاءً حلقياً دائرياً إذا تحقق الشرط : $M = < m >$، لكل m من M .

نتيجة (4) :

ليكن (V,+,•) فضاءً متجهياً على الحقل (F,+,•) ، إن الفضاء V يكون مولــداً

بشكل نهائي كفضاء حلقي على الحقل F ، إذا ، وفقط إذا ، كان V فضاء متجهي على F ذا بعد منته، ويكون دائرياً، إذا وفقط إذا كان $\dim V = 0$ أو $\dim V=1$.

مبرهنة (5) :

إذا كان M فضاءً حلقياً على الحلقة بمحايد $(R,+,\bullet)$ مولداً بالمجموعة $\{x_1,x_2,\dots,x_n\}$ ، فإن :

$$M = \sum_{i=1}^{n} R\,x_i = \{\, r_1 x_1 + r_2 x_2 + \dots + r_n x_n \quad ; \quad r_i \in R \,\}$$

البرهان :

ليكن y,x عنصرين من $\sum_{i=1}^{n} R\,x_i$ وإذا كان $r\in R$ ، فإن :

$$x - y \in \sum_{i=1}^{n} R\,x_i \quad , \quad r.\,x \in \sum_{i=1}^{n} R\,x_i$$

أي أن $\sum_{i=1}^{n} R\,x_i$ يشكل فضاءً حلقياً على الحلقة $(R,+,\bullet)$.

وبما أن $1.x_i = x_i \in R\,x_i \subseteq \sum_{i=1}^{n} R\,x_i$ ، فإن $x_i \in \sum_{i=1}^{n} R\,x_i$.

وبما أن $\sum_{i=1}^{n} R\,x_i$ أصغر فضاء حلقي من M ، يحوي كل عناصر x_i ، إذن $M = \sum_{i=1}^{n} R\,x_i$.

ملاحظة (3) :

إن مجموعة مولدات الفضاءات الحلقية ليس بالضرورة أن تكون وحيدة ، فمثلاً، إذا كانت S مجموعة كل كثيرات الحدود بمتغير x مثلاً على حقل ما وليكن $(F,+,\bullet)$ درجتها أصغر أو تساوي n ، فإن S تشكل فضاء متجهات على الحقل F مجموعاتها المولدة هي :

$$\{1\,,\,x\,,\,x^2\,,\,\dots\,,\,x^n\} \;,\; \{1\,,\,1+x\,,\,x^2\,,\,x^3\,,\,\dots\,,\,x^n\}$$

نتيجة (5) :

إذا كانت $(R,+,\bullet)$ حلقة بمحايد ، وإذا كان M فضاء حلقي بمحايد أيضاً ، إن

الشرط اللازم والكافي لكي تكون المجموعة الجزئية $\phi \neq S \subseteq M$ مولدة لـــ M هو أن يكون بالإمكان كتابة كل عنصر x من M بالشكل $\sum_{i=1}^{n} r_i . x_i$ ، لكل x_i من S وr_i من R وn عدد صحيح موجب .

تعريف (13) الفضاء المتجهي الجزئي الرئيس :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاء حلقــي علــى R ولــيكن x عنصراً ما من M ، فإن $R.x$ هو فضاء حلقي جزئي من M ، يسمى فضاءً حلقياً جزئياً رئيساً مولداً بالعنصر x ، حيث أن :

$$R.x = \{ r.x \ : \ r \in R \}$$

ينتج من التعريف السابق ، أنه إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، وكان M فضـــاء حلقي بمحايد على R ، وإذا كان x عنصراً ما من M ، فإن $R.x = < x >$.

مثال (7) :

لتكن $(R,+,\cdot)$ حلقة ما بمحايد ، ولتكن M_2 مجموعـــة المصـــفوفات المربعـــة الحقيقية ، ولنعرف على M_2 العمليتين الثنائيتين الداخلية والخارجية على الترتيـــب بالشكل التالي :

$$\begin{pmatrix} x_1 & y_1 \\ z_1 & t_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ z_2 & t_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 & y_1 + y_2 \\ z_1 + z_2 & t_1 + t_2 \end{pmatrix}$$

لكل $\begin{pmatrix} x_1 & y_1 \\ z_1 & t_1 \end{pmatrix} , \begin{pmatrix} x_2 & y_2 \\ z_2 & t_2 \end{pmatrix}$ من M_2 .

$$r.\begin{pmatrix} x_1 & y_1 \\ z_1 & t_1 \end{pmatrix} = \begin{pmatrix} r x_1 & r y_1 \\ r z_1 & r t_1 \end{pmatrix} \ ; \forall r \in R$$

إن M_2 فضاء حلقي على R ، أثبت أن المجموعة

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

هي مجموعة مولدة لـــ M_2 .

الحل :

ليكن $A=\begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}$ عنصراً ما من M_2 ، يمكن كتابة المصفوفة A بالشكل :

$$\begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}=\begin{pmatrix} d_1 & 0 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} 0 & d_2 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ d_3 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ 0 & d_4 \end{pmatrix}$$

$$=d_1.\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}+d_2.\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}+d_3.\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}+d_4.\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

مثال (8) :

لنعرف على المجموعة R^2 : $R^2=\{\ (x_1,y_1)\ :\ x_1,y_1\in R\ \}$ ، حيث $(R,+,.)$ حلقة ما بمحايد ، العملية الثنائية الداخلية :

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2\ ,\ y_1+y_2)$$

لكل $x_1,x_2,\ y_1,y_2$ من R ، العملية الخارجية بالشكل :

$$r\,(x_1,y_1)=(r.x_1\ ,\ r.y_1)$$

لكل r من R و x_1,y_1 من R .

من الواضح أن R^2 فضاء حلقي بمحايد على R .

أثبت أن المجموعة $S=\{\ (1,0)\ ,\ (0,1)\}$ مولدة لـ R^2. (إن 0 هو صفر الحلقة و 1 محايدها).

الحل :

إن المجموعة S مولدة لـ R^2 ، لأن إذا كان b,a عنصرين ما من R ، فإن :

$$(a,b)=(a,0)+(0,b)=a\,(1,0)+b\,(0,1)$$

(5-5) المجموع المباشر للفضاءات الحلقية Direct sum of modules :

لتكن $\{N_i\}_{i=1}^{n}$ أسرة من الفضاءات الحلقية الجزئية من الفضاء الحلقي M على الحلقة بمحايد $(R,+,.)$. نقول عن الفضاء الحلقي M، إنه مجموع مباشر داخلي للفضاءات الحلقية الجزئية N_i، حيث $1\le i\le n$ إذا تحقق الشرطان :

$$M = \sum_{i=1}^{n} N_i \quad (1)$$

$$1 \le i, j \le n \text{ لكل ، } N_i \cap \sum_{i \ne j} N_j = \{0\} \quad (2)$$

سنرمز للمجموع المباشر الداخلي بالشكل :

$$M = N_1 \oplus N_2 \oplus \ldots . \oplus N_n = \oplus \sum_{i=1}^{n} N_i$$

المبرهنة التالية ، تبين لنا ، متى يكون فضاء حلقي M على حلقة ما ، مجموعاً مباشراً داخلياً للفضاءات الحلقية الجزئية ، والتي سنقبلها بدون برهان .

مبرهنة (6) :

لتكن $(R,+,\cdot)$ حلقة ما ، إذا كان M فضاءً حلقياً على الحلقة R ، يكون M مجموعاً مباشراً داخلياً للفضاءات الحلقية الجزئية N_i حيث $1 \le i \le n$ إذا ، وفقط إذا ، أمكن كتابة أي عنصر وليكن m من M بشكل وحيد بالشكل :

$$m = \sum_{i=1}^{n} a_i \;\; ; \;\; a_i \in N_i$$

مبرهنة (7) :

لتكن $(R,+,\cdot)$ حلقة ما، وإذا كان M فضاءً حلقياً على R ، وإذا كانت N_i ، حيث $1 \le i \le n$، أسرة من الفضاءات الحلقية الجزئية للفضاء الحلقي M عندئذٍ العبارات التالية متكافئة :

(1) $M = \sum_{i=1}^{t} N_i$ مجموع مباشر لأسرة الفضاءات N_i ، $i \in [1,t]$

(2) إذا كان $\sum_{i=1}^{t} n_i = 0$ ، حيث أن $n_i \in N_i$ ، فإن $n_i = 0$ ، $1 \le i \le t$

(3) $N_i \bigcap_{i \ne j} \sum N_j = \{0\}$ لكل $1 \le i \le t$.

البرهان :

$(1) \Rightarrow (2)$

لنفرض أن $M = \sum_{i=1}^{t} N_i$ مجموعاً مباشراً داخلياً ، وحسب المبرهنة السابقة ، أي عنصر من M وليكن m يكتب بصورة وحيدة ، ومن العلاقة

$\sum_{i=1}^{t} n_i = 0 = \sum O$ نجد أن $n_i = 0$ لكل $1 \le i \le t$.

(2) ⇒ (3)

إذا كـــان $m \in N_i \cap \sum_{i \ne j} N_j$ ، فـــإن $x = n_i = \sum_{i \ne j} n_j$ ، وبالتـــالي يكـــون $n_i - \sum_{i \ne j} n_j = 0$ ، وحسب الفرض $n_i = 0$ يكون $m = 0$ ، وهذا يعني أن :

$$N_i \cap \sum_{i \ne j} N_j = \{0\}$$

(3) ⇒ (1)

إذا كان $m = \sum_{i=1}^{t} n_i \;,\; m = \sum_{i=1}^{t} n'_i$ ، حيث $n_i , n'_i \in N_i$ ، لكـــل $1 \le i \le t$ ، وبالتالي نجد :

$$n_i - n'_i = \sum_{i \ne j} (n_j - n'_j) \in N_i \cap \sum_{i \ne j} N_j = \{0\}$$

وبالتالي فإن $n_i - n'_i = 0$ ، ويكون للعنصر m تمثيل وحيـــد ، ويكـــون $\sum_{i=1}^{t} N_i$ مجموعاً مباشراً داخلياً .

تعريف (14) :

لتكن $(R,+,\cdot)$ حلقة ما بمحايد ، وإذا كان M فضاءً حلقياً على R ، وبفرض أن N_i ، حيث $1 \le i \le r$ ، أسرة من الفضاءات الحلقية الجزئية من الفضاء الحلقـــي M على الحلقة R .

بأخذ الجداء الديكارتي $N_1 \times N_2 \times \ldots \times N_r$ ، وإذا كانت $(n_1,n_2,\ldots,n_r)$ مجموعة جميع المركبات من النوع r ، حيث $n_i \in N_i$ ، لكل $1 \le i \le r$.

لنعرّف عملية الجمع بالشكل :

$$(n_1,n_2,\ldots,n_r) + (m_1,m_2,\ldots,m_r) = (n_1+m_1 \,,\, \ldots\ldots \,,\, n_r+m_r)$$

وعملية الضرب القياسي بالشكل :

$$a\,(n_1,n_2,\dots,n_r) = (a\,n_1 , a\,n_2 , \dots , a\,n_r)$$

عندها نحصل على فضاء حلقي ، نسميه عادةً بالمجموع المباشر الخارجي للفضاءات الحلقية الجزئية N_i حيث $1 \le i \le r$. ونرمز لهذا المجموع بـ $N_1 \oplus N_2 \oplus \dots \oplus N_r$.

مثال (9) :

ليكن $(R,+,\cdot)$ حقل الأعداد الحقيقية ، وإذا كان $(V,+,\cdot) = R^3$ فضاء متجهات على الحقل R، أثبت أن : $V = R\,a_1 + R\,a_2 + R\,a_3$ وأن $V = \oplus\sum_{i=1}^{3} R\,a_i$ ، حيث أن :

$$a_1 = (1,0,0)\ ,\ a_2 = (1,1,0)\ ,\ a_3 = (1,1,1)$$

الحل :

بفرض أن المتجه (α,β,γ) من V ، عندها يكون :

$$(\alpha,\beta,\gamma) = (\alpha-\beta)\,a_1 + (\beta-\gamma)\,a_2 + \gamma\,a_3$$

ومنه يكون : $$V = R\,a_1 + R\,a_2 + R\,a_3$$

لنثبت الآن أن $V = \oplus\sum_{i=1}^{3} R\,a_i$.

ليكن $\alpha\,a_1 + \beta\,a_2 + \gamma\,a_3 = 0$ ، ومنه يكون :

$$\alpha+\beta+\gamma = 0\ ,\ \beta+\gamma = 0\ ,\ \gamma = 0$$

وبالتالي نحصل على ، $\alpha=\beta=\gamma=0$ ، إذن $R\,a_1 + R\,a_2 + R\,a_3$ هو مجموع مباشر داخلي، أي $V = \oplus\sum_{i=1}^{3} R\,a_i$.

(6-5) الفضاء الحلقي لخارج القسمة Quotient module :

ليكن M فضاءً حلقياً على حلقة ما ، ولتكن $(R,+,\cdot)$ ، وإذا كان N فضاءً حلقياً جزئياً من M، إن $(N,+)$ زمرة جزئية من الزمرة الإبدالية $(M,\star)$ (لأن N فضاء حلقي جزئي من M) . وبما أن أية زمرة جزئية من زمرة إبدالية هي زمرة

جزئية ناظمية منها ، فإن $(N,+)$ زمرة جزئية ناظمية من الزمرة $(M,+)$.

لنعرف على عناصر المجموعة M/N التالية :

$$M/N = \{ m + N \ : \ m \in M \}$$

عملية ثنائية داخلية $(+)$ بالشكل :

$$(m + N) + (m` + N`) = (m + m`) + N$$

لكل $m`,m$ من M .

عندها تكون $(M/N,+)$ زمرة إبدالية ، وإذا عرّفنا على M/N عملية خارجيـــة ، بالشكل :

$$r\,(m + N) = r.m + N$$

لكل r من R و m من M .

عندئذٍ تكون هذه العملية حسنة التعريف .

والمبرهنة التالية ، تثبت لنا أن M/N فضاء حلقي على الحلقة $(R,+,\cdot)$.

مبرهنة / تعريف (8) :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وإذا كان N فضاءً حلقياً من M، إذا عرّفنا على المجموعة M/N التالية :

$$M/N = \{ m + N : \ m \in M \}$$

عملية ثنائية داخلية $(+)$ بالشكل :

$$(m + N) + (m' + N) = (m + m') + N$$

لكل m', m من M . وعملية خارجية $(\cdot)$ بالشكل :

$$r\cdot(m + N) = r\cdot m + N$$

لكل r من R و m من M . عندئذٍ M/N فضاء حلقي على R بالنســبة للعمليتــين المعرفتين على المجموعة M/N .

نسمي M/N مع العمليتين الثنائيتين السابقتين ، بفضاء حلقي خارج القسمة لـــ M على N .

البرهان :

لنبرهن أولاً ، أن $(M/N,+)$ زمرة إبدالية .

أ- إن العملية (+) تجميعية على عناصر M/N ، لأن :

لكل $m+N\,,\,m'+N\,,\,m''+N$ من M/N ، فإن :

$$\left[(m+N)+(m'+N)\right]+(m''+N)=\left[(m+m')+N)\right]+(m''+N)$$
$$=\left[(m+m'+m'')\right]+N=\left[m+(m'+m'')\right]+N$$
$$=(m+N)+\left[(m'+m'')+N\right]=(m+N)+\left[(m'+N)+(m''+N)\right]$$

ب- العنصر المحايد في M/N هو $O+N=N$ لأنه :

$$(m+N)+(O+N)=(m+O)+N=m+N=(O+m)+N$$
$$=(O+N)+(m+N)$$

لكل $m+N$ من M/N .

جـ- يوجد لكل عنصر $m+N$ من M/N معكوس وهو $(-m)+N$ لأن :

$$(m+N)+\left[(-m)+N\right]=\left[m+(-m)\right]+N=O+N$$
$$=\left[(-m)+m\right]+N=\left[(-m)+N\right]+(m+N)$$

د- إن العملية (+) إبدالية ، لأنه لكل $m+N\,,\,m'+N\in M/N$ ، يكون :

$$(m+N)+(m'+N)=(m+m')+N=(m'+m)+N$$
$$=(m'+N)+(m+N)$$

لنثبت الآن أن العملية الخارجية حسنة التعريف .

ليكن r عنصراً ما من R، وليكن m',m عنصرين ما من M، بحيث يكون : $m+N=m'+N$، وبالتالي فإن $m-m'\in N$ ، أي أن $r\,(m-m')\in N$ ، وبالتالي يكون : $r.m-r.m'\in N$

إذاً : $r.m+N=r.m'+N$

لنبرهن الآن أن :

1) $r\left[(m+N)+(m'+N)\right]=r(m+N)+r(m'+N)$

2) $(r+s)(m+N)=r(m+N)+s(m+N)$

3) $(r.s)(m+N)=r\left(s(m+N)\right)$

لكل s,r من R و m, m′ من M .

$$1)\quad r\left[(m+N)+(m'+N)\right]=r\left[(m+m')+N)\right]=r(m+m')+N$$
$$=(r.m+r.m')+N=(r.m+N)+(r.m'+N)$$
$$=r(m+N)+r(m'+N)$$

وذلك لكل r من R و m, m′ من M .

$$2)\quad (r+s)(m+N)=(r+s)m+N=(r.m+s.m)+N$$
$$=(r.m+N)+(s.m+N)=r(m+N)+s(m+N)$$

لكل s,r من R و m من M .

$$3)\quad (r.s)(m+N)=(r.s)m+N=r.(s.m)+N=r(s.m+N)$$
$$=r\left[s(m+N)\right]$$

لكل s,r من R و m من M .

نستنتج مما سبق أن M/N فضاء حلقي على M بالنسبة للعمليتين المعرفتين على M/N .

ملاحظة (4) :

إذا كانت (R,+,.) حلقة بمحايد ، وإذا كان M فضاءً حلقياً بمحايد على R ، وإذا كان N فضاء حلقي جزئي من M ، عندئذٍ يكون M/N فضاء حلقي خارج القسمة بمحايد ، لأنه :

$$1.(m+N)=1.x+N=x+N$$

حيث 1 هو العنصر المحايد في الحلقة (R,+,.) ، ولكل x من M .

(7-5) تشاكل الفضاءات الحلقية Homomorphism of modules :

لتكن (R,+,.) حلقة ما ، وإذا كان M و M_1 فضاءين حلقيين على R . نقول

عن التطبيق :

$\varphi: M \longrightarrow M_1$ إنه تشاكل للفضاء الحلقي M في الفضاء الحلقي M_1 ، إذا تحققت الشروط التالية :

1) لكل y,x من M ، إن : $\varphi(x+y) = \varphi(x) + \varphi(y)$

2) لكل x من N و r من R ، فإن : $\varphi(r.x) = r.\varphi(x)$

ويمكن أن نعرف التشاكل السابق بالشكل التالي :

يكون التطبيق $\varphi: M \longrightarrow N$ تشاكلاً بين فضاءين حلقيين على الحلقة $(R,+,.)$ ، إذا ، وفقط إذا، تحقق الشرط :

لكل m',m من M و s,r من R :

$$\varphi(r.m + s.m') = r\,\varphi(m) + s\,\varphi(m')$$

يمكننا تعريف التشاكل الأحادي ، والتشاكل الشامل ، والتماثل لفضاءين حلقيين ، كما عرّفنا تماماً في نظرية الزمر والحلقات ، فمثلاً ، يكون التطبيق $\varphi: M \longrightarrow N$ تماثلاً بين الفضاءين الحلقيين N,M على الحلقة $(R,+,.)$ ، إذا كان φ تشاكلاً وتقابلاً ، أي أن φ متباين وشامل . ويحقق الشرطين الواردين في تعريف التشاكل السابق .

ملاحظات :

(1) لا يمكن تعريف التشاكل لفضاءين حلقيين على حلقتين مختلفتين ، أي يجب أن يكون الفضاءان N,M معرفين على الحلقة $(R,+,.)$ نفسها .

(2) إذا كانت الحلقة $(R,+,.)$ تشكل حقلاً F أو حلقة القسمة، عندها يسمى التشاكل بين الفضاءين الحلقيين N,M على الحقل F تحويلاً خطياً من فضاء متجهي M إلى فضاء متجهي N

(3) يرمز عادةً لمجموعة كل التشاكلات من M إلى N بـ $\mathrm{Hom}\,(M,N)$. وفي حالة خاصة ، إذا كان $N = M$ نسمي عادةً بالتشاكل الداخلي ونرمز له بـ $\mathrm{End}_R(M)$.

وإذا كان φ تماثلاً بين الفضاءين الحلقيين N,M ، وإذا فرضنا أن $N = M$ ، فإن التماثل السابق يسمى بتماثل داخلي $Aut_R(M)$.

(4) نرمز عادةً للتماثل بين فضاءين حلقيين بـــ $\cong$.

تعريف النواة وصورة الفضاء الحلقي Kern , Image module :

ليكن M',M فضاءين حلقيين على حلقة ما ، ولتكن $(R,+,.)$ ولنرمز بـــ O' لصفر الفضاء الحلقي M' ، وإذا كان φ تشاكلاً للفضاء الحلقي M في الفضاء الحلقي M' ، فإن المجموعة :

$$\{ x \in M : \varphi(x) = O' \}$$

تسمى نواة φ ، ويرمز لها عادةً بـــ $Ker\ \varphi$. ونسمي المجموعة $\{\varphi(m)\ ;\ m \in M\}$ بصورة الفضاء الحلقي M ويرمز لها بـــ $Im\ \varphi$.

إذن :

$$Ker\ \varphi = \{ x \in M : \varphi(x) = O' \}$$
$$Im\ \varphi = \{ \varphi(m)\ ;\ m \in M \}$$

حيث O' صفر الفضاء الحلقي M' .

مبرهنة (9) :

إذا كانت $(R,+,.)$ حلقة ما ، وليكن M', M فضاءين حلقيين على R ، ولنرمز بـــ O و O' لصفري الفضاءين الحلقيين M',M على الترتيب إذا كان φ تشاكلاً للفضاء الحلقي M في الفضاء الحلقي M' ، فإن :

1) $\varphi(O) = O'$

2) $\varphi(-m) = -\varphi(m)$ ، لكل m من M

3) $\varphi(m - n) = \varphi(m) - \varphi(n)$ ، لكل m,n من M

4) $\varphi\left(\sum_{i=1}^{n} r_i.m_i\right) = \sum_{i=1}^{n} r_i.\varphi(m_i)$ ، لكل r_i من R و m_i من M و $n \in Z^+$

تبرهن بالطريقة نفسها التي برهنت في الحلقات .

مبرهنة (10) :

إذا كان M و M' فضاءين حلقيين على حلقة ما، ولتكن $(R,+,\cdot)$، وإذا كان $\varphi: M \longrightarrow M'$ تشاكلاً بين الفضاءين الحلقيين M', M ، عندها :

1) $\mathrm{Ker}\,\varphi$ تشكل فضاءً حلقياً جزئياً من M

2) $\mathrm{Im}\,\varphi$ تشكل فضاءً حلقياً جزئياً من N .

البرهان :

إن $\mathrm{Ker}\,\varphi \neq \phi$ ، لأنه $\varphi(O) = O'$ (حسب المبرهنة السابقة) ، وبالتالي فإن $O \in \mathrm{Ker}\,\varphi$. لنبرهن الآن أن : $m - m' \in \mathrm{Ker}\,\varphi$ ، لكل m', m من $\mathrm{Ker}\,\varphi$.

$$\varphi(m - m') = \varphi[m + (-m')] = \varphi(m) + \varphi(-m')$$
$$= \varphi(m) - \varphi(m') = o - o = o$$

إذن $m - m' \in \mathrm{Ker}\,\varphi$.

لنبرهن أخيراً أنه إذا كان r من R و m من $\mathrm{Ker}\,\varphi$ ، فإن $r.m \in \mathrm{Ker}\,\varphi$.

بما أن $\varphi(r.m) = r.\varphi(m) = r.o = o$ ، فإن : $r.m \in \mathrm{Ker}\,\varphi$.

نستنتج مما سبق ، أن : $\mathrm{Ker}\,\varphi$ فضاء حلقي جزئي على الحلقة $(R,+,\cdot)$ من الفضاء الحلقي M .

(2) إن $\mathrm{Im}\,\varphi \neq \phi$ ، لأن $\varphi(o) = o'$ ، وهذا يعني ، حسب تعريف $\mathrm{Im}\,\varphi$ أن $o' \in \mathrm{Im}\,\varphi$.

إذا كان n,n' من $\mathrm{Im}\,\varphi$ ، فإنه يوجد m,m' من M، بحيث يكون :

$\varphi(m') = n', \varphi(m) = n$

ومنه يكون :

$$n - n' = \varphi(m) - \varphi(m') = \varphi(m) + \varphi(-m')$$
$$= \varphi[m + (-m')] = \varphi(m - m')$$

أي أن $n - n' \in \mathrm{Im}\,\varphi$.

وإذا كان r من R و n من $\mathrm{Im}\,\varphi$ ، فإن :

$$r.n = r.\varphi(m) = \varphi(r.m)$$

أي أن $r.m \in \mathrm{Im}\,\varphi$ ، حيث m من M .

نستنتج مما سبق ، أن $\mathrm{Im}\,\varphi$ فضاءً حلقياً جزئياً على الحلقة $(R,+,\cdot)$ ، من الفضاء الحلقي N .

مبرهنة (11) :

الشرط اللازم والكافي، لكي يكون التشاكل $\varphi : M \longrightarrow N$ أحادياً هو أن يكون $\mathrm{Ker}\,\varphi = \{0\}$، حيث N,M فضاءين حلقيين على حلقة ما ولتكن $(R,+,\cdot)$. و o هو صفر الفضاء الحلقي M .

البرهان :

لنفرض أولاً أن التشاكل φ أحادياً ، ولنبرهن أن $\mathrm{Ker}\,\varphi = \{0\}$.

ليكن $m \in \mathrm{Ker}\,\varphi$ ، وهذا يعني أن $\varphi(m) = \varphi(o) = o'$ ، وبما أن التطبيق φ أحادي ، فإن $m = 0$ لكل $m \in \mathrm{Ker}\,\varphi$ ، وهذا يعني أن $\mathrm{Ker}\,\varphi \subseteq \{0\}$ ، وبما أن $\{0\} \subseteq \mathrm{Ker}\,\varphi$ ، إذن $\mathrm{Ker}\,\varphi = \{0\}$.

لنبرهن الآن أن φ أحادي ، علماً أن $\mathrm{Ker}\,\varphi = \{0\}$ ، ليكن $\varphi(m) = \varphi(m')$ ، لكل m′.m من M، وبالتالي يكون: $\varphi(m) - \varphi(m') = o'$ أو $\varphi(m - m') = o'$، وهذا يعني أن $m - m' \in \mathrm{Ker}\,\varphi = \{0\}$ ، إذن $m - m' = 0$ ، وبالتالي يكون لدينا $m = m'$. إذن التشاكل φ أحادي .

(8-5) أمثلة :

مثال (10) :

إذا كان M فضاءً حلقياً على الحلقة $(R,+,\cdot)$، يمكن التحقق بسهولة أن التطبيق $I:M \longrightarrow M$ المعرف بـ $I(m) = m$ ، لكل m من M هو تشاكل على الفضاء الحلقي M . (يسمى عادةً هذا التشاكل بالتشاكل الذاتي المطابق على M) .

كما أن التطبيق $O : M \longrightarrow M$ المعرف بـ $O(m) = O$ حيث $m \in M$ تشاكل

على الفضاء الحلقي M ، O هو صفر هذا الفضاء . (يسمى عادةً هذا التشاكل بالتشاكل الذاتي الصفري) .

مثال (11) :

إذا كان M فضاءً حلقياً على الحلقة الإبدالية $(R,+,\cdot)$ ، أثبت أن التطبيق $\varphi : M \longrightarrow M$ المعرف بالشكل $\varphi(m) = 7m$ لكل m من M هو تشاكل ذاتي على M .

الحل :

لكل m',m من M يكون :

$$\varphi(m + m') = 7(m + m') = 7m + 7m'$$
$$= \varphi(m) + \varphi(m')$$

وكذلك نجد أن : $\varphi(7m) = 7\varphi(m)$ لكل m من M .

مثال (12) :

ليكن M فضاءً حلقياً على حلقة ما $(R,+,\cdot)$ ، وإذا كان L,N فضاءان حلقيان جزئيان من M بحيث إن $M = L \oplus N$ أثبت أن $N \cong M/L$.

الحل :

لنعرّف التطبيق $\varphi : N \longrightarrow M/L$ بالشكل : $\varphi(m) = m + L$ ، لكل m من N.
ولنبرهن أولاً أن φ تشاكل لـ N على M/L .

ليكن m',m عنصرين ما من N ، وإذا كان r من R ، فإن :

$$\varphi(m + m') = (m + m') + L = (m + L) + (m' + L)$$
$$= \varphi(m) + \varphi(m')$$
$$\varphi(r.m) = r.m + L = r\,(m + L) = r\,\varphi(m)$$

إذن φ تشاكلاً ، لنبرهن أن φ تقابلاً (متباين وشامل) .

ليكن m',m عنصرين ما من N بحيث يكون : $\varphi(m) = \varphi(m')$. بما أن m',m

من N (فضاء حلقي جزئي) فإن $m - m' \in N$ وبما أن $\varphi(m) = \varphi(m')$ فإن $m + L = m' + L$ وهذا يعني أن $m - m' \in L$.

نستنتج من : $m - m' \in N$ و $m - m' \in L$ أن $m - m' \in L \cap N$.

وبما أن $M = L \oplus N$ ، فإن : $L \cap N = \{0\}$ حيث 0 هو صفر الفضاء الحلقي M . إذن $m - m' = 0$ ، وبالتالي يكون $m = m'$.

لنبرهن أخيراً أن φ شامل .

ليكن u عنصراً ما من M ، فإنه يمكن كتابته بالشكل : $u = u_1 + u_2$ حيث $u_1 \in L , u_2 \in L$ ، وبالتالي يكون :

$$\varphi(u_2) = u_2 + L = (u_1 + L) + (u_2 + L) = (u_1 + u_2) + L = u + L$$

نستنتج مما سبق أن φ تماثل لـ N على M/L ، أي أن $N \cong M/L$.

مبرهنة (12) تطبيق الغمر القانوني :

ليكن N فضاءً حلقياً جزئياً من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ ، عندئذٍ التطبيق $\varphi : M \longrightarrow M/N$ ، المعرف بالشكل : $\varphi(m) = m + N$ لكل m من M تشاكلاً شاملاً . نسمي عادةً هذا التشاكل بتطبيق الغمر القانوني .

البرهان :

لكل m',m من M ، يكون :

$$\begin{aligned}\varphi(m + m') &= (m + m') + N = (m + N) + (m' + N)\\ &= \varphi(m) + \varphi(m')\end{aligned}$$

وإذا كان r من R و m من M ، فإن :

$$\varphi(r.m) = (r.m) + N = r.(m + N) = r.\varphi(m)$$

وبسهولة نرى أن التطبيق φ شامل ، ويتضح هذا من التعريف مباشرةً .

إذن $M \cong M/N$.

(5-9) المبرهنات الأساسية للتشاكل في الفضاءات الحلقية :

تبرهن المبرهنات الأساسية للتشاكل في الفضاءات الحلقية على حلقة ما ، بنفس

الطريقة التي تمّ برهانها في النظريات للتشاكل في الزمر والحلقات ، لذا لا داعي لبرهانها مرة أخرى .

مبرهنة (13) مبرهنة التماثل الأولي (First isomorphism's theorem) :

بفرض أن التطبيق $\varphi : M \longrightarrow N$ تشاكلاً بين الفضاءين الحلقيين N.M على الحلقة $(R,+,\cdot)$ ، عندئذٍ يكون :

$$M/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

مبرهنة (14) مبرهنة التماثل الثانية (2^{nd} Isomorphism's theorem) :

إذا كان L,N فضاءين حلقيين جزئيين من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ ، عندئذٍ :

$$(N+L)/N \cong L/(N \cap L)$$

مبرهنة (15) المبرهنة الثالثة للتماثلات (3^{nd} Isomorphism's theorem) :

إذا كان L,N فضاءين حلقيين جزئيين من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ ، حيث $L \subseteq N$ ، فإن :

$$M/N \cong M/L \Big/ N/L$$

نتيجة (6) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وإذا كانت I مثالية يسارية في R ، يكون الفضاء M دائرياً إذا ، وفقط إذا ، كان $M \cong R/I$.

البرهان :

لتكن $I = \{r \in R : r.x = 0\}$ مثالية يسارية في R . وليكن $M \cong R.x$ فضاءً حلقياً دائرياً مولداً بالعنصر x . لنعرّف التطبيق : $\varphi : R \longrightarrow Rx$ بالشكل : $\varphi(r) = r.x$ لكل r من R .

لنبرهن الآن أن φ تشاكل :

$$\varphi(r+s) = (r+s)\,x = rx + sx$$

$$\varphi(s.r) = (s.r).x = s.(r.x) = s.\varphi(r)$$

لكل $r,s,x \in R$.

كما أن φ شامل لأنه ، لكل $r.x \in Rx$ ، عندها يوجد $r \in R$ ، حيث أن $\varphi(r) = r.x$.

كما أن نواة التطبيق φ هي :

$$\operatorname{Ker} \varphi = \{r \in R : rx = 0\} = I$$

باستخدام المبرهنة الأولى للتماثلات نجد : $R/I \cong R.x$

لنبرهن العكس :

أي لنبرهن أن R/I دائري .

الفضاء الحلقي R/I على الحلقة بمحايد R مولد بالعنصر $1 + I \in R/I$ ، وبالتالي ، يكون : $R(1+I) = R/I$ ، أي أن ، R/I دائري .

(10-5) الفضاءات الحلقية الحرة :

بدايةً نعرّف الارتباط والاستقلال الخطيان .

تعريف (15) الاستقلال الخطي (Linearly independndt) :

ليكن M فضاء حلقي على الحلقة بمحايد $(R,+,\cdot)$. نقول عن المجموعة $A = \{a_1,a_2,\ldots,a_n\}$ غير الخالية من الفضاء الحلقي M إنها مستقلة خطياً ، إذا وُجِدَتْ عناصر من R ولتكن r_i بحيث يتحقق ما يلي :

إذا كان $\sum_{i=1}^{n} r_i.a_i = 0$ ، فإن $r_1 = r_2 = \ldots. = r_n$.

غير ذلك ، نقول عن المجموعة A إنها مرتبطة خطياً (Linearly dependndt) أي إذا وُجِدَتْ عناصر r_i من R ، ليست جميعها أصفاراً ، بحيث يكون $\sum_{i=1}^{n} r_i.a_i = 0$.

كما في الفضاءات المتجهية على حقل ، المجموعة غير المنتهية لعناصر من الفضاء الحلقي M على الحلقة R تكون مستقلة خطياً ، إذا كانت كل مجموعة

جزئية منتهية منها مستقلة خطياً ، غير ذلك تكون المجموعة غير المنتهية مرتبطة خطياً .

نتيجة (7) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وبفرض أن $\{x_i\}$ حيث $i = 1,2,\ldots,n$ (n عدد صحيح موجب) أسرة عناصر من M . وإذا كانت $\{x_i\}$ مستقلة خطياً على R ، وإذا كان $\sum_{i=1}^{n} a_i.x_i = \sum_{i=1}^{n} b_i.x_i$ ، لكل a_i , b_i من R فإن : $a_i = b_i$ من أجل $i = 1,2,\ldots,n$.

البرهان :

لنرمز بـ o' لصفر الفضاء الحلقي M على R ، ولصفر الحلقة $(R,+,\cdot)$ بـ o عندها يكون :

$$\sum_{i=1}^{n}(a_i - b_i).x_i = o' \Rightarrow \sum_{i=1}^{n} a_i.x_i = \sum_{i=1}^{n} b_i.x_i$$

وبالتالي : $a_i - b_i = o \Rightarrow a_i = b_i \;\; ; \;\; i = 1,2,\ldots,n$

مثال (13) :

بفرض أن $M = R^n$ فضاءً حلقياً على الحلقة بمحايد $(R,+,\cdot)$. يمكن التحقق بسهولة أن المجموعة :

$$S = \{e_1 = (1,0,\ldots,0) , e_2 = (0,1,0,\ldots,0) , \ldots , e_1 = (0,0,\ldots,0,1)\}$$

مستقلة خطياً في M. المجموعة S السابقة من الفضاء R^n تسمى قاعدة (أساساً) معيارياً لـ R^n .

تعريف (16) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وبفرض أن $\{x_i\}$ أسرة عناصر من M حيث $i = 1,2,..,n$. نقول إن $\{x_i\}$ تشكل قاعدة لـ M على R إذا تحقق :

1) $M = (x_1,x_2,\ldots,x_n)$

2) المجموعة $\{x_i\}$ حيث $i = 1,2,..,n$ مستقلة خطياً على R .

تعريف (17) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً بمحايد علـى R ، وإذا كانت N مجموعة جزئية غير خالية من M ، فإننا نقول عن N إنها قاعدة (أساس) لـ M على R إذا تحقق ما يلي :

1) $M = (N)$ أي أن الفضاء الحلقي M يولد بالمجموعة N .

2) المجموعة N مستقلة خطياً على R .

تعريف (18) الفضاء الحلقي الحر Free module :

إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً بمحايد علـى R ، نقول عن M إنه فضاء حر، إذا كان لـ M قاعدة على R أو إذا كـان M هـو الفضاء الحلقي الصفري .

ملاحظة (5) :

ليس ضرورياً أن يكون لكل فضاء حلقي M على الحلقة $(R,+,\cdot)$ أساساً فمثلاً ، إذا كانت $(G,\star)$ زمرة دائرية (يمكن اعتبارها فضـاء حلقـي G علـى الحلقـة $(Z,+,\cdot)$) . إن الزمرة G تملك أساساً إذا ، وفقط إذا ، كانت G غيـر منتهيـة . (يمكن التأكد من ذلك بطريقة نقض الفرض).

مثال (14) :

كل فضاء متجهي V على حقل F يشكل فضاءً حلقياً حراً لأنه يملك قاعدة .

مبرهنة (16) :

لتكن $N = \{e_1,e_2,\ldots,e_n\}$ قاعدة للفضاء الحلقـي الحـر M علـى الحلقـة $(R,+,\cdot)$ ، عندئذٍ : $M \cong R^n$

البرهان :

لنعرّف التطبيق φ : $\varphi : M \longrightarrow R^n$ بالشكل : $\varphi\left(\sum_{i=1}^{n} a_i . e_i\right) = \sum_{i=1}^{n} a_i' . t_i$

حيث أن $t_i = (0,0,\ldots,0,1,0,\ldots,0)$.

بما أن $\sum_{i=1}^{n} a_i.e_i = \sum_{i=1}^{n} a'_i.t_i$ ، حسب الاستقلال الخطي يكون $a_i = a'_i$ لكل i ، وهذا يعني أن φ حسن التعريف .

ليكن m,m' من M ، فإن $m = \sum_{i=1}^{n} a_i.e_i \ , \ m' = \sum_{i=1}^{n} a'_i.e_i$ لكل $a_i , a'_i \in R$.

إن التطبيق φ تشاكل لأنه يحقق :

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

$$\varphi(r.m) = r.\varphi(m)$$

لنبرهن أن φ متباين .

إذا كان $\varphi(m) = 0$، فهذا يعني أن $\sum_{i=1}^{n} a_i.t_i = 0$ وبذلك يكون $(a_1,a_2,\ldots,a_n) = 0$، أي أن $a_i = 0$ وهذا يعني أن φ متباين . وحسب تعريف التطبيق φ نجد أيضاً أن φ شامل .

نستنتج مما سبق أن φ تماثل بين M و R^n .

ملاحظة (5) :

إذا كان V فضاءً متجهياً على الحقل F ، وإذا كانت $N = \{n_1,n_2,\ldots,n_t\}$ مجموعة جزئية في V مرتبطة خطياً ، فإن أي عنصر من عناصر المجموعة N ، يكتب على شكل تركيب خطي لعناصر من N، لكن الأمر يختلف في الفضاءات الحلقية .

المبرهنة التالية تبيّن وجود فضاء حلقي حر بدلالة التشاكل الحلقي للفضاءين الحلقيين M',M .

مبرهنة (17) :

لتكن $(R,+,.)$ حلقة بمحايد ، وإذا كان M',M فضاءين حلقيين بمحايدين على R ، وإذا كان n عدداً صحيحاً موجباً ، ولتكن $\{x'_i\}_{i=1}^{n}$ أسرة عناصر من M' ، بحيث تكون $\{x'_i\}_{i=1}^{n}$ تشكل قاعدة لـ M' على R ، وإذا كان φ تشاكلاً للفضاء

الحلقي M على الفضاء الحلقي M' ، عندئذٍ يوجد فضاء حلقي حر وليكن F من M ويكون من أجله : $M = F \oplus \operatorname{Ker} \varphi$

البرهان :

بما أن التطبيق φ هو تشاكل ، للفضاء الحلقي M على الفضاء الحلقي M' ، فهذا يعني ، أن التطبيق $\varphi : M \longrightarrow M'$ شامل ، وبالتالي توجد عناصر ولتكن $x_1, x_2, \ldots, x_n$ من M بحيث يكون $\varphi(x_i) = x'_i$ لكل $i = 1,2,\ldots,n$.

إن أسرة العناصر $\{x_i\}$ حيث $i=1,2,\ldots,n$ مستقلة خطياً على R ، لأنه إذا فرضنا أن a_i من R حيث $i=1,2,\ldots,n$ وبحيث يكون $\sum\limits_{i=1}^{n} a_i . x = o$ حيث o هو صفر الفضاء الحلقي M، فإن $\varphi\left(\sum\limits_{i=1}^{n} a_i . x_i\right) = o'$ حيث o' هو صفر الفضاء الحلقي M' ، وبالتالي يكون : $\sum\limits_{i=1}^{n} a_i . x_i = o'$ ، أي أن $a_i = o''$ من أجل $i = 1,2,\ldots,n$ ، حيث o'' هو صفر الحلقة R .

لنفرض الآن F هو الفضاء الحلقي الجزئي من M المولد بالمجموعة $\{x_1, x_2, \ldots, x_n\}$ أي أن :

$F = (x_1, x_2, \ldots, x_n)$ ، وبما أن $\{x_i\}_{i=1}^{n}$ مستقلة خطياً على R ، فإن $\{x_i\}_{i=1}^{n}$ تشكل قاعدة لـ F على R . أي أن F هو فضاء حلقي جزئي حر من M .

ليكن x عنصراً ما من M ، وبالتالي يكون $\varphi(x) \in M'$ وهذا يعني أنه بالإمكان كتابة $\varphi(x)$ بالشكل : $\varphi(x) = \sum\limits_{i=1}^{n} b_i . x'_i$ لكل b_i من R . وبالتالي يكون لدينا :

$$\varphi(x) - \sum_{i=1}^{n} b_i . x'_i = o'$$

$$\varphi(x) - \varphi\left(\sum_{i=1}^{n} b_i . x_i\right) = o'$$

$$\varphi\left(x - \sum_{i=1}^{n} b_i . x_i\right) = o'$$

وهذا يعني ، أن : $x-\sum_{i=1}^{n} b_i.x_i \in \operatorname{Ker}\varphi$ ، أي أن $M = F + \operatorname{Ker}\varphi$

ليكن y عنصراً ما من $F \cap \operatorname{Ker}\varphi$، وبالتالي، يمكن كتابة العنصر y بالشكل : $y=\sum_{i=1}^{n} c_i.x_i$ لكل c_i من R .

من ناحية ثانية ، لدينا $\varphi(y) = o'$ ، إذن يكون لدينا : $\varphi\left(\sum_{i=1}^{n} c_i.x_i\right) = o'$ ، أي أن $\sum_{i=1}^{n} c_i.x_i = o'$ ، وهذا يعني أن $c_i = o''$ ، حيث أن $i = 1,2,\dots,n$. إذن $y = 0$.

نستنتج، مما سبق، أنه يوجد فضاء حلقي جزئي حر F من M يكون من أجله $M = F \oplus \operatorname{Ker}\varphi$

(11-5) الفضاء الحلقي البسيط Simple module :

نقول عن الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ بمحايد إنه بسيط أو (غير قابل للتحليل) إذا تحقق ما يلي :

(1) (o) و M هما الفضاءان الحلقيان الجزئيان للفضاء الحلقي M على R فقط.

(2) $R.M \neq (o)$ حيث أن :

$$RM = \left\{ \sum_{i=1}^{n} a_i.m_i \ ; a_i \in R,\ m_i \in M \right\}$$

نلاحظ من التعريف السابق ، أن كل حقل يشكل فضاءً حلقياً بسيطاً .

مبرهنة (18) :

لتكن $(R,+,\cdot)$ حلقة بمحايد، وإذا كان M فضاءً حلقياً على R، عندها الشروط التالية متكافئة :

(1) M فضاء حلقي بسيط على R .

(2) $M \neq (o)$ و M مولد بأي عنصر $m \in M$ حيث $m \neq o$.

(3) $M \cong R/I$ ، حيث أن I مثالية أعظمية يسارية للحلقة R .

البرهان :

$(1) \Rightarrow (2)$

ليكن $m \in M$ ، بحيث $m \neq o$ ، وبالتالي فإن $RM = < m >$ يشكل فضاءً حلقياً جزئياً من M ، مولداً بالعنصر m ، أي أن $M = < m >$.

$(2) \Rightarrow (1)$

إذا كان $N \neq o$ فضاءً حلقياً جزئيا من M على R ، وإذا كان $n \in N$ حيث $n \neq o$ ، فإنه يكون : $M = < m > \subseteq N$ ، أي أن $M = N$ ، وهذا يعني أن M فضاء حلقي بسيط .

$(1) \Rightarrow (3)$

لدينا $RM = M \neq (o)$ ، وهذا يعني أنه يوجد $o \neq m \in M$ وبحيث $Rm \neq o$، بما أن Rm فضاء حلقي جزئي من M على R ، وM فضاء حلقي بسيط إذن $R.m = M$.

لنعرّف التطبيق $\varphi : R \longrightarrow Rm$ بالشكل $\varphi(r) = r.m$ لكل r من R ، ويمكن التأكد من أن φ تشاكل شامل . ليكن $I = Ker\ \varphi$ ، حسب المبرهنة الأساسية الأولى للتماثلات نجد ، أن $R/I \cong R.m$ ، وبما أن R/I بسيط ، فإن المثالية الوحيدة اليسارية التي تحوي I هي الحلقة فقط . وهذا يعني أن I مثالية أعظمية يسارية للحلقة R .

$(3) \Rightarrow (1)$

ينتج مباشرةً من الحقيقية التالية : إذا كان N فضاءً حلقياً جزئياً من الفضاء الحلقي M على الحلقة بمحايد $(R,+,.)$ ، عندئذٍ يوجد تقابل يحافظ على الاحتواء بين مجموعة الفضاءات الحلقية الجزئية من M/N ، وبين مجموعة الفضاءات الحلقية الجزئية L من M حيث $N \subseteq L \subseteq M$.

تعريف (19) الفضاء الحلقي القابل للتحليل تماماً Completely reducible :

نقول عن الفضاء الحلقي M على الحلقة بمحايد $(R,+,.)$ ، إنه قابل للتحليل

تماماً ، إذا كان $M = \sum N_i$ ، حيث أن N_i فضاءات حلقية جزئية بسيطة من M على الحلقة $(R,+,\cdot)$.

تعريف (20) عنصر الفتل (Torsion element) :

التطبيق $\varphi : R \longrightarrow Rm$ المعرف بالشكل $\varphi(r) = r.m$ حيث r من R و m من M (M فضاء حلقي على الحلقة بمحايد R) ، يشكل تشاكل للفضاءات الحلقية R و M ، إن نواته هي :

$$\text{Ker}\,\varphi = \{r \in R : r.m = o\}$$

تشكل مثالية يسارية في الحلقة R ، تسمى هذه المثالية بمثالية الترتيب للعنصر m ويرمز لها بـــ $O(m)$ ، وبالتالي يكون :

$$Rm \cong R/O(m)$$

الآن ، نسمي العنصر $m \in M$ **بعنصر فتل** إذا وُجِدَ عنصر لا يساوي الصفر ، وليكن r من R بحيث $r.m = 0$.

إن الشرط اللازم والكافي ، لكي يكون m عنصر فتل من الفضاء الحلقي M ، هو أن تكون مثالية الترتيب لذلك العنصر لا تساوي الصفر .

نسمي عادةً الفضاء الحلقي على الحلقة بمحايد R **فضاءً حلقياً عديم الفتل** إذا لم يحوِ على عناصر فتل غير معدومة .

تعريف (21) رتبة فضاء حلقي Rank of module :

إذا كان M فضاءً حلقياً على الحلقة الإبدالية $(R,+,\cdot)$ وبأساس (قاعدة) منتهية ، إن رتبة الفضاء الحلقي M هي عدد عناصر أي أساس لهذا الفضاء .

لاحظ أنه إذا كانت الحلقة $(R,+,\cdot)$ هي حقل (في التعريف السابق) ، فإن رتبة الفضاء الحلقي M ، هي بعد ذلك الفضاء ويرمز له بالرمز $\dim_R M$.

تعريف (22) المتممات للفضاءات الحلقية الجزئية :

لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً ما على R ، وإذا كان N فضاءً حلقياً جزئياً من M ، فإن متمم الفضاء الحلقي الجزئي N في M هو مودول

جزئي من M ، وليكن F بحيث يكون :

$$N \oplus F = M$$

يتضح من التعريف السابق ، أن كلاً من الفضاءين الحلقيين الجزئيين $\{o\}$ وM هو متمم للآخر في M .

مثال (15) :

لتكن $(R,+,.)$ حلقة ما ، وإذا كان M فضاء حلقي على R ، ولنفرض أن M_1 وM_2 وN فضاءات حلقية جزئية من M ، بحيث يكون $M_1 \subseteq M_2$ ، ولنفرض أيضاً أن كلاً من M_1 وM_2، هو متمم لـ N في M ، أثبت أن $M_1 = M_2$.

الحل :

بما أن كلاً من الفضاءين الحلقيين الجزئيين M_1 وM_2 هو متمم للفضاء الحلقي الجزئي N في M، فإن :

$$M = N \oplus M_1 = N \oplus M_2$$

وبالتالي يكون لدينا :

$$M = N + M_1 = N + M_2$$

و

$$N \cap M_1 = N \cap M_2 = \{0\}$$

حيث 0 هو صفر الفضاء الحلقي M ، وبالتالي يكون :

$$M_2 = M_2 \cap M = M_2 \cap (N + M_1) = M_1 + (N \cap M_2)$$

$$= M_1 \cap \{0\} = M_1$$

الفصل السادس

تمديد الحقول

Fields Extension

الفصل السادس

تمديد الحقول

Fields Extension

ندرس في هذا الفصل ، كيفية بناء حقل مبني على حقل جزئي منه ، وبالتالي سنتعرف عل تركيب جبري لحقل ، اعتماداً على حقل جزئي منه .

إن نظرية امتداد الحقول تشكل أساساً لنظرية جالوا Galois theory من أجل إيجاد أصفار لكثيرات الحدود على حقل ما .

وسندرس في هذا الفصل أيضاً موضوع حقول الانشطار والتي هي جزء من نظرية امتداد الحقول. وننصح الطالب الكريم أن يقرأ في البداية الفضاءات المتجهة بشكل جيد .

(1-6) تعاريف :

1- تمديد الحقول Field extension :

إذا كان $F \subseteq E$ حلقتين ، حيث أن F حلقة جزئية لـ E ، نسمي F بحقل جزئي من E و E يسمى امتداداً extension للحقل F .

إذا كان E امتداداً للحقل F ، فإن الحقل E يشكل فضاء متجهي على الحقل F .

2- درجة امتداد Degree of extension :

إذا كان E امتداداً للحقل F ، نسمي بُعد الفضاء E على F بدرجة امتداد E على F ، ونرمز لذلك بـ $[E : F]$.

إذا كان $[E : F] = n$، عندها نقول إن الامتداد منته، ونكتب في هذه الحالة : $\dim_F E = [E:F]$، غير ذلك نقول إن الامتداد غير منته (Infinite extension).

3- العنصر الجبري Algebraic element :

نقول عن العنصر $u \in E$ حيث أن الحقل E امتداداً للحقل F ، إنه جبري على

الحقل F ، إذا وجدت كثيرة حدود غير صفرية ، ولتكن $f(x)\in F[x]$ بحيث يكون u جذراً لها على الحقل F ، أي إذا تحقق $f(u) = 0$.

إذا لم يكن بالإمكان إيجاد مثل هذا العنصر u في الحقل E ، فإننا نقول إن العنصر u غير جبري أو متسام (Transcendental) على الحقل F .

ينتج من التعريف السابق ، أن أي عنصر u في الحقل F يكون جبرياً على الحقل F ، لأنه جذر لكثيرة الحدود $x - u$.

4- الامتداد الجبري Algebraic extension :

نقول عن الامتداد E على الحقل F ، إنه امتداد جبري ، إذا كان كل عنصر من E جبري على الحقل F . غير ذلك ، نسمي امتداد E للحقل F امتداداً غير جبرياً أو امتداداً متسامياً على الحقل F .

لنقدم الآن أمثلة حول التعاريف السابقة .

(2-6) أمثلة :

مثال (1) :

إن $C \supseteq R$ هو امتداد منتهي و $[C : R] = 2$ ، لأن المجموعة $\{1,i\}$ تشكل قاعدة لـ R بالنسبة للحقل المركب C .

إن حقل الأعداد الحقيقية $(R,+,\cdot)$ هو امتداد غير منتهٍ لحقل الأعداد النسبية $(Q,+,\cdot)$.

مثال (2) :

العددان $\sqrt[3]{2}$ و i جبريان على حقل الأعداد النسبية Q لأنهما جذران لكثيرة الحدود: $x^3 - 2$ و $x^2 + 1$ على الترتيب .

مثال (3) :

بيّن أن العدد $u = \sqrt{2} - \sqrt{3}$ جبري على الحقل Q .

الحل :

لدينا $u = \sqrt{2} - \sqrt{3} \Rightarrow u^2 = (\sqrt{2} - \sqrt{3})^2 = 2 - 2\sqrt{6} + 3 = 5 - 2\sqrt{6}$

وبالتالي $u^2-5=-2\sqrt{6} \Rightarrow (u^2-5)^2=24$

ومنه نجد :

$$u^4-10u^2+1=0$$

ملاحظة (1) :

الأعداد الحقيقية والمركبة ليست جميعها أعداداً جبرية على حقل الأعداد النسبية Q ، ففي عام 1873 ، أثبت الرياضي هيرميت Hermit أن العدد النيبري e متسامٍ ، وشارك في برهان ذلك الرياضي الألماني هيلبرت (Hilbert) ، كما أثبت الرياضيان جلفاند Gelfond وشنايدر Schneider أنه إذا كان v,u عددان جبريان، وكان v عدد غير نسبي فإن a^b عدد متسامٍ على الحقل Q .

وبرهن الرياضي الألماني لندمان Lindemann أن العدد π متسامٍ ، وكان ذلك في عام 1882 .

مبرهنة (1) :

إذا كان $F \subseteq E$ امتداداً منتهياً ، أي أن $[E:F]=n$ ، وليكن u عنصراً من الحقل E ، عندئذٍ توجد كثيرة حدود غير صفرية $o \neq f(x)\in F[x]$ بحيث تكون $\deg f \leq n$ و $f(u)=o$.

البرهان :

العناصر التي عددها (n+1) التالية $1,u,u^2,\ldots,u^n$ من الحقل E ليست مستقلة خطياً ، لأن $\dim_F E=n$ وبالتالي ، فإن المعادلة :

$$a_0+a_1u+a_2u^2+\ldots+a_nu^n=0$$

محققة ، لبعض قيم a_i من F ، التي جميعها غير معدومة .

الآن وبأخذ كثيرة الحدود $f(x)=a_0+a_1x+\ldots+a_nx^n$ نحصل على المطلوب .

ملاحظة (2) :

لتكن A مجموعة جميع الحقول الجزئية من E ، حيث E امتداداً للحقل F ،

والتي تحوي العنصر a والحقل F . نعلم أن تقاطع مجموعة من الحقول الجزئية في E هو حقل جزئي أيضاً في E ، إذن تقاطع جميع الحقول الجزئية من A هو حقل جزئي في E ، نرمز عادةً له بالرمز $F(a)$ ، إن هذا الحقل يحوي كلاً من العنصر a والحقل F ، لأنه حقل جزئي من A ، كما أن $F(a)$ هو أصغر حقل جزئي من E يحوي العنصر a والحقل F .

تعريف (5) الامتداد البسيط Simple extension :

ليكن E امتداداً للحقل F ، وإذا كان $a \in E$ ، نقول إن E امتداد بسيط للحقل F، إذا كان $E = F(a)$.

مثال (4) :

أثبت أن $C = R(i)$ ، حيث C حقل الأعداد المركبة .

الحل :

إن $R(i) \subseteq C$ ، لأن الحقل $R(i)$ يحوي جميع عناصر الحقل R والعنصر i وبالتالي يحوي جميع الأعداد المركبة التي من الشكل $z = x + i y$ حيث أن y,x من R . وبما أن $C \subseteq R(i)$ ، لأنه أصغر حقل يحوي R والعنصر i ، إذن $C = R(i)$.

مثال (5) :

أثبت أن $$Q(\sqrt{2}) = \left\{ a + b\sqrt{2} \ : a, b \in Q \right\}$$

الحل :

لنكتب أولاً : $$E = \left\{ a + b\sqrt{2} \ : a, b \in Q \right\}$$

من الواضح ، أن المجموعة E محتواة في أي حقل جزئي يحتوي Q والعنصر $\sqrt{2}$ وبالتالي يكون $E \subseteq Q(\sqrt{2})$.

من ناحية ثانية المجموعة E هي حلقة تحتوي على Q و $\sqrt{2}$ ، لذلك يكون $Q(\sqrt{2}) \subseteq E$ ، وينتج ذلك ، أنه إذا أثبتنا E حقل جزئي من R .

إذا كان $u = a + b\sqrt{2} \neq \phi$ عنصراً ما من E ، فيكون لدينا :

$$u\,(a - b\sqrt{2}\,) = a^2 - 2b^2 \neq 0$$

وكذلك :

$$u^{-1} = \frac{1}{a^2 - 2b^2}\left(a - b\sqrt{2}\,\right) \in E$$

مثال (6) :

إذا كان $F \subseteq E$ حقلين ما ، وكان u من E ، عندئـــذٍ $F(u) = F$ إذا وفقـــط إذا كان $u \in F$.

ملاحظة (3) :

إذا كان E امتداداً للحقل F ، ولتكن العناصر v,u من E ، عندئذٍ $F(u) \supseteq E$ ، يمكن تعريف الامتداد $F(u).v$ والذي يمكن اعتباره حقلاً جزئياً من الحقل E يحوي كلاً من العنصرين v,u والحقل F ، وبالتالي يكون لدينا $F(u).F(v) \subseteq F(u,v)$ ، كذلك الحقل الجزئي $F(u,v)$ يحوي الحقل $F(u)$ ، لأنه يحوي u و F معاً وأيضـــاً يحوي العنصر v ، وبالتالي يكون لدينا $F(u,v) \subseteq F(u)\,(v)$.

نستنتج مما سبق أن : $F(u)\,(v) = F(u,v)$

تعريف (6) الحقل المولد Generated field :

ليكن E امتداداً للحقل F ، ولتكن $u_1,u_2,\ldots,u_n$ عناصر من E . نسمي الحقـــل المكون من ضم العناصر $u_1,u_2,\ldots,u_n$ إلى الحقل F ، بالحقل المولد بالعناصـــر $u_1,u_2,\ldots,u_n$ على الحقل F .

تعريف (7) كثيرة الحدود الصغرى Minimal polynomial :

إذا كان E امتداداً للحقل F ، وكان $u \in E$ عنصراً جبرياً على F ، نسمي كثيرة الحدود الواحدية $m = m(x)$ والتي درجتها أصغر ما يمكن ، حيث أن $m(u) = 0$ بكثيرة حدود صغرى (الأصغرية) للعنصر u على الحقل F ، ودرجة كثيرة الحدود الصغرى m تسمى بدرجة العنصر u على F ، ونرمز لذلك بـــ $\deg_F(u)$.

مبرهنة (2) :

إذا كان E امتداداً للحقل F ، وليكن $u \in E$ عنصراً جبرياً على الحقل F ، وبفرض أن $m = m(x)$ كثيرة حدود صغرى ، عندئذٍ يتحقق ما يلي :

1) m غير قابلة للتحليل على الحقل F .

2) إذا كانت $f = f(x) \in F[x]$ كثيرة حدود على الحقل F، فإن $f(u) = 0$ ، إذا، وفقط إذا كان m/f.

3) $m(x)$ كثيرة حدود وحيدة تتحدد بالعنصر u .

البرهان :

1) نفرض أن $m(x) = f(x).g(x)$ في $F[x]$، حيث أن $\deg f < \deg m$ و $\deg g < \deg m$. عندئذٍ يكون $f(u)\, g(u) = m(u) = 0$ وهذا يؤدي إلى أن $f(u) = 0$ أو $g(u) = 0$ وهذا يناقض كون $m(x)$ كثيرة حدود صغرى . وبالتالي ، فإن $m(x)$ غير قابلة للتحليل على الحقل F.

2) إذا كان $f(u) = 0$ ، وباستخدام خوارزمية القسمة ، نكتب : $f = q.m + r$ في $F[x]$ ، حيث أن $r = 0$ أو $\deg r < \deg m$. عندئذٍ يكون :

$$r(u) = f(u) - q(u)\, m(a) = 0$$

وهذا يؤدي إلى أن اختيار $r \neq 0$ يتناقض مع مفهوم كثيرة الحدود الصغرى $m(x)$، إذن $r = 0$ ، وهذا يعطي m/f .

من الواضح برهان العكس .

3) لتكن m' كثيرة حدود صغرى أخرى ، وبحيث يكون $m'(u) = 0$ ، ومن (2) نجد أن m/m' ، وبسبب (2) أيضاً نجد أن m'/m ، وبالتالي $m = m'$ (لأن كل منهما كثيرة حدود واحدية) .

مثال (7) :

أوجد كثيرة الحدود الصغرى للعنصر $u = \sqrt{1+\sqrt{3}}$ على الحقل $(Q,+,\cdot)$.

الحل :

لدينا $u^2 = 1+\sqrt{3}$ ومنه يكون $u^2 - 1 = \sqrt{3}$ وبالتالي يكون $(u^2 - 1)^2 = 3$ ، أي أن $u^4 - 2u^2 - 2$ كثيرة الحدود غير قابلة للتحليل في $Q[x]$ ، وبالتالي فهي كثيرة حدود صغرى للعنصر الجبري u على Q ، ومنه نجد : $\deg_Q(u) = 4$.

سنبرهن في قسم التمارين المحلولة، الحقيقية التالية ، والتي سنستخدمها في صحة برهان المبرهنة القادمة :

إذا كان E امتداداً للحقل F ، وإذا كان u من E ، عندئذ التطبيق $\varphi_u : F \longrightarrow E$، والمعرف بالشكل التالي : $\varphi_u(f(x)) = f(u)$، حيث أن :

$f(x) = \sum_{i=0}^{n} u_i . x^i \in F[x]$ ، يكون تشاكلاً من الحلقة $F[x]$ إلى الحقل E .

مبرهنة (3) :

إذا كان E امتداداً للحقل F ، وإذا كان $u \in E$ عنصراً جبرياً على الحقل F درجته n ، عندها يتحقق ما يلي :

-(1)
$$F(u) = \{a_0 + a_1 u + \dots + a_n u^{n-1} : a_i \in F\}$$
$$= \{f(u) : f(x) \in F[x]\}$$

(2)- المجموعة $\{1, u, u^2, \dots, u^{n-1}\}$ تشكل أساساً (قاعدة) للامتداد $F(u)$ على الحقل F ، بحيث يكون :

$$\deg_F(u) = [F(u) : F] = n$$

-(3) $F(u) \cong F[x]/<m>$ ، حيث أن m كثيرة حدود صغرى للعنصر u على الحقل F.

البرهان :

حسب الحقيقة التي سبقت هذه المبرهنة ، إن التطبيق φ_u يشكل تشاكل حلقي من الحلقة $F[x]$ إلى الحقل E، كما أن :

$$\operatorname{Ker} \varphi = \{f(x) : f(u) = 0\} = <m>$$

لأن m كثيرة حدود صغرى للعنصر u على الحقل F، وحسب النظرية الأساسية الأولى في التماثل يكون :

$$F[x]/<m> \cong \operatorname{Im}\varphi = \{ f(u) \ : f(x)\in F[x]\}$$

الآن ، $\operatorname{Im}\varphi \subseteq F(u)$ ، لأن $F(u)$ حقلاً يحوي العنصر u والحقل F وبالتالي فهو يحوي $f(u)$ ، لكل $f(x)\in F[x]$ ، وبما أن $F[x]/< m >$ حقلاً ، حيث أن m كثيرة حدود غير قابلة للتحليل ، يكون أيضاً $\operatorname{Im}\varphi$ حقلاً يحوي الحقل F والعنصر u ، أي أن $F(u) \subseteq \operatorname{Im}\varphi$. وهكذا يكون :

$$F(u) = \operatorname{Im}\varphi = \{f(u) : f(x)\in F[x]\}$$

وبهذه الصورة نكون قد أثبتنا صحة الشرطين (1) و(3) من نص المبرهنة .
لنثبت الآن أن المجموعة $B = \{1,u,u^2,\ldots,u^{n-1}\}$ تشكل أساساً للامتداد $F(u)$ على الحقل F .
لنثبت أولاً أن المجموعة B مستقلة خطياً . ليكن :

$$a_0 + a_1 u + a_2 u^2 +\ldots + a_n u^{n-1} = 0$$

لكل $a_i\in F$ و $0 \le i \le n-1$. عندئذٍ $g(u) = 0$ ، حيث أن :

$$g(x) = a_0 + a_1 x + a_2 x^2 +\ldots + a_{n-1} x^{n-1}$$

و$0 \neq g(x)\in F[x]$ ، وهذا يناقض حقيقية أن m كثيرة حدود صغرى . إذن $g(x) = 0$ ، لذا $a_i = 0$ من أجل جميع قيم i . إذن المجموعة B مستقلة خطياً .
لنبرهن أخيراً أن المجموعة B تولد الامتداد $F(u)$ على الحقل F . من أجل ذلك لنفرض أن $f(u)\in F(u)$ ولنكتب حسب خوارزمية القسمة :

$f = q.m + r$ في $F[x]$ و $r = 0$ أو $\deg r < \deg m = n$ و $r,q\in F[x]$ ، وبالتالي يكون :

$$r(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \ ; a_i\in F$$

وبسبب $m(u) = 0$ ، نحصل على :

$$f(u) = q(u)\, m(u) + r(u) = r(u) = a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}$$

أي أن المجموعة B تولد $F(u)$. إذن المجموعة B تشكل أساساً للحقل $F(u)$ على الحقل F ويكون أيضاً :

$$\deg_F(u) = [F(u) : F] = n$$

ملاحظة (4) :

يلاحظ من المبرهنة السابقة الشرط (3) أن الحقل F وكثيرة الحدود الصغرى m للعنصر الجبري u ، تحددان تماماً الامتداد $F(u)$ ، وبالتالي ، فإذا كان للعنصرين v,u كثيرة الحدود الصغرى نفسها على الحقل F ، فإن $F(u) \cong F(v)$. كما تبين المبرهنة السابقة الشرط (1) كيفية إيجاد الامتداد $F(u)$ ، وما هي العناصر التي يمكن ضمها إلى الحقل F . ووصف عملية الضرب في امتداد ما . والأمثلة التالية توضح ما سبق .

(3-6) أمثلة :

مثال (8) :

بيّن أن $Q[\sqrt[4]{5}\,i] \cong Q[x]/<x^4 - 5>$ و $[Q(\sqrt[4]{5}\,i) : Q] = 4$

الحل :

بما أن $\sqrt[4]{5}\,i$ هو جذر لكثيرة الحدود x^4-5 وهي غير قابلة للتحليل على Q ، فحسب المبرهنة السابقة نجد أن :

$$Q[\sqrt[4]{5}\,i] \cong Q[x]/<x^4 - 5>$$

مثال (9) :

ليكن u جذراً لكثيرة الحدود $f(x) = x^2 + 1 \in F[x]$ في امتداد الحقل E للحقل R (حقل الأعداد الحقيقية)، أثبت أن الحقل : $R(u) = \{a + b.u : a,b \in R\}$ يحوي جميع أصفار $f(x)$.

الحل :

الحقل $R(u)$ بشكل فضاء متجهي على الحقل R ، أساسه $\{1,u\}$ ، وبالتالي فإن : $R(u) = \{a + b.u : a,b \in R\}$ ، وبما أن u جذراً لكثيرة الحدود $f(x)$ ، فإن $-u$ يكون جذراً ، وبالتالي فإن $R(u)$ يحوي جميع جذور كثيرة الحدود $f(x)$ ، وكذلك الجذر $u = \sqrt{-1}$.

عادةً نسمي $R(u)$ بحقل الأعداد المركبة ، ويرمز لها بـــ C .

مثال (10) :

صف عملية الضرب في الامتداد $Q(1+i)$ للحقل Q .

الحل :

لنضع $u = 1 + i$، وبالتالي يكون لـــدينا : $(u-1)^2 = i^2 = -1$ ومنـــه يكـــون $u^2 - 2u + 2 = 0$.

بأخذ $m(x) = x^2 - 2x + 2$ ، نجد أن $m(x)$ كثيرة حدود غير قابلة للتحليل على Q (لأنه لا يوجد لها جذور في Q) ، وبالتالي تكون $m(x)$ كثيرة حدود صـــغرى للعنصر u .

وبالتالي يكون لدينا :

$$Q(u) = \{a + b.u : a,b \in Q\}$$

وحسب المبرهنة السابقة و$u^2 = 2u - 2$ يكون :

$$(a + bu)(a' + b'u) = aa' + (ab' + ba')u + bb'u^2$$
$$= (aa' - 2bb') + (ab' + ba' + 2bb')u$$

مبرهنة (4) مبرهنة الضرب Multiplication theorem :

إذا كان K امتداداً للحقل E ، وكان E امتداداً للحقل F ، عندئذٍ يكـــون امتـــداد الحقل K للحقل F منتهياً إذا ، وفقط إذا ، كان $[K:E]$ و$[E:F]$ منتهياً ، وفـــي هذه الحالة يتحقق :

$$[K:F] = [K:E] . [E:F]$$

بالإضافة لذلك ، إذا كانت المجموعة $\{e_1,\dots,e_m\}$ تشكل أساساً للحقل E على F والمجموعـــة $\{k_1,\dots,k_n\}$ أساســـاً للحقـــل K علـــى E، فـــإن المجموعـــة $B = \{e_i k_j : 1 \le i \le m , 1 \le j \le n\}$ تشكل أساساً لـــ K على F .

البرهان :

إذا كان $[K:F]$ منتهياً ، فإن $[E:F]$ يكون منتهياً أيضاً ، بســـبب أن E فضـــاء جزئي من K على F . من جهة ثانية ، من أجل أي أساس لـــ K على F يكـــون

$[K : E]$ منتهي .

لنبرهن على العكس ، باستخدام الرموز الواردة في نص المبرهنة ، لنبرهن أن المجموعة B تشكل أساساً للحقل K على F .

لنثبت أولاً أن B تولد K على F . من أجل $c \in K$ ، وبسبب كون المجموعة $\{e_1,e_2,\ldots,e_m\}$ تشكل أساساً لـ K على E ، نكتب :

$$c = \sum_{j=1}^{n} b_j.K_j \qquad (*)$$

حيث أن $b_j \in E$ ، لكل j . لكن من أجل كل j ، يكون لدينا $b_j = \sum_{i=1}^{m} a_{ij}.e_i$ ،

حيث $a_{ij} \in F$ لكل j,i ، وبالتعويض في عبارة (*) نجد :

$$c = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}.e_i\right)k_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}.e_i.k_j$$

ينتج من ذلك أن المجموعة B مولدة بالحقل K على F .

لنثبت أخيراً ، أن المجموعة B مستقلة خطياً على الحقل F .

لتكن $\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}.e_i.k_j = 0$ ، حيث $a_{ij} \in F$ لكل j,i عندئذٍ يكون :

$\sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}.e_i\right)k_j = 0$ ، وهذا يعني أن المجموعة $\{k_1,k_2,\ldots,k_n\}$ مستقلة خطياً على E، $\sum_{i=1}^{m} a_{ij}.e_i = 0$ لكل قيم j . لكن $a_{ij} = 0$ ، لكل قيم j,i لأن $\{e_1,e_2,\ldots,e_m\}$ مستقلة خطياً على F . ينتج من ذلك أن المجموعة B مستقلة خطياً على الحقل F .

تعطي مبرهنة الضرب السابقة العلاقة العددية بين الأبعاد ، والتي تلعب دوراً مهماً في نظرية الحقول ، وبالتالي ، فإن هذه المبرهنة لها دوراً مهماً كما لمبرهنة لاغرانج في نظرية الزمر .

نتيجة (1) :

إذا كان E امتداداً للحقل F ، وليكن $u\in E$ عنصراً جبرياً على الحقل F . وبفرض أن $v\in f(u)$ ، عندئذٍ v عنصر جبري على F ويكون : $\deg_F(v)/\deg_F(u)$.

البرهان :

لدينا أولاً : $F \subseteq F(v) \subseteq F(u)$ ، وبسبب $F \subseteq F(u)$ منته ، و$v\in F(u)$ عنصر جبري على F، يكون لدينا (حسب مبرهنة سابقة) :

$$\deg_F(v) = [F(v) : F] \ , \deg_F(u) = [F(u) : F]$$

وحسب مبرهنة الضرب السابقة نجد أن :

$$\deg_F(v)/\deg_F(u)$$

مثال (11) :

إذا كان $u = \sqrt[3]{2}$ ، أثبت أن $Q(u) = Q(u^2)$.

الحل :

لدينا $Q \subseteq Q(u) \subseteq Q(u^2)$, $[Q(u) : Q] = \deg_Q(u) = 3$ لأن كثيرة الحدود $f(x) = x^3 - 2\in Q[x]$ غير قابلة للتحليل في $Q[x]$. وبما أن u جذراً لها و$f(x)$ واحدية ، إذن كثيرة الحدود $f(x)$ صغرى للعنصر u على الحقل Q . لنبرهن الآن أن :

$$\deg_Q(u^2) = [Q(u^2) : Q] = 3$$

بما أن $u^2\in Q(u)$ ، فإن $\deg_Q(u^2)/\deg_Q(u) = 3$ ، وحسب النتيجة السابقة فإن $\deg_Q(u^2) = 1$ أو $\deg_Q(u^2) = 3$. لكن $\deg_Q(u^2) \neq 1$ ، لأن الحالة الثانية تؤدي إلى أن $u^2\in Q$ ، وهذا تناقض ، إذن $\deg_Q(u^2) = 3$.

مبرهنة (5) :

يكون E امتداداً منتهياً للحقل F ، إذا ، وفقط إذا كان $E = F(u_1,u_2,\ldots,u_n)$ ،

حيث $u_i \in E$ عناصر جبرية على F .

البرهان :

لنفرض ، أولاً أن $[E : F]$ منتهي ، وبطريقة الاستنتاج الرياضي على $[E : F]$ نبرهن أن :

$E = F(u_1,u_2,\ldots,u_n)$ حيث u_i عناصر جبرية على F .

إذا كان $[E : F] = 1$ ، فإن $E = F = F(1)$.

ليكن $[E : F] > 1$ ، أي أن $E \neq F$ ، ولنختر $u \in E$ و $u \notin F$ ، عندها يكون $[F(u) : F] > 1$ ، بسبب كون $u \notin F$ ، وباستخدام مبرهنة الضرب نكتب :

$$[E:F(u)] = \frac{[E:F]}{[F(u);F]} < [E:F]$$

بتطبيق طريقة الاستنتاج للتمديد المنتهي $E \supseteq F(u)$ ، نحصل على :

$$E = F(u)(u_1,u_2,\ldots,u_n) = F(u_1,u_2,\ldots,u_n)$$

علماً أن العناصر $u,u_1,\ldots,u_n$ جبرية على F ، (وذلك حسب مبرهنة سابقة) .

لنبرهن الآن على العكس :

إذا كان $E = F(u_1,u_2,\ldots,u_n)$ حيث أن u_i عناصر جبرية على الحقل F حيث $1 \leq i \leq n$ ، وباستخدام طريقة الاستنتاج الرياضي على العدد n ، نجد أنه إذا كان $n = 1$ ، فإنه (حسب المبرهنة قبل الأخيرة) يتم المطلوب .

لنفرض الآن، أن $n > 1$ ، ولنكتب $L = F(u_1,u_2,\ldots,u_{n-1})$. عندها يكون لدينا : $F \supseteq L \supseteq E$ و $[L : F]$ منتهي أيضاً ، حسب طريقة الاستنتاج الرياضي ، يوضع $E = L(u_n)$ ، يكون $[E : L]$ منتهياً ، (حسب المبرهنة قبل الأخيرة) .

إذن $[E : F]$ يكون منتهياً وذلك حسب مبرهنة الضرب .

نتيجة (2) :

إذا كان E امتداداً للحقل K ، وكان K امتداداً للحقل F . أي أن $F \supseteq E \supseteq K$، عندئذٍ يكون الامتداد E للحقل F جبرياً إذا ، وفقط إذا ، كان كل من الامتدادين E

للحقل K و K للحقل F جبرياً .

البرهان :

لنبرهن أن الامتداد E للحقل F جبرياً ، أما عكس ذلك فهي واضحة .

ليكن $E \supseteq K$ و $F \supseteq E$ امتدادين جبريين ، وليكن $u \in E$ ولنثبت أن العنصر u جبري على F .

لنبين أولاً أن العنصر u يقع في امتداد منته للحقل F . بسبب أن $E \supseteq K$ جبري، ليكن $f(u) = 0$ حيث أن $0 \neq f(x) \in E[x]$.

إذا كان $f(x) = e_0 + e_1x + \ldots + e_nx^n$ ، وبأخذ $L = F(e_0,\ldots,e_n)$ ، عندها يكون $u \in L(u)$ و $L(u) \supseteq F$ امتداد منتهي . كذلك $F \supseteq L \supseteq L(u)$ وهذا نـاتج من المبرهنة قبل الأخيرة ، كذلك $L \supseteq K$ امتداد منتهي (حسب المبرهنة الأخيرة).

إذن $F \supseteq K$ جبري .

تعريف (8) إغلاق الجبري (اللصاقة الجبرية) algebraic closure :

ليكن E امتداداً للحقل F ، نسمي الحقل F_1 المعرف بالمجموعة التالية :

$$F_1 = \{u \in E \ : \ u \text{ عنصر جبري على } F\}$$

باللصاقة الجبرية لـ F في E ، أو بالإغلاق الجبري لـ F في E .

تعريف (9) حقل الأعداد الجبرية Field of algebraic numbers :

نسمي الحقل المعرف بالشكل :

$$A = \{u \in C \ : \ u \text{ عنصر جبري على } Q\}$$

بحقل الأعداد الجبرية .

الحقل A يبين لنا أن كل امتداد منتهي هو امتداد جبـري ، لكـن العكـس لـيس صحيحاً. أي ليس من الضروري أن يكون كل امتداد جبري امتداداً منتهياً .

(4-6) حقول الانشطار Splitting Fields :

يعد الرياضي كرونيكر (1823-1891) Kronecker أول مـن أوجـد هـذا الامتداد ، وذلك في منتصف القرن التاسع عشر .

إذا كان $u \in E$ عنصراً جبرياً على F حيث أن E امتداد للحقل F ، نعلم أن :

$$F[x]/<m> \cong F(u) = \{a_0 + a_1u + \ldots + a_{n-1}u^{n-1} : a_i \in F\}$$

حيث أن $m = m(x)$ كثيرة حدود صغرى (غير قابلة للتحليل) للعنصر u على F و $\deg m = n$، وبالتالي، فإن الامتداد F(u) للحقل F يتعلق بالعنصر u وبالحقل F، وليس له ارتباط بالحقل E . لندرس الحقل F(u) بعمق أكثر من كونه حقلاً جزئياً من الحقل E .

والهدف الآخر ، هو إيجاد امتداد للحقل F يحوي جذراً لكثيرة الحدود f(x) ، حيث $f(x) \in F[x]$. من أجل ذلك نقدم أولاً مبرهنة كرونيكر .

مبرهنة (6) مبرهنة كرونيكر Kronecker theorem :

ليكن $(F,+,\cdot)$ حقلاً ما ، وإذا كانت f(x) كثيرة حدود غير ثابتة من F[x] ، عندئذٍ يوجد امتداد E للحقل F ، وعنصر u من E بحيث يكون $f(u) = 0$.

البرهان :

يمكن كتابة كثيرة الحدود f(x) في الحلقة F[x] ، بالشكل : $f(x) = g(x)\ h(x)$ ، حيث h,g كثيرتي حدود غير قابلة للتحليل . كما أن كثيرة الحدود g(x) هي إحدى عوامل f(x) وغير قابلة للتحليل على F .

ولنبرهن على وجود امتداد E للحقل F يحوي العنصر u وبحيث $g(u) = 0$.

إن g(x) تشكل مثالية أعظمية في الحلقة F[x]، وبالتالي يكون : $F[x]/<g>$ حقل، ولنثبت أن الحقل F يتطابق مع حقل جزئي من الحقل $F[x]/< g >$.

من أجل ذلك، لنعرف التطبيق $\varphi : F \longrightarrow F[x]/<g>$ بالشكل التالي :

$$\varphi(u) = u + <g> ; u \in F$$

يمكن البرهان بسهولة ، أن هذا التطبيق تقابلاً ، ونلاحظ ، أيضاً ، أنه يوجد تماثل للحقل F مع : $\{u + <g> ; u \in F\}$ وبالتالي ، الحقل $F[x]/< g >$ هو امتداد للحقل F .

لنثبت الآن أن هذا الامتداد يحوي أصفاراً لكثيرة الحدود g(x) . من أجل ذلك ، إذا كان $u = x + < g >$ ، حيث $u \in E$ ، وحسب التشاكل $\varphi_u : F[x] \longrightarrow E$ نجد

أن كثيرة الحدود :

$$g(x) = a_0 + a_1x + \dots + a_nx^n \ ; \ a_i \in F$$

فإن :

$$\varphi_u(g(x)) = a_0 + a_1(x + \langle g\rangle) + \dots + a_n(x + \langle g\rangle)^n$$

في $E = F[x]/\langle g\rangle$ ، وبالتالي يكون :

$$g(u) = (a_0 + a_1x + \dots + a_nx^n) + \langle g\rangle = g(x) + \langle g\rangle = \langle g\rangle = 0$$

في الحقل $E = F[x]/\langle g\rangle$. ومنه يوجد عنصر $u \in E$ بحيث $g(u) = 0$ إذن $f(a) = 0$.

المثال التالي يوضح مبرهنة كرونيكر السابقة .

مثال (12) :

أوجد امتداداً للحقل R يحوي جذوراً لكثيرة الحدود $f(x) = x^2 + 1 \in R[x]$ على R .

الحل :

نلاحظ أولاً ، أن كثيرة الحدود $x^2 + 1$ غير قابلة للتحليل على حقل الأعداد الحقيقية R ، ولا تحوي جذوراً فيه ، وبالتالي ، فإن كثيرة الحدود $\langle f \rangle$ تشكل مثالية أعظمية في الحلقة $R[x]$ ، ويكون $R[x]/\langle f \rangle$ حقلاً . لنطابق كل عنصر u من R بعنصر $u + \langle f \rangle$ من الحلقة $R[x]$ (نعتبر في هذه الحالة أن R حقل جزئي من الحقل $R[x]/\langle f\rangle$) .

إذا كان $u = x + \langle f\rangle$ ، وبالتالي ، فإن :

$$u^2 + 1 = (x + \langle x^2+1\rangle)^2 + (1 + \langle x^2+1\rangle) = (x^2+1) + (x^2+1) = 0$$

وهذا يعني أن u هو جذر لكثيرة الحدود $f(x)$.

يستفاد من مبرهنة كرونيكر السابقة ، في تشكيل حقول ذات رتبة معلومة . والمثال التالي يوضح ذلك .

مثال (13) :

شكّل حقلاً رتبته تساوي العدد 8 .

الحل :

لتكن كثيرة الحدود $f(x) = x^3 + x + 1$ ، نلاحظ أولاً أن $f(x)$ غير قابلة للتحليل على الحلقة Z_2 (لا يوجد فيها جذور في Z_2) . وبالتالي ، فإن $< f >$ تشكل مثالية أعظمية في الحلقة $Z_2[x]$ ، ويكون الحقل $E = Z_2[x]/< f >$ امتداداً للحقل Z_2 ، كما أنه لكثيرة الحدود $f(x)$ جذوراً في الحقل E ، ويكون $[E : Z_2] = 3$ وبالتالي يكون لدينا :

$$E = Z_2(u) = \{a_0 + a_1u + a_2u^2 \ ; \ a_i \in Z_2 , f(u) = 0\}$$
$$= \{0 , 1 , u , u^2 , 1+u , 1+u^2 , u+u^2 , 1+u+u^2 , u^3 = u+1\}$$

ويكون أيضاً $| E | = 8$.

لنعرّف الآن **حقل الانشطار** Spilitting field .

تعريف (9) :

لتكن $f(x)$ كثيرة حدود في $F[x]$ على الحقل F ، ومن الدرجة n حيث $n \geq 1$.
نسمي الامتداد E للحقل F بحقل الانشطار لكثيرة الحدود $f(x)$ على الحقل F ، إذا تحقق الشرطان التاليان :

$$f(x) = a\,(x - u_1)\,(x - u_2)\,\ldots.\,(x - u_n) \qquad (1)$$

حيث أن a من F و u_i من E ، لكل قيم i .

$$E = F\,(u_1,u_2,\ldots..,u_n) \qquad (2)$$

الشرط الأول الوارد في التعريف السابق يعني أن كثيرة الحدود $f(x)$ تشطر (Split) على الحقل E . كما أنه ، إذا كان E حقلاً انشطارياً لـ $f(x)$ على الحقل F ، فإن الحقل الجزئي الوحيد في E ، والذي يحوي F وتنشطر فيه كثيرة الحدود $f(x)$ هو الحقل E نفسه .

يمكن تعريف حقل الانشطار بالشكل التالي :

إن أصغر امتداد جبري للحقل F ، والذي يحوي جميع جذور كثيرة الحدود $f(x)$ من $F[x]$ يسمى حقلاً انشطارياً لكثيرة الحدود $f(x)$ على الحقل F .

من التعريف السابق ، نجد أن كل حقل ، وليكن F ، يكون حقلاً انشطارياً لكثيرة الحدود الخطية $f(x) \in F[x]$ على الحقل F .

مثال (14) :

بيّن أن الحقل $Q(i)$ هو حقل انشطاري لكثيرة الحدود $x^2 + 1$ على Q .

الحل :

بما أن $x^2 + 1 = (x + i)(x - i)$ و $Q(i,-i) = Q(i)$ ، فإن الحقل $Q(i)$ هو حقل انشطاري لـ $x^2 + 1$ على Q .

تعطي المبرهنة التالية ، عدد الجذور لكثيرة الحدود $f(x)$ من $F[x]$ ، علماً أن $E \supseteq F$.

مبرهنة (7) :

لتكن f كثيرة حدود من الدرجة n ، حيث $n \geq 1$ على حقل F ، عندئذٍ يوجد حقل انشطاري $E \supseteq F$ لـ f على F يحوي n جذراً لـ $f(x)$ ، ويكون $[E : F] = n!$.

البرهان :

نبرهن بطريقة الاستنتاج الرياضي على n حيث $n \geq 1$.

إذا كان $n = 1$ ، بأخذ $E = F$ ، ستكون المبرهنة محققة .

نفرض الآن أن $n > 1$، ولتكن $g(x)$ كثيرة حدود غير قابلة للتحليل وهي إحدى عوامل كثيرة الحدود $f(x)$، وبالتالي حسب مبرهنة كرونيكر يوجد امتداد E يحوي الحقل F وجميع جذور $g(x)$.

نفرض أن $u_1 \in E$، وبوضع $E_1 = F(u_1)$ ، نحصل : $\deg g = \{E : F] \leq n$ ، وبالتالي يكون: $f(x) = (x-u_1)\, q(x)$ في الحلقة $E_1[x]$، حيث أن $\deg q = n-1$.

بتطبيق طريقة الاستنتاج الرياضي مرة ثانية ، نجد أنه يوجد امتداد وليكن E_2 للحقل E_1 ، وهو عبارة عن حقل انشطار كثيرة الحدود $q(x)$ على الحقل E_1،

ويكون أيضاً: $[E_2:E_1] \le (n-1)!$ وبالتالي :

$$g(x) = a\,(x-u_2)\ldots(x-u_n)\ ;\ a\in E_1\ ,\ u_i\in E$$

لكل $2 \le i \le n$ ، ومنه يكون :

$$E_2 = E_1\,(u_2,\ldots,u_n) = F\,(u_1,u_2,\ldots,u_n)$$

وهذا يعني أن E_2 حقل انشطار لكثيرة الحدود $f(x)$ على الحقل F ، حيث أن :

$$[E_2 : F] = [E_2 : E_1]\,[E_1 : F] = (n-1)!\,.\,n = n!$$

وذلك حسب مبرهنة الضرب .

مثال (15) :

أوجد حقل انشطار كثيرة الحدود $f(x) = x^4 - 2x - 3 \in Q[x]$، وبحيث يكون $[E:Q] = 4$.

الحل :

بما أن $f(x) = (x^2-3)\,(x^2+1)$ ، فإن جذور $f(x)$ في الحقل C هـي $\pm\sqrt{3}$ و $\pm i$ ، وبالتالي فإن $E = Q(\sqrt{3},i)$ حقل انشطار كثيرة الحدود $f(x)$ على الحقل Q ، حيث $E = Q(i)$ و $K = Q(\sqrt{3})$ ، وبالتالي يكون :

$$[E : Q] = [E : K]\,[K : Q] = 2.2 = 4$$

مثال (16) :

لتكن $(F,+,.)$ حقلاً ما ، أثبت أن أي حقل انشطار لكثيرة الحدود من الدرجة الثانية $f(x)\in F[x]$ على الحقل F يشكل امتداداً بسيطاً $F(u)$ للحقل F .

الحل :

ليكن $F \subseteq E$ حقل انشطار لكثيرة الحدود $f(x)$. وإذا كان :

$f(x) = ax^2 + bx + c\ ;\ a \ne 0$ ، وإذا كان v,u جذرين لـــ f في E عندئذٍ يكون:

$$f(x) = a\,(x-u)\,(x-v)$$

في $E[x]$ ، وبالمقارنة بين معاملات x العلاقتين نجد أن : $b = -a\,(u+v)$

وبالتالي يكون : $v = -u - a^{-1}b \in F(u)$ ، إذن :

$$E = F(u,v) = F(u)$$

تعريف (10) الحقل المغلق جبرياً Algebraically closed field :

نقول عن الحقل C إنه مغلق جبرياً إذا تحقق إحدى الشروط المتكافئة التالية :

(1) كل كثيرة حدود غير ثابتة في $C[x]$ تملك جذر في C .

(2) كل كثيرة حدود غير قابلة للتحليل في $C[x]$ لها الدرجة 1 .

(3) كل كثيرة حدود غير ثابتة في $C[x]$ تنشطر في $C[x]$.

(4) إذا كان $E \supseteq C$ امتداد جبري ، عندها يكون $E = C$.

مثال (17) :

إن حقل الأعداد المركبة C مغلق جبرياً .

إن الحقل $(Z_P,\oplus,\otimes)$، حيث P عدد أولي ليس مغلق جبرياً، لأن كثيرة الحدود $f(x) = x^2 + 1 \in Z_P[x]$ لا تملك جذوراً في الحقل $(Z_P,\oplus,\otimes)$.

تعريف (11) العناصر المترافقة Conjugates elements :

ليكن E امتداداً جبرياً للحقل F ، نقول عن العنصرين v,u من E ، إنهما مترافقان على الحقل F ، إذا كان كل من العنصرين v,u جذراً لكثيرة حدود نفسها غير قابلة للتحليل على الحقل F .

مثال (18) :

العنصران $a + i\,b$ و $a - i\,b$ من حقل الأعداد المركبة C مترافقين على الحقل R ، لأنهما يشكلان جذرين لكثيرة الحدود $f(x) = (x - a)^2 + b \in R[x]$ على R .

مبرهنة (8) :

ليكن $(F,+,.)$ حقلاً ما ، وإذا كان v,u عنصران جبريان على F ، وإذا كان $f(x)$ كثيرة حدود صغرى للعنصر u من الدرجة n على F ، عندئذٍ : التطبيق

$\varphi : F(u) \longrightarrow F(v)$ والمعرف بالشكل :

$$\varphi(a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}) = a_0 + a_1 v + \ldots + a_{n-1} v^{n-1}$$

يشكل تماثلاً ، إذا ، وفقط إذا كان العنصران v,u مترافقين على الحقل F .

البرهان :

لنبرهن أولاً ، أنه إذا كان v,u مترافقين على الحقل F ، فإن التطبيق φ يشكل تماثلاً .

ليكن $m = m(x)$ كثيرة الحدود الصغرى للعنصرين v,u على F ، وبالتالي فـإن للتشاكلين :

$$\varphi_v : F[x] \longrightarrow F(v)$$
$$\varphi_v\big(f(x)\big) = f(v)$$
$$\varphi_u : F[x] \longrightarrow F(u)$$
$$\varphi_u\big(f(x)\big) = f(u)$$

النواة نفسها ، أي أن :

$$\operatorname{Ker} \varphi_u = \operatorname{Ker} \varphi_v = < m(x) >$$

وبالتالي يوجد تماثلان :

$$\varphi'_u : F[x]/<m(x)> \longrightarrow F(u)$$
$$\varphi'_u : \big(f(x) + <m(x)>\big) = f(u)$$
$$\varphi'_v : F[x]/<m(x)> \longrightarrow F(v)$$
$$\varphi'_v : \big(f(x) + <m(x)>\big) = f(v)$$

لنفرض الآن أن : $\varphi = \varphi_v . \varphi_u^{-1}$ ، وبالتالي نجد أن التطبيق φ هو التماثل من الحقل F(u) على الحقل F(v) ، لأنه من العلاقة :

$$a_0 + a_1 u + \ldots + a_{n-1} u^{n-1} \in F(u)$$

نجد أن :

$$\varphi_v.\varphi_u^{-1}(a_0 + a_1 u + \dots + a_{n-1} u^{n-1}) = \varphi_v[a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + < m(x) >]$$

$$= a_0 + a_1 v + \dots + a_{n-1} v^{n-1}$$

برهان العكس :

لنبرهن أن العنصرين v,u مترافقان .

ليكن φ تماثلاً من الحقل $F(u)$ على الحقل $F(v)$. ولنفرض أن :

$m(x) = a_0 + a_1 x + \dots + x^n$ ، عندها يكون لدينا :

$$m(u) = a_0 + a_1 u + \dots + u^n$$

وكذلك يكون $m(v) = 0$. إذن كثيرة الحدود الصغرى $m'(x)$ للعنصر v على الحقل F تقسم $m(x)$.

لنأخذ التماثل : $\varphi^{-1}:F(v) \longrightarrow F(u)$ ، وبإجراء نفس الخطوات السابقة نجد أن $m(x)$ يقسم $m'(x)$ ، وبما أن $m(x)$ و$m'(x)$ كثيرتي حدود واحديتين ، فنجد $m(x) = m'(x)$ أي أن العنصرين v,u مترافقان .

(5-6) الحقول المنتهية Finite Fields :

تسمى الحقول المنتهية باسم حقول جالوا (Galois fields) ويعود السبب في ذلك ، أنه عندما درس الرياضي الفرنسي جالوا قابلية حل المعادلات الجبرية ، ظهر مفهوم الحقول المنتهية . وهي الحقول التي عدد عناصرها منتهي . ولهذه الحقول تطبيقات عديدة في البنى الجبرية وفي نظرية التشفير وفي العلوم الهندسية أيضاً .

مثال (19) :

إن حقل الأعداد الصحيحة قياس العدد الأولي P $(Z_P,\oplus,\otimes)$ تشكل حقلاً منتهياً .

مبرهنة (9) :

إذا كان E امتداداً منتهياً للحقل المنتهي F ، درجته n ، وإذا كان عدد عناصر الحقل F هو q، عندئذٍ عدد عناصر الامتداد E يساوي q^n .

البرهان :

لتكن المجموعة $\{a_1,a_2,..,a_n\}$ التي تشكل أساساً للفضاء المتجهي E علـى F . عندها يمكن كتابة كل عنصر من E وليكن α بشكل وحيد بالشكل :

$$\alpha = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n \ ; \ b_i \in F$$

بما أنه توجد q طريقة لاختيار العناصر $b_i \in F$ ، وبالتالي يوجد q^n طريقة لاختيار جميع العناصر b_i ، وبالتالي ، فإن عدد عناصر الامتداد E يساوي q^n .

ينتج من المبرهنة السابقة ، النتيجة التالية :

نتيجة (3) :

إذا كان E حقلاً منتهياً مميزه P، عندئذٍ E تحتوي على P^n عنصر ، حيث n عدد صحيح موجب .

البرهان :

نعلم أن كل حقل منته وليكن E هو امتداد منته لحقل أولـي يتماثـل مـع الحقـل $F = Z_P$ ، حيث P عدد أولي وهو مميز الحقل E ، وبالتالي فحسـب المبرهنـة السابقة يكون عدد عناصر E هو P^n .

تعريف (12) حقل جالوا Galois field :

إذا كان P عدداً أولياً ، وn عدداً صحيحاً موجباً ، نسمي الحقـل الـذي عـدد عناصره P^n بحقل جالوا من المرتبة P^n ، نرمز له عادةً بـ $GF(P^n)$.

مثال (20) :

إن $GF(P) = Z_P$ ، حيث أن P عدد أولي .

مبرهنة (10) :

إن عدد جذور كثيرة الحدود $f(x) = x^{P^n} - x \in Z_P[x]$ في حقل الانشـطار E على الحقل Z_P تكون مختلفة ، وتشكل حقلاً انشطارياً لكثيرة الحـدود f(x) عـدد عناصره P^n ، حيث P عدد أولي وn عدد صحيح موجب .

البرهان :

لدينا $f(x) = x^{P^n} - x \in Z_P[x]$ ، وبالتالي فــإن : $f'(x) = P^n . x^{P^n - 1} - 1 \neq 0$ ، وبالتالي فإن كثيرة الحدود $f(x)$ لا تحوي جذوراً مضاعفة (علّل ذلك) . أي أن لــ $f(x)$ ، n جذراً مختلفاً . لنثبت أن هذه الجذور تشكل حقلاً انشطارياً لــ $f(x)$ على الحقل Z_P .

بفرض أن a و $b \neq 0$ جذوراً لكثيرة الحدود $f(x)$ ، وبالتالي ، يكون :

$$(a \pm b)^{P^n} = a^{P^n} + b^{P^n} = a \pm b$$

$$(a.b^{-1})^{P^n} = a^{P^n} (b^{P^n})^{-1} = a.b^{-1}$$

وبالتالي فإن مجموعة الجذور لكثيرة الحدود $f(x)$ تشكل حقلاً جزئيــاً مــن حقــل الانشطار ، كما أن كثيرة الحدود $f(x)$ تحوي الحقل Z_P ويحوي P^n جذراً مختلفاً ، وهذا يعني أن هذا الحقل يتطابق مع حقل انشطار كثيرة الحدود $f(x)$.

مبرهنة (11) :

الشرط اللازم والكافي ، لكي يكون الحقل المنتهي E والذي رتبتــه P^n حقــلاً جزئياً رتبته P^m هو أن يكون m/n ، حيث P عدد أولي ، m,n أعداد صــحيحة موجبة .

البرهان :

لنبرهن أولاً أن $F \supseteq E$ ، حيث $|F| = P^m$.

بما أن m/n ، فإن $n = m.r$ ، وبما أن :

$$y^r - 1 = (y - 1)(y^{r-1} + y^{r-2} + \dots + y + 1) \Rightarrow P^m - 1 \mid P^n - 1$$

ولنفرض أن $y = P^m$ ، فيكون لدينا :

$$P^n - 1 = (P^m - 1).q \Rightarrow x^{P^m - 1} - 1 / x^{P^n - 1} - 1$$

إذن $x^{P^m - 1} - x / x^{P^n - 1} - x$ ، وبمــا أن E حقــل انشــطار لكثيــرة الحــدود $f(x) = x^{P^n} - x$ من $Z_P[x]$ ، فهو يحوي على جميــع جــذور كثيــرة الحــدود

$g(x) = x^{P^m} - x \in Z_P[x]$ على الحقل Z_P ، أي أن الحقل E يحوي حقل انشطار $g(x)$ على الحقل Z_P وهو الحقل F الذي رتبته P^m . وبالتـــالي $E \supseteq F$ ، حيــث $|F| = P^m$.

برهان العكس :

ليكن $E \supseteq F$ ، وحيث أن $|F| = P^m$ ، عندئذٍ يمكن اعتبـــار الحقــل E كفضـــاء متجهي على F ، بعده منته ويساوي r ، وبالتالي يكون :

$$n = [E : Z_P] = [E : F] . [F : Z_P] = m.r$$

وهذا يعني أن m/n .

مثال (21) :

إذا كان $(F,+,.)$ حقلاً ما ، رتبته P^{20} ، أوجد رتب الحقول الجزئية الفعلية في الحقل F .

الحل :

نلاحظ أن قواسم العدد 20 التي تحـــدد الحقـــول الجزئيـــة فـــي الحقـــل F هـــي 10,5,4,2,1، وبالتالي فإن رتب الحقول الجزئية المطلوبة هي : P, P^2, P^4, P^5, P^{10}.

مثال (22) :

ارسم المخطط الشبكي للحقول الجزئية من حقل جالوا رتبته P^6 .

الحل :

إن الحقول الجزئية من الحقل $GF(P^6)$ هي التالية :

$$Z_P = GF(P^1) , GF(P^2) , GF(P^3) , GF(P^6)$$

وبالتالي فإن المخطط الشبكي لهذه الحقول الجزئية هو :

$$\begin{tikzcd}
 & GF(P^6) \arrow[dl, dash] \arrow[dr, dash] & \\
GF(P^3) \arrow[dr, dash] & & GF(P^2) \arrow[dl, dash] \\
 & GF(P) &
\end{tikzcd}$$

مبرهنة (12) :

إذا كان E حقلاً منتهياً ، عندها توجد كثيرة حدود غير قابلة للتحليل ولتكن f(x) من F[x] من الدرجة n على الحقل E .

البرهان :

إذا كان الحقل K امتداداً للحقل E درجته n ، فإن $K = E(u)$ ، حيث $u \in K$ ، لأن K امتداد منته للحقل E و$u \in K$ عنصر جبري على الحقل E ولتكن f(x) كثيرة حدود صغرى للعنصر u على الحقل F ، عندها يكون :

$$\deg f = [E(u) : E]$$

وبما أن $K = E(u)$ و $[K : E] = n$ ، فإن كثيرة الحدود f(x) غير قابلة للتحليل على F ودرجتها تساوي n .

(6-6) الامتداد القابل للفصل Separable extension :

لنعرّف أولاً كثيرة الحدود القابلة للفصل .

لتكن $f(x) \in F[x]$ كثيرة حدود من الدرجة n ، على الحقل F ، إذا كانت f(x) غير قابلة للتحليل، عندها نقول إن كثيرة الحدود f(x) قابلة للفصل على الحقل F إذا كانت جميع جذورها بسيطة، أي أن f(x) تكتب في أي حقل انشطار E بالشكل:

$$f(x) = a\,(x - u_1)\,(x - u_2)\,\ldots.\,(x - u_n)$$

حيث أن : $a \in F\,,\,(i = 1,2,\ldots,n)\ ;\ u_i \in E\ ,\ i \neq j\ ;\ u_i \neq u_j$

ملاحظة (5) :

كل كثيرة حدود على حقل مميزه يساوي الصفر تكون قابلة للفصل .

مثال (23) :

إن كثيرة الحدود $f(x) = x^2 + 5 \in Q[x]$ قابلة للفصل على الحقل Q .

الحل :

نلاحظ أولاً أن f(x) كثيرة حدود غير قابلة للتحليل على الحقل Q ، وجذورها

تنتمي إلى الحقل C وهي $\pm\sqrt{5}\,i$. وبالتالي حسب التعريف السابق نجد أن $f(x) = x^2 + 5$ كثيرة حدود قابلة للفصل على Q .

لنقدم الآن مفهوم **العنصر القابل للفصل** والمتعلق بمفهوم الامتداد القابل للفصل .

تعريف (13) العنصر القابل للفصل Separable element :

إذا كان E امتداداً للحقل F ، وإذا كان $u \in E$ عنصراً جبرياً على الحقل F ، نقول إن u عنصر قابل للفصل على الحقل F ، إذا كانت كثيرة حدوده الصغرى قابلة للفصل على الحقل F .

تعريف (14) الامتداد القابل للفصل Separable extension :

نقول عن الامتداد الجبري E للحقل F إنه امتداد قابل للفصل ، إذا كان كل عنصر من عناصر الحقل E قابلاً للفصل على الحقل F .

مبرهنة (13) :

إذا كان E امتداداً منتهياً للحقل F ، وكان K امتداداً منتهياً للحقل E ، عندئذ يكون K امتداداً قابلاً للفصل للحقل F ، إذا ، وفقط إذا ، كان K امتداداً قابلاً للفصل للحقل E ، وكذلك كان E قابلاً للفصل للحقل F .

(تقبل بدون برهان) .

نتيجة (4) :

الشرط اللازم والكافي ، لكي تكون كثيرة الحدود $f(x) \in F[x]$ قابلة للفصل ، هو أن يكون القاسم المشترك الأعظم لكثيرتي الحدود $f(x)$ و $f'(x)$ يساوي الواحد في الحلقة $(F[x],+,\cdot)$.

البرهان :

لنبرهن أولاً أن كثيرة الحدود $f(x)$ قابلة للفصل على الحقل F .

نفرض العكس ، أي لنفرض أن $f(x)$ غير قابلة للفصل على الحقل F ، وهذا يعني أنه يوجد جذر وليكن α لـ $f(x)$ رتبة تضاعفه $m > 1$ ، أي :

$f(x) = (x-\alpha)^m . g(x)$ ، ومنه يكون :

$$f'(x) = (x-\alpha)^{m-1}.[m.g(x) + (x-\alpha)g'(x)]$$

نلاحظ أن العامل $(x-\alpha)^{m-1} \neq 1$ قاسماً مشتركاً لكثيرتي الحدود $f(x)$ و $f'(x)$ ، وهذا يناقض الفرض . إذن $f(x)$ كثيرة حدود قابلة للفصل على الحقل F .

لنبرهن العكس :

إذا كان E حقلاً انشطارياً لكثيرة الحدود $f(x)$ من $F[x]$ ، وبفرض أن $f(x)$ قابلة للفصل على الحقل F ، عندئذٍ يكون :

$$f(x) = a\,(x-u_1)\,(x-u_2)\ \ldots .\ (x-u_n)$$

حيث أن u_i هي جميع جذور كثيرة الحدود $f(x)$ على الحقل F و $a \in F$.

لنفرض الآن أن $d \neq 1$ (القاسم المشترك الأعظم لـ $f(x)$ و $f'(x)$) وهذا يعني أنه يوجد عامل مشترك وليكن $(x-u_i)$ لكل منهما ، أي أن :

$$f(x) = (x-u_i)\,g(x)$$

و

$$f'(x) = (x-u_i)\,h(x)$$

من ناحية ثانية ، لدينا :

$$f'(x) = g(x) + (x-u_i)\,g'(x)$$

ومنه يكون :

$$g(x) = (x-u_i)\,[h(x) - g'(x)]$$

أي أن $g(u_i) = 0$، وهذا يعني أن الجذر u_i ليس بسيطاً لكثيرة الحدود $f(x)$ ، وهذا يناقض فرضنا أن $f(x)$ كثيرة حدود قابلة للفصل على الحقل F . إذن القاسم المشترك الأعظم d لكثيرتي الحدود $f(x)$ و $f'(x)$ يساوي الواحد .

(7-6) الحقول التامة Perfect fields :

ليكن $(F,+,.)$ حقلاً ما ، نقول إن الحقل F حقلاً تاماً إذا كان كل امتداد له هو امتداد قابل للفصل .

مبرهنة (14) :

كل حقل مميزه معدوم هو حقل تام .

لبرهان هذه المبرهنة ، نستخدم الحقيقية الجبرية التالية :

إذا كان $\bar{F}$ حقلا الإغلاق الجبري للحقل F ، وإذا كانت f(x) كثيرة حدود واحدية على الحقل $\bar{F}$ حيث $f(x)=\sum_{i=0}^{n} a_i.x^i \in \bar{F}[x]$ ، $a_i \in \bar{F}$ ، وإذا كانت $(f(x))^m \in F[x]$ ، وكان $m.1 \neq 0$ في الحقل F ، عندئذٍ يكون $f(x) \in F[x]$ ، أي أن جميع العناصر a_i من F .

تبرهن بطريقة الاستنتاج الرياضي .

لنبرهن الآن على المبرهنة السابقة :

إذا كان E امتداداً للحقل F ، الذي مميزه معدوم ، ولنفرض أن $u \in E$. إن كثيرة الحدود f(x) غير القابلة للتحليل على الحقل F تتحل في الحلقة $\bar{F}[x]$، بالشكل : $\prod_i (x-u_i)^m$ ، حيث أن u_i جذور مختلفة لكثيرة الحدود f(x) ، لنأخذ $u = u_i$ ، وبالتالي يكون :

$$f(x)=\left(\prod_i (x-u_i)^m\right)$$

وبما أن $m.1 \neq 0$ في الحقل F الذي مميزه معدوم . فحسب الحقيقية السابقة يكون $\left(\prod_i (x-u_i)\right)$ من F[x] . وبما أن كثيرة الحدود f(x) غير قابلة للتحليل ، ودرجتها أصغر ما يمكن في الحلقة F[x] وصفرها هو u ، فنجد أن $m = 1$ ، وبالتالي ، فإن العنصر u قابل للفصل على الحقل F ، من أجل $u \in E$، وهذا يعني أن E هو امتداد قابل للفصل على الحقل F .

نتيجة (5) :

كل حقل منتهٍ هو حقل تام .

لندرس أخيراً الامتدادات الناظمية .

(8-6) الامتداد الناظمي Normal extension :

تعريف (15) :

لتكن E امتداداً للحقل F ، نقول إن الامتداد E للحقل F ناظمياً . إذا وُجِدَ من

أجل أي كثيرة حدود $f(x) \in F[x]$ غير قابلة للتحليل على الحقل F ، جذراً واحداً على الأقل في الحقل E ، أي أن f(x) تنشطر في الحقل E .

من التعريف السابق ، نجد أن الامتداد C (حقل الأعداد المركبة) للحقل R (حقل الأعداد الحقيقية) ناظمي ، لأن كل كثيرة حدود غير قابلة للتحليل في R تنشطر في الحقل C .

ملاحظة (6) :

توجد امتدادات ليست ناظمية ، فعلى سبيل المثال ، ليكن الامتداد Q(a) للحقل Q ، حيث $a = \sqrt[3]{5}$. نلاحظ أن كثيرة الحدود $f(x) = x^3 - 5 \in Q[x]$ غير قابلة للتحليل على الحقل Q ، وجذرها هو $\sqrt[3]{5}$ في الحقل $Q(\sqrt[3]{5})$ ، لكن لا تنشطر في الحقل $Q(\sqrt[3]{5})$ ، لأنها لو انشطرت في الحقل $Q(\sqrt[3]{5})$ لوجدنا ثلاثة جذور حقيقية مختلفة للعدد 2 ، وهذا مستحيل .

إذن الامتداد $Q(\sqrt[3]{5})$ للحقل Q غير ناظمي .

مثال (24) :

بيّن أن الامتداد $Q(\sqrt{-2})$ للحقل Q ناظمي .

الحل :

نلاحظ أولاً أن $a = \sqrt{-2}$ جذر لكثيرة الحدود $f(x) = x^2 + 2 \in Q[x]$ وهي غير قابلة للتحليل على الحقل Q في الحقل $Q(\sqrt{-2})$ ، كما أن كثيرة الحدود x^2+2 تنشطر في الحقل $Q(\sqrt{-2})$. إذن الامتداد $Q(\sqrt{-2})$ للحقل Q ناظمي.

مبرهنة (15) :

إذا كان E امتداداً جبرياً للحقل F محتوى في $\overline{F}$ (الإغلاق الجبري للحقل F) عندها العبارات التالية متكافئة :

(1) كل كثيرة حدود غير قابلة للتحليل في F[x] والتي لها جذراً في الحقل E تنشطر إلى عوامل خطية.

(2) إن الحقل E هو حقل انشطار لأسرة من كثيرات الحدود في F[x] .

(3) إذا كان التطبيق φ يغمر E في $\overline{F}$ ويبقى عناصر الحقل F ثابتة فإن φ تطبيق من E على $\overline{E}$ ، ويمكن عدّه تماثلاً ذاتياً على الحقل E .

البرهان :

$(1) \Rightarrow (2)$

لنفرض أن $u \in E$، ولتكن $m = m(x)$ كثيرة حدود صغرى للعنصر u على الحقل F ، فحسب (1) نجد أن m تنشطر إلى عوامل خطية في الحقل E ، وهذا يعني أن E حقل انشطار لأسرة كثيرات الحدود m_i للعناصر $u_i \in E$.

$(2) \Rightarrow (3)$

لتكن $f_i(x) \in F[x]$ أسرة من كثيرات الحدود ، حيث أن الحقل E هو حقل انشطارها ، $i \in I$ ، وإذا كان u جذراً لبعض كثيرات الحدود $f_i(x)$ في الحقل E ، عندها يمكن غمر E في $\overline{F}$ وفق التطبيق φ ويبقى عناصر الحقل F ثابتة ، وبالتالي يكون $\varphi(u)$ جذر لكثيرة الحدود $f_i(x)$. من ناحية ثانية ، بما أن الامتداد E يُوَلَّدُ بجميع جذور كثيرات الحدود ، وبالتالي ، فإن التطبيق φ تطبيقاً من E إلى F ، أي أن φ تماثلاً ذاتياً .

$(3) \Rightarrow (1)$

إذا كانت $f(x)$ كثيرة حدود غير قابلة للتحليل على الحقل F، ولها جذراً $u \in E$، وبفرض أن $v \in \overline{E}$ جذراً آخر لكثيرة الحدود $f(x)$ ، ولنثبت أن $v \in E$.

بما أن u,v جذرين لكثيرة الحدود $f(x)$، فيكون :

$$F(u) \cong F[x]/<g(x)> \cong F(v)$$

لنرمز بـ $\varphi: F(u) \longrightarrow F(v)$ للتماثل المعرف سابقاً، عندها يكون : $\varphi(u) = v$

ولدينا $\varphi(u) = u$ لكل u من F، إذن التماثل φ يمتد إلى التطبيق $\varphi_1: E \longrightarrow \overline{F}$، والذي يغمر الحقل E في $\overline{F}$ ، وبحسب (3) يكون φ_1 تماثل ذاتي على E ، إذن :

$$\varphi_1(u) = \varphi(u) = v \in E$$

مبرهنة (16) :

ليكن E امتداداً ناظمياً ومنتهياً للحقل F ، عندئذٍ يكون الحقل E انشطارياً لكثيرة حدود على الحقل F .

البرهان :

بما أن E امتداد ناظمي ومنتهي للحقل F ، فيكون : $E = F(u_1,u_2,\ldots,u_r)$ حيث أن u_i عناصر جبرية على الحقل F و $1 \le i \le r$، وبفرض أن $m_i(x)$ كثيرات حدود صغرى للعنصر u_i على الحقل F حيث $1 \le i \le r$. وإذا كان $f(x) = m_1(x) . m_2(x)\ldots\ldots m_r(x)$ ، وبما أن كثيرات الحدود $m_i(x)$ غير قابلة للتحليل على الحقل F وجذورها في الحقل E ، فإن جميع كثيرات الحدود $m_i(x)$ تنشطر على الحقل E ، أي أن $f(x)$ تنشطر أيضاً على الحقل E ، وبسبب أن الحقل E يتكون من الحقل F وجذور كثيرة الحدود $f(x)$ ، إذن (فحسب تعريف حقل الانشطار) E هو حقل انشطار لكثيرة الحدود $f(x)$ على الحقل F .

الفصل السابع

الحلقات الارتينية والنوثيرية

Artinian and Noetherian Rings

الفصل السابع

الحلقات الارتينية والنوثيرية

Artinian and Noetherian Rings

لندرس أخيراً نوعين من أهم أنواع الحلقات ، لكثرة تطبيقاتهما في الهندسة الجبرية ، وفي علومٍ جبريةٍ أخرى . يطلق على إحداهما الحلقات الارتينية نسبة للرياضي الألماني إيمل أرتين ، ويطلق على الثانية الحلقات النوثيرية ، نسبةً للرياضية الألمانية إيمي نوثر .

(1-7) تعاريف :

1- الحلقة الارتينية Artinian Ring :

نقول عن حلقة ما ، ولتكن $(R,+,\cdot)$ ، إنها تحقق خاصية السلسلة التناقصية descending chain condition (d.c.c) للمثاليات I ، إذا كان لأي سلسلة متناقصة من المثاليات $I_1 \supseteq I_2 \supseteq \ldots$ في R ، يوجد عدد صحيح موجب $n \in Z^+$، بحيث يتحقق $I_m = I_n$ ، لكل $m \geq n$.

ونقول عن حلقة $(R,+,\cdot)$. إنها ارتينية ، إذا حققت خاصية السلسلة التناقصية للمثاليات السابقة .

2- الحلقة النوثيرية Noetherian Ring :

نقول عن حلقة ما ، ولتكن $(R,+,\cdot)$ ، إنها تحقق خاصية السلسلة التصاعدية (المتزايدة) ascending chain condition (a.c.c) للمثاليات I_i ، إذا كان لأي سلسلة متصاعدة من المثاليات $I_1 \subseteq I_2 \subseteq \ldots$ في R ، يوجد عدد صحيح موجب $n \ni Z^+$ بحيث يتحقق : $I_m = I_n$ لكل $m \geq n$.

3- الخاصية العظمى Maximum condition :

لتكن $(R,+,\cdot)$ حلقة ما ، نقول عن هذه الحلقة ، إنها تحقق الخاصية العظمى

$\ldots \supset <2^n> \supset \ldots \supset <4> \supset <2>$ ، لكل $n \in Z^+$ تناقصية وغير منتهية من المثاليات في $(Z,+,\cdot)$.

(4) الحلقة المعرفة بالشكل :

$$R = \{ a = \frac{m}{P^n} : 0 < a < 1 \text{ , عدد أولي } P \}$$

حيث أن $a.b = 0$ ، لكل b,a من R و m من Z^+ ، هي حلقة ارتينية ، لأن كل مثالية في R هي من الشكل :

$$I_r = \left\{ \frac{1}{P^r}, \frac{2}{P^r}, \ldots, \frac{P^r - 1}{P^r} \right\} \;,\; |I_r| < \infty$$

وهذا يعني أن الحلقة R ، تحقق خاصة السلسلة التناقصية .

(5) لتكن الحلقة $(Z,+,\cdot)$ ، وإذا كان P عدداً أولياً ، فإن $I = <P>$ مثالية غير قابلة للتحليل في الحلقة Z ، لأنه إذا كانت $I = J \cap K$ ، فإن $I \subseteq J$ و $I \subseteq K$. لكن I مثالية أعظمية في الحلقة Z ، إذن $I = J$ و $I = K$.

لنقدّم الآن بعض الخصائص للحلقتين الارتينية والنوثيرية ، من خلال المبرهنات والنتائج التالية :

(3-7) بعض خصائص (صفات) للحلقتين الارتينية والنوثيرية :

مبرهنة (1) :

لتكن $(R,+,\cdot)$ حلقة ما ، تكون $(R,+,\cdot)$ حلقة ارتينية إذا ، وفقط إذا ، كان $R \in \min - \triangleleft$.

البرهان :

نفرض أولاً ، أن $\ldots \supseteq I_2 \supseteq I_1$ سلسلة تناقصية من المثاليات I_i على الحلقة R ، ولتكن $K = \{I_i : i = 1,2,\ldots\}$ مجموعة من المثاليات . إن $K \neq \phi$ ، وعليه فإن للمجموعة K عنصراً أصغرياً ، وليكن I_n .

والآن $I_m = I_n$ ، لكل $m \geq n$ ، فإذا كان $I_m \neq I_n$ ، فإن $I_m \notin K$ وهذا غير ممكن.

إذن $I_m = I_n$ لكل $m \geq n$ ، إذن $(R,+,\cdot)$ حلقة ارتينية .

لنبرهن العكس :

نفرض أن K مجموعة غير خالية من مثاليات لـ R ولتكن $I_1 \in K$. إذا كان I عنصراً ليس أصغرياً في S ، فيمكننا إيجاد مثالية ولتكن I_2 من K بحيث $I_1 \supset I_2$. وإذا فرضنا عدم وجود عنصر أصغر في K ، فيمكننا إعادة ما سبق مرة ثانية وبالتالي نحصل على سلسلة متناقصة غير منتهية .... $I_1 \supset I_2 \supset I_3 \supset$ من المثاليات في الحلقة R ، وهذا يناقض كون R حلقة ارتينية . إذن لأي مجموعة غير خالية من المثاليات في R ، يوجد عنصر أصغر ، أي $\lhd -$ $R \in \min$.

مبرهنة (2) :

لتكن $(R,+,\cdot)$ حلقة ما ، عندئذٍ العبارات الآتية متكافئة :

(1) $(R,+,\cdot)$ حلقة نوثيرية .

(2) كل مثالية في الحلقة R ذات مولدات منتهية .

(3) لكل مجموعة غير خالية من المثاليات في الحلقة R يوجد عنصر أعظم .

البرهان :

$(1) \Leftarrow (2)$

لتكن $I \lhd R$ ، ولنفرض أن $a_1 \in I$. إذا كانت $I \neq < a_1 >$ ، عندها يوجد $a_2 \in I$ ، بحيث يكون $a_2 \notin < a_1 >$ ، وبالتالي يكون $< a_1 > \subset < a_1,a_2 >$ ، فإذا كانت $I \neq < a_1,a_2 >$ ، عندئذٍ يوجد $a_3 \in I$ ، بحيث يكون $a_3 \notin < a_1,a_2 >$ وعليه يكون :

$$< a_1 > \subset < a_1,a_2 > \subset < a_1,a_2,a_3 >$$

وبتكرار ما سبق ، حتى نحصل على سلسلة من المثاليات في R التالية :

$$< a_1 > \subset < a_1,a_2 > \subset < a_1,a_2,a_3 > \subset \ldots$$

وبما أن R نوثيرية ، يوجد n من Z^+ بحيث $< a_1,\ldots,a_m > = < a_1,\ldots,a_n >$ ، لكل $m \geq n$ ، وعليه يكون $I = < a_1,\ldots,a_n >$. إذن I مثالية ذات مولدات

منتهية.

(2) $\Leftarrow$ (3)

لتكن K مجموعة غير خالية من مثاليات في R ، وبفرض أن $I_1 \in K$ ليس عنصراً أعظمياً . أي أن $I_1 \subset I_2 \in K$ ، فإذا كان I_2 عنصراً غير أعظم في K ، فيوجد $I_3 \in K$ بحيث يكون $I_2 \subset I_3$، وإذا فرضنا عدم وجود عنصراً أعظم في K، فيمكننا إيجاد سلسلة غير منتهية $I_1 \subset I_2 \subset I_3 \subset \ldots$ من المثاليات في R .

بما أن $I = \bigcup_i I_i \lhd R$ ، لأن لكل y,x من I ولكل r من R ، نجد أن $x,y \in I_r$ أو أن $x,y \in I_K$ ، لأن $I_r \subset I_K$ أو $I_K \subset I_r$ ، وبالتالي ، فإن : $r.x$ و $x\text{-}y$ ينتميان إلى نفس المثالية ، وبالتالي يكون : $r.x \in I = \bigcup_i I_i$ و $x\text{-}y$. لكن I ذات مولدات منتهية (فرضاً) ، إذن يوجد $a_1,a_2,\ldots,a_n \in I$ ، حيث أن $I = < a_1,a_2,\ldots,a_n >$ ، وبالتالي يوجد $m \geq 1$ بحيث يكون : $a_1,a_2,\ldots,a_n \in I_m$.

لكن $I_m \subset I = \bigcup_i I_i$ و I هي أصغر مثالية تحوي $a_1,a_2,\ldots,a_n$ ، إذن $I_m = I$ ، وعليه ، فإن : $I_m = I_{m+1} = \ldots$ وهذا يناقض وجود سلسلة غير منتهية من المثاليات في K . إذن يجب أن تحوي K عنصر أعظم .

(3) $\Leftarrow$ (1)

لتكن $I_1 \subseteq I_2 \subseteq \ldots$ سلسلة تصاعدية من المثاليات في R ، وبالتالي، للمجموعة $K = \{I_1 , I_2 , \ldots\}$، عنصر أعظم مثل I_n (حسب (3)) وبالتالي فإن: $I_m = I_n$ لكل $m \geq n$، إذن R حلقة نوثيرية .

مبرهنة (3) :

لتكن $(R,+,.)$ حلقة ذات عنصر محايد ، عندئذٍ ، R حلقة نوثيرية إذا ، وفقط إذا ، كانت كل مثالية أولية في R ذات مولدات منتهية .

البرهان :

لنفرض أولاً أن $(R,+,.)$ حلقة نوثيرية ، ولنبرهن على تحقق الشرط الوارد في

المبرهنة .

بما أن R حلقة نوثيرية ، فإن أي مثالية فيها هي ذات مولدات منتهية ، حسب المبرهنة السابقة ، وعليه، فإن أي مثالية أولية في R ذات مولدات منتهية .

لنبرهن العكس :

لنفرض جدلاً أن R حلقة ليست نوثيرية. ولنفرض أن كل مثالية أولية في R ذات مولدات منتهية، ولتكن K مجموعة جميع المثاليات في R ذات المولدات غير المنتهية ، وبالتالي يكون $K \neq \phi$ ، وعليه فإن للمجموعة عنصر أعظم وليكن I (حسب مبدأ زورن) ، إذن I مثالية ليست أولية في R، وبالتالي يوجد $x,y \notin I$ ، بينما $x.y \in I$. وبما أن $I \subset \langle I,y \rangle$ و $I \subset I : \langle y \rangle$ و$x \in I : \langle y \rangle$، كما أن I عنصر أعظم في K، إذن كل من $\langle I,y \rangle$ و$I : \langle y \rangle$ مثالية ذات مولدات منتهية، وعليه ، إذا كانت :

$$I : \langle y \rangle = \langle d_1,\ldots,d_m \rangle \quad \text{و} \quad \langle I,y \rangle = \langle c_1,c_2,\ldots,c_n \rangle$$

فإن : $c_i = x_i + y\, r_i$ ، حيث $x_i \in I$ و$r_i \in R$ و $i = 1,2,\ldots,n$.

إذن $\langle I,y \rangle = \langle x_1,\ldots,x_n,y \rangle$.

لتكن $J = \langle x_1,\ldots, x_n , yd_1,\ldots, yd_m \rangle$ مثالية في R ، إذن $yd_i \in I$ ، لكل i وبالتالي يكون $J \subseteq I$. لكن إذا كان $a \in I$ ، فإن $a \in \langle I,y \rangle$ ، وعليه يكون $a = \sum_{i=1}^{n} x_i.t_i + y r$ حيث $t_i , r \in R$. لكن x_i من I لكل i ، إذن $y.r \in I$ ، وعليه فإن $r \in I : \langle y \rangle$ ، إذن $r = \sum_{j=1}^{m} d_j.y_j$ ، حيث $y_j \in R$ ، وعليه فإن :

$$a = \sum_{i=1}^{n} x_i.t_i + y\sum_{j=1}^{m} d_j.y_j = \sum_{i=1}^{n} x_i.t_i + y\sum_{j=1}^{m} (y d_j).y_j \in J$$

وبالتالي ، فإن $I \subseteq J$ ، إذن $I = J$ ، وعليه فإن المثالية I ذات مولدات منتهية ، وهذا تناقض كون $I \in K$ ، إذن R حلقة نوثيرية .

مبرهنة (4) :

(a) لتكن $(R,+,\cdot)$ حلقة ارتينية ، وكانت $I \lhd R$ ، عندئذٍ : R/I حلقة ارتينية .

(b) إذا كانت $I \lhd R$ ، وكان كل من I و R/I حلقة ارتينية ، فإن R حلقة ارتينية .

البرهان :

(a) ليكن التشاكل الطبيعي : $\Pi : R \longrightarrow R/I = \overline{R}$ ، وإذا كانت $\overline{I_1} \supseteq \overline{I_2} \supseteq .....$ سلسلة متناقصة من المثاليات في $\overline{R}$ ، ولنفرض أن $I_t = \Pi^{-1}(\overline{I_t})$. إذن $I_1 \supseteq I_2 \supseteq \ldots$ ، سلسلة متناقصة من المثاليات في R ، وبما أن R حلقة ارتينية ، فيوجد عدد صحيح موجب وليكن n بحيث يكون $I_m = I_n$ ، لكل $m \geq n$ ، وعليه يكون $\overline{I_m} = \overline{I_n}$ ، لكل $m \geq n$ ، وبالتالي ، فإن R/I حلقة ارتينية .

(b) لنفرض أن $I_1 \supseteq I_2 \supseteq \ldots$ سلسلة متناقصة من المثاليات في R ، وبالتالي يكون : $(I_1+I)/I \supseteq (I_2+I)/I \supseteq \ldots$ سلسلة متناقصة من المثاليات في R/I و $I_1 \cap I \supseteq I_2 \cap I \supseteq \ldots$ سلسلة متناقصة من المثاليات في I، لكن كلاً من R/I و I حلقة ارتينية، وبالتالي يوجد $s,r \in Z^+$ ، بحيث يكون :

$$(I_r+I)/I = (I_n+I)/I \;\; , \;\; I_s \cap I = I_n \cap I$$

لكل $n \geq r$ ، وعليه يكون :

$$I_r + I = I_n + I \;\; , \;\; I_s \cap I = I_n \cap I$$

لكل $n \geq r$ ، فإذا كان : $m = \max\{t,s\}$ ، نجد أن : $I_m + I = I_n + I$ و $I_m \cap I = I_n \cap I$ ، لكل $m \geq n$. لكن $I_n \subseteq I_m$ ، إذن :

$$I_m = I_m \cap (I_m+I) = I_m \cap (I_n + I) = I_n + (I_m \cap I) = I_n + (I_n \cap I) = I_n$$

إذن تكون $(R,+,\cdot)$ حلقة ارتينية .

مبرهنة (5) :

إذا كانت I و R/I حلقة نوثيرية ، وكان $I \lhd R$ ، فإن R حلقة نوثيرية .

البرهان :

لتكن $I_1 \subseteq I_2 \subseteq \ldots$ سلسلة متصاعدة من المثاليات في R ، وبالتالي يكون : $(I_1+I)/I \subseteq (I_2+I)/I \subseteq \ldots$ سلسلة متصاعدة من المثاليات في R/I . لكن R/I حلقة نوثيرية ، إذن يوجد عدد صحيح موجب ، وليكن r بحيث يكون $(I_r+I)/I = (I_n+I)/I$ ، لكل $n \geq r$ ، وبالتالي يكون : $I_r + I = I_n + I$ ، لكل $n \geq r$، وحيث أن $I_1 \cap I \subseteq I_2 \cap I \subseteq \ldots$ سلسلة متصاعدة من المثاليات في الحلقة النوثيرية I . إذن يوجد عدد صحيح موجب وليكن s بحيث يكون :

$I_s \cap I = I_n \cap I$ ، لكل $n \geq s$ ، فإذا كان : $m = \max\{r,s\}$ ، نجد أن :

$I_m + I = I_n + I$ و $I_m \cap I = I_n \cap I$ لكل $n \geq m$ ، لكن $I_m \subseteq I_n$ ، إذن :

$$I_n = I_n \cap (I_n+I) = I_n \cap (I_m + I) = I_m + (I_n \cap I) = I_m + (I_m \cap I) = I_m$$

إذن R حلقة نوثيرية .

نتيجة (1) :

لنفرض أن $R_1, R_2, \ldots, R_n$ حلقات نوثيرية ، فإن $R = \sum_{i=1}^{n} \oplus R_i$ حلقة نوثيرية .

البرهان :

بطريقة الاستقراء الرياضي على n ، نبرهن هذه النتيجة . ولنبرهن عليها من أجل $n = 2$. إذن $R = R_1 \oplus R_2$ ، وبالتالي يكون : $R/R_1 \cong R_2$. وبما أن R_2 حلقة نوثيرية ، إذن R/R_1 حلقة نوثيرية ، وبما أن R_1 حلقة نوثيرية ، إذن R حلقة نوثيرية ، حسب المبرهنة السابقة .

المبرهنة التالية ، تعرف باسم المبرهنة الأساسية لهيلبرت ، والتي نقبلها بدون برهان .

مبرهنة (6) Hilberts Basis theorm :

إذا كانت $(R,+,\cdot)$ حلقة نوثيرية ، فإن حلقة كثيرات الحدود $(R[x],+,\cdot)$ هي حلقة نوثيرية أيضاً .

نتيجة (2) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية ، عندئذٍ تكون $R[x_1,x_2,\ldots,x_n]$ حلقة نوثيرية أيضاً .

وإذا كانت $R_1,R_2,\ldots,R_n$ حلقات ارتينية ، فإن $R=\sum_{i=1}^{n}\oplus R_i$ حلقة ارتينية

(تبرهن هذه النتيجة بطريقة الاستقراء الرياضي على n) .

(4-7) بعض خواص المثاليات في الحلقة النوثيرية :

نذكِّر الطالب الكريم بمفهوم المثالية معدومة القوى (المتلاشية) ، وبمفهوم المثالية شبه المتلاشية ، وجذر جاكبسون لحلقة ، والجذر الأولي للحلقة R ، والمثالية الأولية .

نقول عن مثالية I في حلقة ما ، ولتكن $(R,+,\cdot)$ إنها **معدومة القوى (متلاشية)** (Nilpotent ideal)، إذا وُجِدَ عدد صحيح موجب وليكن n بحيث يكون : $I^n=0$، حيث 0 هو صفر الحلقة R .

نقول عن المثالية J إنها شبه معدومة القوى (شبه متلاشية) (Nil ideal) في الحلقة $(R,+,\cdot)$ ، إذا كان كل عنصر فيها متلاشياً .

أما **جذر جاكبسون** (Jacobson radical) لحلقة ما ، ولتكن $(R,+,\cdot)$ فيعرف على أنه تقاطع لجميع المثاليات العظمى فيها ، ونرمز له عادةً بـ $J(R)$ أو بـ $Rad(R)$. إذن :

$$J(R)=\bigcap\{M : \text{مثالية عظمى في الحلقة } R \ M\}$$

إذا كان $J(R)=0$ ، قيل عن الحلقة $(R,+,\cdot)$ إنها حلقة شبه بسيطة (Semi simple ring) .

نعرِّف الآن **الجذر الأولي** للمثالية I في الحلقة $(R,+,\cdot)$ ، والذي نرمز له عادةً بـ $rad(R)$.

لتكن $(R,+,\cdot)$ حلقة إبدالية ما ، عندئذٍ :

$$\text{rad}(R) = \{x \in R : \exists n \in Z^{+} : x^{n} \in I\}$$

لنعرّف أخيراً المثالية الأولية في الحلقة R (Prime ideal) .

نقول عن مثالية I في حلقة $(R,+,\cdot)$ ، إنها مثالية أولية (Prime ideal) في تلك الحلقة، إذا كان $J.K \subseteq I$، حيث J و K مثاليتين في R، فإن $J \subseteq I$ أو $K \subseteq I$.

مبرهنة (7) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية ، عندها الجذر الأولي للحلقة rad (R) هو أكبر مثالية معدومة القوى (متلاشية) في الحلقة R .

البرهان :

بما أن R حلقة نوثيرية ، عندها توجد مثالية معدومة القوى عظمى ، ولتكن N في R . ولنفرض أن I مثالية معدومة القوى في R ، وإذا كان $N^{m} = 0$ و $I^{n} = 0$ فإن $(I+N)^{m+n} = 0$ ، وبالتالي يكون $I + N$ مثالية معدومة القوى في R ، كما أن $N \subseteq I + N$. لكن N مثالية معدومة القوى عظمى في R ، إذن $N = I + N$، وبالتالي يكون $I \subseteq N$ ، ومنه يكون N أكبر مثالية معدومة القوى في R . لكن N مثالية شبه معدومة القوى ، إذن $N \subseteq \text{rad}(R)$.

لنثبت أن $\text{rad}(R) \subseteq N$ ، من أجل ذلك نفرض أن $(x + N) \in R/N$ عنصر معدوم القوى، وبالتالي يوجد $m \in Z^{+}$، بحيث يكون: $x^{m} + N = (x + N)^{m} = N$، وبالتالي فإن $x^{m} \in N$. وبما أن N مثالية شبه معدومة القوى ، إذن يوجد $n \in Z^{+}$ بحيث يكون $x^{m.n} = (x^{m})^{n} = 0$ وعليه يكون $x \in R$ عنصر معدوم القوى ، ومنه ينتج أن المثالية $< x >$ معدومة القوى ، ومنه يكون $< x > \subseteq N$ ، إذن N مثالية معدومة القوى عظمى في R . لكن $x \in < x > \subseteq N$ ، إذن $x + N = N$ ، ومنه يكون R/N لا تحوي أي عنصر معدوم القوى غير صفري ، وبالتالي $\text{rad}(R/N) = \overline{0}$ ، لكن rad (R) أصغر مثالية في R بحيث يكون : $\text{rad}(R/\text{rad}(R)) = \overline{0}$، ومنه يكون: $\text{rad}(R) \subseteq N$، وعليه يكون $\text{rad}(R) = N$.

نتيجة (3) :

إذا كانت $(R,+,\cdot)$ حلقة نوثيرية ، فإن أي مثالية شبه معدومة القوى في R ، هي مثالية معدومة القوى .

البرهان :

لتكن I مثالية شبه معدومة القوى في الحلقة R ، إذن $I \subseteq rad\ (R)$ وبما أن $rad\ (R)$ مثالية معدومة القوى في R (حسب المبرهنة السابقة) ، إذن I مثالية معدومة القوى في R .

مبرهنة (8) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية ، فإن أي مثالية في R تحوي حاصل ضرب مثاليات أولية .

البرهان :

لتكن K مجموعة المثاليات في الحلقة النوثيرية R ، التي لا تحوي حاصل ضرب مثاليات أولية في R ، ولنفرض أن $K \neq \phi$ ، وبالتالي فإن S تحوي عنصر أعظم، وليكن N ، وبالتالي فإن N مثالية ليست أولية ، وبالتالي توجد مثاليتين K,J في R بحيث $J.K \subseteq N$ ، لكن $J \not\subseteq N$ و $K \not\subseteq N$. لكن :

$$(N + J)\ (N + K) \subseteq N^2 + N.K + J.N + J.K \subseteq N$$

و $N \subset N + J$ و $N \subset N + K$ ، إذن $N + J \notin K$ و $N + K \in K$ ، وعليه يكون كلاً من $N + J$ و $N + K$ يحوي حاصل ضرب مثالية أولية في R ، وبالتالي فإن : $(N + J)\ (N + K)$ تحوي حاصل ضرب مثاليات أولية في R ، وعليه فإن N تحوي حاصل ضرب مثاليات أولية في R، وهذا يناقض كون $N \in K$. إذن $S \neq \phi$ وعليه ، فإن أي مثالية في R تحوي حاصل ضرب مثاليات أولية في الحلقة R .

مبرهنة (9) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية ما ، عندئذٍ يمكن التعبير عن أي مثالية فعلية ، كتقاطع عدد منتهي من المثاليات غير القابلة للتحليل في الحلقة R .

البرهان :

لتكن K مجموعة جميع المثاليات الفعلية في الحلقة R ، التي لا يمكن التعبير عنها كتقاطع عدد منتهي من المثاليات غير القابلة للتحليل في الحلقة R ، ولنفرض أن $K \neq \phi$. عندئذٍ K تحوي عنصر أعظم وليكن M ، وعليه فإن M مثالية قابلة للتحليل في R ، وهذا يعني ، أنه توجد مثاليتين I و J في R بحيث يكون $M = I \cap J$، $M \subset I$ و $M \subset J$ ، وبما أن M عنصر أعظم في K ، فإن $I,J \notin K$، وبالتالي يمكن التعبير عن كل منهما كتقاطع عدد منتهي من المثاليات غير القابلة للتحليل في R ، وبالتالي يمكن التعبير عن M كتقاطع عدد منتهي من المثاليات غير القابلة للتحليل في R ، وهذا تناقض . وبالتالي ، فإن $K = \phi$ ، إذن كل مثالية فعلية في الحلقة R ، يمكن التعبير عنها كتقاطع عدد منتهي من المثاليات غير القابلة للتحليل .

تعريف المثالية الابتدائية Primary ideal :

لتكن $(R,+,\cdot)$ حلقة إبدالية ما ، وإذا كان $I \lhd R$ ، نقول عن I إنها مثالية ابتدائية في R ، إذا تحقق الشرط التالي :

لكل a و b من R ، وإذا كان $a.b \in I$ و $a \notin I$ ، فإن $b^n \in I$. لبعض قيم n من Z^+.

لاحظ أن I مثالية ابتدائية في R $\Leftrightarrow$ $(a.b \in I , a \notin I) \Rightarrow b \in \sqrt{I} = \text{rad}(I)$

وإذا كانت I مثالية أولية في R ، فإن I مثالية ابتدائية في R أيضاً .

مبرهنة (10) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية ، عندها ، يمكن التعبير عن أي مثالية فعلية فيها كتقاطع عدد منتهي من المثاليات الابتدائية .

البرهان :

لنفرض أن I مثالية ليست ابتدائية في الحلقة R ، ولنبرهن أن أي مثالية غير قابلة للتحليل في R هي مثالية ابتدائية . بما أن I مثالية ليست ابتدائية في R ، لذا

يوجد $a,b\in I$ بحيث $a.b\in I$ و $a\in I$ و $b^r\in I$ لكل $r\in Z^+$ ، لتكن $I_m=\{x\in R : b^n.x\in I\}$، إن $I_m\lhd R$ حيث $m\in Z^+$ ، كما أن $I_1\subseteq I_2\subseteq \ldots$، وبما أن R حلقة نوثيرية، يوجد عدد صحيح موجب n، بحيث يكون $I_n=I_{n+1}=\ldots$ ولنثبت أن : $I=(I+Rb^n)\bigcap(I+<a>)$ ، من أجل ذلك ، إن $I\subseteq(I+Rb^n)\bigcap(I+<a>)$، كما أنه، إذا كان $x\in(I+Rb^n)\bigcap(I+<a>)$ ، فإن : $x=c+yb^n=d+ea+ma$ ، حيث $m\in Z$ و $y,e\in R$ و $c,d\in I$.

بما أن $a.b\in I$ ، فيكون :

$$bx=bc+b\,(yb^n)=bd+eab+mab\in I$$

وبما أن I_n+I_{n+1} ، فيكون : $yb^n\in I$ ، ومنه يكون $x\in I$.

نستنتج مما سبق ، أن $I=(I+Rb^n)\bigcap(I+<a>)$ ، وعليه ، فإن I مثالية قابلة للتحليل في R، لأن $I\subset(I+Rb^n)$ و $I\subset(I+<a>)$.

إذن كل مثالية غير قابلة للتحليل هي مثالية ابتدائية في R .

مبرهنة (11) :

لتكن $(R,+,.)$ حلقة بمحايد ، وإذا كانت I , J مثاليتين في R ، حيث أن $I\,.\,J=I$ ، ولنفرض أن I مثالية ذات مولدات منتهية ، عندئذٍ يوجد $x\in J$ ، بحيث يكون $(1-x).\,I=0$.

البرهان :

لتكن $I=<a_1,\ldots,a_n>$ و $I_i=<a_i\,,a_{i+1}\,,\ldots,a_n>$ و $I_{n+1}=0$. ولنبرهن على وجود العنصر x_i من J ، بطريقة الاستقراء الرياضي على i بحيث يكون $(1-x_i).I\subseteq I_i$.

إذا كان $i=1$ و $I_1=I$، وبالتالي يكون : $x_1=0$ والعلاقة صحيحة من أجل $i=1$.

لنفرض الآن أن $(1-x_i).I\subseteq I_i$ حيث $x_i\in I$. بما أن $I\subseteq I.J$ فيكون :

$$(1-x_i).I\subseteq(1-x_i)\,I.J\subseteq I_i.I$$

وبما أن $a_i\in I$ لكل i ، فيكون : I $(1-x_i)\ a_i\in I_i$ ، ومنه يكون

$(1-x_i)\,a_i=\sum_{r=i}^{n} b_{ir}a_r$ ، حيث أن $b_{ir}\in J$. إذن :

$$(1-x_i-b_{ir})\,a_i \sum_{r=i+1}^{n} b_{ir}a_r \in I_{i+1}$$

ومنه يكون :

$$(1-x_i)\,(1-x_i-b_{ii})\,I \subseteq (1-x_i-b_{ii})\,I \subseteq I_{i+1}$$

نستنتج مما سبق أنه إذا كان :

$$1-x_{i+1}=(1-x_i)\,(1-x_i-b_{ii})$$

فإن $(1-x_{i+1})\,I \subseteq I_{i+1}$ ، وبالتالي ، فإن العلاقة صحيحة من أجل جميع قيم i .

وإذا كان $x=x_{n+1}$ ، فإن $x\in J$ و $(1-x)\,I=0$.

ينتج من المبرهنة السابقة النتيجة التالية والمسماة بتمهيدية نكياما Nakayam's Lemma .

نتيجة (4) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ما، و I مثالية ذات مولدات منتهية فيها، وإذا كان $I.J(R)=I$ ، فإن $I=0$.

البرهان :

بما أن I مثالية ذات مولدات منتهية في R و $I.J(R)=I$ ، فيوجد $x\in J(R)$ بحيث يكون $(1-x).I=0$ (حسب المبرهنة السابقة) ، وبالتالي يكون :

$$I \subseteq \operatorname{ann}(1-x)=\{x\in R:(1-x)\,r=0\}$$

وبما أن $(1-x)$ قابل للانعكاس ، إذن : $\operatorname{ann}(I-x)=0$ ومنه يكون $I=0$.

نتيجة (5) :

لتكن $(R,+,\cdot)$ حلقة نوثيرية بمحايد ، وإذا كانت I مثالية فعلية في R ، عندئذٍ :

$$\bigcap_{n=1}^{\infty} I^n=\{r\in R:\exists a\in I:(1-a)\,r=0\}$$

مبرهنة (12) :

بفرض أن $(R,+,\cdot)$ حلقة ارتينية، عندها يكون $J(R)$ مثالية معدومة القوى

(متلاشية) .

البرهان :

لتكن السلسلة التناقصية من المثاليات في R التالية :

$$J \subseteq J^2 \subseteq \ldots . \;\; ; \;\; J = J(R)$$

بما أن R حلقة ارتينية ، يوجد عدد صحيح موجب ، وليكن n بحيث $J^n = J^{n+1} = \ldots .$.

إذا كان $I = J^n$ ، فإن $I \subseteq J$ و $I^2 = I$. ولنثبت أن $I = 0$.

من أجل ذلك ، نفرض أن $I \neq 0$

$$K = \{ I \lhd R : I \subseteq k \, , k.I \neq 0 \}$$

ومنه يكون $k \neq \phi$ ، لأن $I \in K$ ، وعليه فإن K تحوي عنصر أصغر وليكن M .

إذن $M.I \neq 0$، ومنه يكون $b \in M$ بحيث $b.I \neq 0$.

إذن : $(b.I)\, I = b\, I^2 = b\, I \neq 0$ و $b\, I \subseteq M \subseteq I$ ، ومنه يكون $b.I = M$ (لأن M عنصر أصغر في K) . وبالتالي يوجد $x \in I$ ، بحيث أن ، $b.x = b$. وبما أن $x \in I \subseteq J$ ، إذن $(1 - x)$ قابل للانعكاس في الحلقة R ، وبالتالي يوجد $r \in R$ بحيث $(1 - x)\, r = 1$. إذن :

$$b = b\,(1 - x)\, r = (b - bx)\, r = 0$$

وهذا يناقض كون $b\, I \neq 0$ ، إذن $I = J^n = 0$ ، أي أن J مثالية معدومة القوى في الحلقة R .

نقدّم أخيراً العلاقة بين الحلقة الارتينية والحلقة النوثيرية ، من خلال المبرهنات التالية ، والتي سنقبلها بدون برهان .

(5-7) العلاقة بين الحلقة الارتينية والنوثيرية :

مبرهنة (13) :

لتكن $(R,+,\cdot)$ حلقة بمحايد ، تكون R حلقة ارتينية ، إذا ، وفقط إذا ، كانت R حلقة نوثيرية وكل مثالية أولية فعلية فيها هي مثالية عظمى .

مبرهنة (14) :

بفرض أن $(R,+,\cdot)$ حلقة بمحايد ، ولتكن $I_1,\ldots,I_n$ مثاليات أعظمية في الحلقة R ، حيث $\prod_{i=1}^{n} I_i = 0$ ، عندئذٍ تكون R حلقة نوثيرية إذا ، وفقط إذا ، كانت R حلقة ارتينية .

نستنتج مما سبق ، أنه إذا كانت $(R,+,\cdot)$ حلقة ارتينية بمحايد ، فإن $(R,+,\cdot)$ حلقة نوثيرية .

(ب) القسم العملي

تمارين محلولة وغير محلولة للفصل الأول :

الحلقة والحلقة التامة

Ring & Integral domains

1- تمرينات محلولة للفصل الأول

– الحلقة والحلقة التامة –

(1) لنعرّف على مجموع أزواج الأعداد الصحيحة $Z^2 = Z\times Z$ العمليتين $(+)$ و $(\times)$ بالشكل التالي :

$$(x,y) + (x_1,y_1) = (x + x_1 , y + y_1)$$
$$(x,y) \times (x_1,y_1) = (x x_1 , y y_1 + x y_1 + y x_1)$$

لكل (x,y) و (x_1,y_1) من Z^2 ، المطلوب :

أثبت أن $(Z^2,+,\times)$ حلقة إبدالية ، ثم بيّن فيما إذا كانت هذه الحلقة بمحايد أو حلقة تامة .

الحل :

لنثبت أولاً ، أن $(Z^2,+,\times)$ حلقة إبدالية .

بالاستفادة من أن عملية الجمع على Z تجميعية وإبدالية نجد :

$$\begin{aligned}
[(x,y) + (x_1,y_1)] + (x_2,y_2) &= (x + x_1 , y + y_1) + (x_2,y_2)\\
&= [(x + x_1) + x_2 , (y + y_1) + y_2)]\\
&= [x + (x_1 + x_2) , y + (y_1 + y_2)] = (x,y) + (x_1+x_2 , y_1+y_2)\\
&= (x,y) + [(x_1,y_1) + (x_2,y_2)]
\end{aligned}$$

أي أن $(+)$ تجميعية على عناصر $(Z^2,+,\times)$.

كما أن :

$$\begin{aligned}
(x,y) + (x_1,y_1) &= (x + x_1 , y + y_1) = (x_1 + x , y_1 + y)\\
&= (x_1,y_1) + (x,y)
\end{aligned}$$

أي أن العملية $(+)$ إبدالية على عناصر الحلقة $(Z^2,+,\times)$.

إن العنصر (o,o) محايد بالنسبة لعملية الجمع على Z^2 لأنه، إذا كان y,x من Z، فإن :

$$(x,y) + (o,o) = (o,o) + (x,y) = (x,y)$$

كذلك ، لكل عنصر معكوس بالنسبة لعملية الجمع على Z^2 ، أي أن لكل عنصر مثل (x,y) معكوس بالنسبة لعملية الجمع $(-x,-y)$ على Z^2 ، لأن :

$$(x,y) + (-x,-y) = (-x,-y) + (x,y) = (o,o)$$

نستنتج مما سبق أن $(Z^2,+)$ زمرة إبدالية .

لنثبت الآن أن عملية $(\times)$ تجميعية على عناصر Z^2، ليكن $(x,y),(x_1,y_1),(x_2,y_2)$ ثلاثة عناصر من Z^2 ، فإن :

$$[(x,y)\times(x_1,y_1)]\times(x_2,y_2) = (xx_1,yy_1+xy_1+yx_1)\times(x_2,y_2)$$

$$= [(xx_1)\, x_2 \, , (yy_1+xy_1+yx_1)\, y_2 + (xx_1)\, y_2+(yy_1+xy_1+yx_1)\, x_2] \quad (1)$$

$$(x,y)\times[(x_1,y_1)\times(x_2,y_2)] = (x,y)\times(x_1x_2 \, , y_1y_2+x_1y_2+y_1x_2)$$

$$= [x\,(x_1x_2),y\,(y_1y_2+x_1y_2+y_1x_2) + x\,(y_1y_2+x_1y_2+y_1x_2)+y\,(x_1x_2)] \quad (2)$$

بمقارنة (1) و (2) نجد أن الخاصة التجميعية بالنسبة لعملية الضرب $(\times)$ محققة في Z^2 .

لنثبت الآن أن عملية الضرب $(\times)$ تقبل التوزيع (توزيعية) بالنسبة لعملية الجمع $(+)$ في Z^2 :

$$\begin{aligned}(x,y)\times[(x_1,y_1)+(x_2,y_2)] &= (x,y)\times(x_1+x_2 \, , y_1+y_2)\\ &= [x(x_1+x_2) \, , y\,(y_1+y_2) + x\,(y_1+y_2) + y\,(x_1+x_2)]\\ &= (x\,x_1+x\,x_2 \, , yy_1+xy_1+yx_1+yy_2+xy_2+yx_2)\\ &= (x\,x_1 \, , yy_1+xy_1+yx_1) + (xx_2 \, , yy_2+xy_2+yx_2)\\ &= (x,y)\times(x_1,y_1) + (x,y)\times(x_2,y_2)\end{aligned}$$

لاحظ في هذا البرهان ، استفدنا من أن خاصة توزيع الضرب على الجمع في الأعداد الصحيحة Z .

نستخلص ، مما سبق أن $(Z^2,+,\times)$ حلقة . ولما كان :

$$\begin{aligned}(x,y)\times(x_1,y_1) &= (xx_1 \, , yy_1+xy_1+yx_1)\\ &= (x_1x \, , y_1y+x_1y+y_1x) = (x_1,y_1)\times(x,y)\end{aligned}$$

إذن هذه الحلقة إبدالية .

لكي تكون الحلقة $(Z^2,+,\times)$ بمحايد ، يلزم ويكفي وجود عنصر وليكن (x,y) من Z^2 بحيث يحقق الشرط من أجل أي b,a من Z ، فإن :

$$(a,b)\times(x,y) = (a,b) \Leftrightarrow (ax\,,\, by + ay + bx) = (a,b)$$

$$\Leftrightarrow ax = a\,,\, by + ay + bx = b \Rightarrow x = 1\,,\, y = 0$$

وبالتالي فإن $(1,0)$ من Z^2 عنصر محايد للعملية $(\times)$ في الحلقة $(Z^2,+,\times)$. إذن الحلقة $(Z^2,+,\times)$ بمحايد.

لنبيّن أخيراً ، فيما إذا كانت الحلقة $(Z^2,+,\times)$ تامة .

ليكن (x,y) و (u,v) عنصرين ما من Z^2 ، يحققان العلاقة :

$$(x,y)\times(u,v) = (0,0)$$

إن :

$$(x,y)\times(u,v) = (0,0) \Leftrightarrow (xu\,,\, yv + xv + yu) = (0,0)$$

$$\Leftrightarrow xu = 0\,,\, yv + xv + yu = 0$$

نستنتج من هذا ، أنه إذا كان $u = -v$ و $x = 0$ و y,v أي عددين صحيحين ، فإن علاقتي التساوي السابقتين تكونان محققتين ، وعلى سبيل المثال ، فإن :

$$(0,1)\,(2,-2) = (0,0)$$

إذن الحلقة $(Z^2,+,\times)$ ليست تامة ، لأنها تحتوي على عناصر مغايرة للصفر $(0,0)$ حاصل ضربها يساوي الصفر ، أي أنها تحتوي على قواسم للصفر .

(2) لتكن X مجموعة غير خالية ، وإذا كانت $P(X)$ مجموعة القوة للمجموعة X ، وإذا عرّفنا العمليتين $(+)$ و$(\cdot)$ على المجموعة $P(X)$ بالشكل :

لكل A,B من $P(X)$ ، يكون :

$$A + B = A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$$
$$A \cdot B = B \cap A$$

أثبت أن $(P(X),+,\cdot)$ حلقة إبدالية بمحايد .

الحل :

من السهولة إثبات أن $(P(X),+)$ زمرة إبدالية ، حيث أن صفرها هو المجموعة

الخالية ، لأن :

$$A + \phi = (A \cup \phi) \setminus (A \cap \phi) = A \setminus \phi = A = \phi + A \in P(X)$$

ومحايد هذه الحلقة هي المجموعة X لأن :

$$A \cap X = X \cap A = A$$

كما أن المجموعة A من $P(X)$ هي المعكوس الجمعي لأن :

$$A + A = (A \cup A) \setminus (A \cap A) = A \setminus A = \phi$$

ويمكن التحقق من بقية شروط الحلقة .

(3) قدّم مثالاً على حلقة ولتكن R بها ثلاثة عناصر غير معدومة ، a,b,c بحيث يتحقق $a.b = a.c$ ولكن $b \neq c$.

الحل :

بأخذ الحلقة $(Z_{16},\oplus,\otimes)$، ولتكن العناصر هي $[4]$ و$[8]$، ولدينا: $[4]\otimes[4] = [4]\otimes[8]$ ، لكن $[4] \neq [8]$.

(4) إذا كانت S مجموعة جميع التطبيقات الحقيقية على مجموعة الأعداد الحقيقية هل $(S,+,o)$ حلقة ، حيث o هي عملية تركيب التطبيقات .

الحل :

إن $(S,+,o)$ ليست حلقة ، لأن عملية تركيب التطبيقات لا يمكن أن تتوزع على الجمع ، أي :

$$\forall f,g,h \in S : f\,o\,(g+h) \neq (f\,o\,g) + (f\,o\,h)$$

على سبيل المثال، خذ : $f(x) = 2x + 1 \, , \, g(x) = x^2 \, , \; h(x) = x - 2$

(5) لتكن $(R,+,.)$ حلقة بمحايد ، و$a \in R$ ، ولنفرض أنه يوجد عنصر وحيد $b \in R$ بحيث $a.b = 1$ ، أثبت أن $b.a = 1$.

الحل :

بما أن $a.b = 1$ ، فإن :

$$a.b.a = 1.a \;\Rightarrow a.b.a - a = (a.b - 1).a = o.a = 0$$

وبالتالي يكون :

$$a.b.a - a + a.b = a\,(b.a - 1 + b) = 1.a.b.a - a + 1 = 1$$

ومنه ، فإن : $a.(b.a - 1 + b) = 1$ ومن وحدانية العنصر b نجد أن : $a.b - 1 + b = 1$ ، وبالتالي فإن $b.a = 1$.

(6) لتكن $(R,+,\cdot)$ حلقة بمحايد و$a \in R$ ، أثبت أنه ، إذا كان $a^2 = 0$ ، فإن كلاً من $a + 1$ و$1 - a$ عنصر وحدة .

الحل :

لدينا : $(1 - a)\,(1 + a) = 1 - a + a - a^2 = 1 - a^2$

وبما أن $a^2 = 0$ ، فإن : $(1 - a)\,(1 + a) = 1 - 0 = 1$

وهذا يبيّن لنا أن كل من $(1 + a)$, $(1 - a)$ عنصر وحدة في الحلقة $(R,+,\cdot)$.

(7) لتكن $(Z_{10},\oplus,\otimes)$ حلقة الأعداد الصحيحة قياس 10 ، هل العنصران [7] و[5] عنصرا وحدة فيها ، وبيّن أن $\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$ تمثل عنصر الوحدة في حلقة المصفوفات $(M_2(R),+,\cdot)$.

الحل :

إن العنصر [7] هو عنصر وحدة فيها ، لأنه :

$$[7] \otimes [3] = [1] = [3] \otimes [7]$$

بينما نرى أن [5] ليس عنصر وحدة في هذه الحلقة .

أما بالنسبة للمصفوفة $\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$ في الحلقة $(M_2(R),+,\cdot)$ فهي تمثل عنصر الوحدة فيها ، لأن :

$$\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \cdot \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$$

(8) لتكن $(R,+,\cdot)$ حلقة تامة ، ولنرمز لمحايدها بـ 1 ، ولصفرها بـ o ،

ولنفرض أن $x^2 = x$ ، مهما يكن x من R ، بيّن أن $R = \{0,1\}$.

الحل :

ليكن a عنصراً من R ، فإن $a^2 = a$ ، وبالتـالي ، فـإن : $a^2 - a = 0$ ، أي أن $a(a-1) = 0$.

وبما أن $(R,+,\cdot)$ حلقة تامة ، فإما أن يكون $a = 0$ أو $a - 1 = 0$ ، أي أن $a = 1$، إذن $R = \{0,1\}$.

(9) لتكن الحلقة $(Z_{12},+,\cdot)$ ، حل المعادلة : $x^2 - 5x + 6 = 0$ في هذه الحلقة.

الحل :

$$x^2 - 5x + 6 = (x-2)(x-3) = 0 \Rightarrow x_1 = 2 , x_2 = 3$$

في الحلقة $(Z_{12},+,\cdot)$ ليس فقط $o.a = a.o = o$ ، بما أن :

$$3\cdot 4 = 4\cdot 3 = 2\cdot 6 = 6\cdot 2 = 3\cdot 8 = 8\cdot 3 = 4\times 9 = \ldots$$

إن العددين 11 و6 هي أيضاً حلاً للمعادلة ، وبالتالي ، فإن حلول المعادلـة فـي الحلقة المذكورة هي : $\{2,3,6,11\}$

(10) لتكن $(M_2(R),+,\cdot)$ حلقة المصفوفات الحقيقية المربعـة مـن الدرجـة الثانية. بيّن فيما إذا كانت $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ قاسمتين للصـفر فـي الحلقة المفروضة .

أعد الطلب السابق من أجل المصفوفتين $C = \begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix}, D = \begin{pmatrix} -3 & -9 \\ 2 & 6 \end{pmatrix}$.

الحل :

بما أن : $A \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, A\cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

فإن B,A قاسمتين للصفر في الحلقة المدروسة .

أما بالنسبة للمصفوفتين D,C ، فإننا نلاحظ أولاً أن $C\cdot D \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

نجد أن :

$$\begin{pmatrix} -3 & -9 \\ 2 & 6 \end{pmatrix}\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(11) في حلقة الضرب المباشر $(R\times R,+,.)$ ، بيّن فيما إذا كان كلاً من $(0,3)$ و $(1,0)$ قاسماً للصفر . وفي الحلقة $(Z_{15},\oplus,\otimes)$ بيّن فيما إذا كان $[5]$ قاسم للصفر فيها .

الحل :

بما أن $(0,0) = (1,0)\ (0,3)$ ، هذا يعني أن كلاً من $(0,3)$ و $(1,0)$ قاسم للصفر.

وفي الحلقة $(Z_{15},\oplus,\otimes)$، إن العنصر $[5]$ قاسم للصفر فيها، لأن $[0] = [6]\otimes[5]$ وهذا يعني أيضاً أن $[6]$ هو قاسم للصفر في نفس الحلقة .

(12) لتكن $(R,+,.)$ حلقة ما ، وإذا كان $e^2 = e$ ، حيث e هو العنصر المحايد فيها بالنسبة لعملية الجمع $(+)$ ، برهن أن $1-2e$ هو عنصر الوحدة .

الحل :

لدينا : $(1-2e)^2 = 1-4e+4e^2 = 1-4e+4e = 1$

(13) لتكن $(R,+,.)$ حلقة إبدالية، وإذا كان $a,b\in R$، فإنه لكل عدد صحيح موجب n ، يتحقق ما يلي :

$$(a+b)^n = a^n + \left(\sum_{i=1}^{n-1}\binom{n}{i}.a^{n-i}.b^i\right) + b^n \qquad (*)$$

حيث أن : $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$

البرهان :

من الواضح أن العلاقة $(*)$ صحيحة من أجل $n=1$.

لنفرض أن العلاقة $(*)$ صحيحة من أجل $n>1$ ، ولنبرهن على صحتها من أجل $n+1$.

لدينا :

$$(a+b)^{n+1} = (a+b)^n \, . \, (a+b)$$
$$= a^n + \left(\sum_{i=1}^{n-1} \binom{n}{i} . a^{n-i} . b^i + b^n \right)(a+b)$$
$$= a^{n+1} + b^{n+1} + a^n . b + a . b^n + \sum_{i=1}^{n} \binom{n}{i} . a^{n-i+1} . b^i + \sum_{i=1}^{n} \binom{n}{i} . a^{n-i} . b^{i+1}$$

ولكن :

$$\sum_{i=1}^{n-1} \binom{n}{i} . a^{n-i+1} . b^i = n . a^n . b + \sum_{i=1}^{n-1} \binom{n}{i} . a^{n-i+1} . b^i$$
$$\sum_{i=1}^{n-1} \binom{n}{i} . a^{n-i} . b^{i+1} = n . a . b^n + \sum_{i=1}^{n-2} \binom{n}{i} . a^{n-i} . b^{i+1}$$
$$= n . a . b^n + \sum_{i=1}^{n-1} \binom{n}{i-1} . a^{n-i+1} . b^i$$

وبذلك يكون لدينا :

$$(a+b)^{n+1} = a^{n+1} + b^{n+1} + (n+1)\, a^n . b + (n+1)\, a . b^n +$$
$$\sum_{i=2}^{n-1} \binom{n}{i} + \binom{n}{i-1} . a^{n-i+1} . b^i$$

وبملاحظة أن :

$$\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i} \ \& \ \binom{n+1}{1} = \binom{n+1}{n} = n+1$$

نجد :

$$(a+b)^{n+1} = a^{n+1} + \left(\sum_{i=1}^{n} \binom{n+1}{i} . a^{n+1-i} . b^i \right) + b^{n+1}$$

إذن العلاقة (*) صحيحة من أجل أي عدد صحيح موجب $n > 1$.

(14) لتكن $(M_2(Z_3),+,.)$ حلقة المصفوفات المربعة من الدرجة الثانية على Z_3 . حدّد مميز هذه الحلقة .

الحل :

إن $Char\ M_2(Z_3) = 3$ ، لأن العدد 3 هو أصغر عدد صحيح موجب يحقق العلاقة $3.A = 0$ ، حيث أن $A \in M_2(Z_3)$. إن $Char\ M_2(Z) = 0$ ، لأنه لا يوجد عدد صحيح موجب n يحقق العلاقة $n.A = o$ حيث أن $A \in M_2(Z)$.

(15) لتكن $H = \{(a_1,a_2,a_3,a_4) : a_i \in R\ ;\ i = 1,2,3,4\}$. ولنعرّف عمليتي الجمع والضرب على المجموعة H بالشكل :

$$(a_1,a_2,a_3,a_4) + (b_1,b_2,b_3,b_4) = (a_1+ b_1 , a_2+ b_2 , a_3+ b_3 , a_4+ b_4)$$

$$(a_1,a_2,a_3,a_4)\cdot(b_1,b_2,b_3,b_4) = \big(a_1b_1-a_2b_2- a_3b_3- a_4b_4 , a_1b_2 + a_2b_1 + a_3b_4-a_4b_3 , a_1b_3 + a_3b_1 + a_4b_2 - a_2.b_4 , a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1\big)$$

إن $(H,+,\cdot)$ حلقة بمحايد حيث $(0,0,0,0)$ هو المحايد بالنسبة لعملية الجمع ، كما أن معكوس العنصر (a_1,a_2,a_3,a_4) هو $(-a_1,-a_2,-a_3,-a_4)$. أما محايدها بالنسبة لعملية الضرب فهو $(1,0,0,0)$.

وإذا كان $(a_1,a_2,a_3,a_4) \in H$ عنصراً غير صفري ، فإن :

$$N = a_1^2 + a_2^2 + a_3^2 + a_4^2 \neq 0 \quad , \ N \in R$$

إذن $\left(\frac{a_1}{N},\frac{a_2}{N},\frac{a_3}{N},\frac{a_4}{N}\right)$ ، ومن السهل التأكد من أن :

$\left(\frac{-a_1}{N},\frac{-a_2}{N},\frac{-a_3}{N},\frac{-a_4}{N}\right)$ هو المعكوس الضربي للعنصر (a_1,a_2,a_3,a_4) من H . لذلك فإن H حلقة قاسمية . أو حقل متخالف.

ملاحظة :

الحلقة الأخيرة تسمى بحلقة الرباعيات الحقيقية (Real quaternions) أما الحرف H نسبةً إلى الرياضي الذي عرّفها وهو هاملتون .

(16) أثبت أن حلقة الرباعيات الحقيقية لا تشكل حقلاً .

الحل :

لكي تشكل حلقة الرباعيات الحقيقية حقلاً يجب أن تكون إبدالية .

إن عملية الضرب ليست إبدالية ، فعلى سبيل المثال :

$$(0,1,0,0)\,(0,0,1,0) = (0,0,0,1)$$
$$(0,0,1,0)\,(0,1,0,0) = (0,0,0,-1)$$

أي أن : $(0,0,0,1) \neq (0,0,0,-1)$

(17) أثبت أن $(Z_3(i),+,\cdot)$ حقل مؤلف من تسعة عناصر .

الحل :

بما أن : $Z_3 = \{0,1,2\}$ ، وبالتالي ، فإن :

$$Z_3(i) = \{0\,,\,1\,,\,2\,,\,i\,,\,2i\,,\,1+i\,,\,1+2i\,,\,2+i\,,\,2+2i\}$$

من أجل أي $a = r + s\,i$ من $Z_3(i)$ حيث s,r من R ، نكتب : $\overline{a} = r - s\,i$ ، وبالتالي يكون لدينا $a\,\overline{a} = r^2 + s^2 \in Z_3(i)$.

إذا كان $a \neq 0$ ، فإن $r \neq 0$ أو $s \neq 0$ وهذا يؤدي إلى أن $r^2 + s^2 \neq 0$ في $Z_3(i)$ (في الحقيقة $r^2 = 0$ أو $r^2 = 1$ من أجل r من $Z_3(i)$) . وهكذا ، كما في C $a^{-1} = (r^2 + s^2)^{-1}\,\overline{a}$ في $Z_3(i)$.

(18) لتكن $(R,+,\cdot)$ حلقة بول ، وإذا كانت الحلقة $(R,+,\cdot)$ تملك عنصران على الأقل ، فإن هذه الحلقة تملك قواسم للصفر .

الحل :

من الفرض يوجد $a,b \in R$ حيث $a \neq 0\,,\, b \neq 0\,,\, a \neq b$.

لكن : $a^2\,b - a\,b^2 = a\,b - a\,b = 0$

$$\Rightarrow\; a\,(a-b)\,b = 0$$

فإذا كان $(a-b)\,b \neq 0$ ، فإن a قاسم للصفر في الحلقة $(R,+,\cdot)$ ، وإذا كان $(a-b)\,b = 0$ ، فإن b قاسم للصفر ، لأن $a \neq b$ فرضاً أي أن $a - b \neq 0$. وبذلك يتم المطلوب .

(19) ليكن $(F,T,\star)$ حقلاً ما ، ولنرمز لعنصر الوحدة فيه بالرمز 1 ،

ولصفره بالرمز o ، ولتكن :

$$M = \{x \in F : x = n.e \; ; n \in Z\}$$

وليكن للحقل $(F,T,\star)$ مميز $P \neq 0$. أثبت أنه إذا كان $y \neq 0$ عنصراً ما من M، فإن لـ y معكوساً في M بالنسبة للعملية $\star$.

الحل :

إذا كان $y \neq 0$ عنصراً من M، فإنه يمكن كتابته بالشكل : $y = m.e ; m \in Z \setminus \{0\}$

إن m لا يقبل القسمة على P في Z ، لأنه ، إذا قبل m القسمة على P في Z ، فإن $y = 0$ ، وهذا مخالف لكون $y \neq 0$.

بما أن m لا يقبل القسمة على P في Z ، وبما أن P أولي ، فإن : $(m,P) = 1$ ، وبالتالي ، يمكن إيجاد عددين صحيحين r,q بحيث يكون : $1 = q.m + r.P$ ، ومنه :

$$e = (q.m + r.P)\, e = (q.m)\, e = (q.e)\star(m.e) = (q.e)\star y$$

وأيضاً :

$$e = (m.q + r.P)\, e = (m.q).e = (m.e)\star(q.e) = y\star(q.e)$$

إذاً : $(q.e)\star y = y\star(q.e) = e$

وبملاحظة أن $q.e \in M$ ، يبيّن لنا أن لـ y مقلوباً في M بالنسبة للعملية $\star$.

(20) أثبت وجود حلقة تحوي عنصراً واحداً فقط ، وهل هذه الحلقة إبدالية ، وهل تحوي على عنصر محايد ، وهل هي حلقة تامة . ثم برهن أنه إذا حوت حلقة أكثر من عنصر واحد ، فلا يمكن أن يكون لعمليتي الجمع والضرب المعرّفتين عليها العنصر المحايد نفسه .

الحل :

إذا حوت الحلقة عنصراً واحداً فقط ، فيلزم أن يكون هذا العنصر هو العنصر المحايد O بالنسبة لعملية الجمع، لأن الحلقة زمرة إبدالية بالنسبة لعملية الجمع (+)، وكل زمرة يجب أن تكون غير خالية لأنها تحوي العنصر المحايد على الأقل.

إن $(\{0\},+,\cdot)$ هي حلقة ، حيث نعرّف عمليتي الجمع (+) والضرب (.) بالشكل :

$O+O=O\ ,\ O\cdot O=O$ ، لأن :

إن عملية الجمع عملية مغلقة وإبدالية ، كما أنها تجميعية ، لأن :

$$(O+O)+O=O+(O+O)=O$$

إن العنصر O هو المحايد بالنسبة لعملية الجمع (+) ، وأن معكوس العنصر الوحيد O هو العنصر O نفسه، وبالتالي فإن $(\{0\},+)$ زمرة إبدالية بالنسبة لعملية الجمع.

أما بالنسبة لعملية الضرب (.) ، فمن الواضح أنها تجميعية لأن :

$$O\cdot(O\cdot O)=O\cdot(O\cdot O)=O$$

كما أنها توزيعية على الجمع ، لأن :

$$O\cdot(O+O)=O\cdot O+O\cdot O=O+O=O$$

$$(O+O)\cdot O=O\cdot O+O\cdot O=O+O=O$$

إذن $(\{0\},+,\cdot)$ حلقة ، بالإضافة إلى ذلك ، إنها حلقة إبدالية ، كما أنهـا بمحايـد (بالنسبة لعملية الضرب) ، ومحايدها الذي يرمز له بـ 1 هو O ، أي في هـذه الحالة $O = 1$. كما أن هذه الحلقة تامة لأن O هو دوماً حاصل ضرب عنصرين كل منهما يساوي O .

لنبرهن الآن ، أنه إذا حوت حلقة أكثر من عنصر واحد ، فـلا يمكـن أن يكـون لعمليتي الجمع والضرب العنصر المحايد نفسه .

لنفرض أن الحلقة تحوي بالإضافة إلى العنصر O عنصراً آخراً وهو a ، حيـث $a \neq 0$ ، ولنبرهن أن المحايد بالنسبة لعملية الضرب لا يمكن أن يساوي العنصـر المحايد بالنسبة للجمع O.

بما أن $1.a = a$ ، فإذا فرضنا أن $O = 1$ ، لوجـدنا أن $O.a = 0$ ، ولمـا كـان $O.a = O$ فإنه ينتج من المساواة $O.a = O$ ، والمســاواة $O = a$ ، وهــذا غيـر صحيح لأننا فرضنا $a \neq O$ ، إذاً فرضنا $O = 1$ خاطئ ، أي أن $O \neq 1$.

(21) لتكن $(R,+,\cdot)$ حلقة بول (أي أنها حلقة ويتحقق فيها $x^2 = x$ ، مهما يكن

($x \in R$) ، والمطلوب :

تحقق من أن : $x + x = O$ و $x\,y\,(x + y) = 0$ لكل x,y من R .

الحل :

لدينا من أجل x من R : $(x + x)^2 = x + x$ ، ومنه يكون :

$$(x + x)\,(x + x) = x + x$$

بما أن الضرب توزيعي على الجمع ، لذلك :

$$(x + x)\,.x + (x + x)\,.x = x + x$$
$$x^2 + x^2 + x^2 + x^2 = x + x$$

(لأن الضرب توزيعي على الجمع أيضاً) .

بما أن العملية (+) تجميعية ، لذا :

$$(x + x) + (x + x) = x + x \;\Rightarrow\; x + x = 0$$

من المساواة الأخيرة ، يمكن كتابة ، أي كان y,x من R ، فإن :

$$x.y + x.y = 0$$

وبما أن $x^2 = x$ لكل x من R ، نجد :

$$(x\,x)\,y + x\,(y\,y) = 0$$

وبما أن $(R,+,\cdot)$ إبدالية ، والضرب تجميعي في R فيكون :

$$(x\,y)\,x + (x\,y)\,y = 0$$
$$x\,y\,(x + y) = 0$$

لأن الضرب توزيعي على الجمع في R .

(22) ليكن $n \in Z^+$ ، برهن أن جميع العبارات التالية متكافئة :

(1) n عدد أولي، (2) $(Z/<n>,+,\cdot)$ حلقة تامة، (3) $(Z/<n>,+,\cdot)$ حقل.

الحل :

(1) ⇐ (2)

ليكن : $a + < n > \;\;,\;\; b + < n > \in Z/ < n >$

لكل b,a من Z بحيث يكون :

$$(a + < n >)\,(b + < n >) = < n >$$

أي أن :

$a \cdot b + <n> = <n>$

وهذا يعني أن $a \cdot b \in <n>$ ، وبالتالي يوجد عنصر وليكن r من Z بحيث يكون : $a.b = r.n$ ، أي أن $n/a.b$ ، وبما أن n عدد أولي فإن n/a أو n/b . وهذا يعني أن $a \in <n>$ أو $b \in <n>$ ، وبالتالي فإن :

$a + <n> = <n>$ أو أن $b + <n> = <n>$ ، لذا فإن $Z/<n>$ لا تحوي قواسم للصفر وبالتالي فإن $(Z/<n>,+,\cdot)$ حلقة تامة .

$(2) \Rightarrow (3)$

بما أن $(Z/<n>,+,\cdot)$ حلقة تامة منتهية ، فحسب المبرهنة (كل حلقة تامة منتهية تشكل حقلاً) نجد أن $(Z/<n>,+,\cdot)$ حقل .

$(3) \Rightarrow (1)$

لنفرض أن $(Z/<n>,+,\cdot)$ حقل ، ولنفرض العكس ، أي لنفرض أن n عدداً ليس أولياً ، وبالتالي يكون $n = a.b$ حيث $1 < a , b < n$.

الآن ، كل من $a + <n>$ و $b + <n>$ عنصر غير صفري من $(Z/<n>,+,\cdot)$، كما أن :

$$(a + <n>)(b + <n>) = a.b + <n> = n + <n> = <n>$$

وهذا يناقض كون أن الحقل $(Z/<n>,+,\cdot)$ لا يحوي قواسم للصفر . إذن n عدد أولي .

<u>(23)</u> في حلقة المصفوفات $(M_2(R),+,\cdot)$ ، أثبت أن $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ و $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ متساويا القوى .

الحل :

نلاحظ بسهولة أن :

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \text{ و } \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

وهذا يبيّن لنا أن المصفوفتين $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ و $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ متساويتا القوى .

2- تمرينات غير محلولة للفصل الأول

1- ليكن لدينا النظام $(Q,\oplus,\odot)$ حيث أن :

$$a\odot b = a.b + a + b \quad \text{و} \quad a \oplus b = a + b + 1 \;;\; \forall a,b\in Q$$

بيّن فيما إذا كان هذا النظام يشكل حلقة إبدالية بمحايد .

الجواب : يشكل $(Q,\oplus,\odot)$ حلقة إبدالية بمحايد .

2- أثبت أن النظام $(Z,\oplus,o)$ حيث أن :

$$a \,o\, b = a + b - a.b \quad \text{و} \quad a \oplus b = a + b - 1 \;;\; \forall a,b\in Z$$

يشكل حلقة تامة .

3- برهن أن النظام $(R,\star,T)$ ، حيث أن :

$$r\star s = 2\,(r + s) \quad , \quad r\,T\,s = r.s \;;\; r,s\in R$$

لا يشكل حلقة .

4- برهن أن النظام $(R^*,\star,o)$ ، حيث أن :

$$r\star s = 2r.s \quad , \quad r\,o\,s = r.s \;;\; r,s\in R^*$$

يشكل حلقة .

5- ليكن النظام $(R^+,\star,\perp)$ ، حيث أن :

$$r\star s = r.s \;,\; r\perp s = r^S \;;\; r,s\in R^+$$

أثبت أن هذا النظام يشكل حلقة .

6- ليكن كل من S,R حلقتين إبداليتين بمحايد ، بالنسبة للعمليتين $(+)$ و$(\cdot)$ العاديتين ، أثبت أن $R\times S$ هي حلقة إبدالية بمحايد حيث أن :

$$(a,b) + (c,d) = (a+c\,,\,b+d)$$

$$(a,b)\cdot(c,d) = (a\cdot c\,,\,b\cdot d) \;;\; \forall (a,b)\,,\,(c,d)\in R\times S$$

تسمى عادةً هذه الحلقة بحلقة الضرب المباشر Direct product للحلقتين S,R .

7- أثبت أن حلقة الأعداد المركبة $(C,+,\cdot)$ هي حلقة تامة حيث :

$$C = \{a + ib \ ; \ a,b \in R \, , i = \sqrt{-1}\}$$

بالنسبة للعمليتين $(+)$ و$(\cdot)$ العاديتين .

8- لتكن $(R,+)$ زمرة إبدالية ، هل يكون النظام $(R,+,\cdot)$ حلقة ، حيث $(\cdot)$ عملية معرفة على R بالشكل : $a.b = a$ لكل b,a من R .

9- أثبت أن العنصر $2+\sqrt{3}$ يمثل عنصر وحدة في الحلقة $(Z[\sqrt{3}],+,\cdot)$ ، ثم أوجد عنصر وحدة آخر في هذه الحلقة حيث :

$$Z[\sqrt{3}] = \{a + b\sqrt{3} \ ; \ a,b \in Z\}$$

10- أوجد قواسم الصفر (إن وُجِدَتْ) في الحلقات التالية :

$$(Z_4,+,\cdot) \, , (Z_6,+,\cdot) \, , (Z,+,\cdot)$$

11- لتكن $(R,+,\cdot)$ حلقة ، عنصرها المحايد هو e ، وإذا كان $e^2 = e$ (عنصر متساوي القوى في الحلقة R) ، وإذا كان :

$$e R e = \{e a e \ ; \ a \in R\}$$

أثبت :

(1) $(eRe,+,\cdot)$ حلقة بمحايد ويكون :

$$e R e = \{a \in R \ : \ e a = a = a e\}$$

(2) إذا كانت $S \subseteq R$ ، فإن S تشكل حلقة جزئية من R بالنسبة للعمليات نفسها المعرفة على R ، إذا ، وفقط إذا كانت S حلقة جزئية من $(eRe,+,\cdot)$ ، حيث $e^2 = e$.

12- إذا كانت $(R,+,\cdot)$ حلقة ما ، أثبت أن مجموعة العناصر المعكوسة في R (نرمز لها بـ $U(R)$) تشكل زمرة بالنسبة لعملية الضرب $(\cdot)$.

13- لتكن $Q[\sqrt{2}] = \{r + s\sqrt{2} : r,s \in Q\}$ ، أثبت أن $(Q[\sqrt{2}],+,\cdot)$ حقل .

-14 لتكن $(R,+,.)$ حلقة ، أثبت أن الشروط التالية متكافئة :

(1) إذا كان $a.b = 0$ في R ، عندها إما $a = 0$ أو $b = 0$.

(2) إذا كان $ab = ac$ في R و $a \neq 0$ ، عندئذٍ $b = c$.

-15 لتكن $(P(X),+,.)$ حلقة إبدالية بمحايد (ϕ هو المحايد بالنسبة لعملية الجمع و X لمحايد بالنسبة لعملية الضرب) ، حيث :

$$A + B = A \Delta B \ , \ A \bullet B = A \cap B \ , \ A,B \subseteq X$$

أثبت أن الحلقة $(P(X),+,.)$ هي حلقة بول .

-16 أثبت أن مميز الحلقة البولية يساوي 2 .

-17 أثبت أن العلاقة $(x+y)\,(x-y) = x^2 - y^2$ لا تصح في الحلقة $(R,+,.)$.
إلاّ إذا كانت هذه الحلقة إبدالية ، لكل y,x من R .

-18 لتكن $(R,+,.)$ حلقة ما (غير إبدالية) ، ولنعرّف عليها العملية $\perp$ بالشكل :

$$x \perp y = x.y - y.x \ ; \ \forall x,y \in R$$

المطلوب :

(1) احسب $x \perp y$ و $y \perp x$ ، وماذا تستنتج .

(2) بيّن فيما إذا كانت العملية $\perp$ توزيعية بالنسبة لعملية الجمع (+) .

(3) برهن أن من أجل كل z,y,x من R ، فإن :

(أ) $x \perp (y \perp z) + y \perp (z \perp x) + z \perp (x \perp y) = 0$

(ب) $y \perp (x \perp z) = x \perp (y \perp z) - (x \perp y) \perp z$

-19 لتكن $(R,+,.)$ حلقة ما ، وبفرض أن العنصر x معدوم القوى في الحلقة المدروسة ، (أي يوجد عدد صحيح $n > 0$ بحيث يكون $x^n = 0$) . وإذا كان y,x عنصرين قابلين للمبادلة في الحلقة $(R,+,.)$ وأنّ كلاً منهما معدوم القوة ، أثبت أن $x + y$ و $x.y$ معدوم القوة أيضاً .

-20 لتكن Δ,∇ عمليتين معرفتين على مجموعة الأعداد الصحيحة Z بالشكل :

$$a \,\Delta\, b = a + b - 1 \ , \ a \,\nabla\, b = a + b - a.b$$

لكل b,a من Z ، المطلوب :

هل تشكل هذه الحلقة حقلاً .

21- لتكن $(R,+,\cdot)$ حلقة تامة بمحايد ، وليكن a,b من R . أثبت أنه إذا كان $a^2 = 1$ ، فإن $a = 1$ أو $a = -1$.

22- ليكن $(F,T,\star)$ حقلاً ما ، ولنرمز لعنصر الوحدة فيه بالرمز e ، ولصفره بالرمز O ، ولتكن :

$$M = \{x \in F \ : \ x = n.e \, ; n \in Z\}$$

وليكن للحقل $(F,T,\star)$ مميز $P \neq 0$. بيّن أن M تتألف فقط ، من العناصر المختلفة فيما بينها مثنى مثنى، التالية :

$$O , e , \dots , (P-1)\, e$$

23- إذا كان $(F,+,\cdot)$ حقلاً ما ، مستفيداً من خواص عملية الضرب وتعريف العملية المعاكسة له ، أثبت أنه إذا كان $a,b,c,d \in F$ حيث $b \neq 0 , d \neq 0$ ، فإن :

$$a/b = c/d \ \Leftrightarrow \ a.b^{-1} = c.d^{-1}$$

24- أثبت أن كل عنصر في حلقة $(R,+,\cdot)$ المنتهية وبمحايد ، إما أن يكون عنصر الوحدة ، أو أن يكون قاسم للصفر .

25- لتكن $(M_2(R),+,\cdot)$ حلقة المصفوفات المربعة الحقيقية من الدرجة الثانية.

بيّن فيما إذا كان العنصران $A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} , B = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$ متلاشيان في الحلقة $(M_2(R),+,\cdot)$. ثم أثبت أن العنصر $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ في الحلقة $(M_2(Z_2),+,\cdot)$ متلاشي .

26- لتكن $(R,+,\cdot)$ حلقة ، ونفرض أن a عنصراً متلاشياً فيها ، أثبت أن (1-a) عنصر وحدة فيها .

27- ليكن a عنصراً متساوي القوى في الحلقة $(R,+,\cdot)$ ، أثبت أن 1-a متساوي القوى أيضاً .

تمارين محلولة وغير محلولة للفصل الثاني:

الحلقات والحقول الجزئية والمثاليات

Subring and subfields & Ideals

3- تمرينات محلولة للفصل الثاني

– الحلقات والحقول الجزئية والمثاليات –

1- لتكن الحلقة $(M_2(Z),+,.)$ حيث $M_2(Z)=\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ ، ولتكن المجموعتان:

$$S=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} ;\ a,b\in Z\right\} ,\ T=\left\{\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} ;\ b,c\in Z\right\}$$

برهن أن كلاً من $(S,+,.)$ و$(T,+,.)$ حلقة جزئية من الحلقة $(M_2(Z),+,.)$.

الحل :

نلاحظ أولاً أن $S\neq\phi$، لأن $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in S$ ، ومن ناحية ثانية إن $S\subseteq M_2(Z)$.

إذن $\phi\neq S\subseteq M_2(Z)$.

لكل $A=\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} , B=\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}$ من S ، فإن :

$$A-B=\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}-\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_1-a_2 & b_1-b_2 \\ 0 & 0 \end{pmatrix}\in S$$

$$A\cdot B=\begin{pmatrix} a_1 & b_1 \\ 0 & c \end{pmatrix}\cdot\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_1a_2 & b_1b_2 \\ 0 & 0 \end{pmatrix}\in S$$

إذن $(S,+,.)$ حلقة جزئية من الحلقة $(M_2(Z),+,.)$.

بالطريقة نفسها نبرهن أن $(T,+,.)$ حلقة جزئية من الحلقة $(M_2(Z),+,.)$.

2- إذا كانت $(S,+,.)$ حلقة جزئية بمحايد من الحلقة $(R,+,.)$. من الممكن أن لا يكون للحلقة $(R,+,.)$ محايداً ، هاتِ مثالاً يوضح هذه المقولة .

الحل :

لنأخذ الحلقة التالية :

$$(R,+,.) = \left(\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} ; a,b \in Z\right\},+,.\right)$$

والحلقة الجزئية بمحايد منها التالية :

$$(S,+,.) = \left(\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} ; a \in Z\right\},+,.\right)$$

إن الحلقة $(R,+,.)$ ليست بمحايد ، بينما الحلقة الجزئية $(S,+,.)$ من الحلقة $(R,+,.)$ تملك محايد (بالنسبة لعملية الضرب) وهو $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

-3 لتكن $(R_1,+,.)$ و $(R_2,+,\star)$ حلقتين بمحايدين ما ، ولنرمز لمحايد الحلقة $(R_2,+,\star)$ بالرمز o' ، ولنفرض أن :

$$S = \{(a,b) : a \in R_1 , b \in R_2\}$$

$$S_1 = \{(a,o') : a \in R_1\}$$

ولتكن Δ و Δ' عمليتين جبريتين ثنائيتين معرفتين على S بالشكل :

$$(x,y)\ \Delta\ (x_1,y_1) = (x + x_1\ ,\ y\ T\ y_1)$$

$$(x,y)\ \Delta'\ (x_1,y_1) = (x.x_1\ ,\ y \star y_1)$$

وذلك من أجل أي (x,y) و (x_1,y_1) من S . إن (S,Δ,Δ') حلقة بمحايد . والمطلوب أثبت أن (S_1,Δ,Δ') حلقة جزئية من الحلقة (S,Δ,Δ') .

الحل :

(1) من الواضح أن $\phi \neq S_1 \subseteq S$.

(2) إذا كان a_1 و a_2 عنصرين ما من الحلقة $(R,+,.)$ ، فإن :

$$(a_1,o')\ \Delta'\ (a_2,o') = (a_1.a_2\ ,\ o' \star o')$$
$$= (a_1.a_2\ ,\ o') \in S_1$$

$$(a_1,o')\ \Delta\ \big(-(a_2,o')\big) = (a_1,o')\ \Delta\ (-a_2, -o')$$
$$= (a_1,o')\ \Delta\ (-a_2,o')$$

$$= (a_1\text{-}a_2\ ,\ o'To')$$
$$= (a_1\text{-}a_2\ ,\ o')\in S_1$$

من (1) و(2) نستنتج أن (S_1,Δ,Δ') هي حلقة جزئية من الحلقة (S,Δ,Δ') .

لنثبت الآن أن $(1,o')$ هو المحايد في الحلقة الجزئية (S_1,Δ,Δ') . لنرمز بـــ 1 للمحايد في الحلقة $(R,+,\cdot)$ ، عندئذٍ يكون $(1,o')$ عنصراً ينتمي إلى S_1 ، ومن ناحية ثانية يكون :

$$(a,o')\ \Delta'\ (1,o') = (a.1\ ,\ o'\star o') = (a,o')$$
$$= (1.a\ ,\ o'\star o') = (1.o'\ ,\ o'\star o')$$
$$= (1,o')\ \Delta'\ (a,o')\quad \forall a\in R$$

إذن $(1,o')$ هو المحايد في الحلقة الجزئية (S,Δ,Δ') .

<u>4-</u> لتكن $(R,+,\cdot)$ حلقة بمحايد ، ولنرمز لمحايدها بـــ 1 ، ولتكن I مثالية فـــي الحلقة $(R,+,\cdot)$، وإذا وجد في I عنصر b له معكوس في R ، بالنسبة للعملية $(\cdot)$، فإن $I = R$.

الحل :

ليكن a عنصراً ما من R ، فإن :

$$a = a\cdot 1 = a\,(b^{-1}\cdot b) = (a\cdot b^{-1})\cdot b\in I$$

<u>5-</u> لتكن الحلقة الابتدائية $(Z\times Z,+,\cdot)$. أثبت أن المجموعة التالية :
$I = \{(a,2b)\ ;\ a,b\in Z\}$ مثالية من الحلقة المعطاة .

الحل :

إن $Z\times Z \supseteq I \neq \phi$ ، لأن $(o,o)\in I$ ، أي أن $I\neq\phi$.

ليكن $(a,2b)$ و$(c,2d)$ عنصرين ما من I ، وإذا كان $(x,y)\in Z\times Z$ ، فإن :

$$(a,2b) - (c,2d) = \big(a\text{-}c\ ,\ 2(b\text{-}d)\big)\in I$$
$$(x,y)\cdot(a,2b) = (x\cdot a\ ,\ 2yb)\in I$$

نستنتج مما سبق أن I هي مثالية من الحلقة $(Z\times Z,+,\cdot)$.

6- إذا كانت $(R,+,\cdot)$ حلقة إبدالية ، وإذا كان $a\in R$ ، أثبت أن المجموعة

$$<a> = \{ r\cdot a + n\cdot a \ : r\in R , n\in Z \}$$

مثالية من الحلقة $(R,+,\cdot)$.

الحل :

نلاحظ أولاً أن $a = 0\cdot a + 1\cdot a \in <a>$ ، أي أن $<a> \neq \phi$.

ليكن $r_1a + n_1a , r_2a + n_2a \in I$ حيث أن $r_1,r_2\in R , n_1,n_2\in Z$.

وإذا كان $s\in R$ فإن :

$$(r_1a + n_1a) - (r_2a + n_2a) = (r_1 - r_2).a + (n_1 - n_2).a \in <a>$$

$$s .(r_1a + n_1a) = (s r_1 + s n_1) .a + 0.a \in <a>$$

نستنتج مما سبق أن $<a>$ مثالية من الحلقة $(R,+,\cdot)$.

7- لتكن $(Z\times Z,+,\cdot)$ حلقة ، أثبت أن المجموعة $I = \{(k,k) : k\in Z\}$ ليست مثالية في الحلقة المذكورة .

الحل :

نلاحظ أن $\phi \neq I \subseteq Z\times Z$. لكن الشرط التالي غير محقق : $a\in Z\times Z , \forall x\in I$: فإن $a.x \notin I$ ، فعلى سبيل المثال نأخذ :

$$(2,5)\,(k,k) = (2k,5k) \notin I$$

8- إذا كان كل من $(F,+,\cdot)$ و $(K,+,\cdot)$ حقلاً ، أوجد جميع مثاليات $F\times K$.

الحل :

إن مثاليات $F\times K$ هي $\{o\}\times\{o\}$ ، $F\times\{o\}$ ، $\{o\}\times K$ و $F\times K$.

9- لتكن $(R,+,\cdot)$ حلقة لا تحوي قواسم للصفر وبحيث تكون أي حلقة جزئية من R هي مثالية منها ، أثبت أن $(R,+,\cdot)$ حلقة إبدالية .

الحل :

لنفرض أن $0 \neq a\in R$ ، وبما أن مركز حلقة $C(a)$ هي حلقة جزئية من R حيث:

$$C(a) = \{x \in R : x.a = a.x\}$$

فهي مثالية من الحلقة $(R,+,.)$ ، ولذلك $r.a \in C(a)$ لكل $r \in R$.

بما أن $r.a \in C(a)$ ، فإن $ar.a = ra^2$ ، وبالتالي فإن : $(a.r - r.a).a = 0$ وهذا يؤدي إلى أن $a.r - r.a = 0$ ومنه يكون : $ar = ra$ ، إذن الحلقة $(R,+,.)$ إبدالية.

10- لتكن $\{I_i\}_{i \in I}$ أسرة غير خالية من المثاليات في الحلقة $(R,+,.)$ ، أثبت أن $\bigcap\limits_{i \in I} I_i$ مثالية في الحلقة $(R,+,.)$.

الحل :

نلاحظ ، أولاً أن $\phi \neq \bigcap I_i \subseteq R$. إذا كان y,x عنصرين ما من $\bigcap\limits_{i \in I} I_i$ ، وبالتالي فإن : $\forall i \in I \;\; x,y \in I_i$ ومنه يكون : $\forall i \in I \;\; x-y \in I_i$ ، إذن $x - y \in \bigcap\limits_{i \in I} I_i$.

ليكن الآن y عنصراً ما من $\bigcap\limits_{i \in I} I_i$ و a من R ، أي أن : $y \in \bigcap\limits_{i \in I} I_i$ أي أنه لكل $i \in I$ و $y \in I_i$ وبالتالي : $\forall i \in I \;\; a.y , y.a \in I_i$.

وبالتالي فإن : $a.y , y.a \in \bigcap\limits_{i \in I} I_i$.

نستنتج مما سبق أن : $\bigcap\limits_{i \in I} I_i$ مثالية في الحلقة $(R,+,.)$.

11- إذا كانت $(R,+,.)$ حلقة إبدالية بمحايد ، وإذا كانت I مثالية في الحلقة $(R,+,.)$. أثبت أن $I = I : R$.

الحل :

من مبرهنة قسمة المثاليات نجد أولاً أن : $I \subseteq I{:}R$ لنبرهن الآن أن $I{:}R \subseteq I$ ، ليكن x عنصراً ما من $I{:}R$ ، وبالتالي فإن : $x.R \subseteq I$ ، ومن ثم فإن $x.1 \in I$ حيث 1 هو عنصر الوحدة في الحلقة $(R,+,.)$ ، أي أن $x \in I$. إذن $I = I{:}R$

12- إذا كان n عدداً صحيحاً ، ولتكن I مجموعة كل مضاعفات للعدد n في حلقة الأعداد الصحيحة Z أي أن : $I = \{n.r : r \in Z\}$ أثبت أن I مثالية في الحلقة $(Z,+,.)$.

الحل :

نلاحظ أولاً أن $\phi \neq I \subseteq Z$.

كما أنه ، إذا كان y,x عنصرين ما من I ، فإن $x = n.a\ ,\ y = n.b$ حيث $a,b \in Z$ ، وبالتالي فإن :

$$x - y = n.a - n.b = n\,(a - b) \in I$$

كما أن :

$$b\,(n.a) = n.(b.a)\ \ ;\ \ a,b \in Z$$

إذن $I = n.Z$ تشكل مثالية في الحلقة $(Z,+,\cdot)$.

13- لتكن $R = (M_2(Z),+,\cdot)$ حلقة المصفوفات المربعة من الدرجة الثانية ، أثبت أن $I = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ; a,b \in Z\right\}$ مثالية يمينية .

الحل :

إن $\in I$ $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ وهذا يعني أن $I \neq \phi$.

ليكن
$$A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in I$$

وبالتالي فإن :

$$A - B = \begin{pmatrix} a - c & b - d \\ 0 & 0 \end{pmatrix} \in I$$

كذلك إذا كان $C = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ من الحلقة R ، فإن :

$$A \cdot C = \begin{pmatrix} ax + bz & ay + bt \\ 0 & 0 \end{pmatrix} \in I$$

نستنتج مما سبق أن I هي مثالية يمينية في الحلقة R .

14- أثبت أن لكل حقل $(F,+,\cdot)$ مثاليتان فقط هما $\{o\}$ و F نفسه .

الحل :

إن $\{o\}$ مثالية للحقل لأن : $\quad o \cdot a = a \cdot o = o \;;\; \forall a \in F$

لنفرض الآن أن المثالية I لا تساوي $\{o\}$ ، وهذا يعني أنه يوجد عنصر $a \neq o$ في I ، ويوجد معكوسه a^{-1} في F ، وبالتالي حسب تعريف المثالية سيكون :

$$a^{-1} \cdot a = a \cdot a^{-1} = e \in I$$

وهذا سيؤدي إلى أنه مهما كان العنصر x من F ، فإن :

$$e \cdot x = x \cdot e = x \in I$$

وهذا يبرهن أن $F = I$.

15- لتكن $(Z,+,\cdot)$ حلقة الأعداد الصحيحة ، إن 4Z هي مثالية من الحلقة $(Z,+,\cdot)$. اكتب عناصر المجموعة $Z/4Z$.

الحل :

$$Z/4Z = \{0 + 4Z \,,\, 1 + 4Z \,,\, 2 + 4Z \,,\, 3 + 4Z\}$$

ويمكن التحقق من أن $(Z/4Z,+,\cdot)$ حلقة إبدالية بمحايد، وذلك بالاستفادة من مبرهنة حلقة القسمة .

16- قدّم مثالاً لحلقة تامة ولتكن $(R,+,\cdot)$ ومثالية ، لتكن I من R بحيث يكون R/I حقلاً .

الحل :

بأخذ الحلقة $(R,+,\cdot)$ حلقة الأعداد الصحيحة $(Z,+,\cdot)$ وبأخذ المثالية I بالشكل $I = 2Z$ ، نجد أن $(Z/2Z,+,\cdot)$ تشكل حقلاً .

17- لتكن $(R,+,\cdot)$ حلقة ما ، ولتكن I مثالية فيها ، عندها المثاليات اليسارية (اليمينية) في حلقة القسمة $(R/I,+,\cdot)$ هي من الشكل $\overline{J} = J/I$ حيث J مثالية يسارية (يمينية) في الحلقة $(R,+,\cdot)$ ، وأن $I \subseteq J$.

الحل :

ليكن $\overline{J}$ مثالية يسارية في الحلقة $(R/I,+,\cdot)$. ولنبرهن أن $\overline{J} = J/I$ حيث أن J هي مثالية يسارية في $(R,+,\cdot)$ وتحوي I . لنأخذ المجموعة :

$$J = \{x : x\in R \,;\, x + I\in \overline{J}\,\}$$

ولنثبت أن J هي مثالية في الحلقة $(R,+,\cdot)$.

بما أن $\overline{J}$ مثالية يسارية في $(R/I,+,\cdot)$ ، فإن $\overline{o} = o + I$ وهذا يعنـــي أن $o\in J$ ، أي أن $J \neq \phi$.

ليكن y,x عنصرين من J ، عندئذٍ :

$$\overline{x} = x + I\,,\;\; \overline{y} = y + I$$

ومنه يكون لدينا :

$$(x - y) + I = (x + I) + (-y + I) = \overline{x} - \overline{y} \in \overline{J}$$

إذن $\overline{x} - \overline{y} \in J$.

كذلك ، أياً كان $a\in R$ ، فإن $\overline{a} = a + I\in R/I$ ، وبالتالي يكون :

$$a\cdot x + I = (a + I)\cdot(x + I) = \overline{a}\cdot\overline{x} \in \overline{J}$$

نستنتج مما سبق أن المجموعة J تشكل مثالية يسارية في الحلقة $(R,+,\cdot)$. كما أن أياً كان $a\in I$، فإن $a + I = \overline{o} \in \overline{J}$ أي أن $a\in J$ ، وبالتالي نجد $I \subseteq J$.

لنبرهن أخيراً أن $\overline{J} = J/I$.

ليكن $\overline{Z} = Z+I \in J/I$ ، عندئذٍ $Z\in J$ ومنه $Z + I \in \overline{Z}$ ، أي أن $J/I\subseteq \overline{J}$.

ومن ناحية ثانية، أياً كان $\overline{Z} \in \overline{J} \subseteq R/I$ أي أن : $\overline{Z} = Z+I$ ، فإن $Z\in R$ ، وبالتالي نجد أن : $\overline{Z} = Z+I \in J/I$ أي أن $\overline{J} \subseteq J/I$.

مما سبق نجد أن $\overline{J} = J/I$.

4- تمرينات غير محلولة للفصل الثاني

1- إذا كانت K,J,I ثلاثة مثاليات للحلقة $(R,+,\cdot)$ ، بحيث $J \subseteq I$ ، أثبت أن :

$$I \cap (J+K) = J + (I \cap K)$$

2- لتكن المجموعة التالية : $M = \{m,n,p,q\}$. لنزوّد M بالعمليتين المعرّفتين بالجدولين التاليين :

$\bullet$	M	n	p	q
m	M	m	m	m
n	M	n	m	n
p	M	p	m	p
q	m	q	m	q

+	m	n	p	q
m	m	n	p	q
n	n	m	q	p
p	p	q	m	n
q	q	p	n	m

المطلوب : أثبت أن $(M,+,\cdot)$ حلقة غير إبدالية . أوجد صفر هذه الحلقة ، وإذا كانت $I = \{m,p\}$ ، برهن أن I مثالية في الحلقة $(M,+,\cdot)$.

3- أثبت أن المجموعة $M = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ; a,b \in R \right\}$ حلقة جزئية من حلقة المصفوفات الحقيقية من الدرجة الثانية بالنسبة لعملية الجمع والضرب للمصفوفات، ثم برهن أن M تشكل مثالية يسارية لكنها ليست مثالية يمينية في الحلقة المفروضة.

4- لتكن $(R,+,\cdot)$ حلقة ما، L حلقة جزئية في R ، وإذا كانت I مثالية في الحلقة R ، أثبت أن المجموعة المعرفة بالشكل :

$$L + I = \{x + y \ , x \in L \ و \ y \in I\}$$

حلقة جزئية في الحلقة R تحوي I ، وإن $J \cap I$ مثالية في L .

5- لتكن $(R,+,\cdot)$ حلقة واحدية، وإذا كان $J + J_i = R$ ، حيث $i = 1,2,\ldots,n$، وذلك من أجل المثاليات J_i , J للحلقة R ، أثبت :

$$J + \bigcap_{i=1}^{n} J_i = R = J + \prod_{i=1}^{n} J_i$$

6- نفرض أن $m = -14$, $n = 59$. احسب ناتج قسمة n على m ، واحسب الباقي أيضاً ، ثم أوجد r , q اللذين يحققان العلاقة :

$$n = m.q + r \ ; \ 0 \le r \le |m|$$

أعد حل المسألة من أجل العددين $m = 11$, $n = -79$.

7- لتكن $(Z_{10},\oplus,\otimes)$ حلقة الأعداد الصحيحة بمقاس 10 ، أوجد $3^{-1},-8,-3$ في Z_{10} ، ثم أوجد جذور كثيرة الحدود $f(x) = 2x^2 + 4x + 4$ في الحلقة Z_{10} .

8- لتكن $(Z,+,\cdot)$ حلقة الأعداد الصحيحة وIm متكونة من مضاعفات العدد 2 حيث $m \ge 2$، أثبت أن Im مثالية في Z .

9- لتكن S مجموعة الأعداد الحقيقية التي من الشكل $a + \sqrt{3}\,b$ ، حيث b,a من Q ، بيِّن أن S حقل بالنسبة للعمليتين (+) و(·) .

10- لتكن $(R,+,\cdot)$ حلقة الأعداد الحقيقية ، أثبت أن مجموعة الأعداد الحقيقية التالية :

$$M = \{m + n\sqrt{3} \ : \ m,n \in Z\}$$

هي حلقة جزئية من الحلقة $(R,+,\cdot)$.

ثم برهن أن المجموعة الجزئية I من M حيث n,m أعداد صحيحة زوجية هي مثالية من الحلقة $(M,+,\cdot)$.

11- أوجد الحلقات الجزئية من حلقة الأعداد الصحيحة $(Z,+,\cdot)$.

12- لتكن حلقة المصفوفات المربعة $(M_2(R),+,\cdot)$ ، ولتكن $S = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} ; a,b,c \in R \right\}$. أثبت أن $(S,+,\cdot)$ ليست حلقة جزئية من الحلقة $(M_2(R),+,\cdot)$.

13- لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، ولتكن $(S,+,\cdot)$ حلقة جزئية منها وبمحايد أيضاً . ولنفرض أن $1'$ هو المحايد فيها ، ولنفرض أن المحايد في الحلقة $(R,+,\cdot)$ بالنسبة للعملية (·) لا ينتمي إلى S ، أثبت أن $1'$ قاسم للصفر في الحلقة

$(R,+,\cdot)$.

-14 أثبت أن $Z[\sqrt{2}]=\{a+b\sqrt{2}\ ;\ a,b\in Z\}$ ليست حقلاً جزئياً من الحقل $(R,+,\cdot)$.

-15 لتكن $(M_2(Z),+,\cdot)$ حلقة المصفوفات المربعة من الدرجة الثانية ، أثبت :

(1) أن $I=\left\{\begin{pmatrix}0 & a\\ 0 & b\end{pmatrix};\ a,b\in Z\right\}$ مثالية يمينية ولكنها ليست مثالية يسارية في الحلقة $(M_2(Z),+,\cdot)$.

(2) أما المجموعة $I=\left\{\begin{pmatrix}a & b\\ d & c\end{pmatrix};\ a,b,c\in Z\right\}$ فهي مثالية في الحلقة $(M_2(Z),+,\cdot)$.

(3) المجموعة $I=\left\{\begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix};\ a\in Z\right\}$ هي حلقة جزئية ولكنها ليست مثالية يمينية أو يسارية من الحلقة $(M_2(Z),+,\cdot)$.

-16 أثبت أن المجموعة $I=\{(k,0)\ ;\ k\in Z\}$ هي مثالية من الحلقة $(Z\times Z,+,\cdot)$.

-17 لتكن $\{I_i\}_{i\in I}$ أسرة غير خالية من المثاليات في حلقة ما، ولتكن $(R,+,\cdot)$. نرمز عادةً بـ $\sum_{i\in I} I_i$ لمجموعة كل العناصر التي هي من الشكل $\sum_{i\in I} x_i$ حيث أن $x_i\in I_i$ ، وحيث أن جميع x_i ما عدا عدداً منتهياً منها أصفار . أثبت أن $\sum_{i\in I} I_i$ مثالية في الحلقة $(R,+,\cdot)$.

-18 لتكن $(Z_6,+,\cdot)$ حلقة الأعداد الصحيحة قياس 6 ، وإذا كانت $I=\{0,3\}$ مثالية مولداً بالعنصر <3> . شكّل جدول كيلي لحلقة القسمة .

-19 لنفرض أن $I,J_1,J_2,\ldots,J_n$ مثاليات في حلقة إبدالية ما ، ولتكن $(R,+,\cdot)$. بيّن أن :

$$\left(\bigcap_{i=1}^{n} J_i\right):I=\bigcap_{i=1}^{n}(J_i:I)$$

-20 قدّم مثالاً لحلقة تامة $(R,+,\cdot)$ ولمثالية I من R بحيث تحتوي حلقة القسمة

$(R/I,+,\cdot)$ على قواسم للصفر .

21- إذا كانت $R = (Z_6,+,\cdot)$ حلقة ، وكانت $I = \{0,3\} \subseteq R$ ، أثبت أن I مثالية في R ، ثم أوجد حلقة القسمة Z_6/I للمثالية I في Z_6 .

22- لتكن $(F,+,\cdot)$ حلقة الدوال الحقيقية ، وإذا كانت المجموعة I التالية :

$$I = \{ f \in F ; f(c) = 0 , c \in R \}$$

أثبت أن I مثالية في الحلقة $(F,+,\cdot)$.

23- لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، نقول عن العنصر x من R إنه متلاشي (معدوم) إذا وُجِدَ $n \in Z^+$ بحيث $x^n = 0$. برهن أن مجموع العناصر المتلاشية في الحلقة $(R,+,\cdot)$ تشكل مثالية . ثم أثبت أن $1 - x$ هو عنصر الوحدة في الحلقة $(R,+,\cdot)$.

24- لتكن I مثالية من الحلقة بمحايد $(R,+,\cdot)$. وإذا كان $a \in I$ عنصر وحدة أثبت أن $I = R$.

25- لتكن $R = (M_2(Z),+,\cdot)$ حلقة المصفوفات المربعة من الدرجة الثانية . بيّن فيما إذا كانت المجموعة $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ; a,b \in Z \right\} = I$ تشكل مثالية يسارية في الحلقة R .

26- لتكن $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ; a,b,c \in Z \right\}$ حلقة المصفوفات المربعة من الدرجة الثانية . وإذا كانت $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} ; a,b \in Z \right\}$ و $J = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} ; a,b \in Z \right\}$ مثاليتين فيها ، أثبت أن $I \cdot J$ و $I + J$ مثاليتين في الحلقة R .

تمارين محلولة وغير محلولة للفصل الثالث:

التماثل الحـــلقي

Isomorphism of ring

5- تمرينات محلولة للفصل الثالث

– التماثل الحلقي –

1- لتكن الحلقتان $R = (Z_4,\oplus,\otimes)$ و $S = (Z_6,\oplus,\otimes)$ ، وإذا كان التطبيق $\varphi : R \longrightarrow S$ ، معرفاً بالشكل : $\varphi(\overline{a}) = 3\overline{a}$ ، لكل $\overline{a}$ من R ، برهن أن φ تشاكل حلقي ، ثم أوجد نواته .

الحل :

لكل $\overline{a}$ و $\overline{b}$ من R نجد :

$$\varphi(\overline{a} \oplus \overline{b}) = 3(\overline{a \oplus b}) = 3\overline{a} \oplus 3\overline{b} = \varphi(\overline{a}) \oplus \varphi(\overline{b})$$

$$\varphi(\overline{a} \otimes \overline{b}) = 3(\overline{a \otimes b}) = 3\overline{a} \otimes 3\overline{b} = \varphi(\overline{a}) \otimes \varphi(\overline{b})$$

$$\text{Ker}\,\varphi = \{\overline{a} \in R : \varphi(\overline{a}) = o\}$$

حيث o صفر الحلقة S .

$$= \{\overline{a} \in R : 3\overline{a} = o\}$$

$$= \{\overline{o}, \overline{2}\} \subseteq R$$

2- لتكن $(R,+,\cdot)$ حلقة بمحايد ، وليكن a عنصر وحدة في R ، ولنعرف التطبيق $\varphi : R \longrightarrow R$ بالشكل :

$$\varphi(r) = a.r.a^{-1} \;\; ; \;\; \forall r \in R$$

المطلوب : أثبت أن التطبيق φ تماثل .

الحل :

لكل r_1,r_2 من R يكون لدينا :

$$\varphi(r_1 + r_2) = a.(r_1 + r_2).a^{-1} = a.\,r_1.a^{-1} + a.r_2.a^{-1} = \varphi(r_1) + \varphi(r_2)$$

$$\varphi(r_1.r_2) = a.\,(r_1.r_2).a^{-1} = a.r_1\,(a.a^{-1}).r_2.a^{-1}$$

$$= (a.r_1.a^{-1})\,.\,(a.r_2.a^{-1}) = \varphi(r_1)\,.\,\varphi(r_2)$$

نستنتج مما سبق أن φ تشاكل من الحلقة R إلى نفسها .

لنبرهن الآن أن التطبيق φ متباين (أحادي) :

ليكن $r \in Ker\ \varphi$ ، وهذا يعني أن $\varphi(r) = o$ ، وبالتالي ، فإن $a.r.a^{-1} = 0$ ، بالضرب من اليمين a ومن اليسار بـ a^{-1} نجد أن $r = 0$ ، وهذا يعني أن φ متباين .

لنبرهن أخيراً ، أن φ شامل ، إذا كان $r \in R$ ، فإن :

$$\varphi(a^{-1}.r.a) = a\,(a^{-1}.r.a).a^{-1} = (a.a^{-1})\,r.(a.a^{-1}) = r$$

وهذا يعني أن التطبيق φ شامل .

نستنتج مما سبق أن φ تماثل . يسمى عادةً هذا التماثل بالتماثل الذاتي .

3- لتكن $(R,+,.)$ حلقة، وليكن φ تطبيقاً من R إلى نفسها ، معرفاً بالشكل $\varphi(a) = a$ ، لكل a من R، أثبت أن φ تشاكل حلقي .

الحل :

لكل b,a من R لدينا :

$$\varphi(a + b) = a + b = \varphi(a) + \varphi(b)$$
$$\varphi(a.b) = a\,.b = \varphi(a)\,.\varphi(b)$$

نستنتج أن φ تشاكل حلقي .

4- ليكن φ تشاكلاً للحلقة $(Z,+,.)$ في نفسها ، وإذا كان m عدداً صحيحاً بحيث يكون : $\varphi(m) \neq o$ ، أثبت أن : $\varphi(n) = n$ لكل n من Z .

الحل :

بما أن $m = 1.m$ ، وبالتالي ، فإن :

$$\varphi(m) = \varphi(1.m) = \varphi(1).\varphi(m)$$

ومنه يكون $\varphi(1) = 1$.

لنفرض الآن أن n عدداً صحيحاً موجباً ، وبالتالي ، فإن :

$$\varphi(n) = \varphi(1 + 1 + \dots + 1) = \varphi(1) + \varphi(1) + \dots + \varphi(1)$$
$$= \underbrace{1+1+\dots\dots+1}_{n \text{ مرة}} = n$$

لنفرض الآن أن n عدداً صحيحاً سالباً ، وبالتالي يمكن كتابة $n = -t$ حيث t عــدد صحيح موجب، ومنه يكون :

$$\varphi(n) = \varphi(-t) = -\varphi(t) = -t = n$$

بالإضافة إلى ذلك ، إذا كان $n = 0$ ، فإن :

$$\varphi(o) = \varphi(o) = o = n$$

5- لتكن $(R,+,.)$ حلقة بمحايد (وليكن e) ، أثبت أن φ تشاكلاً من حلقة الأعداد الصحيحة $(Z,+,.)$ إلى الحلقة $(R,+,.)$ معرفاً بالشكل : $\varphi(n) = n.e$ حيث n من Z . ثم برهن أن $n.e = 0$ ، إذا وفقط إذا، كان مميز الحلقة a يقسم n .

الحل :

لنرمز بـــ o' لصفر الحلقة $(R,+,.)$ ، وليكن m,n عنصران من Z ، وبالتـــالي ، فإن :

$$\varphi(m + n) = (m + n).e = m.e + n.e = \varphi(m) + \varphi(n)$$

كما أن :

$$\varphi(m) . \varphi(n) = (m.e) . (n.e) . \underbrace{(e+e+\dots.+e)}_{m \text{ مرة}} . n.e$$

$$= e.n.e + \dots.. + e.n.e = n.e^2 + \dots\dots.+ n.e^2$$

$$= n.e + \dots + n.e = m.n.e = \varphi(m . n)$$

بما أن φ تشاكل ، فإن حسب الطلب السابق نجد :

$$\varphi(n) = n.e = 0 \Leftrightarrow n \in \mathrm{Ker}\, \varphi = a.Z \Leftrightarrow a.n$$

6- لـــيكن $\varphi: R \longrightarrow S$ تشـــاكلاً حلقيـــاً ، حيـــث أن $R = (Z,+,.)$ و $S = (Z_n,\oplus,\otimes)$ معرفاً بالشكل : $\varphi(a) = [a] \equiv a.\mathrm{mod}\, n$ لكل a من R . أثبت أن φ تشاكل حلقي ، ثم أوجد نواته .

الحل :

لكل b,a من R ، يكون :

$$\varphi(a+b)=[a+b]=[a]\oplus[b]=\varphi(a)\oplus\varphi(b)$$

$$\varphi(a.b)=[a.b]=[a]\otimes[b]=\varphi(a)\otimes\varphi(b)$$

إذن φ تشاكل حلقي ، لنوجد الآن نواته .

$$\text{Ker}\,\varphi=\{a\in R:\ \varphi(a)=o\}$$

حيث o هو صفر الحلقة S ، وبالتالي ، فإن :

$$\begin{aligned}&=\{a\in R:\ [a]=[o]\}\\&=\{a\in R:\ a\equiv o \bmod n\}\\&=\{a\in R:\ a=n.r\,;r\in R\}\\&=\{n.r:r\in R\}=n\,.\,Z\end{aligned}$$

7- ليكن φ تشاكلاً من الحلقة $(R,+,.)$ في الحلقة $(S,T,\star)$. أثبت أن φ تماثلاً للحلقة $(R,+,.)$ في الحلقة $(S,T,\star)$ إذا ، وفقط إذا ، كان $\text{Ker}\,\varphi=\{o\}$. حيث o هو صفر الحلقة $(R,+,.)$.

الحل :

لنرمز بـــ o' لصفر الحلقة $(S,T,\star)$ ، ولنبرهن أولاً أن $\text{Ker}\,\varphi=\{o\}$ علماً أن φ تماثلاً للحلقة $(R,+,.)$ في الحلقة $(S,T,\star)$.

ليكن x عنصراً ما من $\text{Ker}\,\varphi$، وهذا يعني أن $\varphi(x)=o'$، وبالتالي يكون لـــدينا: $\varphi(x)=\varphi(o)$، أي أن $x=0$.

لنبرهن أن φ تماثل علماً أن $\text{Ker}\,\varphi=\{o\}$.

بما أن φ تشاكلاً للحلقة $(R,+,.)$ في الحلقة $(S,T,\star)$، لذا يكفـــي أن نبـــرهن أن التطبيق φ متباين.

ليكن x_2 , x_1 عنصرين ما من R ، بحيث يكون :

$$\varphi(x_1)=\varphi(x_2)$$

ومنه :

$$\varphi(x_1)\, T\, \big(-\varphi(x_2)\big) = o'$$

$$\varphi(x_1)\, T\, \varphi(-x_2) = o'$$

$$\varphi\big(x_1 + (-x_2)\big) = o' \Rightarrow x_1 + (-x_2) \in \operatorname{Ker} \varphi$$

وبما أن $\operatorname{Ker} \varphi = \{o\}$ ، فإن :

$$x_1 + (-x_2) = 0$$

ومنه يكون $x_1 = x_2$ ، أي أن φ متباين .

<u>**8-**</u> ليكن φ تشاكلاً شاملاً من الحلقة $(R,+,\cdot)$ إلى الحلقة $(S,+,\cdot)$ وإذا كانت I مثالية للحلقة $(R,+,\cdot)$ تحوي $\operatorname{Ker} \varphi$ ، أثبت :

(1) $R|I \cong S|\varphi(I)$

(2) إذا كان J مثالية في الحلقة $(S,+,\cdot)$ ، فإن : $R|\varphi^{-1}(J) \cong S|J$.

الحل :

(1) لنعرّف التطبيق $\Phi : R/I \longrightarrow S/\varphi(I)$ بالشكل :

$$\Phi(a + I) = \varphi(a) + \varphi(I) \;;\; \forall a \in R$$

لنثبت أولاً ، أن Φ تشاكل ، لكل b,a من R ، فإن :

$$\begin{aligned}\Phi(a + b + I) &= \varphi(a + b) + \varphi(I)\\ &= \varphi(a) + \varphi(b) + \varphi(I)\\ &= \big(\varphi(a) + \varphi(I)\big) + \big(\varphi(b) + \varphi(I)\big)\\ &= \Phi(a + I) + \Phi(b + I)\end{aligned}$$

$$\begin{aligned}\Phi(a.b + I) &= \varphi(a.b) + \varphi(I)\\ &= \varphi(a).\varphi(b) + \varphi(I)\\ &= \big(\varphi(a) + \varphi(I)\big).\big(\varphi(b) + \varphi(I)\big)\\ &= \Phi(a + I).\Phi(b + I)\end{aligned}$$

إذن Φ تشاكل .

لنثبت الآن أن التطبيق Φ شامل ، لكل $b \in S$ ، نفرض أن $b + \varphi(I) \in S/\varphi(I)$ ، وبما φ شامل، فإنه يوجد عنصر من R وليكن a بحيث يكون $\varphi(a) = b$ ، إذن :

$$\Phi\,(a+I)=\varphi(a)+\varphi(I)=b+\varphi(I)$$

وهذا يعني أن التطبيق Φ شامل .

لنفرض الآن ، أن $\Phi\,(a+I)=\varphi(I)$ وهذا يؤدي ، إلى أن :

$$\varphi(a)+\varphi(I)=\varphi(I)$$

وبالتالي ، يكون : $\varphi(a)\in\varphi(I)$.

ليكن الآن $\varphi(a)=\varphi(x)$، حيث x من I. بملاحظة أن $\varphi(a-x)=0$، أي أن $a-x\in \mathrm{Ker}\,\varphi$، وبما أن $\mathrm{Ker}\,\varphi\subset I$ ، لذلك $a\in I$ ، وبالتالي يكون $a+I=I$ ، أي أن $a+I$ هو صفر الحلقة R/I ، إذن التطبيق Φ متباين .

نستنتج مما سبق أن : $R/I\cong S/\varphi\,(I)$

(2) بما أن $\varphi^{-1}(I)$ مثالية للحلقة $(R,+,\cdot)$، وبما أن :

$\mathrm{Ker}\,\varphi=\varphi^{-1}(o')\subset\varphi^{-1}(J)$ ، لأن $o'\in J$ ، حيث o' هو صفر الحلقة $(S,+,\cdot)$ ، وباستخدام الطلب (1) السابق نجد أن :

$$R/\varphi^{-1}(J)\cong S/\varphi\,\varphi^{-1}(J)=S/J$$

9- إذا كانت $(R,+,\cdot)$ و$(S,+,\cdot)$ حلقتين ، إذا كان φ تشاكلاً من R إلى S ، فأثبت أن $\mathrm{Im}\,\varphi$ حلقة جزئية من الحلقة S .

الحل :

ليكن b,a من $\mathrm{Im}\ \ \varphi$، وبالتالي، يوجد عنصران y,x في الحلقة R، بحيث يكون $b=\varphi(y)\,,\,a=\varphi(x)$.

الآن :

$$\begin{aligned}a-b&=\varphi(x)-\varphi(y)=\varphi(x)+\varphi(-y)\\&=\varphi(x-y)\ \Rightarrow\ a-b\in \mathrm{Im}\,\varphi\end{aligned}$$

كذلك :

$$a.b=\varphi(x).\varphi(y)=\varphi(x.y)\ \Rightarrow\ a.b\in\mathrm{Im}\,\varphi$$

نستنتج مما سبق أن $\mathrm{Im}\,\varphi$ حلقة جزئية من الحلقة $(S,+,\cdot)$.

10- لتكن $R = (Z,+,.)$ حلقة الأعداد الصحيحة ، وإذا كانت المثاليات $I = 4z$ و$J = 6z$ ، حقق المبرهنة الثانية لتماثل الحلقات .

الحل :

بما أن :

$$I \cap J = 4z \cap 6z = 12z \quad , \quad I + J = 4z + 6z = 2z$$

وباستخدام المبرهنة الثانية لتماثل الحلقات نجد :

$$2z/6z \cong 4z/12z$$

11- لتكن $(C,+,.)$ حلقة الأعداد المركبة ، ولـيكن التطبيـق $\varphi : C \longrightarrow C$ معرفاً بالشكل $\varphi(x) = \overline{x}$ (حيث أن $\overline{x}$ هو مرافق العنصر x في C) ، أثبت أن φ تماثل حلقي .

الحل :

نعلم أنه في حلقة الأعداد المركبة ، ومن أجل أي $x,y \in C$ ، إن :

$$\overline{x+y} = \overline{x} + \overline{y} \quad , \quad \overline{x.y} = \overline{x} . \overline{y}$$

ومنه يكون :

$$\varphi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(x) + \varphi(y)$$

$$\varphi(x.y) = \overline{x.y} = \overline{x} . \overline{y} = \varphi(x) . \varphi(y)$$

إذن φ تشاكل حلقي .

ويمكن الإثبات بسهولة ، أن التطبيق φ تقابلاً .

12- لتكن $(R,+,.)$ حلقة إبدالية ، وإذا كانت I مثالية أولية في R ، وإذا كانت I_2 , I_1 مثاليتين في الحلقة $(R,+,.)$ بحيث $I_1.I_2 \subseteq I$ ، بيّن أن إحـدى المثـاليتين I_2 , I_1 على الأقل محتواة في I .

الحل :

لنفرض جدلاً عكس ذلك ، وهذا يعني أن بالإمكان إيجاد عنصرين y,x مـن I_2,I_1

على الترتيب بحيث يكون : $y \notin I , x \notin I$. لكن :

$$x \in I_1 , y \in I_2 \Rightarrow x.y \in I_1.I \Rightarrow x.y \in I$$

وبما أن I مثالية أولية في الحلقة $(R,+,\cdot)$ ، فإن انتماء أحد العنصرين $x.y$ إلى I يؤدي إلى انتماء أحد العنصرين y,x على الأقل ، إلى I ، وهذا مخالف لكون $y \notin I , x \notin I$. إذن إحدى المثاليتين I_2 , I_1 على الأقل محتواة في المثالية I .

ملاحظة :

يمكن تعميم التمرين السابق بالشكل :

إذا كانت I مثالية أولية في الحلقة الإبدالية $(R,+,\cdot)$ ، وإذا كان n عدداً صحيحاً موجباً ، وإذا كانت I_1 مثالية في الحلقة $(R,+,\cdot)$ بحيث يكون :

$$I_1^n = \underbrace{I_1.I_1......I_1}_{n\text{مرة}} \subseteq I$$

فإن $I_1 \subseteq I$.

13- لتكن I مثالية في الحلقة الإبدالية $(R,+,\cdot)$ ، بحيث $I \neq R$. أثبت أن الشرط اللازم والكافي لكي تكون المثالية I مثالية أولية في الحلقة $(R,+,\cdot)$ ، هو أن لا تحوي الحلقة $(R/I,+,\cdot)$ قواسم للصفر .

الحل :

لنبرهن أولاً ، أن الحلقة $(R/I,+,\cdot)$ لا تحوي قواسم للصفر ، علماً أن المثالية I مثالية أولية في الحلقة $(R,+,\cdot)$.

إذا حوت الحلقة $(R/I,+,\cdot)$ قواسم للصفر ، فإنه يمكن إيجاد عنصرين y,x من R بحيث يكون :

$$x + I \neq I \ , \ y + I \neq I$$
$$(x + I) . (y + I) = I$$

لكن :

$$(x + I) . (y + I) = I \Rightarrow x.y + I = I$$

وهذا يؤدي إلى أن $x.y$ من I . وبما أن I مثالية أولية فرضاً في الحلقة $(R,+,.)$ ، فإن انتماء $x.y$ من I يؤدي إلى انتماء أحد العنصرين y,x على الأقل إلى I ، وهذا يعني أن أحد العنصرين $x + I$ ، $y + I$ ، على الأقل ، يساوي I ، وهذا مخالف كون : $x + I \neq I \ , \ y + I \neq I$. إذن الحلقة $(R/I,+,.)$ لا تحوي قواسم للصفر .

لنبرهن العكس ، أي لنبرهن أن المثالية I مثالية أولية في الحلقة $(R,+,.)$ ، علماً أن الحلقة $(R/I,+,.)$ لا تحوي قواسم للصفر . من أجل ذلك ، ليكن y,x عنصرين ما من R ، وبحيث يكون $x.y \in I$.

بما أن $x.y \in I$ ، فإن : $x.y + I = I$ وهذا يعني أن : $(x + I) . (y + I) = I$

وبما أن الحلقة $(R/I,+,.)$ (لا تحوي قواسم للصفر ، فإن المساواة الأخيرة تبين أن أحد العنصرين $x + I$ ،$y + I$ على الأقل ، يساوي I ، وهذا بدوره يعني أن أحد العنصرين y,x ، على الأقل ، ينتمي إلى I . إذن المثالية I مثالية أولية في الحلقة $(R,+,.)$.

14- لتكن $(R,+,.)$ حلقة ما ، أثبت صحة ما يلي :

(1) المثالية اليسارية I عديمة القوى في الحلقة $(R,+,.)$ إذا ، وفقط إذا ، وُجِدَ عدد طبيعي n بحيث $I^n = 0$.

(2) كل مثالية يسارية معدومة القوى تكون عديمة .

(نقول عن المثالية I إنها عديمة إذا كان كل عنصر من I هو عنصر عديم القوى ، ونقول عن المثالية اليسارية I في R إنها معدومة القوى ، إذا وُجِدَ عدد طبيعي n يحقق $x_1.x_2\ldots x_n = 0$ لكل $x_i \in I$ و $1 \leq i \leq n$) .

البرهان :

(1) لنبرهن أولاً ، على وجود العدد الطبيعي n بحيث يكون $I^n = 0$ ، بفرض أن المثالية اليسارية I معدومة القوى ، وهذا يعني أنه يوجد $n \in N$ بحيث يكون $a_1.a_2\ldots a_n = 0$ ، لكل $a_i \in I$ و $1 \leq i \leq n$.

ليكن $b \in I^n$ ، عندئذٍ يكون $b = \sum x_{i1}.x_{i2}\ldots.x_{in} = 0$ ، حيث أن $x_{ij} \in I$ لكل

$1 \le j \le n$ ، ومنه يكون $I^n = 0$.

لنبرهن الآن كفاية الشرط ، نفرض أنه يوجد عدد طبيعي n بحيث يكون $I^n = 0$ ، وليكن $a_1.a_2...a_n \in I$، عندها يكون $a_1.a_2...a_n \in I^n = 0$. وهذا يعني أن المثالية اليسارية I معدومة القوى .

(2) لتكن J مثالية يسارية معدومة القوى في الحلقة $(R,+,.)$ ، وهذا يؤدي إلى وجود عدد طبيعي n يكون من أجله $J^n = 0$ ، من ناحية ثانية ، إذا كان $x \in J$ ، عندها يكون : $x^n = x.x...x \in J^n = 0$ ، أي أن كل عنصر من المثالية اليسارية J هو عنصر عديم القوى ، إذن المثالية اليسارية J عديمة .

<u>15-</u> بداية هذا التمرين ، نذكّر القارئ الكريم بمفهوم الجسم .

لتكن $(R,+,.)$ حلقة ما ، نقول عن هذه الحلقة إنها جسم (Skew – Field) إذا كان $0 \neq 1$ وكل عنصر من الحلقة R مغايراً للصفر يملك معكوس ، ونسمي كل جسم إبدالي حقل .

لتكن $(R,+,.)$ حلقة ما ، لا تحوي مثاليات عديمة القوى مغايرة للصفر ، وكان e عنصراً جامد من R ولا يساوي الصفر ، عندها الشروط التالية متكافئة :

(1) المثالية اليسارية R.e أصغرية في الحلقة $(R,+,.)$.

(2) الحلقة e.R.e جسم .

البرهان :

(2) ⇐ (1)

بفرض أن المثالية اليسارية R.e أصغرية في الحلقة R ، ونعلم أن e.R.e هي حلقة إبدالية بمحايد لـ e هو العنصر المحايد فيها) . وإذا كان $e.r.e \in e.R.e$ لا يساوي الصفر ، عندها يكون R.e.r.e مثالية يسارية في الحلقة R لا تساوي الصفر ، كما أن $R.e.r.e \subseteq R.e$ ، وبما أن المثالية اليسارية R.e أصغرية ، يكون $R.e.r.e = R.e$ ، وبما أن $e \in R.e = R.e.r.e$ ، فإنه يوجد عنصر x من R بحيث $e = x\,e\,r\,e$ ، كما أن :

$$e = e.e = e\,(x.e.r.e) = e\,(x.e^2.r.e) = (e.x.e)\,(e.r.e)$$

وبما أن $e.x.e \in e.R.e$ ، نجد أن العنصر $e.r.e$ قابل للعكس من اليسار في $e.R.e$ ، وبالتالي تكون الحلقة $e.R.e$ جسم .

$(1) \Leftarrow (2)$

لنفرض الآن أن الحلقة $e.R.e$ جسم ، ولنبرهن أن المثالية اليسارية $R.e$ أصغرية ، لتكن I مثالية يسارية لا تساوي الصفر في الحلقة $(R,+,.)$ حيث $I \subseteq R.e$ ، عندها يكون $e.I \neq 0$ ، لأنه إذا كان $e.R = 0$. فإن :

$$R^2 = R.R \subseteq (R.e) R = R (e.R) = 0$$

وهذا يبيّن لنا أن المثالية اليسارية I معدومة القوى ، وبالتالي يوجد في الحلقة $(R,+,.)$ مثالية معدومة القوى ، وهذا مناقض للفرض ، إذن $e.I \neq 0$ ، ومنه يوجد عنصر وليكن x من I بحيث يكون $e.x \neq 0$ ، وبما أن $x \in I \subseteq R.e$ ، يوجد عنصر a من R بحيث $x = a.e$ ، وبالتالي يكون لدينا :

$$o \neq e.x = e.a.e = (e.a.e).e = e (a.e).e = e.a.e \in e.R.e$$

وبما أن $e.R.e$ جسم ، فإن العنصر $e.x$ قابل للعكس في الحلقة $e.R.e$ ، أي أنه يوجد العنصر $e.y.e \in e.R.e$ حيث : $(e.y.e)(e.x) = e$.

كما أن :

$$e = (e.y.e)(e.x) = (e.y.e)\, x \in R.x \subseteq R I \subseteq I$$

وهذا يبين لنا أن المثالية اليسارية $R.e$ أصغرية في الحلقة $(R,+,.)$.

<u>**16-**</u> إذا كانت $(Z,+,.)$ حلقة تامة ، حيث Z مجموعة الأعداد الصحيحة ، أثبت أن $(Z,+,.)$ حلقة إقليدية .

الحل :

لنعرّف الدالة الإقليدية d بالشكل : $d(n) = |n|$ حيث n عدد صحيح مختلف عن الصفر .

ليكن n_2,n_1 عددين صحيحين مختلفين عن الصفر ، بحيث أن n_1 يقسم n_2 في Z ، وبالتالي يوجد عدد صحيح n_3 مختلف عن الصفر بحيث يكون : $n_2 = n_1.n_3$ ،

ومنه يكون :

$$d(n_2) = |n_2| = |n_1.n_3| = |n_1|.|n_3| \geq |n_1| = d(n_1)$$

إذن الشرط الأول محقق ، وإذا كان m_1 و $m_2 \neq 0$ عددين صحيحين ، فإنه استناداً إلى نظرية التقسيم الخوارزمي ، يوجد عددان صحيحان r,q ، بحيث يكون : $m_1 = q.m_2 + r$ ، لكل $0 \leq r < |m_2|$ ، أي لكل $m_1 = q\,m_2 + r$ و r إما أن يكون صفراً ، أو أن يكون $d(r) \leq d(m_2)$.

نستنتج مما سبق أن $(Z,+,.)$ حلقة إقليدية .

17- إذا كانت $(R,+,.)$ حلقة تحليل وحيد ، صفرها هو o ، وإذا كان y,x عنصرين مغايرين للصفر من R ، أثبت أن لـ y,x قاسماً مشتركاً أعظم في R .

الحل :

بما أن $(R,+,.)$ حلقة تحليل وحيد وy,x عنصرين مغايرين للصفر في R ، فإن y,x يمكن كتابتهما بالشكل :

$$x = u.P_1^{S_1}.P_2^{S_2}........P_n^{S_n}$$

$$y = v.P_1^{t_1}.P_2^{t_2}........P_n^{t_n}$$

حيث أن v,u عنصران قابلان للعكس في R ، و$P_1 , P_2 , \ldots , P_n$ عناصر من الحلقة R ، وS_i وt_i أعداد صحيحة غير سالبة و $1 \leq i \leq n$ و P_{i_1} وP_{i_2} ليسا مترادفين في الحلقة R ، وذلك من أجل أي i_1 وi_2 من المجموعة $\{1,2,\ldots,n\}$ و $i_1 \neq i_2$.

ليكن $d = P_1^{r_1}.P_2^{r_2}........P_n^{r_n}$ حيث أن :

$$r_i = \min(S_i , t_i) \;;\; 1 \leq i \leq n$$

ولنثبت أن d هو قاسم مشترك أعظم لـ y,x في R .

بما أن $x = u.P_1^{S_1}.P_2^{S_2}........P_n^{S_n}$ ، فإن :

$$\begin{aligned} x &= u.P_1^{r_1}.P_1^{S_1-r_1}.P_2^{r_2}.P_2^{S_2-r_2}.......P_n^{r_n}.P_n^{S_n-r_n} \\ &= u.P_1^{S_1-r_1}.P_2^{S_2-r_2}......P_n^{S_n-r_n}.P_1^{r_1}.P_2^{r_2}......P_n^{r_n} \\ &= u.P_1^{S_1-r_1}.P_2^{S_2-r_2}......P_n^{S_n-r_n}.d \end{aligned}$$

وهذا يبين لنا أن d يقسم x في R .

بنفس الطريقة يمكن إثبات أن d يقسم y في R . لنبرهن الآن على تحقق الشرط الثاني الوارد في تعريف القاسم المشترك الأعظم .

إذا وُجِدَ قاسم مشترك آخر وليكن d_1 لـ y,x في R ، فإنه يمكن كتابته بالشكل :

$$d_1 = \alpha\ q_1^{m_1}.q_2^{m_2}.....q_n^{m_n}$$

حيث أن α عنصر قابل للعكس في الحلقة R ، وq_i عناصر من R ، وكل منها غير قابل للتحليل و$1 \leq i \leq n$ و$m_i \in Z^+$ و q_{i_2}, q_{i_1} ليسا مترادفين في R ، وذلك من أجل أي i_2 , i_1 من المجموعة $\{1,2,.....,n\}$ ، $i_1 \neq i_2$ ، ومن ثم ، فإن كلاً من العناصر $q_1,q_2,...,q_n$ يقسم x في R وبالتالي تكون العناصر $q_1,q_2,...,q_n$ تقسم على الأقل ، أحد العناصر $P_1,P_2,...,P_n$ في R . وبالتالي فإن كلاً من العناصر $q_1,q_2,...,q_n$ هو مرادف لأحد العناصر P_i ; $1 \leq i \leq n$ في R وهذا يبين لنا أنه يمكن كتابة العنصر d_1 بالشكل :

$$d_1 = \beta\ P_1^{k_1}.P_2^{k_2}.....P_n^{k_n}$$

حيث أن β عنصر قابل للعكس في A و$k_i \in Z^+$ و $1 \leq i \leq n$ ، وبما أن d_1 يقسم كلاً من y,x في R ، وكلاً من العناصر P_i ، حيث $1 \leq i \leq n$ غير قابلة للتحليل في R و P_{i_2} ،P_{i_1} ليسا مترادفين في R ، وذلك من أجل أي i_1 وi_2 من المجموعة$\{1,2,.....,n\}$ و $i_1 \neq i_2$ ، فإن : $k_i \leq t_i$ و $k_i \leq S_i$ حيث $1 \leq i \leq n$.

إذن $k_i \leq \min(t_i , S_i)$ حيث $1 \leq i \leq n$ ، وبالتالي فإن d_1 يقسم d في R .

نستنتج مما سبق أن d هو قاسم مشترك أعظم لـ y,x في الحلقة R .

18- إذا كانت $(R,+,.)$ حلقة ما، وI مثالية يسارية في R ، أثبت صحة تكافؤ الشروط التالية :

(1) المثالية اليسارية I ، هي حد مباشر للحلقة R .

(2) يوجد في الحلقة R عنصر جامد وليكن e حيث $I = R.e$.

الحل :

$(1) \Leftarrow (2)$

بما أن I هي حد مباشر للحلقة R ، فيوجد في R مثالية يسارية ولتكن J بحيث يتحقق $R = I \oplus J$. ومنه يكون : $1 = a + b$ حيث $a \in I$ و $b \in J$ ومنه $a = a^2 + a.b$ أي أن :

$$a - a^2 = a.b \in I \ , \ a - a^2 = a.b \in J$$

وبالتالي يكون : $a - a^2 \in I \cap J = 0$ أي أن $a = a^2$ ، وهذا يعني أن a هو عنصر جامد في الحلقة R ، وأن $a \in I$ ، ومنه $R.a \subseteq I$.

ليكن $x \in I$ ، عندئذٍ $x = x.a + x.b$ ، وبالتالي فإن :

$$x - x.a = x.b \in I, J$$

أي أن : $x - x.a \in I \cap J = 0$ ، وبالتالي : $x = x.a \in R.a$ ، إذن : $I \subseteq R.a$.

نستنتج مما سبق أن : $I = R.a$.

$(2) \Leftarrow (1)$

إذا كان e عنصراً جامداً في R حيث $I = R.e$ ، عندها يكون $R = R.e \oplus R$ $(1 - e)$ لأن $R(1 - e)$ مثالية يسارية في R ، كما أن $R.e + R(1 - e) \subseteq R$.

من ناحية ثانية ، لكل $x \in R$ يكون $x.e + x(1 - e) = x$ ، وبالتالي :

$$R \subseteq R.e + R(1 - e)$$

إذن : $R = R.e + R(1 - e)$.

ليكن $b \in R.e \cap R(1 - e)$، عندئذٍ $b = r.e = r_0(1 - e)$ ، حيث r , r_0 من R ، وبالتالي ، فإن:

$$b.e = r . e^2 = r_0(1 - e).e$$

$$= r.e = r_0.e - r_0 e^2 = r.e = r_0.e - r_0 e = 0$$

$$\Rightarrow b = b.e = 0$$

نستنتج مما سبق أن $R = R.e \oplus R(1-e)$. إذن المثالية اليسارية I حد مباشر في الحلقة R .

-19 لتكن $\left(\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in Z\right\},+,\cdot\right)$ حلقة . أثبت أن $P = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in Z\right\}$ مثالية في R ولكنها ليست أولية .

الحل :

إذا كان :

$$A = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in Z\right\} , B = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b,c \in Z\right\}$$

مثاليتين في R ، وأن :

$$A \cdot B = \left\{\begin{pmatrix} 0 & a.b + b.c \\ 0 & 0 \end{pmatrix} : a,b,c \in Z\right\} \subseteq P$$

بينما $A \not\subset P$ و $B \not\subset P$. إذن P ليست مثالية أولية في R .

-20 لتكن $(R,+,\cdot)$ حلقة إبدالية بمحايد ، وإذا كانت الحلقة R تملك مثالية أعظمية وحيدة ، فإن العناصر الجامدة فيها ، هي فقط صفر الحلقة وواحدها أي 0 و 1 .

الحل :

ليكن $a \in R$ عنصراً جامداً، حيث $0 \neq a \neq 1$، وكون a عنصر جامد، فإن $a^2 = a$ أي أن $a(1-a) = 0$ ، إذن لكل من a و $1-a$ قواسم للصفر في الحلقة R ، إذن كل منهما غير معكوس في R وعليه ، فإن كلاً من $<a>$ و $<1-a>$ مثالية حقيقية في R . إذن : $<a> \subseteq I$ و $<1-a> \subseteq I$ حيث I مثالية أعظمية في R ، وبما أن I مثالية أعظمية وحيدة في R ، فإن $1-a, a \in I$ ، أي أن $1 = (1-a) + a \in I$ أي أن $R = I$ ، وهذا غير ممكن لأن $I \neq R$ ، وعليه

يكون 0 و 1 هما العنصران الجامدان الوحيدان في R .

21- إذا كانت الحلقة $(Z_6, \oplus, \otimes)$ ، أوجد عناصر الوحدة والعناصر المترادفة في Z_6 .

الحل :

لدينا زمرة عناصر الوحدة في الحلقة $(Z_6, \oplus, \otimes)$ هي $(G_R, \oplus)$ حيث أن $G_R = \{1,5\}$. من العلاقتين التاليتين :

$$3 = 3 \otimes 1 \ , \ 4 = 2 \otimes 5$$

نجد أن العنصر 4 يترادف مع العنصر 2 ، وأن العنصر 3 يترادف مع نفسه .

22- لتكن الحلقة $(Z[\sqrt{2}], +, .)$ ، أثبت أن العنصر $a = 9 + 5\sqrt{2} \in Z[\sqrt{2}]$ يترادف مع العنصر $b = 1 + 4\sqrt{2}$ في هذه الحلقة .

الحل :

لدينا أولاً :

$$u = \frac{a}{b} = \frac{(9+5\sqrt{2}).(1-4\sqrt{2})}{(1+4\sqrt{2}).(1-4\sqrt{2})}$$

$$= \frac{-31-31\sqrt{2}}{-31} = 1+\sqrt{2} \in Z[\sqrt{2}]$$

وبما أن $u = 1+\sqrt{2}$ عنصر وحدة في الحلقة $(Z[\sqrt{2}], +, .)$ ، لأن :

$$u^{-1} = \frac{1}{1+\sqrt{2}} \cdot \frac{1-\sqrt{2}}{1-\sqrt{2}} = -1+\sqrt{2} \in Z[\sqrt{2}]$$

وبالتالي ، نرى أن العنصرين $9+5\sqrt{2}$ و $1+4\sqrt{2}$ مترادفان .

23- لتكن $(Z[\sqrt{-3}], +, .)$ حلقة ، أثبت أن العنصر $P = \sqrt{-3}$ ، غير أولي في هذه الحلقة .

الحل :

ليكن y,x عنصرين ما من $Z[\sqrt{-3}]$ ، عندها يمكن كتابة :

$x = a + b\sqrt{-3} \quad , \quad y = c + d\sqrt{-3}$

لنعـرف الآن أن : $P|x.y$ ، أي أن $x.y = P.k$ حيـث $k \in Z[\sqrt{-3}]$ ، أي أن $k = s + t\sqrt{-3}$ علماً أن $s,t \in Z$. وبالتالي يمكن كتابة :

$$\left(a + b\sqrt{-3}\right).\left(c + d\sqrt{-3}\right) = \sqrt{-3}\left(s + t\sqrt{-3}\right)$$

ومنه نجد :

$$(a^2 + 3b^2)(c^2 + 3d^2) = 3(s^2 + 3t^2) \Rightarrow$$
$$3/(a^2 + 3b^2)(c^2 + 3d^2) \Rightarrow 3/3a^2d^2 + 3b^2c^2 + 9b^2d^2$$

ومنه $3/a^2c^2$ ، ومن كون 3 عدداً أولياً في Z ، فإما $3/a^2$ أو $3/c^2$ ويكـون $3/a$ أو $3/c$. لنفرض أن $3/a$ ، وبما أن $3 = \left(\sqrt{-3}\right).\left(\sqrt{-3}\right)$ فإن $\sqrt{3}/a$.

إذن $x = a + b\sqrt{-3}$ يقبل القسمة على $\sqrt{-3}$ أي أن $P = \sqrt{-3}$ عنصر غيـر أولي في الحلقة المدروسة .

<u>24-</u> أثبت من خلال مثال أن عكس المبرهنة : إذا كانت $(R,+,.)$ حلقة تامة ، فإن أي عنصر أولي فيها، هو عنصر غير قابل للتحليل ، ليس صحيحاً بشكل عام.

الحل :

لنأخذ الحلقة التامة $(Z[\sqrt{-5}],+,.)$ وليكن العنصر $P = 1+\sqrt{-5}$ منهـا غيـر قابل للتحليل فيها، ولنثبت أنه غير أولي .

بما أن :

$$2.3 = 6 = \left(1 + \sqrt{-5}\right).\left(1 - \sqrt{-5}\right) = P\left(1 - \sqrt{-5}\right)$$

وإذا فرضنا أن P عدد أولي ، يكون إما $P/2$ أو $P/3$ في الحلقة $Z[\sqrt{-5}]$ فـإذا كان $P/2$ ، أي أن $2 = d.P$ ، وبأخذ :

$$\left|a + b\sqrt{-5}\right| = a^2 + 5b^2$$

وباستخدام العلاقة $|a.b| = |a| . |b|$ حيث b,a مـن $Z[\sqrt{-5}]$ ، ومـن العلاقـة $2 = d.P$ ، يكون لدينا :

$4 = |2| = |d| . |P| = 6 |d|$

وهذا غير ممكن . بالطريقة نفسها نجد أن $P/3$ غير ممكن أيضاً . إذن P عدد غير أولي .

25- أثبت أن الحقل $(F,+,\cdot)$ هو حلقة إقليدية .

الحل :

إن $(F,+,\cdot)$ حلقة تامة ، كما ويمكن إيجاد دالة إقليدية من الشكل $d : F^* \longrightarrow N$ معرّفة بالشكل : $d(x) = 1 \; ; x \in F^*$ عندها يتحقق ما يلي :

1- $d(x) \geq 0$ ، لكل x من F^* .

2- لكل x,y من F^* ، فإن $x.y \neq 0$ ، ويكون $d(x) = 1 = d\,(x.y)$.

3- إذا كان $a,b \in F$ ، وكان $b \neq 0$ ، فإن $a = (a.b^{-1})\, b + 0$.

إذن $(F,+,\cdot)$ حلقة إقليدية .

26- لتكن الحلقة $(Z[\sqrt{3}],+,\cdot)$ ، أثبت أنها تشكل حلقة إقليدية .

الحل :

إن الحلقة $R = (Z[\sqrt{3}],+,\cdot)$ حلقة تامة . الدالة الإقليدية : $d : R^* \longrightarrow N$ المعرفة بالشكل : $d\,(a + b\sqrt{3}\,) = |a^2 - 3b^2|$ حيث $x = a + b\sqrt{3} \in R^*$ تحقق الشروط التالية :

(1) $d(x) \geq 0$ لكل $x \in R^*$

(2) لكل $x,y \in R^*$ يكون لدينا :

$$d(x) = d(x).1 \leq d(x).d(y) = d(x.y)$$

(3) إذا كان y,x من R ، $y \neq 0$ فإن $\frac{x}{y} \in Q$ ويكون لدينا $\frac{x}{y} = c + d\sqrt{3}$ ،

لكل d,c من Q . لنختر الأعداد بحيث يتحقق $|c-a| \leq \frac{1}{2}$ و $|d-b| \leq \frac{1}{2}$ ، عندها يكون :

$$\frac{x}{y} = c + d\sqrt{3} = a + b\sqrt{3} + \left[(c-a) + (d-b)\sqrt{3}\,\right]$$

أو :

$$x = (c + d\sqrt{3}\,).y = (a + b\sqrt{3}\,).y + \left[(c\text{-}a) + (d\text{-}b)\sqrt{3}\,\right].y$$
$$= q.y + r$$

حيث أن :

$$q = a + b\sqrt{3} \quad , \quad r = \left[(c\text{-}a) + (d\text{-}b)\ \sqrt{3}\,\right].y$$
$$d(r) = d\left(\left[(c\text{-}a) + (d\text{-}b)\ \sqrt{3}\,\right].y\right)$$
$$= d\left(\left[(c\text{-}a) + (d\text{-}b)\ \sqrt{3}\,\right].d(y)\right.$$
$$= \left|(c-a)^2 - 3(d-b)^2\right|.dy \le \left|\frac{1}{4} - \frac{3}{4}\right|.dy$$
$$= \frac{1}{2}d(y) < dy$$

نستنتج مما سبق أن $(Z[\sqrt{3}],+,.)$ حلقة إقليدية .

<u>27-</u> أثبت أن العدد الأولي P في Z أولي في الحلقة $(Z(i),+,.)$.

الحل :

نفرض العكس ، نفرض أن $P = P_1.P_2 \dots P_n$ ، وهو تحليل وحيد للعدد P ، على شكل عدد منته من الأعداد الأولية P_i ، حيث $1 \le i \le n$ ، ويكــون $d(P_i) > 1$ ، وبالتالي فإن :

$$P^2 = d(P) = d(P_1)\ .\ d(P_2)\ \dots\dots\ d(P_n)$$

وبما أن Z حلقة تحليل وحيد، ينتج أن $n = 2$ و $P=P_1.P_2$ و $P = d(P_1) = d(P_2)$.

وإذا كان $P_1 = a + i\,b$ ، فإن :

$$P = d(P_1) = a^2 + b^2 = (a + i\,b)\,(a - i\,b) \Rightarrow P_2 = a - i\,b$$

وإذا كان العدد الأولي $P \in Z$ يتحلل في $Z(i)$ ، يكون لدينا :

$$P = (a + i\,b)\,(a - i\,b) = a^2 + b^2$$

حيث أن $a + i\,b$ و $a - i\,b$ أعداد أولية في $Z(i)$، فمثلاً العدد $2 = (1+i)(1-i)$ غير أولي في الحلقة $Z(i)$.

-28 إذا كان a عنصر ما من الحلقة $(R,+,\cdot)$ ، أثبت أنه إذا كان a عنصراً ليس معدوم القوى في R، فإنه يوجد في الحلقة R مثالية أولية لا تحوي العنصر a.

الحل :

لنأخذ المجموعة التالية :

$$M = \{\, I \;:\; \text{مثالية في } R \; I \;;\; a^n \notin I \;;\; \forall n \in N \}$$

نلاحظ أن : $M \neq \phi$ لأن $\{0\} \in M$ ، 0 هو صفر الحلقة $(R,+,\cdot)$ كما أن M مرتبة جزئياً بالنسبة لعلاقة الاحتواء ، لأنه إذا كانت M_0 مجموعة جزئية من M وغير خالية ومرتبة كلياً ، فيكون $\bigcup_{A \in M_0} A$ مثالية في R ، ويمثل حداً أعلى للمجموعة M_0 في M ، وحسب تمهيدية زورن ، يوجد في M عنصراً أعظمياً وليكن L ، وبالتالي ، فإن : L مثالية في الحلقة R ، كما أن $a^n \notin L$ لكل $n \in N$ ، أي أن $a \notin L$.

لنبرهن الآن أن المثالية L أولية في R .

إذا كان y,x عنصرين ما من R بحيث $x.y \in L$ ، ولنفرض جدلاً أن كلاً من $y,x \notin L$ ، عندها يكون :

$$J = L + x.R \;,\; K = L + y.R$$

مثالية في R ، وأن $L \not\subset K$ و $L \not\subset J$ ، وبما أن للمثالية L عنصر أعظمي في M، فإن $J,K \notin M$ ، وحسب تعريف المجموعة M يوجد $n,m \in N$ بحيث $a^n \in K$ و $a^m \in J$ ، وبالتالي يوجد r_1 , r_2 من R و $m_1,m_2 \in L$ بحيث يكون :

$$a^m = m_2 + y.r_2 \;,\; a^n = m_1 + x.r_1$$

$$a^{n+m} = a^n.a^m = m_1\, m_2 + m_1\, y.r_2 + x.r_1.m_2 + x.y.r_1.r_2 \in L$$

وهذا يناقض كون $L \in M$.

نستنتج مما سبق أنه إما $x\in L$ أو $y\in L$ ، إذن المثالية L أولية في R ، وأن $a\notin L$.

29- أثبت أن الشرط اللازم والكافي لكي يكون العنصر x غير المعدوم من الحلقة التامة $(R,+,.)$ أولياً، هو أن تكون المثالية $x.R$ أولية في R .

الحل :

لنفرض أولاً أن العنصر x أولي في الحلقة R ، لنبرهن أن المثالية $x.R$ أولية في R ، بما أن x أولي في R ، عندئذٍ $x.R \neq R$ لأن x عنصر غير قابل للعكس في R . إذا كان b,a عنصرين ما من الحلقة R وبحيث $a.b\in x.R$ ، عندئذٍ يوجد r من R بحيث يكون $a.b = x.r$ أي أن x يقسم a.b . وحسب الفرض إما x يقسم a أو x يقسم b ، ولنفرض أن x لا يقسم b ، وهذا يعني أن x يقسم a وبالتالي يوجد عنصرا وليكن c من R بحيث يكون $a = c.x$. إذن $a\in x.R$ ومنه المثالية $x.R$ أولية في الحلقة $(R,+,.)$.

لنبرهن على العكس ، أي لنبرهن أن العنصر x من R أولي .

لنفرض أن المثالية $x.R$ أولية في R ، وهذا يؤدي إلى أن x غير قابل للعكس في R ، لأن $x.R \neq R$ ، ليكن $a,b\in R$ حيث أن x يقسم الجداء a.b ، وبالتالي يوجد d من R يحقق :

$$a.b = x.d\in x.R$$

وبما أن المثالية $x.R$ أولية ، فإن $a\in x.R$ أو $b\in x.R$ ، وبفرض أن $a\notin x.R$ ، فإن $b\in x.R$. وبالتالي يوجد $e\in R$ حيث $b = x.e$ ، أي أن x قاسم للعنصر b في R .

نستنتج مما سبق أن العنصر x أولي في الحلقة R .

6- تمارين غير محلولة للفصل الثالث

1- ليكن φ تشاكلاً ما لحلقة $(R,+,.)$ على حلقة ما $(S,T,\star)$ ، عندئـذٍ يوجـد تقابل بين مجموعة كل المثاليات في الحلقة $(S,T,\star)$ ومجموعة كل المثاليـات ، التي تحوي كل منها $\text{Ker}\,\varphi$ ، في الحلقة $(R,+,.)$.

2- بيّن فيما إذا كان التطبيق المعرف من حلقة الأعداد الصحيحة Z إلى حلقـة الأعداد الزوجية الصحيحة E ليس تشاكلاً .

3- لتكن $(R,+,.)$ و $(S,+,.)$ حلقتين ما ، وإذا كان $\varphi : R \longrightarrow S$ تشاكلاً وإذا كانت I مثالية يسارية (يمينية) في الحلقة R ، وكان φ شاملاً ، فإن $\varphi(I)$ مثاليـة يسارية (يمينية) في الحلقة $(S,+,.)$.

وإذا كانت J مثالية يسارية (يمينية) في الحلقة S ، فـإن $\varphi^{-1}(J)$ مثاليـة يسـارية (يمينية) في الحلقة $(R,+,.)$.

4- أثبت أن $\varphi : Z \longrightarrow R$ المعرف بالشكل $\varphi(n) = n.1$ ، حيث n من Z هو تشاكل حلقي.

5- حقّق المبرهنة الثالثة لتماثل الحلقات ، علماً أن $R = (Z,+,.)$ حلقة الأعداد الصحيحة ، والمثاليات $I = 6Z$ و $J = 2Z$.

6- لتكن A مجموعة تتألف من عنصـر واحـد فقـط ، أثبـت أن التطبيـق $\varphi : P(A) \longrightarrow Z_2$ والمعرف بالشكل $\varphi(\Phi) = \bar{o}$ و $\varphi(A) = \bar{1}$ هو تشـاكل حلقي بين الحلقتين $(P(A),\Delta,\cap)$ و $(Z_2,\oplus,\otimes)$.

7- لتكن $R = (M_2(R),+,.)$ حلقة المصفوفات المربعة الحقيقية من الدرجـة الثانية ، والتي لها الشكل :

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a, b \in R \right\}$$

ولتكن C حلقة الأعداد المركبة . أثبـت أن التطبيـق $\varphi : C \longrightarrow R$ والمعـرف

بالشكل : $\varphi(a+ib)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ ، يشكل تماثلاً حلقياً .

8- إذا كان φ تشاكلاً شاملاً من الحلقة $(R,+,\cdot)$ في الحلقة $(S,+,\cdot)$ ، ولتكن I مثالية في R ، وإذا كانت J مثالية في R ، أثبت أن $R/\varphi^{-1}(J)\cong S/J$.

وإذا كان $B \le S$ ، فإن :

$$\varphi^{-1}(B)/\mathrm{Ker}\varphi \cong B$$

9- لتكن $(R,+,\cdot)$ حلقة مثاليات رئيسة ، وإذا كان العنصر a من R أولياً مع كلٍ من العنصرين c,b من R ، أثبت أن a أولي مع b.c .

10- مستفيداً من عملية التقسيم الإقليدي أوجد القاسم المشترك الأعظم d للعددين 118 و26، ثم أوجد العددين n,m، اللذين يحققان العلاقة : $d = 26\,m + 118\,n$.

11- اكتب العدد 1 كتركيب خطي للعددين الأوليين معاً 8 و27 .

12- بفرض أن d هو القاسم المشترك الأعظم للعددين k,n وm هو المضاعف المشترك الأصغر للعددين n,k ، وإذا كانت $(Z,+,\cdot)$ حلقة المثاليات الرئيسة ، أثبت أن :

$$nZ \cap kZ = mZ$$
$$nZ + kZ = dZ$$

تطبيق : أوجد

$$8Z \cap 6Z \ , \ 3Z \cap 2Z$$
$$8Z + 6Z \ , \ 3Z + 2Z$$

13- إذا كانت $(R,+,\cdot)$ حلقة إبدالية واحدية ، وإذا كانت $R \neq I$ مثالية ، أثبت أن المثالية الأعظمية I هي مثالية أولية في الحلقة R .

14- أثبت أن التطبيق المعرف بالشكل التالي :

$$\varphi : R \longrightarrow F$$
$$\varphi(a)=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

هو تماثل من حلقة الأعداد الحقيقية $(R,+\ \cdot)$ إلى حلقة المصفوفات

$\left(F = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, +, \cdot\right)$.

15- بفرض أن $(R,+,\cdot)$ حلقة تامة ، ولنرمز لصفرها بـ 0 ، وإذا كان $a \neq 0$ عنصراً ما من R ، أثبت أن الشرط اللازم والكافي لكي تكون المثالية (a) مثالية أولية في الحلقة $(R,+,\cdot)$ هو أن يكون العنصر a غير قابل للتحليل في R أو قابلاً للعكس .

16- لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت I مثالية يسارية في R بحيث $R \neq I$ ، أثبت أنه يوجد في الحلقة $(R,+,\cdot)$ مثالية يسارية أعظمية تحوي I .

17- إذا كانت $(R,+,\cdot)$ حلقة ما ، لا تحوي مثاليات معدومة القوى مغايرة للصفر ، وإذا كان e عنصر جامد مغاير للصفر في الحلقة R . أثبت أن الشروط التالية متكافئة :

(1) المثالية اليسارية $R.e$ أصغرية في الحلقة R .

(2) المثالية اليمينية $e.R$ أصغرية في الحلقة R .

18- إذا كانت $(R,+,\cdot)$ حلقة إقليدية ، وليكن $a \neq 0$ و $b \neq 0$ عنصرين من R حيث 0 صفر الحلقة R، ولنفرض أن b غير قابل للعكس في R . أثبت أن $d(a) < d(a.b)$.

19- لتكن $(Z_6,\oplus,\otimes)$ حلقة ، وإذا كان $P = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}\}$.

أثبت أن P مثالية في Z_6 ، وأنها أولية . وإذا كانت $(Z_8,\oplus,\otimes)$ ، وإذا كانت $I = \langle 4 \rangle$. أثبت أن I مثالية في R ، ولكنها ليست أولية .

20- إذا كانت $(2Z,+,\cdot)$ حلقة ، وليكن $I = \langle 4 \rangle$ ، أثبت أن I مثالية أعظمية في $2Z$ ، ولكنها ليست أولية .

21- لتكن $(R,+,\cdot)$ حلقة تامة ، عندها العبارات التالية متكافئة من أجل c,b,a من R :

(1) $a|b$ و $b|a$.

(2) $a = u.b$ ، حيث u عنصر وحدة في R .

(3) $<b> = <a>$.

22- لتكن $(Z(i),+,\cdot)$ حلقة غاوص الصحيحة ، أوجد عناصر الوحدة والعناصر المترادفة في هذه الحلقة .

23- أثبت أن العنصر $P = 1 + i$ غير قابل للتحليل في الحلقة $(Z(i),+,\cdot)$.

24- لتكن الحلقة $(Z[\sqrt{-5}],+,\cdot)$ ، برهن أن العنصر $P = 1+\sqrt{-5}$ غير قابل للتحليل في الحلقة $(Z[\sqrt{-3}],+,\cdot)$.

25- إذا كانت $(R,+,\cdot)$ حلقة تامة، وإذا كانت $P \neq 0$ عنصر منها، وليس عنصر وحدة فيها، أثبت أن العبارات التالية متكافئة :

(1) P عنصر غير قابل للتحليل .

(2) إذا كان $d|P$ ، إما $d \sim 1$ أو $d \sim P$ ($\sim$ علاقة ترادف) .

(3) إذا كان $P = a.b$ في R ، فإنه إما $P \sim a$ أو $P \sim b$.

(4) إذا كان $P \sim a.b$ في $P \sim a$ ، فإن $P \sim a$ أو $P \sim b$.

26- بيّن فيما إذا كانت الحلقة $(Z[\sqrt{-5}],+,\cdot)$ حلقة تحليل وحيد .

27- أثبت أن حلقة أعداد غوص الصحيحة $(Z(i),+,\cdot)$ تشكل حلقة إقليدية .

إرشاد للحل : خذ الدالة الإقليدية : $d : Z^*(i) \longrightarrow N$ المعرفة بالشكل :

$$d(x) = a^2 + b^2 \; ; \; x \in Z^*(i)$$

28- من المعلوم أن $Q(\sqrt{5}) = \{a + b\sqrt{5} \; ; \; a, b \in Q\}$ تشكل حقلاً ، بالنسبة للعمليتين $(+)$ و$(\cdot)$ العاديتين ، المطلوب أثبت أن $Q(\sqrt{2}) \neq Q(\sqrt{5})$.

29- إذا كان $(F,+,\cdot)$ حقلاً ما ، أثبت أن رتب جميع العناصر غير الصفرية في الزمرة $(F,+)$ متساوية .

30- حدّد مميز الحقول التالية : Q , R , C , Z_2 , Z_3 .

31- نذكر بأن المثالية I في الحلقة $(R,+,\cdot)$ يكون خاصاً ، إذا كان مختلفاً عن

$\{0\}$ وعن R، أثبت أن أي حقل لا يحوي مثاليات خاصة .

ثم أثبت أن الشرط اللازم والكافي لتكون الحلقة الواحدية الإبدالية $(R,+,\cdot)$ حقلاً ، هو ألاّ تملك مثاليات خاصة .

-32 أثبت أن المجموعة : $F = \{a + b\sqrt{13}\ ;\ a, b \in Q\} = Q(\sqrt{13})$ تشكّل حقلاً جزئياً من الحقل $(R,+,\cdot)$.

-33 إذا كان $(F,+,\cdot)$ حقلاً مميزه P حيث P عدد أولي ، أثبت أن التطبيق الذي يقابل العنصر $a \in F$ بالعنصر $a^P \in F$ هو تشاكل .

-34 لتكن F هي مجموعات المصفوفات من $M_2(R)$، لها الشكل: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\ ;\ a, b \in R$ ، أثبت أن $(F,+,\cdot)$ تشكل حقلاً .

-35 لتكن الحلقتان $R = (2Z,+,\cdot)$ و $R' = (3Z,+,\cdot)$ (أي أن R تتكون من كل مضاعفات العدد 2 ، وتتكون R' من كل مضاعفات 3) ، بيِّن أن R ليست متشاكلة تقابلياً مع R' .

-36 نقول عن العنصر $b \in R$ إنه مشارك لـ $a \in R$ ، إذا كان $b = u.a$ ، من أجل عنصر وحدة u من R ، حيث $(R,+,\cdot)$ ، حلقة ، المطلوب أوجد العناصر المشاركة للعدد 4 في الحلقة Z_{10}. ثم أوجد العناصر المشاركة للعدد 5 في الحلقة Z_{10} .

عبّر عن العدد 12 في الحلقة $(Z,+,\cdot)$ ، كجداء لعناصر غير قابلة للتحليل .

-37 بفرض أن $\varphi : F \longrightarrow F'$ تشاكلاً من حقل F إلى حقل F' ، بيِّن أن φ تطبيق متباين .

-38 أثبت أن العدد الأولي P في Z يكون أولياً في الحلقة $(Z(i),+,\cdot)$، إذا، وفقط إذا ، $P = 4k - 1$.

-39 ليكن العنصر u من الحلقة $(Z,+,\cdot)$. أثبت أن العنصر u يمكن كتابته على شكل مجموع مربعي عددين b,a من Z ، إذا ، وفقط إذا ، أمكن تحليل u إلى

جداء أعداد أولية يكون كل عدد بسيط $P = 4k - 1$ على شكل قوى زوجية .

40- لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت $M \neq R$ مثالية في الحلقة R . أثبت أن الشرط اللازم والكافي لكي تكون المثالية M أعظمية في R هو أن يتحقق الشرط التالي :

$$\forall m \in M \Rightarrow \exists\, x \in R : 1 - x.m \in M$$

41- إذا كانت $(R,+,\cdot)$ حلقة ما ، أثبت صحة ما يلي :

(1) $J(R)$ مثالية يسارية (يمينية) صغير في الحلقة R .

(2) الشرط اللازم والكافي كي تكون المثالية اليسارية N في R صغيراً في R هو أن يكون : $N \subseteq J(R)$.

(3) إذا كانت I مثالية يسارية (يمينية) صغيراً في الحلقة $(R,+,\cdot)$ و J مثالية يسارية (يمينية) في الحلقة R حيث $J \subseteq I$ ، فإن J تكون صغيراً في الحلقة R .

تمارين محلولة وغير محلولة للفصل الرابع :

حلقة كثيرات الحدود

Ring of polynomials

7- تمرينات محلولة للفصل الرابع

- حلقة كثيرات الحدود -

(1) بفرض أن :

$$f(x) = 2x^3 + x^2 + 2x + 2 \in Z_3[x]$$
$$g(x) = 2x^2 + 2x + 1 \in Z_3[x]$$

أوجد : $f(x) + g(x)$, $f(x).g(x)$.

الحل :

$$f(x) + g(x) = (2 + o)\,x^3 + (1 + 2)\,x^2 + (2 + 2)\,x + (2 + 1)$$
$$= 2x^3 + o.x^2 + 1.x + o = 2x^3 + x \in Z_3[x]$$
$$f(x)\bullet g(x) = x^5 + o.x^4 + 2x^3 + o.x^2 + o.x + 2$$
$$= x^5 + 2x^3 + 2$$

(2) أوجد ناتج قسمة كثيرة الحدود $f(x) = 3x^4 + x^3 + 2x^2 + 1 \in Z_5[x]$ على كثيرة الحدود : $g(x) = x^2 + 4x + 2 \in Z_5[x]$ في $Z_5[x]$ ، ثم أوجد باقي القسمة .

$$\begin{array}{r|l}
 & 3x^2 + 4x \\ \hline
x^2 + 4x + 2 & 3x^4 + x^3 + 2x^2 + 1 \\
 & 3x^4 + 2x^3 + x^2 \\ \cline{2-2}
 & \quad 4x^3 + x^2 + 1 \\
 & \quad 4x^3 + x^2 + 3x \\ \cline{2-2}
 & \qquad\qquad 2x + 1
\end{array}$$

نلاحظ من عملية القسمة السابقة، أن ناتج القسمة $f(x)/g(x)$ هو $3x^2 + 4x$ والباقي هو $2x + 1$، وذلك في الحلقة $Z_5[x]$.

إذن :

$$3x^4 + x^3 + 2x^2 + 1 = (x^2 + 4x + 2)\,(3x^2 + 4x) + 2x + 1$$

(3) في الحلقة $Z_3[x]$ ، أثبت أن : $x^4 + x$ و $x^2 + x$ تحدد نفس الدالة من Z_3 إلى Z_3 .

الحل :

لنضع : $f(x) = x^4 + x$, $g(x) = x^2 + x$ ، عندها يكون لدينا :

$$f(o) = o = g(o) , f(1) = 2 = g(1) , f(2) = o = g(2)$$

وذلك في الحلقة $Z_3[x]$.

(4) إذا كانت $(R,+,.)$ حلقة بمحايد ، ولتكن $x = (0,1,0,...)$ كثيرة حـدود ، أثبت ما يلي :

1- $x^n = (0,...,1,0,...)$ (أي الحد الذي ترتيبه $n + 1$ في كثيرة الحدود x^n يساوي الواحد وجميع الحدود الأخرى تساوي الصفر) .

2- إذا كانت $(S,+,.)$ حلقة كثيرات الحدود على الحلقة R ، فإن أي عنصـر $f \in S$ ، حيث : $f = (a_0,a_1,...,a_n,0,...)$ ، يكتب بالشكل :

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

الحل :

1- بطريقة الاستنتاج الرياضي على n نبرهن :

إذا كان $n = 1$ ، فإن $x^1 = x = (0,1,0,...,)$ ، حسب الفرض العلاقة محققة .

لنفرض الآن أن العلاقة محققة من أجل $n = m$ ، ولنبرهن على صحتها من أجـل $m + 1$.

لدينا $x^m = (0,0,...,1,0,...,)$ ، وبما أن :

$$\begin{aligned} x^{m+1} = x^m . x &= (0,0,...,1,0,...,)\,(0,1,0,....) \\ &= (0,0,...,0,1,0,...) \end{aligned}$$

أي أن الحد الذي ترتيب موضعه $m + 2$ في كثيرة الحدود يسـاوي 1 ، وجميـع الحدود الأخرى تساوي الصفر ، وبالتالي فالعلاقة محققة من أجـل $n = m + 1$ ،

وبالتالي فهي صحيحة لجميع عناصر n من Z^+ .

2- لتكن $f = (a_0, a_1, \ldots .) \in S$ ، وبالتالي يكون :

$$\begin{aligned}
f &= (a_0, a_1, \ldots .) \\
&= (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, 0, \ldots, a_n, 0, \ldots .) \\
&= (a_0, 0, ..) (1, 0, \ldots) + (0, a_1, 0, \ldots) (0, 1, 0, \ldots) + \ldots + \\
&\qquad + (0, 0, \ldots, a_n, 0, \ldots .) (0, 0, .., 1, 0, \ldots) \\
&= a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i
\end{aligned}$$

<u>(5)</u> ضع إشارة (✓) أمام العبارة الصحيحة وإشارة (×) أمام العبارة الخاطئة في الجمل التالية :

1- كثيرة الحدود $(x - 2)$ غير قابلة للتحليل على الحلقة Q (✓)

2- كثيرة الحدود $(x^2 - 3)$ غير قابلة للتحليل على الحلقة Q (✓)

3- كثيرة الحدود $(x^2 + 3)$ غير قابلة للتحليل على الحلقة Z_7 (×)

4- كثيرة الحدود $f(x)$ من الدرجة n بمعاملات من الحقل $(F,+,\cdot)$ تحتوي على الأكثر n جذراً في الحقل F (✓)

5- كل كثيرة حدود $f(x)$ من الدرجة الأولى في الحلقة $(F[x],+,\cdot)$ يكون لها جذر واحد على الأقل في F (✓)

6- كثيرة الحدود $a_n x^n + \ldots + a_1 x + a_0 \in R[x]$ تساوي الصفر، إذا وفقط، إذا كانت $a_i = 0$ ، لكل $i = 0,1,2,\ldots,n$ (✓)

7- إذا كانت $(R,+,\cdot)$ حلقة إبدالية، فإن $(R[x],+,\cdot)$ حلقة إبدالية أيضاً (✓)

8- إذا كانت $(R,+,\cdot)$ حلقة تامة، فإن $(R[x],+,\cdot)$ حلقة تامة (✓)

9- إذا حوت الحلقة $(R,+,\cdot)$ قواسم للصفر، فإن الحلقة $(R[x],+,\cdot)$ تحوي قواسم للصفر (✓)

10- إذا كانت f و g كثيرتي حدود من $R[x]$ ، ودرجة $f(x)$ تساوي 3 ودرجة

$g(x)$ تساوي 4 ، فإن كثيرة الحدود $f(x).g(x)$ من الدرجة 8 في $R[x]$ $(\times)$

11- إذا كان E حقلاً جزئياً من الحقل $(F,+,.)$، وكان α جذراً لكثيرة الحدود $f(x)$ في $E[x]$، عندئذٍ يكون α جذراً لـ $h(x) = f(x).g(x)$ لكل $g(x)\in E[x]$

$(\checkmark)$

12- ليكن $(F,+,.)$ حقلاً، عندئذٍ عنصر الوحدة في $F[x]$ هو عنصر الوحدة في F $(\checkmark)$

13- إذا كانت $(R,+,.)$ حلقة ، عندئذٍ قواسم للصفر في الحلقة $R[x]$ هي قواسم للصفر في R $(\times)$

(6) أثبت أن $\deg\big(f(x).g(x)\big) < \deg f(x) + \deg g(x)$ ، حيث أن :

$$f(x) = 3x^2 + 2 \ , \ g(x) = 2x + 3$$

وذلك في الحلقة $(Z_6[x],+,.)$.

الحل :

لدينا أولاً :

$$f(x) . g(x) = (3x^2 + 2)(2x + 3) = 6x^3 + 9x^2 + 4x + 6$$
$$= 3x^2 + 4x$$

وبالتالي فإن :

$$\deg\big(f(x).g(x)\big) = 2 < \deg f(x) + \deg g(x) = 2 + 1 = 3$$

(7) لتكن الحلقة $(Q[x],+,.)$ ، أوجد القاسم المشترك الأعظم $d(x)$ لكثيرتي الحدود :

$$f(x) = x^4 - x^2 + x - 1 \ , \ g(x) = x^3 - x^2 + x - 1$$

في $Q[x]$ ، ثم عبّر عنه كتركيب خطي لـ $f(x)$ و $g(x)$.

الحل :

باستخدام خوارزمية القسمة نجد :

$$f(x) = (x + 1)\, g(x) + (-x^2 + x)$$

$$g(x) = (-x)\,(-x^2 + x) + (x - 1)$$

$$-x^2 + x = (-x)\,(x - 1) + o$$

إذاً : $d(x) = x - 1$ (القاسم المشترك الأعظم لــ $f(x)$ و $g(x)$) . إن :

$$\begin{aligned} x - 1 &= g(x) + x\,(-x^2 + x) \\ &= g(x) + \left[f(x) - (x + 1)\, g(x)\right] \\ &= x\, f(x) - (x^2 + x + 1)\, g(x) \end{aligned}$$

(8) إذا كانت $(R,+,.)$ حلقة تامة ، وليكن $f = \sum_{i=0}^{t} a_i.x^i\ ,\ g = \sum_{j=0}^{m} b_j.x^j$ كثيرتي حدود ابتدائيتين في $R[x]$ ، المطلوب :

أثبت أن $f.g$ كثيرة حدود ابتدائية في $R[x]$.

الحل :

نفرض العكس ، أي نفرض أن $f.g$ كثيرة حدود غير ابتدائية ، وهذا يؤدي إلى وجود عنصر وليكن p من R غير قابل للتحليل في R ، وبحيث يكون P يقسم جميع معاملات $f.g$ في R . ولنبرهن أن هذا لا يمكن .

بما أن f و g كثيرتي حدود ابتدائيتان في $R[x]$ ، فإن P لا يمكن أن يقسم جميع معاملات f في R، وكذلك P لا يمكن أن يقسم جميع معاملات g في R .

لنفرض أن a_S هو أول معاملات f الذي لا يقبل القسمة على P ، حيث $0 \le s \le t$، ولنفرض أن b_q هو أول معاملات g الذي لا يقبل القسمة على P ، حيث $0 \le q \le m$. وبما أن $f.g = \sum_{n=0}^{t+m} r_n.x^n$ ، حيث أن :

$$r_n = \sum_{i+j=n} a_i.b_j\ ,\ r_{S+q} = \sum_{i+j=S+q} a_i.b_j\ ;\ n = 0,1,2,\ldots,t+m$$

وبما أن P يقسم r_{s+q} ، ويقسم أيضاً ، جميع حدود الطرف الأيمن ، تي تختلف عن الحد $a_s.b_q$ في R ، فإنه يجب أن يقسم $a_s.b_q$ في R ، وبالتالي فإن P يجب أن يقسم أحد العنصرين a_s وb_q، على الأقل ، في R ، وهذا مخالف للفرض أن a_s

وb_q لا يقبلان القسمة على P في R . إذن f.g كثيرة حدود ابتدائية في R[x] .

(9) اكتب كثيرة الحدود التالية $(x+1)^2$ في الحلقة $(Z_2[x],+,.)$. ثم احسب $(x+1)+(x+1)$ في نفس الحلقة .

الحل :

$$(x+1)^2 = (x+1)(x+1) = x^2 + (1+1).x + 1 = x^2 + 1$$

$$(x+1) + (x+1) = (1+1)x + (1+1) = 0.x + 0 = 0$$

(10) ليكن التشاكل الحلقي : $\Phi_2 : Q[x] \longrightarrow R$ المعرف بالشكل التالي :

$$\Phi_2 (a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1 .2 + \ldots + a_n .2^n$$

المطلوب ، أوجد $\Phi_2 (x^2 + x - 6)$ وماذا تستنتج .

الحل :

نلاحظ أولاً : $\Phi_2 (x^2 + x - 6) = 2^2 + 2 - 6 = 0$

وهذا يعني أن $x^2 + x - 6$ هي نواة التطبيق Φ_2 .

بالطبع :

$$x^2 + x - 6 = (x-2)(x+3)$$

وبالتالي ، وبسبب أن $\Phi_2 (x^2 + x - 6) = 0$ ، يكون لدينا :

$$\Phi_2 (x-2) = 2 - 2 = 0$$

(11) إذا كانت $(R[x],+,.)$ حلقة كثيرات الحدود على الحلقة $(R,+,.)$ ، وبالتالي يمكن غمر الحلقة R في R[x] ، أي أنه توجد حلقة جزئية $(R_1[x],+,.)$ في الحلقة $(R[x],+,.)$ ، ويكون $R \cong R_1$.

الحل :

إن $R_1[x] = \{(a,0,\ldots) ; a \in R\}$ ، كما أن :

$$f - g = (a-b, 0, \ldots) \in R_1$$

$$f \cdot g = (a.b, 0, \ldots) \in R_1$$

لكل $f=(a,0,\dots)$ و $g=(b,0,\dots)$ ، إذن $R_1[x] \le R[x]$.

لنثبت الآن أن $R \cong R_1$ ، من أجل ذلك نعرّف التطبيق : $\varphi : R \longrightarrow R_1$ بالشكل الآتي : $\varphi(a)=(a,0,\dots)$ ، لكل a من R .

بما أن :

$$(1) \quad \varphi(a+b)=(a+b,0,\dots.)=(a,0,\dots)+(b,0,\dots.) \\ =\varphi(a)+\varphi(b)$$

$$(2) \quad \varphi(a\,.\,b)=(a.b,0,\dots.)=(a,0,\dots)\,.\,(b,0,\dots.) \\ =\varphi(a)\,.\,\varphi(b)$$

نستنتج من (1) و(2) ولكل b,a من R إن φ تشاكل حلقي من الحلقة R إلى الحلقة $(R_1[x],+,\cdot)$، لنثبت أن φ شامل . من أجل كل عنصر $(a,0,\dots)$ مـــن $R_1[x]$ ، يوجد عنصر a من R ، بحيث يتحقق : $\varphi(a)=(a,0,\dots)$ وهذا يعني أن التطبيق φ شامل .

أخيراً لنثبت أن φ متباين ، لنفرض أن : $\varphi(b,0,\dots) = \varphi(a,0,\dots)$ وبالتـــالي ، يكون : $(a,0,\dots)=(b,0,\dots)$ ، وهذا يعطي $a=b$ ، إذن التطبيق φ متباين .

نستنتج مما سبق أن φ تماثل بين الحلقتين R و$R_1[x]$. أي $R \cong R_1$.

(12) أثبت أن كثيرة الحدود $P_2(x)=x^2-3 \in Q[x]$ غير قابلة للتحليل على الحلقة $(Q,+,\cdot)$.

الحل :

لنفرض العكس ، أي لنفرض أن $P_2(x)$ قابلة للتحليل على $(Q,+,\cdot)$ ، وهذا يعنـــي أنه بالإمكان إيجاد عددين b,a من Q بحيث يكـــون : $a.b=-3$ و $a+b=0$ ، بحل جملة المعادلتين السابقتين نجد $a^2=3$ أي $a=\pm\sqrt{3}$ ، وهذا لا يمكن ، لأن $a=\sqrt{3}\notin Q$.

إذن كثيرة الحدود x^3-3 غير قابلة للتحليل على الحلقة $(Q,+,\cdot)$.

(13) بيّن أي من كثيرات الحدود التالية بدائية :

$f(x)=15x^3+51x^2+9 \in Q[x]$

$$g(x) = 15x^3 + 6x^2 + 10 \in Q[x]$$
$$h(x) = 5x^4 + 25x^2 + 10x - 57 \in Q[x]$$

الحل :

بما أن $c(f) = 3$ ، فإن كثيرة الحدود $f(x)$ غير بدائية .

لكن $c(g) = 1$ ، فإن كثيرة الحدود $g(x)$ بدائية .

كما أن $c(h) = 1$ ، وبالتالي فإن $h(x)$ بدائية .

(14) لتكن كثيرة الحدود $P_4(x) = x^4 - 3x^2 + 2x + 1 \in Q[x]$ ، المطلوب بيّن هل يمكن تحليل كثيرة الحدود $P_4(x)$ إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل على الحلقة $(Q,+,.)$.

الحل :

لنكتب أولاً :

$$\begin{aligned} P_4(x) &= x^4 - 3x^2 + 2x + 1 \\ &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + a.c)x^2 + (bc + ad)x + b.d \end{aligned}$$

وبالمطابقة يكون لدينا :

$$b.d = 1 \;,\; bc + ad = 2 \;,\; a + c = 0 \;,\; b + d + ac = -3$$

بحل جملة المعادلات السابقة نجد أن :

$$b = d = \pm 1 \;,\; b\,(a + c) = 2$$

أي أن $a + c = \pm 2$ ، وهذا يناقض الفرض أن $a + c = 0$. إذن كثيرة الحدود ، $P_4[x]$ غير قابلة للتحليل على $(Q_4,+,.)$.

(15) أوجد جذور كثيرة الحدود $P_2(x) = x^2 - 2x - 3$ في الحلقة $(Z_5[x],+,.)$.

الحل :

بما أن $P_2(3) = P_2(4) = 0$ ، فإن $3,4 \in Z_5[x]$ جذور لكثيرة الحدود $P_2(x)$ على $Z_5[x]$.

(16) أثبت أن كثيرة الحدود $f(x)$ التالية : $f(x) = x^3 + 3x^2 + x + 2$

غير قابلة للتحليل على الحلقة $(Z_5[x],+,\cdot)$.

الحل :

نعلم أن $Z_5 = \{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \}$ ، وبما أن :

$$f(\overline{0}) = 2 \text{ , } f(\overline{1}) = 2 \text{ , } f(\overline{2}) = 4 \text{ , } f(\overline{3}) = 4 \text{ , } f(\overline{4}) = 4$$

فإن كثيرة الحدود لا تملك جذوراً في الحلقة $(Z_5[x],+,\cdot)$ ، وهذا يعني أن $f(x)$ غير قابلة للتحليل على Z_5 .

(17) أثبت أن $(Q[x]/<f>,+,\cdot)$ تشكل حقلاً ، حيث أن :

$$f(x) = x^2 - 71 \in Q[x]$$

الحل :

بما أن جذور كثيرة الحدود $f(x)$ هي $x = \pm\sqrt{71}$ ، وأن درجة كثيرة الحدود $f(x)$ هي من الدرجة الثانية ، فإن $f(x)$ غير قابلة للتحليل على Q ، وبالتالي فإن $< f >$ هي مثالية أعظمية في الحلقة $(Q[x],+,\cdot)$. وبالتالي فإن : $Q[x] \ / < f >$ تشكل حقلاً .

(18) بيّن فيما إذا كانت كثيرة الحدود التالية :

$$P_4(x) = x^4 - 2x^2 + 8x + 1 \in Z[x]$$

قابلة للتحليل على الحلقة $(Z,+,\cdot)$.

الحل :

نعلم أنه إذا كانت $P_4(x)$ قابلة للتحليل على الحلقة $(Q,+,\cdot)$ ، فهي قابلة للتحليل على الحلقة $(Z,+,\cdot)$ ، وبالتالي سيكون لها جذراً $\alpha \in Z$ حيث $\alpha/1$ ، ويكون $\alpha = \pm 1$ ، لكن لدينا :

$$P_4(1) = 8 \text{ , } P_4(-1) = -8$$

إذن لا يمكن تحليل كثيرة الحدود $P_4(x)$ إلى حاصل ضرب عوامل في الحلقة

. $Z[x]$

نفرض ، أن كثيرة الحدود $P_4(x)$ تتحلل في $Z[x]$ بالشكل :

$$P_4(x) = (x^2 + ax + b)(x^2 + cx + d) \;;\; \forall\, a,b,c,d \in Z$$

بفك الأقواس والمطابقة مع $P_4(x)$ نجد :

$$b.d = 1 \,,\, ad + bc = 8 \,,\, ac + b + d = -2 \,,\, a + c = 0$$

من المعادلة الأولى $b.d = 1$ نجد أن $b = d = 1$ أو $b = d = -1$ ، ومن المعادلة $ad + bc = 8$ نجد أن $d\,(a + c) = 8$ ، وهذا يناقض كون $a + c = 0$ ، إذن التحليل غير صحيح ، وبالتالي فإن كثيرة الحدود $P_4(x)$ غير قابلة للتحليل .

(19) لتكن $f(x) \,,\, g(x) \in K[x]$ ولا تساويان الصفر ، وإذا كانت كثيرة الحدود $c(x)$ هي المضاعف المشترك الأصغر لـ $f(x)$ و$g(x)$ ، عندئذٍ يكون :

$$c(x).K[x] = f(x).K[x] \cap g(x).K[x]$$

الحل :

لنأخذ التقاطع $f(x).K[x] \cap g(x).K[x]$ للمثاليتين الرئيسيتين المولدين بـ $g(x)$ و$f(x)$ ، فتكون مثالية مغايرة للصفر ، وهذا يعني أنه توجد كثيرة حدود مثل $\varphi(x)$ بحيث يكون التقاطع السابق يساوي المثالية الرئيسة $\varphi(x).K[x]$ ، وبالتالي يكون $\varphi(x)$ المضاعف المشترك الأصغر لكثيرتي الحدود المفروضتين . وبما أن $c(x)$ المضاعف المشترك الأصغر لـ $f(x)$ و$g(x)$ نفسيهما فإن $\varphi(x) = c(x)$.

(20) لتكن كثيرة الحدود $f(x) = x^6 + 9x^4 + 12x^2 + 6 \in Z[x]$ ، وإذا كان $P = 3$ أثبت أن $f(x)$ غير قابلة للتحليل في $Q[x]$.

الحل :

لدينا : $a_n = 1 \,,\, a_0 = 6 \,,\, a_1 = 9 \,,\, a_2 = 12$

إن $P = 3$ لا يقسم $a_n = 1$ وP يقسم $9,12,6$ ، كما أن $P^2 = 9$ لا تقسم $a_0 = 9$ ، فحسب معيار اينشتاين كثيرة الحدود $f(x)$ غير قابلة للتحليل في $Q[x]$.

(21) لتكن كثيرة الحدود :

$$f(x)=\frac{5}{2}x^5+\frac{9}{2}x^4+15x^3+\frac{3}{7}x^2+6x+\frac{3}{14}$$

من الحلقة $(Z[x],+,.)$ ، أثبت أن $f(x)$ غير قابلة للتحليل على $Q[x]$ ، علماً أن $P=3$.

الحل :

لنأخذ كثيرة الحدود ، $h(x)$:

$$h(x) = 14\ f(x) = 35x^5 + 63x^4 + 14.15x^3 + 6x^2 + 84x + 3$$

من أجل $P=3$ نجد أن P لا تقسم 35 و P يقسم جميع المعاملات الحقيقية ، كما أن $P^2=9$ لا يقسم $a_0=3$ ، وبالتالي حسب معيار اينشتاين ، فإن كثيرة الحدود $h(x)$ غير قابلة للتحليل في $Q[x]$ ، وبالتالي فكثيرة الحدود $f(x)$ تكون غير قابلة للتحليل في $Q[x]$.

(22) بيّن أي من العبارات التالية صحيحة ، وصحّح العبارة الخاطئة :

1- كثيرة الحدود $f(x)=2x^2+4$ غير قابلة للتحليل على Q لكنها قابلة للتحليل على Z .

2- كثيرة الحدود السابقة قابلة للتحليل على R ، وعلى C .

3- كثيرة الحدود $f(x)=x^2-2$ غير قابلة للتحليل على Q ، لكنها قابلة للتحليل على R .

4- كثيرة الحدود $f(x)=x^2+1$ غير قابلة للتحليل على Z_3 ، لكنها قابلة للتحليل على Z_5 .

الحل :

العبارة الأولى (1) صحيحة .

العبارة الثانية (2) خاطئة، وتصحيحها هو : كثيرة الحدود $2x^2+4$ غير قابلة للتحليل على R ولكنها قابلة للتحليل على C .

العبارتان (3) و(4) صحيحتان .

(23) حسب اختبار اينشتاين ، بيّن أن كثيرة الحدود التالية :

$$f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$$

غير قابلة للتحليل على Q ، اعتبر $P = 5$.

الحل :

بسبب أن $5 \not| 3$ و $25 \not| 20$ ، لكن 5 تقسم كلاً من 10,-20,15 ، وبالتالي تحققت الشروط الثلاثة الواردة في اختبار اينشتاين ، إذن $f(x)$ غير قابل للتحليل على Q .

(24) صف الحلقة $R = Z_2[x] / < x^3 + 1 >$.

الحل :

لدينا : $h(x) = x^3 + 1$ ، و $m = 3$, $t^3 + 1 = 0$. وبالتالي يكون :

$$R = \{a + b\,t + c\,t^2 \ : \ a,b,c \in F \ ; \ t^3 + 1 = 0\}$$

الآن $|R| = 8$ ، إن :

$$R = \{0 , 1 , t , t^2 , 1 + t , 1 + t^2 , t + t^2 , 1 + t + t^2\}$$

وبما أن $Char\ Z_2 = 2$ يكون لدينا $1 + 1 = 0$ و $t^3 = 1$ في R ، كما أنه يمكـن كتابة في R :

$$(1 + t)\,(1 + t + t^2) = 1 + 2t + 2t^2 + t^3 = 1 + 0 + 0 + 1 = 0$$

وبنفس الطريقة ، يمكن التحقق من الحالة الثانية أي بين $1 + t + t^2$ و $1 + t^2$ في R .

8- تمرينات غير محلولة للفصل الرابع

1- لتكن :

$$f(x) = 4x^3 + 2x^2 + x + 3 \quad , \quad g(x) = 3x^4 + 3x^3 + 3x^2 + x + 4$$

كثيرتي حدود من الحلقة $(Z_5[x],+,.)$ ، المطلوب ، احسب : $f(x) + g(x)$ و $f(x).g(x)$.

2- إذا كانت :

$$f(x) = x^3 + 2x + 4 \in Z_5[x] \ , \ g(x) = 3x + 2 \in Z_5[x]$$

أوجد ناتج قسمة $f(x)/g(x)$ في الحلقة $Z_5[x]$ ، ثم استنتج باقي القسمة .

3- أوجد القاسم المشترك الأعظم $d(x)$ لكثيرتي الحدود :

$$f(x) = x^4 + x^3 + 3x - 9 \ \in Q[x]$$

$$g(x) = 2x^3 - x^2 + 6x - 3 \ \in Q[x]$$

4- عبّر عن القاسم المشترك الأعظم $d(x)$ لكثيرتي الحدود :

$$f(x) = x^2 - 1 \ , \ g(x) = 2x + 1$$

في الحلقة $(Q[x],+,.)$ كتركيب خطي لـ $f(x)$ و $g(x)$ في $Q[x]$.

5- ليكن التشاكل الحلقي : $\Phi_i : Q[x] \longrightarrow C$ ، والمعرف بالشكل :

$$\Phi_i\,(a_0 + a_1x + \ldots + a_n x^n) = a_0 + a_1\, i + \ldots + a_n\, i^n \ ; \ \Phi_i(x) = i$$

المطلوب ، أوجد $\Phi_i\,(x^2 + 1)$ ، وماذا تستنتج .

6- أوجد حاصل مجموع وضرب كثيرة الحدود التالية ، وذلك في الحلقات المشار إليها جانباً :

1- $g(x) = 2x^2 - 4x + 2 \ , \ f(x) = 4x - 5$ ، في الحلقة $(Z_8[x],+,.)$

2- $g(x) = 3x^2 + 2x + 3 \ , \ f(x) = 2x^2 + 3x + 4$ ، في الحلقة $(Z_6[x],+,.)$

3- $f(x) = 2x^3 + 4x^2 + 3x + 2$, $g(x) = 3x^4 + 2x + 4$ ، في الحلقة $(Z_5[x],+,\cdot)$

-7 إذا كانت $f_1(x) , \ldots , f_n(x) \in R[x]$ كثيرات حدود غير صفرية ، وكانت كثيرة الحدود $g(x) \in R[x]$ تقسم جداء كثيرات الحدود : $f_1(x).f_2(x)\ldots f_n(x)$ ، فإن $g(x)$ تقسم أحد العوامل $f_i(x)$ ، حيث $1 \leq i \leq n$.

إرشاد للحل : يُبَرْهن بطريقة الاستنتاج الرياضي على العدد الطبيعي n .

-8 لتكن $(R_1,+,\cdot)$ حلقة إبدالية بمحايد ، ولنرمز لعنصر الوحدة فيها بالرمز 1 ولصفرها بـ o ، ولتكن $(R,+,\cdot)$ حلقة جزئية منها بحيث $1 \in R$ ، ولنفرض أن $(R,+,\cdot)$ حلقة تامة ، ولنفرض أيضاً أن الحلقة $(R_1,+,\cdot)$ هي حلقة كثيرات الحدود فوق R ، وليكن x مولداً لـ R_1 فوق R ، ولنفرض أيضاً ، أن :

$x_1 = \sum_{i=0}^{n} a_i.x^i \neq o$ عنصراً من R_1 درجته بالنسبة لـ x تساوي n $(n > 0)$ ،

وإذا كان $f(x) = \sum_{j=0}^{m} b_j.x^j$ كثيرة حدود على R درجته m $(m \geq 0)$ والمطلوب:

1- أثبت أن درجة $f(x_1)$ بالنسبة لـ x تساوي m.n .

2- برهن أن الشرط اللازم والكافي لكي يكون x_1 مولداً لـ R_1 على R هو أن يكون $n = 1$ وأن يكون a_n قابلاً للعكس في R .

3- إذا كان x_1 مولداً لـ R_1 على R ، فإن درجة أي عنصر من R_1 بالنسبة لـ x_1 تساوي درجة العنصر نفسه بالنسبة لـ x .

-9 حلّل كثيرة الحدود $P_3(x) = x^3 - 1 \in Z_5[x]$ إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل في الحلقات التالية :

$Z_5[x] , Q[x] , R[x] , C[x]$

-10 حدّد رتبة تضاعف كثيرة الحدود التالية :

$f(x) = x^4 + 5x^3 + 3x^2 + 12$

في الحلقة $(Z_8[x],+,\cdot)$.

-11 ليكن $(F,+,\cdot)$ حقلاً ما ، وإذا كان $K \leq F$ ، ولتكن $f(x) \in K[x]$ كثيرة

حدود على الحقل K ، عندئذٍ أثبت ما يلي :

(1) يكون العنصر α من F جذراً لكثيرة الحدود $f(x)$ إذا ، وفقط إذا ، كــان $f(x) = (x - \alpha)\, g(x)$ ، حيث أن $g(x) \in K[x]$.

(2) إن الشرط اللازم والكافي لكي تكون العناصر المختلفة مــن الحقــل F : $a_1, a_2, \ldots, a_n$ جذوراً لكثيرة الحدود $f(x)$ هو أن يكون :

$$f(x) = (x - a_1)\,(x - a_2)\,\ldots\,(x - a_n).g(x)$$

لكل $g(x) \in K[x]$.

12- إذا كانت $f(x)$ و$g(x)$ كثيرتي حدود واحديتين ، بحيث أن كلاً منهما تقسم الأخرى ، أثبت أن $f(x) = g(x)$.

13- إذا كانت $\deg f(x) = n \geq 1$ حيث أن $f(x) \in R[x]$ ، وإذا كــان $a \in C$ جذراً لكثيرة الحدود $f(x)$ ، فإن المرافق $\overline{a}$ يكون أيضاً جذراً لها .

14- أوجد القاسم المشترك الأعظم لكثيرتي الحدود :

$$f(x) = x^4 - x^2 + x - 1\ ,\ g(x) = x^3 - x^2 + x - 1$$

في $Q[x]$ ، ثم عبّر عن القاسم المشترك الأعظم $d(x)$ الناتج كتركيب خطي لــــ $f(x)$ و$g(x)$ في الحلقة $Q[x]$.

15- لتكن كثيرة الحدود : $P_3(x) = x^3 + 3x + 2$ من $(Z_5[x],+,\cdot)$. أثبت أن $f(x)$ غير قابل للتحليل على الحقل Z_5 ، ثم استنتج أن $Z_5[x]/\langle f \rangle$ تشكل حقلاً .

16- أثبت أن القاسم المشترك الأعظم لكثيرتي الحدود المغايرتين للصفر $f(x)$ و$g(x)$ تتعين بشكل وحيد.

17- لتكن حلقة الأعداد الصحيحة $(Z,+,\cdot)$ ، إذا كانت $f(a) = 0$ ، حيث :

$$f(x) = x^n + a_{n-1}\, x^{n-1} + \ldots + a_0\ ,\ a \in Q\ \ ;\ \ a_0 \neq 0$$

المطلوب : أثبت أنه يوجد عدد صحيح وليكن m بحيث : $f(m) = 0$، وأن $m | a_0$.

تطبيق :

أثبت أن كثيرة الحدود $g(x)$ قابلة للتحليل على الحلقة $(Z,+,\cdot)$:

$$g(x) = x^5 + 6x^3 - x^2 - 6 \in Z[x]$$

18- أثبت بأكثر من طريقة ، أن كثيرة الحدود $f(x) = x^2 - 2 \in Q[x]$ غير قابلة للتحليل على الحلقة $(Q,+,\cdot)$.

19- لتكن $g(x) = x^3 + x^2 + 1 \in Z_2[x]$ ، أثبت أن $Z_2[x]/ < g >$ تشكل حقلاً .

20- مستخدماً معيار اينشتاين ، بيّن أي من كثيرات الحدود التالية ، قابلة للتحليل على الحقل المشار إليه جانباً :

(1) $f(x) = x^7 + 2x^3 + 12x^2 - 2 \in Z[x]$ على Q .

(2) $g(x) = x^n - P \in Z[x]$ ، حيث n,P عددان أوليان ، على Q .

(3) $h(x) = x^5 - 2 \in Z[x]$ ، على Q .

(4) $L(x) = 2x^3 + 9x - 3 \in Z[x]$ ، على Q .

21- أثبت صحة النتيجة التالية :

تكون كثيرتا الحدود المغايرتان للصفر $f(x)$ و$g(x)$ أوليتين فيما بينهما ، إذا ، وفقط إذا ، وُجِدَتْ $u(x)$ و$v(x)$ ، بحيث يكون :

$$1 = f(x).u(x) + g(x).v(x)$$

22- حدّد رتبة تضاعف الجذر α لكل من كثيرات الحدود التالية :

(1) $f(x) = x^3 - 2x^2 - 4x + 3 \in Z_6[x] \quad ; \ \alpha = 3$

(2) $f(x) = x^4 + 2x^2 + 2x + 2 \in Z_3[x] \quad ; \ \alpha = -1$

(3) $f(x) = 4x^4 - 8x^3 + x^2 - 3x + 9 \in Q[x] \quad ; \ \alpha = 3/2$

(4) $f(x) = x^5 - 2x^4 - 2x^3 + 8x^2 - 7x + 29 \in Q[x] \quad ; \ \alpha = 1$

23- أوجد كثيرة حدود في $Z[x]$ تكون غير قابلة للتحليل على Q ، لكنها قابلة للتحليل على Z_2 , Z_3 , Z_5 , Z_7 .

24- أوجد درجة تضاعف كثيرة الحدود التالية :

$x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1$ في الحلقة $(Z_5,+,\cdot)$.

25- لتكن $f(x) = x^2 + 1$ و $g(x) = x^4 + 3x^3 + x + 1$ ، أوجد كثيرتي الحدود $q(x)$ و $r(x)$ بحيث يكون : $g(x) = q(x).f(x) + r(x)$ و $r(x) = 0$ أو $\deg r(x) < 2 = \deg f(x)$.

26- لنفرض التطبيق $\varphi : R[x] \longrightarrow R$ بالشكل : $\varphi[f(x)] = f(x)$ ، أثبت أن φ تشاكل حلقي .

27- احسب $(1 + x)^5$ في الحلقة $Z_5[x]$، واحسب $(1 + x)^7$ في الحلقة $Z_7[x]$.

28- أوجد جذور كثيرة الحدود $f(x) = (x - 4)(x - 5)$ في الحلقة Z_6 ثم في الحلقة Z_7 .

29- أوجد عدد الجذور لكثيرة الحدود $x^2 - x$ في Z_4 و $Z_2 \times Z_2$ ثم في الحلقة Z_6 .

30- حدّد قيمة للعدد الأولي P ، بحيث يكون $x - 1$ عاملاً (معاملاً) لكثيرة الحدود :

$$f(x) = 3x^4 + 5x^3 + 2x^2 + x + 4$$

وذلك في الحلقة $Z_P[x]$.

31- أوجد جميع كثيرات الحدود من الدرجة الثانية غير القابلة للتحليل على الحلقة Z_2 .

32- إذا كان P عدداً أولياً ، وكان $P \equiv 3 \pmod 4$ ، أثبت أن كثيرة الحدود $x^2 + 1$ غير قابلة للتحليل على الحلقة Z_P .

33- لتكن $P(x)$ كثيرة حدود واحدية من الدرجة الرابعة في الحلقة $Z_3[x]$ ، المطلوب أوجد ستة كثيرات حدود في $Z_3[x]$ بحيث تكون $P(x)$ غير قابلة للتحليل، إذا وفقط إذا ، كان ليس لها جذور في Z_3.

34- حدّد قيمة العدد الأولي P ، حتى تكون كثيرة الحدود : $P(x) = x^5 + 6x^4 + 12x + 15$ غير قابلة للتحليل ، (حسب اختبار اينشتاين) ، ثم تحقق من ذلك .

35- أوجد القاسم المشترك الأعظم لكثيرات الحدود التالية :

$$f(x) = x^2 + 2 \ , \ g(x) = x^3 + 4x^2 + x + 1 \ : \ F = Z_5$$

$$f(x) = x^2 - x - 2 \ , \ g(x) = x^5 - 4x^3 - 2x^2 + 7x - 6 \ : \ F = Q$$

ثم اكتب $d(x)$ كتركيب خطي لكثيرتي الحدود $f(x)$ و $g(x)$.

36- أوجد جذور لكثيرة الحدود $P_2(x) = x^2 - 5x + 6$ في الحلقة $(Z_{12},+,\cdot)$.

37- إذا علمت أن العدد 1 هو جذر لكثيرة الحدود :

$$g(x) = x^4 + 3x^2 + 2x + 4 \in Z_5[x]$$

والمطلوب ، باستخدام عملية القسمة المطلوبة حلّل كثيرة الحدود $g(x)$ في $Z_5[x]$.

38- طبّق مبرهنة التقسيم الخوارزمي لتقسيم كثيرة الحدود التالية :

$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ في $Z_5[x]$ على كثيرة الحدود $g(x) = x^2 - 2x + 3$.

(لاحظ على سبيل المثال في الحلقة $Z_5[x]$: $4x - (-3x) = 2x$) .

39- حلّل كثيرة الحدود $g(x) = x^4 + 4$ إلى عوامل خطية في الحلقة $Z_5[x]$.

40- ادرس قابلية تحليل كثيرة الحدود $f(x) = x^2 + 8x - 2$ على الحقول التالية C , R , Q . ثم حلّل كثيرة الحدود $f(x) = 2x^3 + 3x^2 - 7x - 5$ إلى عوامل خطية في الحلقة $Z_{11}[x]$.

41- بيّن فيما إذا كانت كثيرة الحدود التالية: $f(x) = x^4+2x^3 + 2x^2 - x + 1$، غير قابلة للتحليل في الحلقة $Q[x]$. اعتبر $P = 2$ ، وذلك بطريقتين مختلفتين.

42- صِفْ حلقة القسمة $R = R[x]/I$ ، حيث أن : $I = < x^2 + 1 >$.

43- أثبت أن التطبيق : $\varphi : F \longrightarrow R[x]/I$ المعرّف بالشكل : $\varphi(a) = \overline{a}$ هو تماثل حلقي. حيث أن I مثالية $o \neq$ ، F حقلاً ما .

44- صِفْ حلقة القسمة $R = Q[x]/< x^2 - 2 >$.

45- أوجد كثيرة حدود واحدية $h(x)$ في $F[x]$ ، بحيث يكون $I = < h(x) >$

وذلك :

$I = \{f(x)\in F[x]$: يساوي الصفر $f(x)$ المعامل الثابت لـــ $\}$

46- صِفْ حلقة القسمة $R = F[x] / < h(x) >$ ، ثم اكتـــب جــدولي الجمـــع والضرب لـــ R في الحالات التالية :

(a) $h(x) = x^2 \quad , \quad F = Z_2$

(b) $h(x) = x^3 + 1 \quad , \quad F = Z_2$

(c) $h(x) = x^2 \quad , \quad F = Z_3$

47- أنشئ حقلاً من المرتبة الثامنة ، ثم اكتب جدول بالنسبة لعملية الضرب .

48- إذا كان $p/q\in Q$ جذراً لكثيرة الحدود :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1x + a_0\in Z[x]$$

حيث أن q , p أوليان نسبياً و$a_n \neq 0$ ، أثبت أن P/a_0 وq/a_0 .

تطبيق : أوجد الجذور النسبية (الكسرية) لكثيرة الحدود :

$$P(x) = 6x^4 - 25x^3 + 32x^2 + 3x - 10$$

49- إذا كانت $f = (1,2,3,1,0)$ و $g = (2,1,1,3,0)$ كثيرتي حدود على الحلقة $(Z,+,\cdot)$ ، أوجد $f + g$ و$f.g$. ثم بيّن فيما إذا كانـــت $h = (0,1,0,1,\dots,0,1,\dots)$ كثيرة حدود على $(Z,+,\cdot)$.

50- إذا كان العدد المركب $a + i\,b$ جذراً لكثيرة الحدود $P(x)$ ، ذي الأمثـــال الحقيقية ، فإن مرافق هذا الجذر ، أي $a - i\,b$ يكون جذراً لـــ $P(x)$ أيضاً . وماذا تستنتج من ذلك .

51- بفرض أن K حقلاً مميزه الصفر ، يكون كثير الحدود في $R[x]$ متطابقين إذا ، وفقط إذا، تساوت الأمثال في قوى x ، أي أن :

$$\sum a_i x^i = \sum b_i x^i \Leftrightarrow a_i = b_i \;\; ; \forall i$$

فهل هذا الأمر صحيح من أجل الحقول التي ليست مميزاتها أصفاراً .

52- إذا كان P عدداً أولياً ما ، أثبت أن كثيرة الحدود :

$$P(x) = x^{P-1} + x^{P-2} + ... + x + 1$$

غير قابلة للتحليل على الحلقة $(Q,+,\cdot)$.

إرشاد للحل : بدّل كل x بـــ y + 1 ، ثم استفد من معيار اينشتاين .

53- أثبت أن رتبة تضاعف الجذر $(x = -2)$ لكثيرة الحدود :

$$P(x) = x^4 + \frac{13}{2}x^3 + 15x^2 + 14\,x + 4$$

تساوي العدد 3 .

54- ليكن $(F,+,\cdot)$ حقلاً ما ، ولتكن P وQ كثيرتي حدود غير صفريتين من الحلقة $F[x]$ ، ولتكن $R \in F[x]$ كثيرة حدود واحدية ، وإذا كانت $R.F[x]$ مثالية رئيسية والتي تساوي $P.F[x\} + Q.F[x]$.

أثبت أن كثيرة الحدود R هي القاسم المشترك الأكبر لكثيرتي الحدود P وQ . وهل العكس صحيح ، علّل ذلك .

55- أثبت أن كثيرات الحدود التالية والتي هي من الحلقة $(R[x],+,\cdot)$ أولية فيما بينها :

$$P(x) = x^3 - x^2 + x - 1$$

$$Q(x) = x^2 + x - 2$$

$$R(x) = x^2 + 1$$

56- إذا كانت كثيرة الحدود $g(x)$ تقسم كثيرة الحدود $f(x)$، بيّن أن :

$$\deg g(x) \leq \deg f(x)$$

57- أثبت أن العناصر غير الصفرية في الحلقة $(R,+,\cdot)$ هي عناصر وحدة للحلقة $R[x]$.

58- إذا كانت A مصفوفة مربعة حقيقية ، وإذا كانت P مصفوفة غير شاذة ، أي أن $|P| \neq 0$ من نفس المرتبة لـ A ، أثبت أنه من أجل أية كثيرة حدود $f(x)$ يتحقق :

$$f(P^{-1}.A.P) = P^{-1}\, f(A).P$$

ثم أثبت أنه إذا كانت المصفوفة B مشابهة للمصفوفة A ، (أي أنه توجد مصفوفة غير شاذة ولتكن P بحيث $B = P^{-1}.A.P$) فإن $f(B)$ مشابهة لـ $f(A)$ ، من أجل أي كثيرة حدود $f(x) \in R[x]$.

تمارين محلولة وغير محلولة للفصل الخامس :

الفضاءات الحلقية (الحلقيات)

Modules

9- تمرينات محلولة للفصل الخامس

– الفضاءات الحلقية (الحلقيات) –

1- لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان n عدداً صحيحاً موجباً ، وإذا كان :

$$R^n = \{(a_1,a_2,\ldots,a_n) : a_i \in R \,,\, i = 1,\ldots,n\}$$

ولنعرّف على R^n عملية ثنائية داخلية (+) بالشكل :

$$(a_1,a_2,\ldots,a_n) + (b_1,b_2,\ldots,b_n) = (a_1 + b_1 \,,\, a_2 + b_2 \,,\, \ldots \,,\, a_n + b_n)$$

لكل $(a_1,a_2,\ldots,a_n) \,,\, (b_1,b_2,\ldots,b_n) \in R^n$

وعملية خارجية $(\cdot)$ بالشكل :

$$b\cdot(a_1,a_2,\ldots,a_n) = (b\cdot a_1 \,,\, b\cdot a_2 \,,\, \ldots \,,\, b\cdot a_n)$$

لكل $b \in K \,,\, (a_1,a_2,\ldots,a_n) \in R^n$

المطلوب ، أثبت أن R^n فضاء حلقي على R .

الحل :

يمكن التحقق ، بسهولة ، من أن $(R^n,+)$ زمرة إبدالية .

لنتحقق الآن من بقية الشروط :

ليكن $(a_1,a_2,\ldots,a_n)$ و $(b_1,b_2,\ldots,b_n)$ عنصرين ما من R^n ، وإذا كان y,x عنصرين ما من R، فإن :

$$\begin{aligned}
1)\;\; x\,[(a_1,a_2,\ldots,a_n) + (b_1,b_2,\ldots,b_n)] &= x\,(a_1+b_1 \,,\, \ldots\ldots \,,\, a_n+b_n) \\
&= [x\,(a_1+b_1) \,,\, \ldots\ldots \,,\, x\,(a_n+b_n)] \\
&= (xa_1+xb_1 \,,\, \ldots\ldots \,,\, xa_n+xb_n) \\
&= (xa_1,\ldots, xa_n) + (xb_1,\ldots,xb_n) \\
&= x\,(a_1,\ldots, a_n) + x\,(b_1,\ldots,b_n)
\end{aligned}$$

$$2)\ (x+y)(a_1,a_2,\dots,a_n) = [(x+y)a_1, \dots\dots, (x+y)a_n]$$
$$= (x a_1 + y a_1, \dots\dots, x a_n + y a_n)$$
$$= (x a_1,\dots, x a_n) + (y a_1, \dots\dots, y a_n)$$
$$= x(a_1,\dots, a_n) + y(a_1, \dots\dots, a_n)$$

$$3)\ (x\cdot y)(a_1,a_2,\dots,a_n) = [(x\cdot y)a_1, \dots\dots, (x\cdot y)a_n]$$
$$= [x\cdot(y\cdot a_1), \dots\dots, x\cdot(y\cdot a_n)]$$
$$= x\cdot(y\cdot a_1, \dots\dots, y\cdot a_n)$$
$$= x\cdot[y(a_1,\dots, a_n)]$$

نستنتج مما سبق أن R^n فضاء حلقي على R .

ملاحظة :

إذا كان $n = 1$ ، عندها يمكن النظر إلى R على أنها فضاء حلقي فوق نفسه . ويجدر الانتباه، أنه إذا كانت الحلقة $(R,+,\cdot)$ بمحايد ، فإن الفضاء الحلقي R^n بمحايد أيضاً ، لأنه ، إذا رمزنا لعنصر الوحدة (المحايد) في الحلقة $(R,+,\cdot)$ بالرمز 1 ، فإن :

$$1.(a_1, \dots\dots, a_n) = (1.a_1, \dots\dots, 1.a_n) = (a_1, \dots\dots, a_n)$$

لكل $(a_1, \dots\dots, a_n)$ من R^n .

<u>2-</u> لتكن $(R,+,\cdot)$ حلقة ما ، ولتكن $M_2(R)$ مجموعة المصفوفات الحقيقية المربعة من المرتبة (الدرجة) الثانية ، أي أن :

$$M_2(R) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} ; a_{11}, a_{12}, a_{21}, a_{22} \in R \right\}$$

ولنعرّف على $M_2(R)$ عملية ثنائية داخلية (+) وعملية خارجية (.) على النحو التالي :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$x.\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} x.a & x.b \\ x.c & x.d \end{pmatrix}$$

لكل x من R و $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ و $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ من $M_2(R)$.

المطلوب ، برهن أن $M_2(R)$ فضاء حلقي على R .

الحل :

نلاحظ أولاً أن $M_2(R) \neq \phi$. ولنبرهن أولاً أن $(M_2(R), +)$ زمرة إبدالية .

لتكن $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ و $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ و $\begin{pmatrix} \ell & m \\ n & j \end{pmatrix}$ ثلاثة عناصر من $M_2(R)$ ، عندئذٍ :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} \ell & m \\ n & j \end{pmatrix}\right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e+\ell & f+m \\ g+n & h+j \end{pmatrix}$$

$$= \begin{pmatrix} a+(e+\ell) & b+(f+m) \\ c+(g+n) & d+(h+j) \end{pmatrix} = \begin{pmatrix} (a+e)+\ell & (b+f)+m \\ (c+g)+n & (d+h)+j \end{pmatrix}$$

$$= \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} + \begin{pmatrix} \ell & m \\ n & j \end{pmatrix} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] + \begin{pmatrix} \ell & m \\ n & j \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$= \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

لنرمز للعنصر المحايد بالنسبة لعملية الجمع في الحلقة $(R,+,\cdot)$ بـــ o ، فإن :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} o & o \\ o & o \end{pmatrix} = \begin{pmatrix} a+o & b+o \\ c+o & d+o \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

لكل $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من $M_2(R)$.

إذا كان $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ عنصراً ما من $M_2(R)$ ، فإن :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}=\begin{pmatrix} a-a & b-b \\ c-c & d-d \end{pmatrix}=\begin{pmatrix} o & o \\ o & o \end{pmatrix}$$

نستنتج مما سبق أن $(M_2(R),+)$ زمرة إبدالية . عنصرها المحايد هو $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

ومعكوس كل عنصر $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من $M_2(R)$ هو $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

لنتحقق الآن من بقية شروط الفضاء الحلقي :

ليكن y,x عنصرين ما من R ، وإذا كان $\begin{pmatrix} a & b \\ c & d \end{pmatrix},\begin{pmatrix} e & f \\ g & h \end{pmatrix}\in M_2(R)$ فإن :

$$\begin{aligned}
x.\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] &= x.\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \\
&= \begin{pmatrix} x(a+e) & x(b+f) \\ x(c+g) & x(d+h) \end{pmatrix} \\
&= \begin{pmatrix} xa+xe & xb+xf \\ xc+xg & xd+xh \end{pmatrix} \\
&= \begin{pmatrix} xa & xb \\ xc & xd \end{pmatrix}+\begin{pmatrix} xe & xf \\ xg & xh \end{pmatrix} \\
&= x\begin{pmatrix} a & b \\ c & d \end{pmatrix}+x\begin{pmatrix} e & f \\ g & h \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
(x+y).\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} (x+y)a & (x+y)b \\ (x+y)c & (x+y)d \end{pmatrix} \\
&= \begin{pmatrix} x.a+y.a & x.b+y.b \\ x.c+y.c & x.d+y.d \end{pmatrix} \\
&= \begin{pmatrix} x.a & x.b \\ x.c & x.d \end{pmatrix}+\begin{pmatrix} y.a & y.b \\ y.c & y.d \end{pmatrix} \\
&= x.\begin{pmatrix} a & b \\ c & d \end{pmatrix}+y.\begin{pmatrix} a & b \\ c & d \end{pmatrix}
\end{aligned}$$

$$(x.y).\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} (x.y).a & (x.y).b \\ (x.y).c & (x.y).d \end{pmatrix}$$
$$= \begin{pmatrix} x.(y.a) & x.(y.b) \\ x.(y.c) & x.(y.d) \end{pmatrix} = x.\begin{pmatrix} y.a & y.b \\ y.c & y.d \end{pmatrix}$$
$$= x.\left[y.\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right]$$

نستنتج مما سبق ، أن $M_2(R)$ فضاء حلقي على الحلقة $(R,+,.)$.

بالاستفادة من التمرين السابق ، يمكن حل التمرين التالي :

3- بفرض أن $M_{n\times m}(R)$ مجموعة المصفوفات من الشكل $n\times m$ على الحلقة بمحايد $(R,+,.)$، عندئذٍ : $M_{n\times m}(R)$ تشكل فضاءً حلقياً على R .

الحل :

إن $(M_{n\times m},+)$ تشكل زمرة إبدالية (بالنسبة لعملية جمع المصفوفات) ، وبسهولة يمكن التحقق من جميع شروط الفضاء الحلقي، حيث أن عملية الضرب (القياسي) $r.a_{ij}$ للمصفوفة (a_{ij}) بالعنصر r من R معرفة.

4- لتكن $(End(M),+,.)$ حلقة التشاكلات الذاتية للزمرة الإبدالية $(M,+)$. برهن أن M يشكل فضاء حلقي من اليسار على الحلقة $(End(M),+,.)$.

الحل :

لدينا فرضاً $(M,+)$ زمرة إبدالية ، لنبرهن على بقية الشروط الواردة في تعريف الفضاء الحلقي .

ليكن $r_1,r_2,r\in End(M)$ و $m_1,m_2,m\in M$ ، عندئذٍ يتحقق ما يلي :

$$r.(m_1+m_2) = r.m_1 + r.m_2$$
$$(r_1+r_2).m = r_1.m + r_2.m$$
$$(r_1.r_2).m = r_1.(r_2.m)$$

كما أن $1.m = m$

5- لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وإذا كـــان x,a عنصرين من M,R على الترتيب ، بحيث يكون $a.x = 0$ ، علماً أن 0 هـــو صفر الفضاء الحلقي M . وإذا كان لـــ a معكوس في R بالنسبة للعملية $(\cdot)$ ، فإن $x = 0$.

الحل :

بما أن $a.x = 0$ ، فإن :

$$a^{-1}.(a.x) = a^{-1}.0$$

أي أن

$$(a^{-1}.a).x = 0$$

$$1.x = 0$$

إذاً

$$x = 0$$

6- لتكن $(R,+,\cdot)$ حلقة إبدالية ، وإذا كان M فضاءً حلقياً مـــا علـــى R ، و L فضاءً حلقياً جزئياً من M ، ولنفرض أن A مجموعة جزئية غير خالية مـــن R ، لنثبت أن $A.L$ فضاءً حلقياً جزئياً من M على R .

الحل :

إن $\phi \neq A.L \subseteq M$.

ليكن y,x عنصرين ما من $A.L$ ، فإنه يمكن كتابتهما على الشكل :

$$x = \sum_{i=1}^{n} a_i.x_i \quad , \quad b = \sum_{j=1}^{m} b_j.y_j$$

لكل a_i , b_j من A وx_i , y_j من L ، m,n عددان صحيحان موجبان، وبالتالي فإن:

$$x - y = \sum_{i=1}^{n} a_i.x_i - \sum_{j=1}^{m} b_j.y_j$$

$$= \sum_{i=1}^{n} a_i.x_i + \sum_{j=1}^{m} b_j.(-y_j) \in A.L$$

ليكن y,a عنصرين من R و A على الترتيب ، وبالتالي يمكن كتابـــة العنصـــر y بالشكل :

$$y = \sum_{k=1}^{t} c_k . y_k$$

لكل c_k من A وy_k من L ، و t عدد صحيح موجب ، وبالتالي ، فإن :

$$a.y = a.\left(\sum_{k=1}^{t} c_k . y_k\right) = \sum_{k=1}^{t} a(c_k . y_k)$$

$$= \sum_{k=1}^{t} (c_k . a) . y_k = \sum_{k=1}^{t} c_k . (a . y_k) \in A.L$$

نستنتج مما سبق ، أن A.L فضاء حلقي جزئي من M .

7- ليكن $(F,+,.)$ حقلاً ما ، وإذا كانت A مصفوفة من الشكل $m\times n$ على F ، وليكن التطبيق:

$\varphi : F^n \longrightarrow F^n$ المعرف بالشكل : $\varphi(m) = m.A$ ، حيث أن F^m وF^n مصفوفات من الشكل $1\times m$ و$1\times n$ على الترتيب ، برهن أن φ تشاكلاً .

الحل :

لكل m,m_1,m_2 من F^n و $r\in F$ يكون لدينا :

$$\varphi(m_1 + m_2) = (m_1 + m_2) .A = m_1.A + m_2.A$$

$$= \varphi(m_1) + \varphi(m_2)$$

$$\varphi(r.m) = (r.m) .A = r\,(m.A) = r.\,\varphi(m)$$

8- لتكن $(R,+,.)$ حلقة بمحايد ، وإذا كان M و N فضاءين حلقيين بمحايدين على R ، أثبت أن $\varphi : M \longrightarrow N$ تطبيقاً ، ثم أثبت أن الشرط اللازم والكافي لكي يكون φ هو تشاكل للفضاء الحلقي M في الفضاء الحلقي N على R هو أن يتحقق :

$$\varphi(a.x + b.y) = a\,\varphi(x) + b\,\varphi(y) \qquad (*)$$

لكل b,a من R و x,y من M .

الحل :

لنبرهن أولاً ، أن الشرط (*) محقق ، علماً أن φ تشاكلاً .

بما أن φ هو تشاكل على R للفضاء الحلقي M في الفضاء الحلقي N ، فإن :

$$\varphi(ax + by) = \varphi(ax) + \varphi(by) = a\,\varphi(x) + b\,\varphi(y)$$

وذلك مهما يكن b,a من R و x,y من M .

لنبرهن الآن أن φ تشاكل ، علماً أن الشرط (*) محقق .

لنرمز لصفر الحلقة $(R,+,.)$ بالرمز 0 ، ولعنصر الوحدة فيها بالرمز 1 ، بما أن :

$$\varphi(ax + by) = a\,\varphi(x) + b\,\varphi(y)$$

لكل y,x من M و b,a من R ، فإن :

$$\varphi(1.x + 1.y) = 1.\,\varphi(x) + 1.\varphi(y)$$

$$\varphi(ax + 0.y) = a\,\varphi(x) + 0\,\varphi(y)$$

لكل y,x من M و a من R ، وبالتالي ، فإن :

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

$$\varphi(a.x) = a\,\varphi(x)$$

لكل y,x من M و a من R .

إذن φ هو تشاكل للفضاء الحلقي M في الفضاء الحلقي N ، على R .

9- إذا كانت $(R,+,.)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وإذا كان N,L فضاءين حلقيين جزئيين من M بحيث يكون $L \subset N$ ، عندئذٍ $\left. M/L \middle/ N/L \right. \cong M/L$.

الحل :

التطبيق $\varphi : M/L \longrightarrow M/L$ المعرف بالشكل : $\varphi\,(x + L) = x + N$ لكل x من M هو تشاكل للفضاء الحلقي M/L على الفضاء الحلقي M/N ، كما أن نواته هي N/L ، وحسب المبرهنة الأساسية للتشاكل نجد :

$$\left. M/L \middle/ N/L \right. \cong M/N$$

10- لتكن Z مجموعة الأعداد الصحيحة ، والتي يمكن عدّها فضاءً حلقياً على

حلقة الأعداد الصحيحة $(Z,+,.)$ ، ولنعرف التطبيق $\varphi:Z \longrightarrow Z$ بالشكل : $\varphi(m) = 3m$ لكل m من Z .

أثبت أن φ تشاكل على الفضاء الحلقي Z وأوجد نواته ، وصورته .

الحل :

لكل n,m من Z ولكل a من Z ، وبالتالي يكون لدينا :

$$\varphi(m+n) = 3\,(m+n) = 3m + 3n$$
$$= \varphi(m) + \varphi(n)$$
$$\varphi(a.m) = 3\,(a.m) = (3a).m = (a.3)\,m = a\,(3m)$$
$$= a\,\varphi(m)$$
$$\mathrm{Ker}\,\varphi = \{3m = 0\} \Rightarrow \mathrm{Ker}\,\varphi = \{0\}$$
$$\mathrm{Im}\,\varphi = \{3m : m \in Z\} = 3.Z$$

لاحظ أيضاً ، أن كلاً من الفضاءين $\mathrm{Ker}\,\varphi$ و $\mathrm{Im}\,\varphi$ فضاء حلقي جزئي على الحلقة $(Z,+,.)$ من الفضاء الحلقي Z .

-11 بفرض أن N,M فضاءين حلقيين ما ، على حلقة ولتكن $(R,+,.)$. وإذا كان $M_1,M_2,\ldots,M_n$ حيث $n \in N$ و $n \geq 2$ فضاءات حلقية جزئية من M بحيث يكون $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$

وإذا كانت $N_1,N_2,\ldots,N_n$ فضاءات حلقية جزئية من N بحيث يكون $N = N_1 \oplus N_2 \oplus \ldots \oplus N_n$

وإذا كان $M_i \cong N_i$ ، من أجل $i = 1,2,\ldots,n$ ، المطلوب ، بيّن أن $M \cong N$.

الحل :

بما أن $M_i \cong N_i$ ، يوجد تماثلاً φ_i ، على الأقل ، للفضاء الحلقي M_i على الفضاء الحلقي N_i من أجل $i = 1,2,\ldots,n$. وبما أن $M = \overset{n}{\underset{i=1}{\oplus}} M_i$ ، فإنه يمكن كتابة كل عنصر x من M بشكل وحيد بالصورة : $x = \sum_{i=1}^{n} x_i$ لكل x_i من M_i .

الآن ، نعرّف التطبيق $\varphi : M \longrightarrow N$ بالشكل :

$$\varphi(x_1 + \ldots + x_n) = \varphi_1(x_1) + \ldots + \varphi_n(x_n)$$

لكل $x_i \in M_i$ و $i = 1,2,\ldots,n$. ولنثبت أن φ هو تماثل للفضاء الحلقي M على الفضاء الحلقي N .

ليكن r عنصراً ما من R ، و x_i , y_i من M_i حيث $i = 1,2,\ldots,n$ ، فإن :

$$\begin{aligned}
\varphi\left[(x_1+\ldots+x_n) + (y_1+\ldots+y_n)\right] &= \varphi\left[(x_1+y_1) +\ldots+ (x_n+y_n)\right] \\
&= \varphi_1(x_1+y_1) +\ldots+ \varphi_n(x_n+y_n) \\
&= \left[\varphi_1(x_1) + \varphi_1(y_1)\right] +\ldots+ \left[\varphi_n(x_n) + \varphi_n(y_n)\right] \\
&= \left[\varphi_1(x_1)+\ldots+\varphi_n(x_n)\right] + \left[\varphi_1(y_1) +\ldots+ \varphi_n(y_n)\right] \\
&= \varphi(x_1+\ldots+x_n) + \varphi(y_1+\ldots+y_n)
\end{aligned}$$

$$\begin{aligned}
\varphi\left[r\,(x_1+\ldots+x_n)\right] &= \varphi(r.x_1 +\ldots+ r.x_n) \\
&= \varphi_1(r\,x_1) +\ldots+ \varphi_n(r\,x_n) \\
&= r\,\varphi_1(x_1) +\ldots+ r\,\varphi_n(x_n) \\
&= r\left[\varphi_1(x_1) +\ldots+ \varphi_n(x_n)\right] \\
&= r\,\varphi(x_1+\ldots+x_n)
\end{aligned}$$

الآن ، ليكن x_i , y_i من M_i ، حيث أن $i = 1,2,..,n$ بحيث يكون :

$$\varphi(x_1+\ldots+x_n) = \varphi(y_1+\ldots+y_n)$$

عندئذٍ يكون لدينا :

$$\varphi_1(x_1) +\ldots+ \varphi_n(x_n) = \varphi_1(y_1) +\ldots+ \varphi_n(y_n)$$

وبما أن $N = N_1 \oplus N_2 \oplus \ldots\ldots \oplus N_n$ ، فإن :

$$\varphi_i(x_i) = \varphi_i(y_i) \;;\; i = 1,2,..,n$$

وبما أن φ_i هو تماثل للفضاء الحلقي M_i على الفضاء الحلقي N_i ، حيث أن $i = 1,2,\ldots,n$ ، فيكون :

$$x_i = y_i \;;\; i = 1,2,..,n$$

أي أن :

$$x_1+\ldots+x_n=y_1+\ldots+y_n$$

بفرض أن a عنصراً ما من N، وبالتالي يمكن كتابته بالشكل : $a=a_1+\ldots+a_n$

حيث a_i من N_i (لأن $N=\overset{n}{\underset{i=1}{\oplus}}N_i$) ، وبالتالي ، فإن :

$$\varphi\left(\varphi_1^{-1}(a_1)+\ldots+\varphi_n^{-1}(a_n)\right)=\varphi_1\left(\varphi_1^{-1}(a_1)\right)+\ldots+\varphi_n\left(\varphi_n^{-1}(a_n)\right)$$
$$=\left(\varphi_1\ o\ \varphi_1^{-1}\right)(a_1)+\ldots+\left(\varphi_n\ o\ \varphi_n^{-1}\right)(a_n)$$
$$=a_1+\ldots+a_n=a$$

نستنتج مما سبق أن φ هو تماثل للفضاء الحلقي M على الفضاء الحلقي N أي أن $M\cong N$.

12- إذا كانت $(A,+)$ و$(B,+)$ زمرتين إبداليتين ، (يمكن اعتبارهما كفضاءين حلقيين على حلقة الأعداد الصحيحة $(Z,+,\cdot)$) ، أثبت أن كل تشاكل زمري $\varphi:A\longrightarrow B$ بين الزمرتين المفروضتين هو تشاكل بين الفضاءين الحلقيين A و B على الحلقة $(Q,+,\cdot)$.

الحل :

لكل x,y من A و $a\in Z^+$ ، فإن :

$$\varphi(x+y)=\varphi(x)+\varphi(y)$$
$$\varphi(a\,x)=a\,\varphi(x)$$

لكن ، إذا كان $a\in Z^-$ ، فإننا نضع $a=-b$ ، فنجد أن الشرط الثاني سيكون :

$$\varphi(ax)=\varphi(-bx)=-\varphi(bx)=-b\,\varphi(x)=a\,\varphi(x)$$

13- إذا كانت $(R,+,\cdot)$ حلقة ما ، و M فضاءً حلقياً على R ، وإذا كانت N_i، حيث $i=1,2,3$ فضاءات حلقية جزئية من M بحيث يكون: $M=N_1\oplus N_2\oplus N_n$، ولنرمز بـ L_i بـ $\sum_{\substack{j=1\\i\neq j}}^{3}N_j$ حيث $i=1,2,3$ والمطلوب :

1- أثبت أن $N_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{3} L_j \quad ; \quad i = 1,2,3$

2- $L_i + \bigcap_{\substack{j=1 \\ j\neq i}}^{3} L_j = M \quad ; \quad i = 1,2,3$

3- $L_1 \cap L_2 \cap L_3 = \{0\}$ ، حيث أن 0 هو صفر الفضاء الحلقي M على R.

الحل :

1) لنبرهن على سبيل المثال : $N_1 = L_2 \cap L_3$ ، وبنفس الطريقة يمكن التحقق من أن : $N_2 = L_1 \cap L_3$ و $N_3 = L_1 \cap L_2$.

ليكن x عنصراً ما من N_1 ، وبالتالي يكون :

$$x \in N_1 + N_3 = L_2 \quad , \quad x \in N_1 + N_2 = L_3$$

ومنه يكون $x \in L_2 \cap L_3$.

ليكن الآن y عنصراً ما من $L_2 \cap L_3$ ، وبالتالي ، فإن :

$$y \in M \, , \, y \in L_2 \, , \, y \in L_3$$

وبالتالي ، فإنه يمكن كتابة العنصر y بالأشكال التالية :

$$y = y_1 + y_2 + y_3 \; ; \; y_i \in N_i \quad ; \quad i = 1,2,3 \qquad (1)$$

$$y = y'_1 + y'_3 \quad ; \quad y'_1 \in N_1 \, , \, y'_3 \in N_3 \qquad (2)$$

$$y = y''_1 + y''_2 \quad ; \quad y''_1 \in N_1 \, , \, y''_2 \in N_2 \qquad (3)$$

من (1) و(2) ، وبما أن : $M = N_1 \oplus N_2 \oplus N_n$ نستنتج أن :

$$y_2 = 0 \qquad (4)$$

ومن العلاقتين (1) و(3) وحسب $M = N_1 \oplus N_2 \oplus N_3$ نجد أن :

$$y_3 = 0 \qquad (5)$$

من العلاقات (1) و(4) و(5) نجد أن : $y = y_1 \in N_1$.

نستنتج ، مما سبق أن $N_1 = L_2 \cap L_3$.

2) لأن $L_i = \bigcap\limits_{\substack{j=1\\ j\neq i}}^{3} N_j$ وحسب الطلب السابق (1): $N_i = \bigcap\limits_{\substack{j=1\\ j\neq i}}^{3} L_j$ حيث

$i = 1,2,3$ يكون لدينا :

$$L_i + \sum_{\substack{j=1\\ i\neq j}}^{3} L_j = \left(\sum_{\substack{j=1\\ i\neq j}}^{3} N_j \right) + N_i = \sum_{j=1}^{3} N_j = M \quad ; \quad i = 1,2,3$$

3) لأن : $M = N_1 \oplus N_2 \oplus N_3$ ، فإن : $N_3 \cap (N_1+N_2) = \{0\}$ ومنه يكون :

$$L_1 \cap (L_2 \cap L_3) = (L_1 \cap L_2) \cap L_3 = N_3 \cap (N_1+N_2) = \{0\}$$

ملاحظة :

يمكن تعميم التمرين السابق بالشكل التالي :

إذا كانت $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً ما على R ، وإذا كان $n \geq 2$ و $n \in N$; $N_1,\ldots,N_n$ فضاءات حلقية جزئية من M بحيث يكون : $M = N_1 \oplus \ldots\ldots \oplus N_n$.

وإذا رمزنا بـ L_i بـ $\sum\limits_{j=1}^{m} N_j$ و $i \neq j$ و $i = 1,2,\ldots,n$ ، عندئذٍ يتحقق ما يلي :

1) $N_i = \bigcap\limits_{\substack{j=1\\ i\neq j}}^{n} L_i$ ، حيث $i = 1,2,..,n$

2) $L_i + \bigcap\limits_{\substack{j=1\\ j\neq i}}^{n} L_j = M$ ، حيث $i = 1,2,..,n$

3) $L_1 \cap \ldots \cap L_n = \{0\}$ ، حيث أن 0 هو صفر الفضاء الحلقي M على R.

<u>14-</u> لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كانت C,B,A فضاءات حلقية جزئية من فضاء حلقي M على R ، وبحيث يكون $C \subseteq A$ ، أثبت أن :

$$A \cap (B + C) = (A \cap B) + C$$

الحل :

بما أن حاصل جمع فضاءين حلقيين جزئيين هو فضاء حلقي جزئي ، فإن :

$$A \cap B \subseteq A \;\Rightarrow\; (A \cap B) + C \subseteq A + C$$

$$A\cap B\subseteq B \Rightarrow (A\cap B)+C\subseteq B+C$$

وبالتالي يكون :

$$(A\cap B)+C\subseteq (A+C)\cap (B+C)$$

$$(A\cap B)+C\subseteq A\cap (B+C) \qquad (1)$$

لأنه $C\subseteq A$ فرضاً .

من جهة ثانية ، إذا كان $x\in A\cap(B+C)$ ، فإن $x\in A$ ، و$x\in(B+C)$ ، وبالتالي نكتب العنصر a بالشكل $a=b+c$ حيث $b\in B$ و$c\in C$.

لدينا $b=a-c$ ، وبما أن $c\in C\subseteq A$ فيكون $b\in A$ ، وبالتالي فإن : $b\in A\cap B$ ، ومن ذلك ينتج أن : $a\in(A\cap B)+C$ ، أي أن :

$$A\cap (B+C)\subseteq (A\cap B)+C \qquad (2)$$

من الاحتواءين (1) و(2) تتحقق المساواة المطلوبة .

<u>15-</u> ليكن M فضاءً حلقياً بمحايد على حلقة بمحايد $(R,+,.)$ ، وإذا كانت : $S=\{x_1,\ldots,x_n\,;\, n\in N\,,\, n\geq 2\}$ مجموعة من M بحيث $M=(S)$ ، وليكن $1\leq K\leq n$ بحيث يتحقق : $x_k=\sum\limits_{\substack{i=1\\ i\neq k}}^{n} b_i.x_i$ لكل $b_i\in R$. أثبت أن المجموعة $S-\{x_k\}$ مولدة لـ M .

الحل :

ليكن x عنصراً ما من الفضاء الحلقي M ، وبالتالي يمكن كتابته بالشكل : $x=\sum\limits_{i=1}^{n} a_i.x_i$ ، لكل a_i من R ، وبالتالي :

$$\begin{aligned} x=a_k.x_k+\sum_{\substack{i=1\\ i\neq k}}^{n} a_i.x_i &= a_k\left(\sum_{\substack{i=1\\ i\neq k}}^{n} b_i.x_i\right)+\sum_{\substack{i=1\\ i\neq k}}^{n} a_i.x_i \\ &=\sum_{\substack{i=1\\ i\neq k}}^{n}(a_k.b_i).x_i+\sum_{\substack{i=1\\ i\neq k}}^{n} a_i.x_i \\ &=\sum_{\substack{i=1\\ i\neq k}}^{n}(a_k.b_i+a_i).x_i \end{aligned}$$

وهذا يبين لنا أن المجموعة $S-\{x_k\}$ مولدة لـ M .

16- لتكن $(R,+,.)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً بمحايد على R ، وإذا كانت المجموعة المنتهية S التالية : $S=\{x_1,\dots,x_n\}$ من M بحيث يكون $M=(S)$ ، وإذا كان $1\le t\le n$ بحيث يتحقق :

$$x_k = b.y + \sum_{\substack{i=1\\ i\neq k}}^{n} b_i.x_i \quad ; \quad b,b_i\in R\,,\, y\in M \text{ لكل}$$

المطلوب ، أثبت أن المجموعة $S-\{x_k\}\cup\{y\}$ مولدة لـ M .

الحل :

ليكن x عنصراً ما من M ، وبالتالي يمكن كتابته بالشكل : $x=\sum_{i=1}^{n} a_i.x_i$ ، لكل a_i من R . وبالتالي :

$$x = a_t.x_t + \sum_{\substack{i=1\\ i\neq t}}^{n} a_i.x_i$$

$$= a_t\left(b.y + \sum_{\substack{i=1\\ i\neq t}}^{n} b_i.x_i\right) + \sum_{\substack{i=1\\ i\neq t}}^{n} a_i.x_i$$

$$= (a_t.b)\,y + \sum_{\substack{i=1\\ i\neq t}}^{n} (a_t.b_i + a_i)\,x_i$$

17- لنرمز لعنصر الوحدة للحلقة $(R,+,.)$ بـ 1 ، ولصفرها بـ 0 ، ولنعرّف على المجموعة التالية :

$$R^4 = \{(a,b,c,d) : a,b,c,d\in R\}$$

العملية الثنائية الداخلية (+) بالشكل :

$$(a,b,c,d) + (e,f,g,h) = (a+e\,,\, b+f\,,\, c+g\,,\, d+h)$$

لكل a, b, c, d, e, f, g, h من R . والعملية الخارجية (•) بالشكل :

$$x\bullet(a,b,c,d) = (x\bullet a\,,\, x\bullet b\,,\, x\bullet c\,,\, x\bullet d)$$

لكل a , b , c , d من R .

يمكن التأكد بسهولة أن R^4 فضاء حلقي بمحايد علــى R . المطلــوب أثبــت أن المجموعة :

$$S = \{(1,0,0,0) , (0,1,0,0) , (0,0,1,0) , (0,0,0,1)\}$$

مستقلة خطياً على R .

الحل :

لتكن x , y , z , t عناصر من R بحيث يكون :

$$x\,(1,0,0,0) + y\,(0,1,0,0) + z\,(0,0,1,0) + t\,(0,0,0,1) = (0,0,0,0)$$

علماً أن $(0,0,0,0)$ هو صفر الفضاء الحلقي R^n ، وبالتالي يكون لدينا :

$$(x,0,0,0) + (0,y,0,0) + (0,0,z,0) + (0,0,0,t) = (0,0,0,0)$$

أي أن :

$$(x,y,z,t) = (0,0,0,0)$$

إذن :

$$x = 0 , y = 0 , z = 0 , t = 0$$

18- ليكن N,M فضاءين حلقيين بمحايدين على الحلقة بمحايد $(R,+,\cdot)$. وإذا كانت $\{a_i\}$ أسرة عناصر من الفضاء الحلقي M بحيث $\{a_i\}$ تشكل قاعدة لــ M على R ، وإذا كانت $\{b_i\}$ أسرة عناصر من الفضاء الحلقي N بحيث $1 \le i \le n$، المطلوب بيّن أنه يمكن إيجاد تشاكل وحيد φ لــ M في N ، يكــون مــن أجلــه $\varphi(a_i) = b_i$ ، لكل $1 \le i \le n$.

الحل :

بما أن $\{a_i\}$ تشكل قاعدة لــ M على R ، حيث $1 \le i \le n$ ، فإنه يمكن كتابة كل عنصر x من M ، بصورة وحيدة ، بالشكل : $x = \sum_{i=1}^{n} a_i . x_i$ ، لكل x_i من R .

لنعرف الآن ، التطبيق $\varphi : M \longrightarrow N$: φ ، بالشكل :

$$\varphi(x) = \sum_{i=1}^{n} x_i . b_i$$

ولنبرهن الآن ، أن φ تشاكل .

ليكن b,a عنصرين ما من M ، وإذا كان x عنصراً ما من R ، فإنه يمكن كتابة b,a على الشكل التالي :

$$a = \sum_{i=1}^{n} x_i . a_i \quad ; \quad x_i \in R$$

$$b = \sum_{i=1}^{n} y_i . a_i \quad ; \quad y_i \in R$$

وبالتالي يكون :

$$a + b = \sum_{i=1}^{n} (x_i + y_i) . a_i \quad \text{و} \quad x . a = \sum_{i=1}^{n} x (x_i . a_i) = \sum_{i=1}^{n} (x\, x_i) . a_i$$

وبالتالي يكون :

$$\varphi(a + b) = \sum_{i=1}^{n} (x_i + y_i) . b_i = \sum_{i=1}^{n} x_i . b_i + \sum_{i=1}^{n} y_i . b_i$$

$$= \varphi(x) + \varphi(y)$$

$$\varphi(x . a) = \sum_{i=1}^{n} (x . x_i) . b_i = x . \left(\sum_{i=1}^{n} x_i . b_i \right)$$

$$= x . \varphi(a)$$

لنبرهن الآن ، أن $\varphi(a_i) = b_i$ ، لكل $i = 1,2,..,n$.

لنرمز لعنصر الوحدة في الحلقة $(R,+,\cdot)$ بـ 1 ، وبالتالي يكون : $a_i = 1.\ a_i$ لكل $i = 1,2,..,n$

ومنه يكون : $\varphi(a_i) = 1.\ b_i = b_i$ ، لكل $i = 1,2,..,n$

وإذا كان Ψ هو أيضاً تشاكل لـ M في N من أجله يكون : $\Psi(a_i) = b_i$ ، لكل $i = 1,2,..,n$ ، فإن $\Psi = \varphi$ ، لأن : إذا كان a عنصراً ما من M ، وبالتالي يمكن كتابته ، بالشكل $a = \sum_{i=1}^{n} x_i . a_i$ ، لكل x_i من R ، وبالتالي يكون :

$$\Psi(a)=\Psi\left(\sum_{i=1}^{n}(x_i.a_i)\right)=\sum_{i=1}^{n}\Psi.(x_i.a_i)=\sum_{i=1}^{n}x_i.\Psi(a_i)=\sum_{i=1}^{n}x_i.b_i$$

نستنتج مما سبق أن φ هو التشاكل الوحيد لــ M في N ، يكون من أجله $\varphi(a_i)=b_i$ ، لكل $i=1,2,..,n$.

19- ليكن M فضاءً حلقياً على الحلقة $(R,+,.)$ ، وإذا كان M,L فضاءان حلقيان جزئيان من M بحيث $L\subseteq N$ ، وبفرض أن الفضاء الحلقي الجزئي L متمماً في M ، أثبت أن للفضاء الحلقي الجزئي L متمماً في N .

الحل :

لنرمز بــ 0 لصفر الفضاء الحلقي M .

بما أن للفضاء الحلقي الجزئي L متمماً في M ، فإنه يوجد فضاء حلقي جزئي F من M ، يكون من أجله : $M=L\oplus F$ ، وبالتالي فإن :

$$M=L+F\ ,\ L\cap F=\{0\}$$

ومنه يكون :

$$N=N\cap M=N\cap(L+F)=L+(N\cap F)$$
$$L\cap(N\cap F)=N\cap(L\cap F)=N\cap\{0\}=\{0\}$$

إذن $N=L\oplus(N\cap F)$ ، أي أن للفضاء الحلقي الجزئي L متمماً في N هو الفضاء الحلقي الجزئي $N\cap F$.

20- من المعلوم ، أن الفضاء المتجهي $(V,+,.)$ على الحقل $(F,+,.)$ يمكن اعتباره فضاءً حلقياً على الحقل $(F,+,.)$ ، بيّن أن V عديم الفتل .

الحل :

ليكن a عنصراً غير صفري من الحقل $(F,+,.)$ ، ومن الشرط $a.x=0$ حيث x من m ، فإن :

$$0=a^{-1}.0=a^{-1}.(a.m)=(a^{-1}.a).m=1.m=m$$

إذن $m=0$.

21- أثبت أن الفضاء الحلقي Z على الحلقة $(Z,+,.)$ هو فضاء حلقي حر مولد

بالمجموعة $A = \{2,3\}$.

الحل :

لأن الفضاء الحلقي الجزئي المولد بالمجموعة A يحوي $1 = 2 - 3$ ويولد Z ، كما أن A لا تشكل أساساً للفضاء الحلقي Z ، لأن : $3.2 - 2.3 = 0$ مرتبطة خطية على Z ، وكذلك ، أي مجموعة جزئية فعلية من A لا تشكل قاعدة لأن: $\{2\},\{3\},\phi$ تولد فضاءات حلقية جزئية فعلية.

22- لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، أثبت أن M المولد نهائياً على الحلقة R هو صورة لفضاء حلقي حر منتهي التوليد على R بالنسبة لتشاكل ما .

الحل :

لتكن المجموعة $A = \{m_1,m_2,\ldots,m_n\}$ مولدة لـ M ، وإذا كانت المجموعة :

$$B = \{e_1 = (1,0,\ldots,0) , e_2 = (0,1,0,\ldots,0) , \ldots , e_n = (0,0,\ldots,0,1)\}$$

تولد بحرية الفضاء الحلقي R^n على R .

لنعرّف التطبيق φ بالشكل : $\varphi : R^n \longrightarrow M$:

$$\varphi\left(\sum_{i=1}^{n} r_i.e_i\right) = \sum_{i=1}^{n} r_i.m_i$$

وبما أن لكل عنصر وليكن a من R^n تمثيل وحيد بدلالة التركيب $\sum_{i=1}^{n} r_i.e_i$ ، فإن φ حسن التعريف .

ليكن $x = \sum_{i=1}^{n} r'_i.e_i$ و $y = \sum_{i=1}^{n} r_i.e_i$ عنصرين ما من R^n ، عندئذٍ يمكن التحقق بسهولة ، أن :

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$
$$\varphi(r.x) = r.\varphi(x)$$

إذن φ تشاكل من R^n على M .

وإذا كانت $\operatorname{Ker}\varphi = k$ ، فحسب المبرهنة الأساسية الأولى للتماثل ، يكون : $R^n/K \cong M$.

10- تمرينات غير محلولة للفصل الخامس

1- لتكن K^S مجموعة التطبيقات للمجموعة $S \neq \phi$ في الحلقة $(R,+,\cdot)$ أي :

$$K^S = \{ f : S \longrightarrow R : \text{تطبيق } f \}$$

ولنعرّف على المجموعة K^S عملية الجمع بالشكل :

$$(f+g)(x) = f(x) + g(x) \quad ; \quad \forall x \in S$$

وقانون التشكيل الخارجي التالي مجموعة مؤثراته K :

$$(\alpha f)(x) = \alpha f(x) \quad ; \quad x \in S , \alpha \in R$$

أثبت أن المجموعة K^S تشكل فضاءً حلقياً على الحلقة $(R,+,\cdot)$.

2- إذا كان $(V,+,\cdot)$ فضاءً حلقياً على الحلقة $(R,+,\cdot)$ ، وكانت C,B,A فضاءات حلقية جزئية من V ، بحيث $C \subseteq A$. أثبت صحة العلاقة :

$$A \cap (B + C) = (A \cap B) + C$$

3- لتكن $(R,+,\cdot)$ حلقة إبدالية ما ، وكانت $(V,+,\cdot)$ فضاءً حلقياً على R ، وإذا فرضنا أن L فضاءً حلقياً من V ، وA مجموعة جزئية غير خالية من K ، والمطلوب ، أثبت أن المجموعة :

$$A.L = \{ \sum_{i=1}^{n} a_i . x^i \quad : \quad a_i \in A , x_i \in L \}$$

تشكل فضاءً حلقياً جزئياً من V .

4- إذا كان $(V,+,\cdot)$ فضاءً حلقياً على الحلقة $(R,+,\cdot)$ ، وإذا كانت I مثالية يسارية في R ، أثبت أن المجموعة التالية :

$$A.V = \{ \sum_{i=1}^{n} a_i . x_i = a_1 x_1 + \ldots\ldots + a_n x_n \quad : a_i \in A , x_i \in V \}$$

تشكل فضاءً حلقياً جزئياً من الفضاء الحلقي V .

-5 لتكن $(R,+,\bullet)$ حلقة إبدالية ، وإذا كان M فضاءً حلقياً حراً مولداً بمجموعة منتهية على R ، أثبت أن أي قاعدة للفضاء M يكون له عدداً من العناصر نفسها .

-6 لنعرّف تحويلاً خطياً من الفضاء المتجهي $(V,+,\bullet)$ على نفسه ، وإذا كان $(F,+,\bullet)$ حقلاً ما، أثبت أن V فضاءً حلقياً على الحقل $(F,+,\bullet)$.

-7 ليكن M فضاءً حلقياً بمحايد على الحلقة بمحايد $(R,+,\bullet)$ ، وإذا كانت المجموعة التالية :

$$S=\{x_1,x_2,\ldots,x_n \;\; ; \;\; n\in N\,,\, n\geq 2\}$$

من M بحيث يكون : $(S) = M$ ، وإذا كان k عدداً من المجموعة $\{1,2,\ldots,n\}-\{1\}$ ، بحيث يكون : $x_k=\sum_{i=1}^{k-1} b_i.x_i$ لكل b_i من R ، والمطلوب برهن أن المجموعة $S-\{x_k\}$ مولدة لـ M .

-8 لتكن $(R,+,\bullet)$ حلقة بمحايد ، وإذا كان N فضاءً حلقياً جزئياً من الفضاء الحلقي M على R ، أثبت أنه يوجد تقابل يحافظ على الاحتواء ، بين مجموعة الفضاءات الحلقية الجزئية من M/N وبين مجموعة الفضاءات الحلقية الجزئية L من M ، حيث يتحقق $N\subseteq L\subseteq M$.

-9 لتكن $(R,+,\bullet)$ حلقة إبدالية، وإذا كان M فضاءً حلقياً حراً مولداً بمجموعة منتهية على R، أثبت أن أي أساس للفضاء M يكون منتهياً .

-10 إذا كان M فضاءً حلقياً على الحلقة بمحايد $(R,+,\bullet)$. أثبت أن $Hom_R(M,M)$ حلقة جزئية من الحلقة $Hom(M,M)$.

-11 لتكن $(R,+,\bullet)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R وليكن $m\in M$. أثبت أن المجموعة N التالية :

$$N=\{\, r.m+n.m \;\; ; \;\; r\in R\,,\, n\in Z\}$$

تشكل فضاءً حلقياً جزئياً من الفضاء M تحوي العنصر m من M . ثم أثبت أن $N=R.m$.

-12 لتكن $(R,+,\bullet)$ حلقة ما ، وليكن N,M فضاءين حلقيين ما على R ، إذا

كان φ تشاكلاً للفضاء الحلقي M على الفضاء الحلقي N ونواته M' ، عندئذٍ :

1- يوجد تقابل (تطبيق متباين وشامل) بين مجموعة كل الفضاءات الحلقية الجزئية من الفضاء الحلقي N ومجموعة كل الفضاءات الحلقية الجزئية ، التي يحوي كل منها M' من الفضاء الحلقي M .

2- وإذا كان L فضاءً حلقياً جزئياً من N ، فإن :

$$M/\varphi^{-1}(L) \cong M/N' \ , \ \varphi^{-1}(L)/N \cong L$$

13- لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كان N,M فضاءين حلقيين بمحايدين على R ، وبفرض أن $\{a_i\}$ أسرة عناصر من M ، بحيث أن $\{a_i\}$ تشكل قاعدة لـ M على R ، وبفرض أن $\{b_i\}$ أسرة عناصره من N ، حيث $i = 1,2,\ldots,n$، المطلوب :

أثبت أنه يمكن إيجاد تماثل وحيد φ لـ M في N يكون من أجله : $\varphi(a_i) = b_i$ لكل $i = 1,2,\ldots,n$.

14- ليكن N,M فضاءين حلقيين على الحلقة بمحايد $(R,+,\cdot)$ ، وإذا كان F,L فضاءين حلقيين جزئيين من الفضاءين الحلقيين N,M على الترتيب ، أثبت أن :

$$M \times N \big/ L \times F \cong M/L \times N/F$$

إرشاد للحل : استفد من مبرهنة التماثل الأولى .

15- إذا كان M فضاءً حلقياً ما على الحلقة $(R,+,\cdot)$ ، وإذا كان L,N فضاءين حلقيين جزئيين من M، فإن :

$$L/(L \cap N) \cong (L+N)/N$$

16- بفرض أن Q,P,N فضاءات جزئية حلقية من الفضاء الحلقي M على الحلقة $(R,+,\cdot)$ ، برهن ما يلي :

1) $N + (P \cap Q) = (N+P) \cap (N+Q)$

2) $(N \cap P) + (P \cap Q) + (Q \cap N) = (N+P) \cap (P+Q) \cap (Q+N)$

17- لتكن $(R,+,\cdot)$ حلقة ما ، وإذا كان M فضاءً حلقياً على R ، وبفرض أن

$N_1,N_2,\ldots,N_n$ حيث $n\in N$ و $n \geq 2$ فضاءات حلقية جزئية من M، بحيث يكون: $N = N_1\oplus N_2\oplus \ldots\oplus N_n$ ، وإذا كانت $L_1,L_2,\ldots,L_n$ فضاءات حلقية جزئية من $N_1,N_2,\ldots,N_n$ على الترتيب ، وإذا رمزنا بـ L لـ $L_1 + L_2 + \ldots + L_n$ ، المطلوب :

1) أثبت أن المجموع $L_1 + L_2 + \ldots + L_n$ هو مجموع مباشر .

2) إذا كان φ هو التطبيق $\varphi : M \longrightarrow M/L$ المعرف بالشكل :

$$\varphi(x) = x + L;\ x\in M$$

وبفرض أن φ هو تشاكل للفضاء الحلقي M على الفضاء الحلقي M/L، أثبت أن :

(a) $$M/L = \varphi(N_1) \oplus \ldots\ldots \oplus \varphi(N_n)$$

(b) $$N_i/L_i \cong \varphi(N_i)\ \ ; i = 1,2,\ldots,n$$

-18 لتكن $(R,+,\bullet)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، وإذا كان M^n فضاءً حلقياً على R ، حيث $n\in Z^+$ ، فإن M^n تشاكلاً مع M .

-19 ليكن M فضاءً حلقياً على الحلقة $(R,+,\bullet)$ ، وبفرض أن L,F,N فضاءات حلقية جزئية من M بحيث أن كلاً من الفضاءين الحلقيين الجزئيين F و L هو متمم للفضاء الحلقي الجزئي N في M ، المطلوب أثبت أن $F \cong L$.

-20 لتكن $(R,+,\bullet)$ حلقة بمحايد ، وإذا كان M فضاءً حلقياً على R ، أثبت ما يلي :

الفضاء الحلقي M دائرياً ، إذا ، وفقط إذا ، كان $M \cong R/I$ حيث I مثالية يسارية في R .

-21 ليكن M فضاءً حلقياً على حلقة ما ، ولتكن $(R,+,\bullet)$ ، وإذا كانت N_i حيث $i = 1,2,\ldots,n$ فضاءات حلقية جزئية من M ، بحيث يتحقق ما يلي :

$$\bigcap_{i=1}^{3} N_i = \{0\}$$ ؛ (o هو صفر الفضاء الحلقي M)

$$N_1 + (N_2\cap N_3) = N_2 + (N_1\cap N_3) = N_3 + (N_1\cap N_2) = M$$

ولنرمز لـــ $N_2 \cap N_3$ بـــ M_1 و $N_1 \cap N_3$ بـــ M_2 و $N_1 \cap N_2$ بـــ M_3 ، والمطلوب :

1) أثبت أن $M = M_1 \oplus M_2 \oplus M_3$

2) $N_1 = M_2 + M_3 \ , N_2 = M_1 + M_3 \ , N_3 = M_1 + M_2$

22- لتكن $(Z_n,+,\cdot)$ حلقة، وإذا كان Z_n الفضاء الحلقي على الحلقة المفروضة. أثبت أن Z_n هو فضاء حلقي حر ، وأن Z_n لا يشكّل فضاءً حلقياً حراً على الحلقة Z .

تمارين محلولة وغير محلولة للفصل السادس :

تمديد الحقول

Fields Extension

11- تمرينات محلولة للفصل السادس

– تمديد الحقول –

1- إذا كان P عدداً أولياً ، أثبت أن الامتداد $Q(\sqrt{P})$ للحقل Q امتداد منته .

الحل :

بما أن المجموعة $A=\{1,\sqrt{P}\}$ تشكل أساساً للفضاء المتجهي $Q(\sqrt{P})$ على الحقل Q ، وبالتالي فإن $Q(\sqrt{P})$ امتداد منته للحقل Q ، كما أن :

$$\dim Q(\sqrt{P})=[Q(\sqrt{P}):Q]=2$$

2- أثبت أن الأعداد التالية $5, \sqrt{3}, 3+\sqrt[n]{7}$ جبرية على الحقل Q .

الحل :

بما أن الأعداد المذكورة سابقاً تشكل جذوراً لكثيرات الحدود التالية على الترتيب :

$$x-5 \;,\; x^2-7 \;,\; (x-3)^n-7$$

فإن هذه الأعداد جبرية على الحقل Q .

3- إذا كان $u=\sqrt[3]{2}+\sqrt{5}$ ، أوجد كثيرة الحدود $f(x)\in Q[x]$، بحيث يكون العدد u جذراً لها.

الحل :

لدينا $u-\sqrt{5}=\sqrt[3]{2}$ ، وبالتالي فإن $(u-\sqrt{5})^3=2$ ، ومنه يكون $u^3-3\sqrt{5}\,u^2+15u-5\sqrt{5}=2$ ، وبالتالي يكون :

$$u^3-15u-2=\sqrt{5}\,(3u^2+5)$$

وبتربيع العلاقة الأخيرة نجد :

$$(u^3-15u-2)^2=5\,(3u^2+5)^2$$

وبالتالي يكون u جذراً لكثيرة الحدود :

$$f(x)=x^6-15x^4-4x^3+75x^2-60x-121=0$$

4- أثبت أن $Q(i,-i) = Q(i)$.

الحل :

إن $Q(i,-i) \supseteq Q(i)$ ، لأن $Q(i,-i)$ تحتوي على Q وعلى i ، لكن $Q(i)$ حقل يحوي Q و i ، وبالتالي فهو يحوي $-i$ أيضاً وبذلك يكون $Q(i,-i) \subseteq Q(i)$.

5- ليكن E امتداد للحقل F ، وإذا كان $u,v \in E$ ، ولنفرض أن $u+v,u$ عنصرين جبريين على F ، أثبت أن العنصر v جبري على F .

الحل :

لنبرهن أن $F \supseteq F(u,v)$ منتهي ، لدينا $F(u,v) = F(u,u+v)$.

لنكتب $L = F(u+v)$ لنحصل على سلسلة الحقول :

$$F(u+v) \supseteq L(u) \supseteq L \supseteq F$$

الآن $F \supseteq L$ منتهي ، بسبب أن $u+v$ جبري على الحقل F ، و $L \supseteq L(u)$ منتهي بسبب أن u جبري على الحقل L . وهكذا يكون $F \supseteq F(u,v)$ منتهي ، وذلك حسب مبرهنة الضرب .

6- هاتِ مثالاً لكثيرتي حدود ، غير قابلتين للتحليل ومختلفتين ، بحيث يكون لهما حقل الانشطار نفسه .

الحل :

بأخذ : $f(x) = x^2 - 2$ و $g(x) = x^2 - 2x - 1$ ، نجد أنهما يملكان نفس حقل الانشطار $Q(\sqrt{2})$ ، والسبب لأن جذور $f(x)$ و$g(x)$ هي $\pm\sqrt{2}$ و $1 \pm \sqrt{2}$ على الترتيب .

7- أثبت أن العدد $u = \cos\left(\frac{2\pi}{5}\right)$ جبري على الحقل Q .

الحل :

باستخدام علاقة دوموافر نجد أولاً أن :

$$\left(\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\right)^5=\cos 2\pi+i\sin 2\pi=1$$

بوضع $x=\cos\frac{2\pi}{5}$ و $y=\sin\frac{2\pi}{5}$ ، وبأخذ القسم الحقيقي نجد أن :

$$x^5-10x^3y^2+5y^4x=1 \qquad (*)$$

وباستخدام العلاقة $y^2=1-x^2$ (لأن $x^2+y^2=1$) في (*) نجد :

$$x^5-10x^3(1-x^2)+5(1-x^2)^2x=1$$

وبالتالي تكون كثيرة الحدود $f(x)$:

$$f(x)=16x^5-20x^3+5x-1$$

التي يكون العنصر $u=\cos\frac{2\pi}{5}$ جذراً لها . إذن العدد u جبري على الحقل Q .

8- بيّن فيما إذا كان الامتداد $E=Q(i,-i,\sqrt{5},\sqrt{-5})$ للحقل Q هو امتداد بسيط .

الحل :

لنبرهن أولاً ، أن $E_1=Q(i+\sqrt{5})$ يتطابق مع الحقل E ، أي أن $i,\sqrt{5}\in E_1$،
بما أن $(i+\sqrt{5})^2\in E_1$ ، وبالتالي فإن :

$$(i+\sqrt{5})^2=-1+2i\sqrt{5}+5=4+2i\sqrt{5}\in E_1$$

كذلك نجد أن :

$$(i+\sqrt{5})\,(4+2i\sqrt{5})=14i-2\sqrt{5}\in E_1$$

ويكون :

$$14i-2\sqrt{5}+2(i+\sqrt{5})=16i\in E_1$$

وبالتالي ، فإن $i\in E_1$ ، ومنه نجد أن : $(i+\sqrt{5})-i=\sqrt{5}\in E_1$

إذن $i,\sqrt{5}\in E_1$ ، وهذا يعني أن $E_1\supseteq E$ ، وبما أن $E\supseteq E_1$ ، فيكون $E=E_1$.

إذن الامتداد $E=Q(i,-i,\sqrt{5},\sqrt{-5})$ بسيط للحقل Q .

9- بيّن أن حقل الأعداد المركبة C هو إغلاق جبري لحقل الأعداد الحقيقية R ، لكنه لا يشكّل إغلاق جبري لحقل الأعداد النسبية Q .

الحل :

إن الحقل C يشكل إغلاقاً جبرياً للحقل R ، لأنه امتداد جبري بسيط وحيث أن $C = R(i)$ ، كما أن C مغلق جبرياً ، ولكن الحقل C لا يشكل إغلاقاً جبرياً للحقل Q لأنه ليس امتداداً جبرياً للحقل Q حيث أن العنصرين e و π من C متساميان على الحقل Q .

10- أوجد كثيرة حدود f ، التي يكون $Q(u)$ حقل انشطار لها على الحقل Q ، خذ $u = \sqrt{2} + i$.

الحل :

بما أن $u = \sqrt{2} + i$ ، فإن $u^2 = 1 + 2\sqrt{2}\,i$ ، ومنه يكون : $(u^2-1)^2 = -8$ ، بذلك يكون u جذراً لكثيرة الحدود : $f(x) = x^4 - 2x^2 + 9$ ، وبالتالي يكون :

$$f(x) = (x - \sqrt{2} - i)\,(x + \sqrt{2} + i)\,(x - \sqrt{2} + i)\,(x + \sqrt{2} - i)$$
$$= (x^2 - 2\sqrt{2}\,x + 3)\,(x^2 + 2\sqrt{2}\,i\,x + 3)$$

حيث أن جذور f(x) الأخرى هي : $-(\sqrt{2} + i), -\sqrt{2} + i, \sqrt{2} - i$

إذن f(x) كثيرة حدود غير قابلة للتحليل على Q ، ومنه يكون f كثيرة حدود صغرى للعنصر u على Q . كما أن درجة امتداد $Q(\sqrt{2} + i)$ هي أربعة ، كما أن عناصر الأساس له هي :

$$1 , \sqrt{2} + i , (\sqrt{2} + i)^2 , (\sqrt{2} + i)^3$$

ومنه يكون :

$$Q(\sqrt{2} + i) = \{a_0 + a_1 u + a_2 u^2 + a_3 u^3 \ ; \ a_0, a_1, a_2, a_3 \in Q\}$$

إن $\sqrt{2} \in Q(\sqrt{2} + i)$ ، وبالتالي فإن كل جذور f(x) تنتمي إلى $Q(\sqrt{2} + i)$. وبما أن $Q(\sqrt{2} + i)$ يحوي Q ، إذن $Q(\sqrt{2} + i)$ هو حقل انشطار لـ f(x) على الحقل Q .

11- حدّد رتبة الحقول الجزئية الفعلية من الحقل المنتهي F والذي رتبته P^{40} ، حيث أن P عدد أولي .

الحل :

بما أن القواسم الفعلية للعدد 40 هي : 20 , 10 , 8 , 5 , 4 , 2 , 1 وهي التي تحدد الحقول الجزئية الفعلية من الحقل F ، الذي رتبته P^{40} ، إذن رتب جميع الحقول الجزئية الفعلية منه هي :

$$P , P^2 , P^4 , P^5 , P^8 , P^{10} , P^{20}$$

12- إذا كان E امتداداً للحقل F ، وإذا كان $u \in E$ ، أثبت أن التطبيق $\varphi_u : F[x] \longrightarrow E$ ، المعرف بالشكل : $\varphi_u(f(x)) = f(u)$ حيث أن $f(x) = \sum_{i=0}^{n} u_i . x^i \in F[x]$ يشكل تشاكلاً من الحلقة F[x] إلى الحقل E .

الحل :

لتكن $f(x) = \sum_{i=0}^{n} u_i . x^i$ و $g(x) = \sum_{i=0}^{m} v_i . x^i$ كثيرتي حدود في الحلقة F[x] ، ولتكن كثيرة الحدود : $h(x) = f(x) + g(x) = \sum_{i=0}^{s} w_i . x^i$ في F[x] ، عندها يكون :

$$\varphi_u[f(x) + g(x)] = \varphi_u[h(x)] = h(u) = f(u) + g(u)$$

ومن ناحية ثانية يكون :

$$\varphi_u[f(x)] + \varphi_u[g(x)] = f(u) + g(u)$$

إذن :

$$\varphi_u[f(x) + g(x)] = \varphi_u(f(x)) + \varphi_u(g(x))$$

لنفرض الآن أن :

$$f(x).g(x) = m(x) = \sum_{i=0}^{n+m} d_i . x^i$$

وبالتالي يكون :

$$[\varphi_u.f(x)]\,.[\varphi_u.g(x)] = m(u) = f(u)\,.\,g(u)$$

ومن ناحية أخرى ، لدينا :

$$\varphi_u[f(x)]\,.\varphi_u[g(x)] = f(u)\,.\,g(u)$$

إذن :

$$\varphi_u[f(x)\,.\,g(x)] = \varphi_u(f(x))\,.\,\varphi_u(g(x))$$

نستنتج مما سبق أن φ_u تشاكل حلقي من الحلقة $F[x]$ إلى الحقل E .

13- برهن أن الامتداد $Q(u)$ للحقل Q ناظمي ، حيث أن :

$$u = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$$

الحل :

بما أن $Q(u)$ حقل انشطار لكثيرة الحدود $f(x) = x^4 + 1 \in Q[x]$ إذن $Q(u)$ امتداد ناظمي للحقل Q .

14- بيّن فيما إذا كان الامتداد $[R : Q]$ منتهٍ .

الحل :

بما أن كثيرة الحدود $f(x) = x^n - 2 \in Q[x]$ غير قابلة للتحليل على الحقل Q حيث $n > 1$ ، وبأخذ $E = Q(\sqrt[n]{2})$ ، أي $[E : Q] = n$ فيكون الامتداد R للحقل Q يحوي فضاءات متجهة أبعادها كبيرة ، وبالتالي ، فإن الامتداد R للحقل Q لا يمكن أن يكون منتهياً . إذن $[R:Q]$ غير منتهٍ .

15- لتكن $f(x) = x^4 - 8x^2 + 15 \in Q[x]$ كثيرة حدود على الحقل Q ، المطلوب ، أوجد امتداداً للحقل Q بحيث يحوي جذوراً لكثيرة الحدود $f(x)$.

الحل :

إن :
$$x^4 - 8x^2 + 15 = (x^2 - 3)\,(x^2 - 5)$$

وبأخذ $g(x) = x^2 - 3$ و $h(x) = x^2 - 5$ من $Q[x]$ ، نجـد أن $g(x) = x^2 - 3$ كثيرة حدود غير قابلة للتحليل على الحقل Q ، وبالتالي يوجد امتـداد للحقـل Q يحوي جذوراً لكثيرة الحدود $g(x)$ ، إذن :

$$E = Q(u) = Q(\sqrt{3}) \cong Q[x]/<g>$$

$$= \{a_0 + a_1u\ ;\ a_0, a_1 \in Q\ ,\ u^2 - 3 = 0\}$$

ومنه نجد : $[Q(\sqrt{3}) : Q] = 2$.

وبنفس المناقشة تماماً ، لأجل كثيرة الحدود $h(x) = x^2 - 5$ ، حيث $h(x)$ كثيـرة حدود غير قابلة للتحليل :

$$K = E(v) = E(\sqrt{5}) \cong E[x]/<h>$$

$$= \{b_0 + b_1v\ ;\ b_0, b_1 \in E\ ,\ v^2 - 5 = 0\}$$

ويكون $[K : E] = 2$ ، وحسب مبرهنة الضرب يكون :

$$[K : Q] = [K : E]\ .\ [E : Q] = 2.2 = 4$$

16- حدّد العناصر المترافقة على الحقل Q لكثيرة الحدود :

$$f(x) = x^2 - 3\ \in Q[x]$$

الحل :

نلاحظ بسهولة أن العنصرين $\sqrt{3}$ و $-\sqrt{3}$ من الحقـل R متـرافقين علـى Q ، لأنهما جذور لكثيرة الحدود $f(x)$ على الحقل Q .

17- ليكن E امتداداً للحقل F ، وإذا كان φ تماثلاً على الحقل E ، نقول عـن العنصر $u \in E$ إنه يبقى ثابتاً تحت تأثير التماثل φ ، إذا كان $\varphi(u) = u$.

أثبت أن مجموعة كل التماثلات S على الحقل E ، والتي تبقـي العناصـر $u \in E$ ثابتة تشكل حقلاً جزئياً من E ، نرمز له عادةً بـــ E_s ويســمى الحقـل الثابـت للمجموعة S .

الحل :

بما أن φ_i تماثل لكل $i \in I$ ، عندئذ فإن $\varphi_i(o) = 0$ و $\varphi_i(1) = 1$.

ليكن $\varphi_i(u) = u$ و $\varphi_i(v) = v$ ، لكل $i \in I$ ، وبالتالي يكون لكل $u,v \in E_s$ ، ولكل $i \in I$:

$$\varphi_i(u \pm v) = \varphi_i(u) \pm \varphi_i(v) = u \pm v$$

$$\varphi_i(u.v) = \varphi_i(u) \,.\, \varphi_i(v) = u.v$$

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

إذن E_S حقل جزئي من الحقل E .

تطبيق :

وجدنا في المثال (16) السابق أن جذور كثيرة الحدود $x^2-3 \in Q[x]$ في الحقل R هما $\pm\sqrt{3}$، وبالتالي فإن $\varphi : Q(\sqrt{3}) \longrightarrow Q(\sqrt{3})$ المعرف بالشكل $\varphi : (u + b\sqrt{3}) \longrightarrow (u - b\sqrt{3})$ تماثل ذاتي على الحقل $Q(\sqrt{3})$. وتكون العلاقة $\varphi(a) = a$ محققة ، إذا كان $u + v\sqrt{3} = u - v\sqrt{3}$ أي أن $v = 0$. إذن الحقل الثابت للتماثل φ هو الحقل Q .

18- إذا كان E و F إغلاقين جبريين للحقل K ، أثبت أن $F \cong E$.

الحل :

لنأخذ التطبيق الشامل $\varphi : K \longrightarrow L$ والمعرف بالشكل : $\varphi(u) = u$ لكل u من K ، ومنه . يمتد التطبيق φ إلى التطبيق الأحادي $\phi : E \longrightarrow F$.

وبما أن $\phi(E) = E$ و $\phi(E)$ حقل مغلق جبرياً يحوي الحقل K ، وبما أن F امتداد جبري للحقل K ، فإن F يكون امتداداً جبرياً للحقل $Q(E)$ والذي يقع بين K و F ، وبما أن $\phi(E) = F$ ، فإن ϕ يكون تماثلاً من E إلى F .

19- إذا كان $E \supseteq Z_2$ ويحوي جذر a لكثيرة الحدود :

$f(x) = x^3 + x + 1 \in Z_2[x]$ على الحقل Z_2 ، أثبت أن $F = Z_2(a)$ حقل انشطار لكثيرة الحدود $f(x)$ التي تتحلل إلى عوامل خطية في $F[x]$.

الحل :

بما أن مميز الحقل Z_2 يساوي 2، فإن $f(x) = (x + a)\, g(x)$.

إن $g(x) = x^2 + 9x + (1 + a^2)$، وذلك بعد استخدام عملية القسمة المطلوبة، لنبيّن أن $g(x)$ تتشطر على الحقل F ، عندئذٍ يكون:

$$F = \{b_0 + b_1 u + b_2 u^2 \ ; \ b_i \in Z_2\}$$

بالتقسيم نجد أن :

$$g(x) = (x + a^2) + (x + b) \ ; \ b \in F$$

بمقارنة المعاملات للمتغير x نجد أن :

$$b = a + a^2 \ , \ a = a^2 + b$$

وبالتالي فإن كثيرة الحدود $f(x)$ تأخذ الشكل :

$$f(x) = (x + a) + (x + a)^2 (x + a + a^2) \ \in F[x]$$

أي أنها تتحلل على الحقل F .

20- أثبت أن $f(x) = x^4 + x + 1$ غير قابلة للتحليل على الحقل Z_2 ، ثم صف حقل جالوا $GF(16)$.

الحل :

بما أن كثيرة الحدود $f(x)$ لا تملك جذر في Z_2 ، لذا يمكن كتابة التابع في $Z_2[x]$:

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) \ \in Z_2[x]$$

بمقارنة الأمثال نجد أن :

$$b + ac + d = 0 \ , \ a + c = 0 \ , \ bd = 1 \ , \ ad + bc = 1$$

من المعادلات السابقة نجد أن : $a = c$, $b = d = 1$ ، ومن المعادلة $b + ac + d = 0$ يكون $a = c = 0$ ، وهذا تناقض مع $ad + bc = 1$. إذن $f(x)$ غير قابلة للتحليل ، ويكون لدينا :

$$GF(16) = GF(2^4) = \{a + b + c\,t^2 + d\,t^3 : a,b,c,d \in Z_2 : t^4 = t + 1\}$$

21- أنشئ حقل جالوا : $GF(125)$

الحل :

إن $5^3 = 125$ ، وبالتالي يمكن بناء حقل ، لنوجد أولاً كثيرة الحدود غير القابلــة

للتحليل ومن الدرجة الثالثة على الحقل Z_5 ، ونعلم أن كثيرة الحدود من الدرجة الثالثة قابلة للتحليل على الحقل Z_5 إذا وُجِدَ معامل خطي ، وبالتالي ، فإن كثيرة الحدود $f(x) = x^3 + ax^2 + bx + c$ تكون غير قابلة للتحليل في $Z_5[x]$ ، إذا ، وفقط إذا ، كان $f(u) \neq 0$ حيث $u = 0,1,2,3,4$ في Z_5. وبالتالي توجد كثيرة حدود $f(x) = x^3 + x + 1$ وهي غير قابلة للتحليل على Z_5 ، لأن :

$$f(0) = 1 , f(1) = 3 , f(2) = 11 , f(3) = 31 , f(4) = 4$$

إذن :

$$GF(125) \cong Z_5[x]/(x^3 + x + 1)$$

22- ضع علامة (✓) أمام العبارة الصحيحة وعلامة (×) أمام العبارة الخاطئة في العبارات التالية :

1- كل امتداد منتهي لحقل ما ، يكون امتداد جبري (✓)

2- كل امتداد جبري لحقل ما ، هو امتداد منتهي (×)

3- حقل الأعداد الحقيقية R مغلق جبرياً (×)

4- حقل الأعداد المركبة C مغلق جبرياً في C[x] حيث x متغير (✓)

5- الحقل المغلق جبرياً يجب أن يكون مميزه صفراً (×)

6- لكل عنصرين $u,v \in E$ يوجد دائماً تماثل ذاتي على E بنقل u على v (×)

7- إذا كان v,u عنصران جبريان على الحقل F ومترافقين ، عندئذٍ يوجد دائماً تماثل من F(u) على F(v) (✓)

8- العدد π متسامٍ على الحقل Q (✓)

9- الحقل C هو امتداد بسيط للحقل R (✓)

10- كل عنصر من حقل F يكون جبرياً عليه (✓)

11- حقل الأعداد الحقيقية R هو امتداد للحقل Q (✓)

12- حقل الأعداد النسبية Q هو امتداد للحقل Z_2 (×)

13- كل كثيرة حدود غير ثابتة في الحلقة F[x] يكون لها جذر في امتداد ما للحقل F (×)

12- تمرينات غير محلولة للفصل السادس

1- برهن أن العنصر $u \in C$ جبري على الحقل Q في الحالات التالية :

(a) $u = \sqrt{2} + \sqrt{3} + \sqrt{5}$ (b) $u = 1 + \sqrt{1 + \sqrt[3]{2}}$

(c) $u = \sqrt{\sqrt{3} - 2i}$ (d) $u = 1 + i$

2- أثبت أن العنصر $u \in C$ جبري على الحقل Q ، ثم أوجد كثيـرة الحـدود الصغرى للعنصر u ، وذلك في الحالات التالية :

(a) $u = \sqrt{2} + \sqrt{3}$ (b) $u = \sqrt{1 + \sqrt{3}}$

(c) $u = \sqrt{2} + i$ (d) $u = \sqrt{1 + i}$

3- بيّن أي من العناصر التالية جبرية وأي منها متسامٍ على الحقل F المشـار إليه جانباً ، في كل من الحالات التالية :

(a) $u = \sqrt{\pi}$, $F = Q(\pi)$ (b) $u = \pi^2$, $F = Q$

4- أثبت أن كثيرة الحدود الصغرى لـ $u = \sqrt{3} - i$ على الحقل R ، هي من الشكل :

$$x + 4\sqrt{3}x^2 - 2$$

5- أوجد أساساً (قاعدة) للامتداد E على الحقل Q ، وذلك في كل مما يلي :

(a) $E = Q(\sqrt[3]{2})$ (b) $E = Q(\sqrt{3}, \sqrt[3]{3})$

(c) $E = Q(1 - i)$ (d) $E = Q(\sqrt{2}, \sqrt[3]{3})$

6- أوجد [E : F] في كلٍ من الحالات التالية :

(a) $E = Q(\sqrt{3} + \sqrt{5})$, $F = Q(\sqrt{3})$

(b) $E = Q(\sqrt{3} + i)$, $F = Q(i)$

7- إذا كان E امتداداً للحقل F وكان v,u عنصران جبريان من E على F من الدرجتين n,m على الترتيب ، أثبت أن $[F(u,v) : F] \leq m.n$.

8- إذا كان العنصر $u^2 \in E$ جبرياً على الحقل F ، برهن أن العنصر u جبري على F .

9- أوجد حقل انشطار كثيرة الحدود $f(x) = x^3 - 2 \in Q[x]$ على الحقل Q ثم حدّد درجته .

10- أوجد حقل الانشطار E لكثيرات الحدود على الحقل Q ثم أوجد درجة الامتداد E على Q في كل من الحالات التالية :

(a) $f(x) = x^3 + 1$ (b) $f(x) = x^4 - 6x^2 - 7$

(c) $f(x) = x^4 + 1$ (d) $f(x) = x^6 + 2x^3 - 3$

(e) $f(x) = x^4 - 2x^3 - 7x^2 + 10x + 10$

11- إذا كان E امتداداً للحقل F ، وإذا كان u عنصراً جبرياً على الحقل F ، عندئذٍ ، كل تشاكل أحادي φ للحقل $F(u)$ في $\overline{F}$ (إغلاق جبري) ، حيث $\varphi(a) = a$ لكل $a \in F$ ينقل العنصر u إلى مرافقه v عبر F .

12- أثبت أن مجموعة كل التماثلات الذاتية للحقل E تشكل زمرة بالنسبة لعملية حاصل تركيب التطبيقات .

13- إذا كان E امتداداً للحقل F ، أثبت أن مجموعة كل التماثلات الذاتية على E والتي تبقي F ثابتة ، تشكل زمرة جزئية من زمرة كل التماثلات الذاتية على E (نرمز عادةً لها بـ $G(E/F)$) .

14- ليكن $\varphi : F \longrightarrow L$ تطبيقاً أحادياً من الحقل F إلى الحقل المغلق جبرياً L، وإذا كان $E = F(u)$ امتداداً جبرياً للحقل F ، أثبت أن التطبيق φ يمكن أن يمتد إلى التطبيق الأحادي $\phi : E \longrightarrow L$ ، وتكون درجة الامتداد مساوية لعدد الجذور المختلفة لكثيرة الحدود الصغرى للعنصر u .

15- أنشئ الحقل $Q(\sqrt{2}, \sqrt{3})$ على حقل الأعداد النسبية Q .

16- بيّن أنه إذا كان u جذراً لكثيرة الحدود $f(x) = x^2 + x + 1 \in Z_2[x]$ فإن $Z_2[u]$ هو حقل انشطار لكثيرة الحدود $f(x)$ على Z_2 .

17- أوجد حقل انشطار لكثيرة الحدود $f(x) = x^3 - 2 \in Q[x]$ على الحقل Q، وحدّد درجة امتداده وأساسه على Q باعتباره فضاء متجهي .

18- أوجد كثيرة حدود f والتي يكون $R(u)$ حقل انشطار لها على الحقل R ، حيث أن $u = \sqrt{3} + i$.

19- أوجد حقل الانشطار E لكثيرة الحدود $x^3 - 5$ على Q ثم أثبت أن $[E : Q] = 6$.

20- أوجد حقل الانشطار لكثيرة الحدود $f(x) = x^6 + x^4 + x + 1 \in Z_2[x]$ على الحقل Z_2.

21- أثبت أن كل حقل منته هو حقل تام .

22- أثبت أن $m(x) = x^2 - 3 \in Q[x]$ هي كثيرة حدود صغرى للعنصر الجبري $\sqrt{3} \in R$ على الحقل Q .

23- إذا كان u جذراً لكثيرة الحدود $f(x) = x^2 + x + 1 \in Z_2[x]$: $f(x)$ ، في امتداد E للحقل Z_2 ، بيّن أن الحقل الجزئي $Z_2(u)$ من الامتداد E يتكون من أربعة عناصر .

24- برهن أنه لا يوجد حقل بين الحقلين Q و $Q[x]/<x^2 - 2>$.

25- هاتِ مثالاً ، توضح فيه أنه ليس من الضروري أن يكون كل امتداد جبري هو امتداد منتهي .

إرشاد للحل : خذ الامتداد $E = Q(\sqrt{2}, \sqrt{3}, ..., \sqrt{p}, ...)$ للحقل Q .

26- ليكن $(F,+,.)$ حقلاً ما ، مميزه $P \neq 0$ ، أثبت أن الحقل F يكون تاماً ، إذا وفقط ، إذا تحقق الشرط $F = F^P$.

27- ليكن $E = Q(\sqrt{2}, \sqrt{5})$ ، والمطلوب : أوجد $[E:Q]$ ، ثم أثبت أن $E = Q(\sqrt{2} + \sqrt{5})$، ثم أوجد كثيرة الحدود الصغرى للعنصر $u = \sqrt{2} + \sqrt{5}$

على الحقل Q.

28- إذا كان E امتداداً للحقل F ، ولتكن K مجموعة جزئية من E مكوَّنةً من العناصر الجبرية على F، فإن K يشكل حقلاً جزئياً من E يحوي F .

29- أثبت أن لكل حقل ، وليكن F يوجد إغلاق جبري له $\overline{F}$.

30- أوجد العناصر المترافقة لكل مما يلي :

(a) $\sqrt{2}+\sqrt{3}$; $F = Q$ (b) $\sqrt{3}+i$; $F = R$

31- أنشئ الحقل GF(4) .

32- إذا كان القاسم المشترك الأكبر للعددين m,n هو $d = (m,n)$ ، أثبت أن :

$$GF(P^n) \cap GF(P^m) = GF(P^d)$$

حيث أن : $GF(P^n)\,,\, GF(P^m) \subseteq E$

33- أثبت أنه إذا كانت الزمرة $(F^*,\cdot)$ دائرية ، فإن F حقل منته .

34- إذا كانت f(x) كثيرة حدود غير قابلة للتحليل في F[x] على الحقل F أثبت أن جميع جذور كثيرة الحدود f(x) تكون مختلفة .

35- أثبت أن كثيرة الحدود $f(x) = x^4 + x^3 + x^2 + x + 1 \in Q[x]$ قابلة للفصل على الحقل Q .

36- ليكن P عدداً أولياً ، وإذا كان $F = Z_P$ و $E = F(u)$ ، حيث u عنصر متسامٍ على الحقل F ، ولتكن كثيرة الحدود $f(x) = x^P - u \in E[x]$ والتي حقل انشطارها هو K على E ، وإذا كان v جذراً لكثيرة الحدود f(x) في الحقل K . أثبت أن $v^P = u$.

37- إذا كان E امتداداً للحقل F ، أثبت أن E يكون امتداداً قابلاً للفصل للحقل F ، إذا ، وفقط إذا كان كل عنصر $u \in E$ قابلاً للفصل على الحقل F .

وإذا كان $f(x) \in F[x]$ كثيرة حدود قابلة للفصل للحقل F ، أثبت أن حقل الانشطار E لكثيرة الحدود f(x) هو امتداد قابل للفصل للحقل F .

-38 إذا كان $(F,+,\cdot)$ حقلاً ما ، وكان $\varphi:F \longrightarrow L$ تطبيقاً متبايناً من الحقل F إلى الحقل المغلق جبرياً L . وليكن $E = F(a)$ امتداداً جبرياً للحقل F . برهن إن التطبيق φ يمكن أن يمتد إلى التطبيق المتباين $\Psi:E \longrightarrow L$ ، وتكون درجة الامتداد مساوية لعدد الجذور المختلفة لكثيرة الحدود الصغرى للعنصر a .

تمارين محلولة وغير محلولة للفصل السابع:

الحلقات الارتينية والنوثيرية

Artinian and Noetherian Rings

13- تمرينات محلولة للفصل السابع

- الحلقات الارتينية والنوثيرية -

①ضع علامة (✓) أمام العبارة الصحيحة وعلامة (×) أمام العبارة الخاطئة:

1- كل حقل هو حلقة نوثيرية (✓)

2- $(Z_n,\oplus,\otimes)$ حلقة نوثيرية حيث $n \geq 3$ (×)

3- R حلقة ارتينية $\Leftrightarrow$ $R \in \max -\lhd$ (×)

4- R حلقة نوثيرية $\Leftrightarrow$ $R \in \min -\lhd$ (×)

5- R حلقة نوثيرية $\Leftrightarrow$ كل مثالية في R ذات مولدات منتهية (✓)

6- إذا كانت $R_1,\ldots,R_n$ حلقات نوثيرية، فإن $\sum_{i=1}^{n} \oplus R_i$ حلقة نوثيرية (✓)

7- إذا كانت $R[x]$ حلقة نوثيرية ، فإن R حلقة نوثيرية (×)

8- الجذر الأولي للحلقة $\text{rad}(R)$ هو أكبر مثالية معدومة القوى في R ، حيث R حلقة نوثيرية (✓)

9- كل مثالية شبه معدومة القوى في أية حلقة نوثيرية هي مثالية معدومة القوى (✓)

10- إذا كانت $R = (2Z,+,\cdot)$ ، فإن $I = < 4 >$ مثالية غير قابلة للتحليل في R (×)

② لتكن $(R,+,\cdot)$ حلقة بمحايد ، وإذا كانت كل مثالية عظمى فيها مولدة بعنصر متعادل (أي $\forall a \in R : a^2 = a$) أثبت أن R حلقة نوثيرية .

الحل :

لتكن M مثالية عظمى في R .

ولتكن I مثالية ابتدائية في R لكنها ليست عظمى ، وبالتالي فإن $I \subset M$. وبما أن $M = <a>$ حيث $0 \neq a \neq 1$ عنصر متعادل ، فإن : $a(1-a) = 0 \in I$ ، وبما أن I مثالية و $a \notin I$ ، وبالتالي يوجد عدد صحيح موجب وليكن n ، بحيث $(1-a)^n \in I$. وبما أن M مثالية أولية ، فيكون $(1-a) \in M$ ، أي أن $1 \in M$ ومنه $R = M$ وهذا غير ممكن . إذن I مثالية أعظمية في الحلقة R ، وبالتالي ، فإن كل مثالية أولية في R هي مثالية أعظمية ، إذن كل مثالية أولية في R مولدة بعنصر واحد . وهذا يعني أن R حلقة نوثيرية .

③ (1) أثبت أنه إذا كانت R حلقة نوثيرية فإن R/I حلقة نوثيرية .

(2) كما أن الصورة التشاكلية لحلقة نوثيرية هي حلقة نوثيرية أيضاً .

الحل :

(1) لنفرض أن $I \lhd R$ ، حيث R حلقة نوثيرية ، وليكن $\Pi : R \longrightarrow R/I = \overline{R}$ تشاكل طبيعي ، وإذا كانت $\overline{I_1} \subseteq \overline{I_2} \subseteq ....$ سلسلة تصاعدية من المثاليات في $\overline{R}$.

ولنفرض $A_i = \Pi^{-1}(\overline{A_i})$ ، وبالتالي $I_1 \subseteq I_2 \subseteq ...$ سلسلة تصاعدية من المثاليات في R ، وبما أن R حلقة نوثيرية ، فيوجد عدد صحيح موجب وليكن n بحيث يكون $I_m = I_n$ حيث $m \geq n$ إذن $\overline{I_m} = \overline{I_n}$ لكل $m \geq n$ ، وبالتالي فإن $R/I = \overline{R}$ حلقة نوثيرية .

(2) ليكن $\varphi : R \longrightarrow K$ تشاكلاً حلقياً شاملاً . وبالتالي يكون : $S = \operatorname{Ker} \varphi \lhd R$ و $R/S \cong K$ ، (حسب النظرية الأساسية في التماثل) . وبما أن R/S حلقة نوثيرية حسب (1) ، إذن K حلقة نوثيرية .

④ هاتِ مثالاً يوضح ، أنه إذا كانت $(R,+,\cdot)$ حلقة نوثيرية ، فقد لا يكون التعبير عن كل مثالية فعلية كحاصل ضرب عدد منتهي من المثاليات الابتدائية بشكل وحيد .

الحل :

لنأخذ $R = F[x,y]$ ، إذن R حلقة نوثيرية ولنأخذ المثالية $I = <x^2, xy> \lhd R$.

لكن :

$$I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, xy . y^2 \rangle$$

وكل من $\langle x \rangle$ و $\langle x^2, y \rangle$ و $\langle x^2, xy, y^2 \rangle$ مثاليات أولية في الحلقة R .

⑤ لتكن $(R,+,\cdot)$ منطقة تكاملية ارتينية ، أثبت أن R حقل .

الحل :

إذا كان $0 \neq x \in R$ ، فيكون $\langle x \rangle \supseteq \langle x^2 \rangle \supseteq \langle x^3 \rangle \supseteq \ldots$

سلسلة متناقصة من المثاليات في الحلقة R ، وبما أن R حلقة ارتينية فيوجد عدد صحيح موجب ، وليكن n بحيث يكون $\ldots = \langle x^{n+1} \rangle = \langle x^n \rangle$ وبالتالي يوجد عنصر r من R بحيث يكون $x^n = r\, x^{n+1}$.

وبما أن R منطقة تكاملية ، فيكون $r.x = 1$ ، وبالتالي فإن العنصر x قابل للانعكاس في R ، إذن R حقل .

⑥ لتكن $(R,+,\cdot)$ حلقة ارتينية ، و S مجموعة جزئية من R ، أثبت من خلال مثال ، أنه قد لا تكون S حلقة ارتينية .

الحل :

لنأخذ الحلقة $R = (Q,+,\cdot)$ و $S = (Z,+,\cdot)$ ، لاحظ أن R هي حلقة ارتينية و $S \leq R$ ، لكن S ليست ارتينية .

14- تمرينات غير محلولة للفصل السابع

① ضع علامة (✓) أمام العبارة الصحيحة ، وعلامة (×) أمام العبارة الخاطئة :

1- كل حلقة ارتينية هي حقل ( )

2- $(Z,+,\cdot)$ حلقة ليست ارتينية ( )

3- R حلقة نوثيرية ⇔ $R\in\min\text{-}\triangleleft$ ( )

4- إذا كانت R حلقة ارتينية ، وكانت $I \triangleleft R$ ، فإن R/I حلقة ارتينية ( )

5- إذا كانت $(R,+,\cdot)$ حلقة إبدالية، فإن R حلقة نوثيرية ⇔ كل مثالية أولية في R ذات مولدات منتهية ( )

6- لتكن R/I و I حلقة نوثيرية حيث $I \triangleleft R$ ، فإن R حلقة ارتينية ( )

7- إذا كانت R حلقة نوثيرية ، فإن $R[x,y,z]$ هي حلقة نوثيرية ( )

8- لتكن $(R,+,\cdot)$ حلقة بمحايد ، R حلقة ارتينية ⇔ R هي حلقة نوثيرية وكانت كل مثالية أولية فعلية فيها مثالية ابتدائية ( )

9- إذا كانت $M_1,\ldots,M_n$ مثاليات أعظمية في الحلقة $(R,+,\cdot)$ بمحايد ، فإن R حلقة نوثيرية ⇔ R حلقة ارتينية ( )

10- كل حلقة منتهية هي حلقة ارتينية ( )

② أثبت أن الشروط التالية متكافئة من أجل أي حلقة :

(1) الحلقة R نوثيرية .

(2) كل مثالية من R منتهية التوليد .

③ لتكن $(R,+,\cdot)$ حلقة نوثيرية ، وإذا كانت $I \triangleleft R$ ، عندئذٍ يوجد $n\in Z^+$ بحيث يكون : $(\text{rad}\,(I))^n \subseteq I$.

④ إذا كانت J مثالية ابتدائية في الحلقة النوثيرية R ، وإذا كانت I , K مثاليتين في R بحيث $I.K \subseteq J$ ، فإما $I \subseteq J$ أو يوجد $n \in Z^{+}$ بحيث يكون $(\sqrt{k})^{n} \subseteq J$.

⑤ إذا كانت $(R,+,\cdot)$ حلقة نوثيرية ، وكانت I , J مثاليتين ابتدائيتين فيها ، فإن $I \cap J$ قد لا يكون مثالية ابتدائية في R . المطلوب قدّم مثالاً يوضّح هذه الحقيقية الجبرية .

⑥ إذا كانت $R = \left(\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in Z_2 \right\}, +, \cdot \right)$ ، أثبت أن R حلقة ارتينية .

⑦ لتكن $(R,+,\cdot)$ حلقة ارتينية ، أثبت أن كل مثالية أولية فيها هي مثالية أعظمية .

⑧ أثبت أنه إذا كانت R حلقة ارتينية ، فإن :

(1) $J(R)$ هي أكبر مثالية معدومة القوى في R .

(2) كل مثالية شبه معدومة القوى في R هي مثالية معدومة القوى .

⑨ لتكن $(R,+,\cdot)$ حلقة ما ، أثبت أن الشروط التالية متكافئة :

(1) الحلقة R نوثيرية .

(2) الحلقة R تحقق شرط السلاسل المتزايدة (المتصاعدة) من المثاليات في الحلقة R ، والتي كل منها لا يساوي الصفر .

⑩ أثبت أنه إذا كانت $(R,+,\cdot)$ حلقة بمحايد ، فإن الشرط اللازم والكافي لكي تكون R حلقة ارتينية هو أن تكون R حلقة نوثيرية وكل مثالية أولية فعلية فيها هي مثالية أعظمية .

ثبت المصطلحات العلمية

ثبت المصطلحات العلمية

أ

Commutative	إبدالية
Abelian	آبلية
Union	اتحاد
Trace	أثر
Embedding	إدخال
Linearly dependence	ارتباط خطي
Basis	أساس
Linearly independence	استقلال خطي
Projection	إسقاط
Algebraic numbers	أعداد جبرية
Algebraic integers	أعداد جبرية صحيحة
Relatively prime integers	أعداد صحيحة أولية نسبياً
Restriction of mapping	اقتصار تطبيق
Eucledian	إقليدي
Extension	امتداد
Simple extension	امتداد بسيط
Algebraic extension	امتداد جبري
Finite extension	امتداد منته
Normal extension	امتداد ناظمي
Reflexive	انعكاسة

Prime	أولي

ب

Quadratic residue	باقي تربيعي
Primitive	بدائي
Dimension	بُعد
Structure	بنية

ت

Permutation	تبديل
Even permutation	تبديل زوجي
Partition	تجزئة
Associative	تجميعي (دامج)
Linear transformation	تحويل خطي
Idempotent linear transformation	تحويل متساوي القوى
Nilpotent linear transformation	تحويل معدوم القوى
Normal linear transformation	تحويل خطي ناظمي
Hermition linear transformation	تحويل خطي هرميتي
Unitary linear transformation	تحويل خطي واحدي
Conjugation	ترافق
Composition of mapping	تركيب تطبيقات
Homomorphism	تشاكل
Homomorphism of rings	تشاكل الحلقات
Homomorphism of groups	تشاكل الزمر
Homomorphism of modules	تشاكل الفضاءات الحلقية
Homomorphism of vector spaces	تشاكل فضاءات المتجهات

Congruence	تطابق
Congruence module n	تطابق قياس n
Mapping	تطبيق
One - to - one mapping	تطبيق أحادي
Onto mapping	تطبيق غامر
Transitivity	تعدي
Decomposition	تفريق
One - to - one correspondence	تقابل
Division	تقسيم
Multiplicity	تكرار
Multiplicity of roots	تكرار الجذور
Multiplicity of characteristic roots	تكرار الجذور المميزة
Isomorphism	تماثل
Isomorphism of rings	تماثل الحلقات
Automorphism	تماثل ذاتي
Outer automorphism	تماثل ذاتي خارجي
Inner automorphism	تماثل ذاتي داخلي
Isomorphism of groups	تماثل الزمر
Isomorphism of modules spaces	تماثل الفضاءات الحلقية
Isomorphism of vector spaces	تماثل فضاءات المتجهات
Representation	تمثيل
Symmetric	تناظر
Linear span	توليد خطي

جـ

Algebra	جبر
Boolean algebra	جبر بوليني
Algebra of linear transformation	جبر التحويلات الخطية

Linear algebra	جبر خطي
Algebraic division algebra	جبر القسمة الجبري
Matrix algebra	جبر المصفوفات
Algebraic	جبري
Algebraic of degree n	جبري من الدرجة n
Root	جذر
Primitive root	جذر بدائي
Primitive root of prime number	جذر بدائي للعدد الأولي
Primitive root of nth root of unity	جذر بدائي للواحد من رتبة n
Root of polynomial	جذر كثيرة الحدود
Radical of an ideal	جذر المثالية
Multiple of root	جذر مكرر
Characteristic root	جذر مميز
Sum	جمع
Direct sum	جمع مباشر
External direct sum	جمع مباشر خارجي
Internal direct sum	جمع مباشر داخلي

حـ

Field	حقل
Splitting field	حقل انشطار
Skew- field	حقل تخالفي
Field of quotients	حقل خوارج القسمة
Isomorphic rings	حلقات متماثلة
Ring	حلقة
Commutative ring	حلقة إبدالية
Artinian ring	حلقة ارتينية
Eucledian ring	حلقة إقليدية

Ring of linear transformation	حلقة التحويلات الخطية
Ring of 2x2 matrices	حلقة المصفوفات من نوع 2x2
Ring with unity	حلقة بعنصر وحدة
Boolean ring	حلقة بولينية
Integral domain	حلقة تامة (منطقة تكاملية)
Associative ring	حلقة تجميعية
Ouotient ring	حلقة خارجة
Semi simple ring	حلقة شبه بسيطة
Non associative ring	حلقة غير تجميعية
Division ring	حلقة قسمة
Ring of polynomials	حلقة كثيرات الحدود
Ring of polynomials in n variable	حلقة كثيرات الحدود في n متغير
Noetherian ring	حلقة نوثيرية

خـ

Ouotient	خارج
Ascending chain condition	خاصية السلسلة المتصاعدة
Descending chain condition	خاصية السلسلة المتنازلة (المتناقصة)
Linear	خطي
Algorithm	خوارزم
Eucledian algorithm	خوارزم إقليدي
Division algorithm	خوارزم القسمة
Left division algorithm	خوارزم القسمة الأيسر

د

Functional	دالِّي
Linear functional	دالِّي خطي
Degree	درجة

Degree of extension	درجة الامتداد
Degree of polynomial	درجة كثيرة الحدود
Index	دليل
Index of nilpotence	دليل انعدام القوى
Elementary functions	دوال ابتدائية
Rational functions	دوال نسبية
Period	دور
Period of an element	دور العنصر
Cyclic	دوري

ر

Order	رتبة
Order of agroup	رتبة الزمرة
Order of an element	رتبة العنصر

ز

Isomorphic groups	زمر متماثلة
Conjugate subgroups	زمر جزئية مترافقة
Group	زمرة
Commutative group	زمرة إبدالية
Abelian group	زمرة آبلية
Simple group	زمرة بسيطة
Permutation group	زمرة التبديلات
Group of outer automorphism	زمرة التماثلات الذاتية الخارجية
Group of inner automorphism	زمرة التماثلات الذاتية الداخلية
Symmetric group of degree n	زمرة التناظر من الدرجة n
Galios group	زمرة جالوا
Subgroup	زمرة جزئية

Trivial subgroup	زمرة جزئية تافهة
Cyclic subgroup	زمرة جزئية دورية
Normal subgroup	زمرة جزئية ناظمية
Quotient group	زمرة خارجة
Cyclic subgroup	زمرة دورية
Dihedral group	زمرة زوجية
Solvable group	زمرة قابلة للحل
Nilpotent group	زمرة معدومة القوى
Finite group	زمرة منتهية

ش

Singular	شاذ
Associate	شريك

ص

Row of matrix	صف المصفوفة
Image	صورة
Inverse image	صورة معكوسة
Quadratic form	صورة صيغة تربيعية
Real quadratic form	صورة صيغة تربيعية حقيقية
Canonical form	صورة قانونية

ض

Product of mappings	ضرب تطبيقات
Inner product	ضرب داخلي
Cartesian product	ضرب ديكارتي
Scalar product	ضرب قياسي
Direct product	ضرب مباشر
External direct product	ضرب مباشر خارجي

ضرب مباشر داخلي	Internal direct product

ع

عامل مرافق	Cofactor
عدد جبري	Algebraic number
عدد جبري صحيح	Algebraic integer
عدد متسامٍ	Transcendental number
علاقة	Relation
علاقة انعكاسية	Reflexive relation
علاقة تكافؤ	Equivalence relation
علاقة ثنائية	Binary relation
علاقة متعدية	Transitive relation
علاقة متناظرة	Symmetric relation
عمود مصفوفة	Column of matrix
عنصر أعظمي	Maximal element
عنصر أولي	Prime element
عنصر جبري	Algebraic element
عنصر غير مختزل	Irreducible element
عنصر محايد	Identity element

غ

غامر (شامل)	Onto
غير إبدالي	Non commutative
غير تجميعي	Non associative
غير متغير	Invariant
غير مختزل	Irreducible
غير منته	Infinite

ف

Symmetric difference	فرق تناظري
Conjugacy class	فصل ترافق
Similarity class	فصل تشابه
Congruence class	فصل تطابق
Equivalence class	فصل تكافؤ
Module	فضاء حلقي
Submodule	فضاء حلقي جزئي
Ouotient module	فضاء حلقي خارج
Irreducible module	فضاء حلقي غير مختزل
Finitely generated module	فضاء حلقي منته التوليد
Unital module	فضاء حلقي واحدي
Vector space	فضاء متجهات
subspace	فضاء متجهات جزئي
Real vector space	فضاء متجهات حقيقي
Ouotient vector space	فضاء متجهات خارج

ق

Solvable	قابل للحل
Separable	قابل للفصل
Divisibility	قابلية القسمة
Divisor	قاسم
Zero divisor	قاسم للصفر
Greatest common divisor	قاسم مشترك أعظم
Associative law	التجميع (الدمج)
Adjoint	قرين

Division	قسمة
Algebraic division	قسمة جبرية
Elementary divisors	قواسم ابتدائية
Distribution laws	قوانين التوزيع
Scalar	قياسي

ك

Polynomial	كثيرة حدود
Minimal polynomial	كثيرة حدود دنيا
Primitive polynomial	كثيرة حدود بدائية
Cyclotomic polynomial	كثيرة حدود دورية
Irreducible polynomial	كثيرة حدود غير مختزلة
Symmetric polynomial	كثيرة حدود متناظرة
Characteristic polynomial	كثيرة حدود مميزة

م

Commutator	مبدل
Theorem	مبرهنة
Inequality	متباينة
Complement	متممة
Maximal ideal	مثالي أعظمي
Prime ideal	مثالي أولي
Left ideal	مثالي أيسر
Right ideal	مثالي أيمن
Principal ideal	مثالي رئيس
Ideal	مثالية
Primary ideal	مثالية ابتدائية
Prime ideal	مثالية أولية

Nil ideal	مثالية شبه معدومة القوى
Irreducible ideal	مثالية غير قابلة للتحليل
Nilpotent ideal	مثالية معدومة القوى
Disjoint sets	مجموعات منفصلة
Set	مجموعة
Set of integrs moduls n	مجموعة الأعداد الصحيحة قياس n
Decomposable set of linear transformation	مجموعة التحويلات الخطية القابلة للتفريق
Irreducible set of linear transformation	مجموعة التحويلات الخطية غير المختزلة
Index set	مجموعة الدليل
Subset	مجموعة جزئية
Proper subset	مجموعة جزئية فعلية
Empty set	مجموعة خالية
Infinite set	مجموعة غير منتهية
Coset	مجموعة مشاركة
Double coset	مجموعة مشاركة مزدوجة
Determinant	محدّدة
Range	مدى
Conjugate	مرافق
Rank	مرتبة
Rank of linear transformation	مرتبة التحويل الخطي
Rank of module	مرتبة الفضاء الحلقي
Rank of matrix	مرتبة المصفوفة
Center of a group	مركز الزمرة
Similar	مشابه
Derivative	مشتقة

Matrix	مصفوفة
Matrix unit	مصفوفة الوحدة
Permutation matrix	مصفوفة تبديلية
Zero matrix	مصفوفة صفرية
Diagonal matrix	مصفوفة قطرية
Orthogonal matrix	مصفوفة متعامدة
Symmetric matrix	مصفوفة متناظرة
Companion matrix	مصفوفة مصاحبة
nxn matrix	مصفوفة من نوع nxn
Least common multiple	مضاعف مشترك أصغر
Congruent	مطابق
Coefficients	معاملات
Inverse	معكوس
Right inverse	معكوس أيسر
Right inverse	معكوس أيمن
Inverse of mapping	معكوس تطبيق
Inverse of element	معكوس عنصر
Criterion	معيار
Annihilator	مفني
Modulus	مقياس
Centralizer	ممركز
Characteristic	مميز
Characteristic of integral domain	مميز الحلقة التامة
Zero characteristic	مميز صفري
Finite	منته
Finite dimensional	منته البعد
Finite characteristic	منته المميز

منظم (معاير)	**Normalizer**
منقول	**Transpose**
مولد	**Generator**

ن

نظام ضربي	Multiplicative system
نواة	Kernal

و

واحدي	Unital
وحدة	Unit

الرموز المستخدمة

الرموز المستخدمة

$\mathbb{Z}$	حلقة الأعداد الصحيحة
$\mathbb{Q}$	حلقة الأعداد النسبية
$\mathbb{R}$	حلقة الأعداد الحقيقية
$\mathbb{C}$	حلقة الأعداد المركبة
Z_n	حلقة الأعداد الصحيحة قياس n
R/I	حلقة القسمة للحلقة R بالمثالية I
M/N	حلقة القسمة للحلقة M على N
$R[x]$	حلقة كثيرات الحدود على الحلقة R
$\deg f$	درجة كثير الحدود f
$\det (A)$	محدد المصفوفة A
Aut R	زمرة التشاكلات الذاتية للحلقة R
Im R	زمرة التشاكلات الذاتية الداخلية للحلقة R
$Hom_R(M) = End_R(M)$	حلقة التشاكلات الذاتية للحلقية M على الحلقة R
$\langle a \rangle$	الزمرة الدائرية المولدة بالعنصر a
(a)	مثالية مولدة بالعنصر a
char R	مميز الحلقة R
G_R	زمرة الوحدات للحلقة R
$GL_n(F)$	الزمرة الخطية العامة من الدرجة n على الحقل F
$[S]$	صفوف التكافؤ لـــ S
$\equiv$	علاقة توافق أو يوافق قياس

$\cong$	تماثل حلقي
$Z(R)$	مركز الحلقة R
gcd	القاسم المشترك الأعظم
ℓcm	المضاعف المشترك الأصغر
$\|S\|$	رتبة لـــ S
Rank (A)	رتبة المصفوفة A
dim (V)	بُعْد الفضاء المتجهي V
ord (f)	رتبة كثيرة الحدود f
f'	مشتق كثيرة الحدود f
$[L : K]$	درجة الحقل L على K (درجة التوسعة)
Ker f	نواة للتشاكل f
[a,b]	القاسم المشترك الأصغر
(a,b)	القاسم المشترك الأعظم
$(a,b) = 1$	b,a أوليان نسبياً
a/b	العنصر a يقسم العنصر b
I	مثالية
$[a] = \overline{a}$	فصل تكافؤ a
J(R)	أساس جاكبسون للحلقة R (جذر جاكبسون)
rad (R)	الأساس الأولي للحلقة R ، أو جذر الحلقة R
$\triangleleft$	الزمرة الجزئية الناظمية
$S \leq R$	S حلقة جزئية من الحلقة R
$\oplus$	مجموع مباشر للحلقات

$R[x]$	حلقة كثيرات الحدود بمتحول واحد **على R**
$U(R)$	مجموعة العناصر القابلة للانعكاس في R
$I \lhd R$	I مثالية في الحلقة $(R,+,\cdot)$
$\sqrt{I}$	جذر المثالية I
$GF(P^n)$	حقل جالوا
E_S	الحقل الثابت للمجموعة S

المراجع

References

المراجع العربية

١- د. صفوان عويرة، أ. محمد عبد الباقي، نظرية الزمــر، مكتبــة المتنبــي ١٤٢٧ - ١٤٢٨ هـ .

٢- د. يوسف الوادي، د. حمزة حاكمي، البنى الجبريـــة ، جامعـــة دمشـــق ، ١٤٢٧ - ١٤٢٨ هـ .

٣- د. نادر النادر ، الجبر (3) - جامعة حلب ١٤٠١ - ١٤٠٢ هـ .

٤- د. فوزي الذكير ود. علي السحيباني، مواضيع في الجبر، جامعـــة الملـــك سعود ، ١٤١٤ هـ .

٥- فالج الدوسري - مقدمة في نظرية الحلقات والحقول ، مكة المكرمة ١٤٢٠ هـ .

المراجع الأجنبية

Carl Faith , Algebra II Ring theory , Springer-Verlay, Berlin,1976 (١)

Donald S.passam,Acourse in Ring theory California, 1991 (٢)

Flachsmeyer . J, Prohaska,L, Algebra VEB Deutscher verlay der wissenschaften , Berlin , 1976 (٣)

Günter Scheja , Lehrbuch der Algebra ,B. G. Teubner, Stuttgart, 1988 (٤)

Hideyuki Matsumura,Commutative Ring theory Cambridge university Press,2002 (٥)

Iain T. Adamson , Introduction to Field theory , New york, 1964 (٦)

John B.Fraleigh, Afirst course in Abstract Algebra ,Newyork,2003 (٧)

Joseph A.Gallian,Contemporary Abstract Algebra,Newyork,2002 (٨)

Kuhnert,Verlesungen über Algebra , VEB Deutscher verlay Berlin , 1976 (٩)

Nathan Jacobso, Lectures in Abstract Algebra New york, 1999 (١٠)

Oniscik. A. L, Sulanke, R, Algebra und Geometric VEB Deutscher verlay der wissenschaften , Berlin , 1976 (١١)

Renschuch. B, Elementar und praktische Idealtheorie , VEB Deutscher verlay der wissenschaften , Berlin , 1979 (١٢)

Rudoff lial , Introduction to finite field,s and their application , New york , 1988 (١٣)

UI.N.Hersteim,Topics Algebra,printed in the U.S.A , 1975 (١٤)

Keitb W. Nicbolson, Introduction to Abstract Algebra,London,1993 (١٥)

Lam.Y.T , Exercises in classical Ring theory Spring-Verlay,Berlin,1994 (١٦)

Zariski ,O, Samuel,P,Commutative algebra ,Vol, Springer, 1958 ,New york. (١٧)